Trust Modelling in 5G mobile networks*

Mike Surridge
IT Innovation Centre
Southampton, UK
ms@it-innovation.soton.ac.uk

Gianluca Correndo
IT Innovation Centre
Southampton, UK
gc@it-innovation.soton.ac.uk

Ken Meacham
IT Innovation Centre
Southampton, UK
kem@it-innovation.soton.ac.uk

Juri Papay
IT Innovation Centre
Southampton, UK
jp@it-innovation.soton.ac.uk

Stephen C. Phillips
IT Innovation Centre
Southampton, UK
scp@it-innovation.soton.ac.uk

Stefanie Wiegand
IT Innovation Centre
Southampton, UK
sw@it-innovation.soton.ac.uk

Toby Wilkinson
IT Innovation Centre
Southampton, UK
stw@it-innovation.soton.ac.uk

ABSTRACT

5G technologies will change the business landscape for mobile network operation. The use of virtualization through SDN, NFV and Cloud computing offer significant savings of CAPEX and OPEX, but they also allow new stakeholders to rent infrastructure capacity and operate mobile networks, including specialized networks supporting so-called vertical applications serving specific business sectors. In the resulting diverse stakeholder communities, the old trust assumptions between network operators will no longer apply. There is a pressing need for a far broader understanding of trust in such networks if they are to operate safely and securely for the engaged stakeholder communities. This paper describes the work carried out in the 5G-ENSURE project to address this need.

CCS CONCEPTS

• **Networks** → **Network security**; *Network reliability*;

KEYWORDS

Telecommunications Networks, 5G, Security, Trust

ACM Reference Format:
Mike Surridge, Gianluca Correndo, Ken Meacham, Juri Papay, Stephen C. Phillips, Stefanie Wiegand, and Toby Wilkinson. 2018. Trust Modelling in 5G mobile networks. In *SecSoN '18: Workshop on Security in Softwarized Networks: Prospects and Challenges, August 24, 2018, Budapest, Hungary.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3229616.3229621

*Produces the permission block, and copyright information

SecSoN '18, August 24, 2018, Budapest, Hungary

ACM ISBN 978-1-4503-5912-2/18/08…$15.00
https://doi.org/10.1145/3229616.3229621

1 INTRODUCTION

5G technologies will change the business landscape for mobile network operation, largely through the use of virtualization technologies such as SDN, NFV and Cloud computing. The trend towards increased virtualization is driven by the potential for significant reductions of capital expenditures (CAPEX) and operational costs (OPEX). But virtualization also makes it possible for organizations to very quickly commission and operate substantial IT networks by renting a slice of the capacity provided by hardware infrastructure and using it as an essentially separate network controlled not by the hardware operator but by the customer. In 5G networks this will allow new stakeholders to rent infrastructure capacity and operate mobile networks, including specialized networks supporting so-called vertical applications serving specific business sectors such as health care, connected vehicles and associated services, or advanced energy distribution networks. In the resulting diverse stakeholder communities, the old trust assumptions between network operators will no longer apply. There is a pressing need for a far broader understanding of trust in such networks if they are to operate safely and securely for the engaged stakeholder communities. The starting point for this work is the recognition that trust is a response to risk, and in a mobile network trust assumptions are made regarding the contributions made by each stakeholder to manage risks to themselves and to other stakeholders.

The main sections of the paper are as follows: Section 2 provides a short survey of published work on trust analysis and the related problem of risk identification and analysis. Section 3 describes the trust modelling principles and introduces the Trust Builder tool, and the methodology by which it allows risks, dependencies and trust relationships to be analyzed. Section 4 presents a simplified model and analysis based on the analysis of 31 use case scenarios developed within the 5G-ENSURE project. Section 5 summarizes the paper and outlines future work.

2 RELATED WORK

A recent survey on trust modelling concluded that this topic is still far from being fully understood especially regarding modelling and quantifying trust [2]. The paper introduces the notion of a

composite trust that attempts to bring together the results of trust related research in different disciplines such as social sciences, philosophy and economics. In our paper we use a simpler definition of trust and consider trust as one of the possible responses to risk. Starting from this definition we identify the possible threats that may cause loss of trust and select appropriate counter measures.

One of the first significant contributions to trust related research was the thesis of Stephen Marsh who investigated trust in various contexts and made a direct link between trust and risk [7]. The OPTET (OPerational Trustworthiness Enabling Technologies) project used a multi-disciplinary and integrated approach to identify and address the drivers of trust and confidence, improvement of trustworthiness of internet based socio-technical systems, using a methodology in which trust is explicitly defined in relation to threats (i.e. sources of risk) [1], [9], [10]. The work described here is based to a large extent on OPTET, though where OPTET focused on describing trust relationships in terms of threats, here we have the additional problem of discovering trust relationships needed to implement measures to address those threats. The Trust Builder tool we developed and used to conduct our analysis of threats and associated trust relationships is based on the tools from the OPTET project. Other threat modelling and analysis tools and methods exist, and fall mainly into three classes: software-centric, attacker-centric, and asset-centric.

Software centric tools, for example VsRisk [13], Threat Modelling Tool (TMT) [8], ThreatModeler [11] are based on vulnerability databases. The most common approach with software centric tools is still based on providing checklists such as the OWASP [15] which are used for manual analysis by software developers for the identification of attack paths. Software centric methods are extremely valuable for software developers who need to find and address software vulnerabilities (i.e. programming errors). They cannot easily identify or address threats involving human factors or threats from inappropriate use of system functions, so are not useful or particularly relevant in the analysis of trust.

The attacker centric tools such as SeaMonster [4] and Securicad [3] are better at identifying threats from or involving humans. However, these approaches are difficult to automate, as they depend on expert knowledge of likely attackers and attack methods, and since experts often disagree (at least in detail), the results are rarely 100% reproducible. It may also be difficult to decide how various attacks relate to individual components of the system being analyzed, and where security measures could be introduced to counter specific threats. This makes such approaches less than ideal as a basis for analyzing trust, since one needs stakeholders to agree on what threats are present, and where (or more importantly by whom) security measures should be introduced to counter them.

The third category of tools are based on Asset centric methods include the standardized approach from ISO 27005 [6] and ISO 31010 [5]. These also suffer from a dependence on analysis by a security expert with extensive knowledge of the types of threats that could potentially affect the system, so different analyses may not reach the same conclusions.

3 TRUST MODELLING

There are three key terms that form the backbone of this paper, these are risk, threat and trust. The risks to 5G network (including application) stakeholders arise from threats. The stakeholders facing a threat have several options to treat the associated risk. They can (a) reduce the risk by implementing security measures to make the threat less likely, (b) accept the risk, i.e. assume the threat won't happen or won't cause much harm, (c) transfer responsibility for the threat consequences to another stakeholder, either explicitly (by agreement) or implicitly (because they seem trustworthy), or (d) avoid the risk by refusing to use network features through which the threat could affect them. Options (b) or (c) involve trust: the stakeholder either trusts that the 5G network will not misbehave due to its inherent resilience against threats or security measures implemented by others, or trusts another stakeholder to compensate them for any harm caused. In practice, option (b) also involves trust between stakeholders, because in practice the reason the 5G network does not succumb to a threat is because of the security measures introduced by different stakeholders. If a stakeholder (the trustor) is affected (i.e. harmed) by a potential threat, then they are trusting other stakeholders (the trustees) who are responsible for those parts of the network where security measures are needed to prevent the threat. This is actually the main source of stakeholder inter-dependency, as it is usually more appropriate to prevent a threat than to (say) insure against losses.

The 5G-Ensure project has developed a tool called Trust Builder that addresses the automated identification of threats that may compromise a multi-stakeholder system. The tool enables automated and systematic identification of risks to the assets (both human and technological) as well as their knock-on consequences and countermeasures to mitigate these risks. Trust Builder works by representing security threats using a layered set of ontologies: a) a core ontology expresses basic concepts such as assets (including stakeholders), threats and controls (i.e. security measures); b) a domain model describes the types of assets from which a system can be composed, the types of threats that can affect such a system, and potential control strategies (combinations of controls) that can be used to reduce the risks from each type of threat; c) a system model describes the system in terms of the domain model asset types and their relationships, and (once analyzed) the catalogue of threats that could disrupt the system.

The domain model plays a key role in a Trust Builder analysis. This was developed by analyzing 31 use case scenarios provided by 5G-ENSURE partners, each describing the use of a set of interacting network functions in a 'sunny day' scenario (one free of threats), along with one or more ways in which the 'sunny day' could be disrupted (i.e. descriptions of potential threats and consequences). These models were mainly used to determine the types of assets from which 5G networks could be constructed, and the types of threats that could affect them. Two types of threats are included in the domain model. Primary threats represent causes of adverse behavior due to faults or malicious intent within system assets, or to malicious intervention from an external agent. The final domain model contained 66 distinct primary threat classes ranging from software faults to remote network attacks. Secondary threats represent ways in which the adverse behavior caused could then

propagate through the system, e.g. if a service is overloaded, that could overload its host; if a host is overloaded, it could suffer a loss of availability; if a host is unavailable, that causes a loss of availability in every service it hosts. These effect propagation mechanisms are very relevant in virtualized networks (since they share an infrastructure). The 5G-ENSURE domain model contains 263 secondary threats, the majority of which express effects in or between virtual network components. Secondary threats are also very important in trust analysis, because they capture how far the effects of a threat can propagate and hence which stakeholders will be affected. In fact, a stakeholder's loss of trust is modelled as an adverse behavior in the stakeholder (treating the stakeholder as a system asset). This is caused by a range of secondary threats each representing the effect some disruption in the system has on a stakeholder's feeling of confidence in the system. Threats to trust are based on stakeholder concerns, linked to some other asset(s) whose behaviour the trustor can sense (at the time or later). The behaviour of those assets is disrupted due to some other threat in the system, which may itself be a secondary threat. To understand which stakeholder(s) are in a position to address each trustor concern, we must find the root causes of the trust threat representing that concern, i.e. the primary threats that can trigger a cascade of secondary effects that end in the stakeholder's loss of trust. This capability is built into the Trust Builder. One can select any adverse behavior in the system model (in this case LossOfTrust in a relevant Stakeholder), and get a list of the primary threats that contribute to causing their loss of trust.

The last step is to determine what security measures (controls) should be used to prevent primary threats that could affect each stakeholder, and establish who is responsible for each control. One can do this by finding root causes for each type of stakeholder concern, and choosing an appropriate control strategy to counter them. However, this would be a very time-consuming process. Because the models created by Trust Builder are represented as RDF graphs, it is possible to automate parts of this analysis, and auxiliary tools were developed in the project for this purpose. Having created and analyzed a system model using Trust Builder, one can export the graph and use these tools to find security measures that contribute most to preventing a loss of trust. This is done by extracting paths leading from each root cause (primary threat) to each threat to trust, and counting how many of these paths can be blocked by the use of each security control. The selection of controls cannot be fully automated because sometimes a control is inappropriate (e.g. one cannot block a remote attack on a service by using a firewall if that would also block its legitimate clients). It is also possible that critical network functions may affect only a few stakeholders, but controls for those functions will be needed, so it makes sense to apply them first before one uses the path counting procedure.

Each security control has to be located at an asset within the system, so once they are specified one can check which stakeholders have direct relationships to each asset, and which of them should be responsible for the security control. It should be noted that to block a threat may require multiple controls at different assets (e.g. to prevent client impersonation the client must have an electronic ID, and the service must authenticate clients using this ID). A single control may also require action by multiple stakeholders (e.g. security patching a device depends on the device manufacturer to supply security updates, and the device operator to apply those updates). Consequently, multiple stakeholders (including the trustor) may contribute to blocking each threat to trust.

4 EXAMPLE NETWORK MODEL

The example network model captures a high level description of a mobile 5G communication network containing hardware assets, services and stakeholders (see Figure 1). The hardware assets are: Mobile Equipment (ME), SIMBus is the interface between UICC and the Mobile Equipment, Universal Integrated Circuit Card (UICC), Public Space represents a physical region where the assets can be accessed, Radio Access N/W (AN), eNodeB (evolved Node B), Serving N/W, Serving N/W Gateway (SGW) provides access to the network, Home N/W (HN), Home Subscriber Server (HSS-Server), Packet Gateway (PGW) connecting to the internet. The hardware assets host various processes: SIM, User Agent (UA), Mobility Management Entity (MME), Home Subscriber Service (HSS), Access Accounting Agent (AAA). The stakeholders considered in this use case are: Access N/W operator, Home N/W operator, Serving N/W operator, Subscriber, Mobile Equipment Manufacturer, Network Equipment Manufacturer, UICC Manufacturer. The full analysis conducted in 5G-ENSURE produced 2 larger models (one addressing multiple stakeholders and one virtualisation) but this model is sufficient to show the main features of the trust model. See [12] for more details.

The system model is constructed in Trust Builder by drawing the diagram (Figure 1 is a screen shot from the Trust Builder session), and then automatically analyzed. This step uses semantic reasoning to generate inferred assets, threats and control measures. The inferred assets represent points in the network that could be compromised by or contribute to the control of threats, e.g. interfaces between hosts (devices) and networks to which they are connected, or paths through the network. These assets are inferred by Trust Builder wherever possible so the user doesn't have to add them manually, which would be a very laborious process. The system model shown in Figure 1 contains 154 assets (more than half of which are inferred), 474 asset relationships, and 758 distinct threats including 544 primary and 214 secondary threats. It is unlikely that an expert would be able to identify all these threats manually in a short time, or that any two experts would identify the same set of threats. This clearly demonstrates the benefits of machine inference to find threats in a system based on a library of threat types from a reusable knowledge base for the domain.

Trust concerns in this network are represented by a subset of the threats representing stakeholder concerns, i.e. adverse system behaviour that would undermine the confidence of a stakeholder in the system. In the system shown in Figure 1 there are 58 distinct threats to trust (i.e. just over 25% of the secondary threats in the system represent adverse effects undermining trust). There are also 2078 paths connecting these 58 threats to trust to root causes (i.e. to the 544 primary threats). The controls needed to block these paths include security patching of network devices, identification of most processes running in the network including but not limited to the User Agent (UA), along with client or service authentication based on these identification mechanisms, access control to protect data (primarily user profiles and identifiers sent from the SIM,

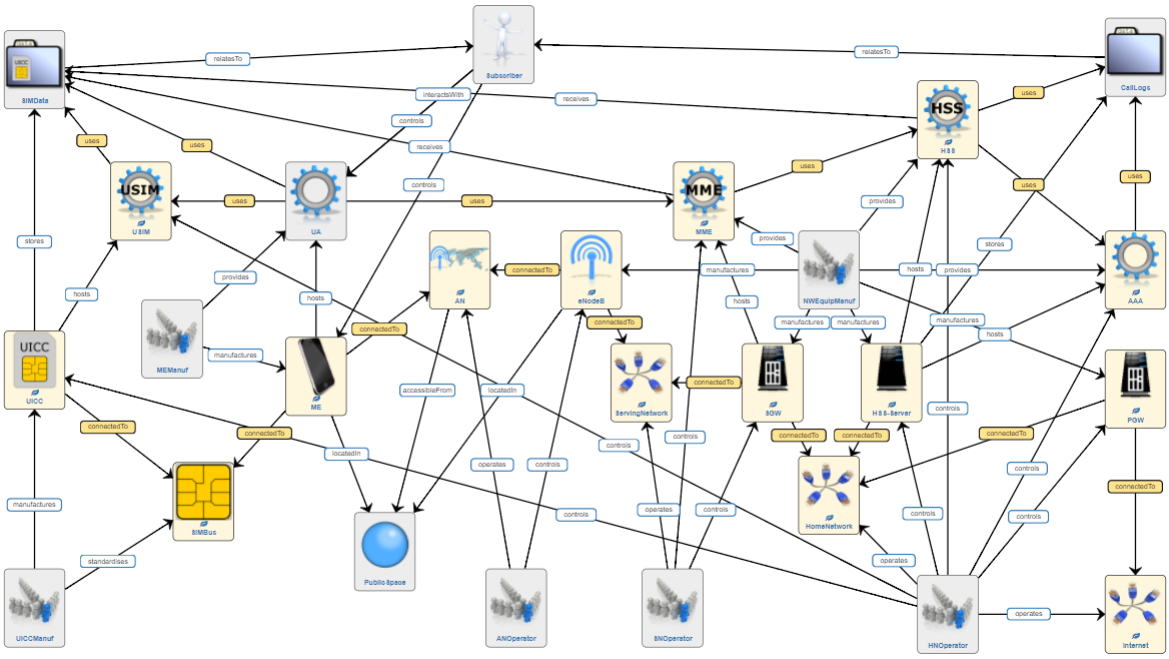

Figure 1: 5G network model constructed by Trust Builder

Table 1: Stakeholder trust dependencies

	Trustee						
Trustor	Access N/W op	Home N/W op	Serving N/W op	Subscriber	ME Manuf	N/W Equip Manuf	UICC Manuf
Access N/W op	17	0	0	0	0	17	0
Home N/W op	30	608	80	18	0	324	78
Serving N/W op	15	164	152	20	0	191	0
Subscriber	59	804	283	159	56	471	177
External Depend	104	968	363	38	56	1003	255

and accounting data collected by the Home N/W operator), secure communications between the USIM, UA and MME, plus monitoring of most devices and services linked to malicious traffic suppression on network segments including (at the PGW) malicious traffic from the Internet. One can then extract the trustees, i.e. stakeholders contributing to the control strategies blocking each paths from root causes leading to loss of trust. The results are summarised in Table 1, which shows the number of root causes for threats whose control strategy involves each trustee (the rows represent the 'trustor' and the columns the 'trustee'). Table1 provides a measure for the degree of trust represented by the number of root cause threats. In this case the trustors assume that the trustees will help to prevent the threats by implementing the relevant control measures.

The data in Table 1 can be summarised as follows: a) all stakeholders need to contribute to the security of the network, b) security begins at home i.e. the trustor always has to contribute significantly (often more than any trustee) to controlling threats to themselves, c) there is a concentration of responsibilities at the Home N/W operator, and d) the Access N/W operator doesn't depend on other operators and is also relatively little trusted by the others.

The increased dependency on the Home N/W operator and reduced dependency on the Access N/W operator compared to previous generation networks is a hallmark of 5G. The main reason for making the Access N/W relatively untrusted is in part because for some time Access N/W coverage will only use 5G technology in the most populated regions, so 5G technology must be capable of working over older generation (and less secure) Access N/W technology. In previous mobile networks, the Access and Serving N/W were more trusted, yet the security they provided was limited so actually they were less trustworthy than is the case in 5G networks. By defining a trust model, one can avoid such misplaced confidence, ensuring that all stakeholders know what they can expect from each other. Only then can 5G networks provide better security

Table 2: Security responsibilities of trustees

	Type of Security Control							
Trustee	SW Patch Mgmt	N/W Sec Monit	N/W Traf Sprt	Ident/ Cert	Client Auth	Service Auth	Access Crt	Encr Comm
Access N/W op	31	30	60	0	0	0	0	0
Home N/W op	930	154	106	65	125	5	188	3
Serving N/W op	290	72	60	55	35	0	0	3
Subscriber	56	30	0	75	0	30	0	6
ME Manuf	56	0	0	0	0	0	0	0
N/W Equip Manuf	1003	0	0	0	0	0	0	0
UICC Manuf	248	7	0	0	0	0	0	0

than previous networks despite the diversity of stakeholders and extensive use of virtualisation.

Next we identify the stakeholder responsibilities by considering the types of security measures the trustees are expected to implement (see Table 2). The smallest number of measures needed to prevent threats to trust were software patch management, network security monitoring, network traffic suppression, identification/certification, client and service authentication, access control, and encrypted communication. Our model does not specify how these measures should be implemented. In some cases, off-the-shelf security technologies can be used, but to work in the control plane of the 5G network one must respect standardized protocols and support large networks with potentially very large numbers of devices.

Software patch management to address vulnerabilities in software or devices is the most important measure in our model, if one measures importance in terms of the number of paths from root cause to loss of trust the measure helps to block. This can use off-the-shelf technology (though applying it in a running network may not be trivial). Other measures must be customized for 5G networks and many are supported by 5G-ENSURE security enablers. Network security monitoring uses analytics to detect malicious traffic and identify its source, and 5G-ENSURE developed a suite of monitoring enablers to support this. Monitoring is used in conjunction with network traffic suppression to restrict devices identified (by monitoring) to be the source of malicious traffic. This is important in 5G networks to prevent DoS attacks on key services concentrated in the Home N/W, where in older networks the same functions could also be provided by the Serving or Access N/A. Client or Service Authentication used in conjunction with Identification or Certification is needed to prevent spoofing attacks. Access Control and Encrypted Communication is then able to prevent unauthorized access to subscriber identities or their call data including access via snooping on the Radio Access N/W. 5G-ENSURE implemented enablers using encryption on the control plane to support end-to-end protection for subscriber privacy. The Home N/W operator is the data controller for subscriber information, and subject to the GDPR from May 2018, so 5G networks must prevent subscriber identity and location data leaking from the Home N/W.

5 CONCLUSIONS

In this paper trust is described as a decision to accept (or not) risks arising from one or more threats. The authors argue that the elusive concept of trust can be rigorously defined in terms of risks of possible malfunctions or misbehaviour of a system. This contextualization allows trust to be characterized as well as quantified, and related to the trustworthiness of systems based on eliminating or mitigating the identified threats.

Analysis of the 5G-ENSURE architecture using Trust Builder helped to clarify trust dependencies between trustors (stakeholders affected by threats) and trustees (stakeholders responsible for the security measures needed to address those threats). The main findings are that in 5G networks the Home N/W operator will have more responsibilities and be highly trusted compared to previous generation networks, while the Access N/W operator will have few responsibilities and the Access N/W will be largely untrusted, partly because it may have to operate using previous generation technology with lower levels of security, and partly because it is one of the most accessible entry point for attacks on the network communications and devices. These changes also lead to certain security measures becoming more important, notably security monitoring and blocking access to sources of malicious traffic (especially DoS attacks) which is needed to maintain access to the key control plane services provided by the Home N/W, and secure authentication and encryption to protect subscriber identity and location as they connect over the (largely untrusted) access N/W.

In future, we believe that a trust analysis of this type should accompany any multi-stakeholder architectural specification or standard, to define the responsibilities of each stakeholder, and to clarify what assumptions they can make of other stakeholders.

Acknowledgments. The 5G-ENSURE project was funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 671562.

REFERENCES

[1] Ajay Chakravarthy, Xiaoyu Chen, Bassem Nasser, and Michael Surridge. 2015. Trustworthy systems design using semantic risk modelling. (February 2015). https://eprints.soton.ac.uk/383465/
[2] Jin-Hee Cho et al. 2015. A Survey on Trust Modeling. *ACM Comput. Surv.* 48, 2, Article 28 (Oct. 2015), 40 pages. https://doi.org/10.1145/2815595
[3] Foreseeti. 2018. SECURICAD. https://www.foreseeti.com/.
[4] Per Hakon et al. 2008. SeaMonster: Providing tool support for security modeling.

[5] ISO. 2009. ISO 31010: Risk management - Risk assessment techniques. https://www.iso.org/standard/51073.html.
[6] ISO. 2011. ISO/IEC 27005: Information technology-Security techniques - Information security risk management. https://www.iso.org/standard/56742.html.
[7] S. Marsh. 1994. *Formalising Trust as a Computational Concept.* Ph.D. Dissertation. Queensland.
[8] Microsoft. 2018. Threat Modelling Tool. http://microsoft.com/security.
[9] Nazila Gol Mohammadi et al. 2014. Maintaining Trustworthiness of Socio-Technical Systems at Run-Time. In *Trust, Privacy, and Security in Digital Business*. Cham, 1–12.
[10] Nazila Gol Mohammadi et al. 2015. Combining Risk-Management and Computational Approaches for Trustworthiness Evaluation of Socio-Technical Systems. In *Proceedings of CAiSE 2015*. 237–244.
[11] MyAppSecurity. 2018. Threat Modeller. http://threatmodeler.com/.
[12] M. Surridge et al. 2017. 5G-ENSURE DELIVERABLE D2.5 'TRUST MODEL'. https://5gensure.eu/deliverables.
[13] VsRisk. 2018. Risk Assessment Software. https://www.vigilantsoftware.co.uk/topic/vs-risk.