Building on a Secure Foundation for the Internet of Things

Zinopoulou M., Ranchhod Ashok, Wills Gary, Atlam H.F, Nik Zulkipli NH

IOT SECURITY FOUNDATION

University of Southampton ECS

The Digital Marketing Association

Email:mz@dmaglobal.com

***Abstract*- The Internet of Things (IoT) is growing in different ways. The adoption rate of the IoT is at least five times faster than the adoption of electricity and telephony. Moreover, it is becoming the backbone of the future of the Internet that encompass various applications and devices. The IoT faces many challenges that stand as a barrier for the successful deployment. The security is considered the most difficult challenge that need to be addressed. Our work was instructed by the Internet of Things Security Foundation (IoTSF) in order to guide the future focus for the steering group to identify which areas of the IoT security to prioritize its efforts. The IoTSF has a mission to address the security needs of the IoT in order to ensure that its adoption can meet its predicted aspirations for establishing the business value. An initial focus on providing advice and best practice to hinder repeats of the mayhem enabled by the Mirai infection of consumer remote cameras and mainstream consumer vehicles, that is working towards building consensus for an internationally "approved by" mark that consumers can look for to determine security. This is addressing the need for trusted boot, root of trust, signed binary images and encrypted communication channels to secure the remote device.**

This paper suggests that the next area for consideration for The IoTSF is a co-operative security, a means of building trust into a group such that a collection of data sources that provide different telemetry data that are used in analytics to formulate an action are of known, secure origin.

I. Overview of the IoT

The Internet of Things (IoT) becomes a broadly examined subject among researchers, specialists and experts. It is considered the next stage toward the evolution of the Internet. In addition, the IoT is moving towards a phase where all items around us will be connected to the Internet and will have the ability to communicate with each other with minimum human intervention [1].

The concept of IoT was first mentioned by Kevin Ashton in 1999 [2,3]. He has said "The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so". Later, the IoT was formally presented by the International Telecommunication Union (ITU) in 2005 [4]. The IoT has many definitions suggested by many organizations and researchers. According to the ITU [5] it stated:" a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies". Also, [6] have suggested one of the simplest definitions of the IoT. It stated: "The Internet of Things allows people and things to be connected Anytime, Anyplace, with anything and anyone, ideally using any path/network and any service".

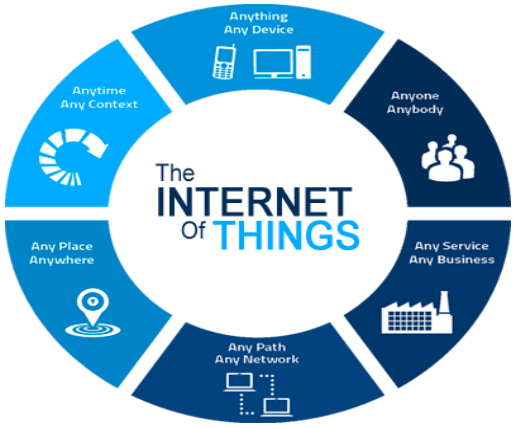

Figure 1. The connected world using the IoT

II. IoT is a reality!

Although many people have not heard about the term IoT, there were already more objects connected to the Internet than people from 2008 as shown in Figure 1. Predications are made that by 2020; the number of Internet connected devices will reach or even exceed 50 billion [7]. Furthermore, the IoT becomes the most massive device market that make companies save billions of dollars. The global market for IoT was around $1.928 billion in 2013. it is expected to reach to $ 2.065 trillion by 2020 [8].

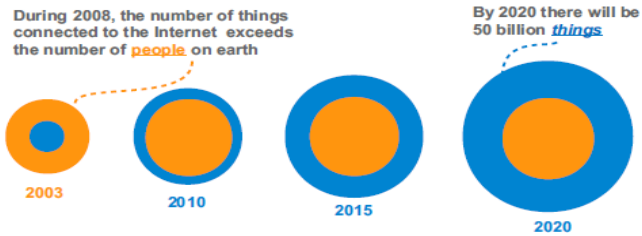

Figure 2. Growing number of things connected to the Internet

III. IoT Security Challenges

To make the IoT easily accessible at low overhead with many devices communicating with each other, the security challenges need to be addressed. Establishing an efficient security technique between IoT devices and Internet users is an important issue. The cryptographic algorithms solutions are not sufficient, so the future research should focus on developing an efficient end-to-end security measures [9]. For instance, the provision of data connection to the cellular phone has caused an incredibly rapid expansion and enabled a connected world. The connectivity we now all carry with us has had a huge impact on the business world and consumer world, whether its subscribing to streaming music, constant access to email and text based communications or sharing an image of our evening meal with remote friends [10]. Yet these connected devices are primarily communication devices, the security they include is there to ensure some form of privacy, or to extend services such as internet banking in a safe manner. These "things" we call phones grew up with security in mind, whether the route is via the cellular network (wide area network, WAN) or a local wireless network (local area network, LAN). The pervasive nature of network connectivity has gone on to establish an appeal to the world of the "thing". The vision of a commercial business accessing live data from an array of data sources and bringing the data back into the business to process and, through combining using analytics, deliver new, disruptive services is quite intoxicating; so intoxicating that it's been subject to the Gartner hype cycle for some time. The rapid success of social media, a "hot new thing" that appeared and established value rapidly, has the world looking for the "next big thing". This catalyst has fired up the imagination (Einstein said "imagination is more important than knowledge … ") and has engaged many to run to deliver something, anything, with many short cuts relating to security and privacy being taken.

Security traditionally has been as strong as the weakest link, that weakest link has been human until the mass deployment of the Internet connected devices has appeared. The attacker is likely to attack the weakest part, through an untrusted data source being enabled into a secure system. This has happened, Target's ~$1bn cost from the breach that had the attackers steal data from 40 million customer credit card via the HVAC system was financial. In a Smart City an attacker accessing transportation and utilities could turn an IoT dependent City into a very dangerous place indeed [11].

This paper takes stock of where we are regarding security now and outlines the journey we have yet to take, a journey where already IoT Distributed Denial of service (DDoS) attacks on security bloggers, enabled by a million-strong botnet of connected cameras, lightbulbs, thermostats and more have occurred. It then explores where the focus may want to be taken for the future, a future where if a significant number of the predicted 21 billion IoT devices by 2020 are compromised so the scale of botnets will be at truly unimaginable levels.

IV. The IoT applications in our life

The IoT have the capability to connect everyday objects. It enables many applications in different fields. The IoT applications can be essentially segmented into Consumer-facing and Business-facing.

Consumer-facing = Home, Lifestyle (Music, Drones), Health (Fitness), Mobility (Connected cars, bikes)

Business-facing = Retail, Health, Energy, Mobility, Cities, Manufacturing, Public Services, Others (Environment, Military, Agriculture, Hospitality).

The Consumer-facing has received significant attention, with items such as home heating controllers, kettles, dolls, TV's, car hacking, cameras, video recorders and baby monitors subject to the attentions of Mirai malware. In the case of the recent camera/DVR originated DDoS attacks the devices had hardcoded username and password combinations. The solution, suggested by many, is an industry certification from a security association such as IoTSF as a seal of approval for consumers to look for. Cached passwords on a phone mean whatever password you have on your phone is gated just by your phone pin. Additionally, the Consumer Mobility market, primarily the Automotive market, is also known to have shipped vehicles that can be hacked in minutes with the lights, aircon, theft alarm, steering, brakes and more. The challenge is that makers of consumer things are not historically familiar with cyber threats [12].

The Business-facing segment has also had some attention, and of course has the benefits of corporate IT departments and engineering departments who understand the challenges of security. The IT competence often extends to trusted boot and two-factor authentication to ensure security, but also to protect intellectual property. Yet, despite the IT competence that the business world understands, very recently the San Francisco Municipal Transport Agency had over 2,000 machines subject to ransomware. While the trains and safety systems were not affected this time, however the ticket machines were shutdown enabling free travel over the weekend. While the consumer segment may appear to be large through the size of deployments, the Business-facing segment is large due to its complexity and fragmented components [16].

V. Threats and attack vector in The IoT

IoT is been exposed to the cyber threats and attacks which these vector can be classified into a few categories [10, 11]. The main sources of threats in IoT has been identified as follows:

1) **Malicious user** – the owner of the IoT device which can perform attacks to learn the secret of the manufacture, gain access to restricted functionality.

2) **Bad manufacturer** – the producer of the device ability to exploit the technology to gain information about the users and exposing it to third parties.
3) **External adversary** - an outsider entity that is not part of the IoT system and has no authorised access to it. An adversary would try to gain information about the user of the system for malicious purposes. May causing the malfunction by manipulating the IoT entities.

Cyber-attacks on IoT devices has been classified into a few classes as discussed in [13,14] as shown in Table 1.

Classes of Attacks Vectors	Descriptions
Node Tampering / Node Compromised	An adversary can tamper with the device and use it to insert impostor to the system, use the device maliciously or out of its intended functionality like such as secret stealing, software manipulation, and hardware tampering
Denial of Service	Can be performed by stealing the device, manipulating its software, or disrupting the communication channel
Spoofing	Adversary use the credentials belonging to others in order to gain access to otherwise inaccessible service. The credentials can be obtained directly from a device, eavesdropping on the communication channel, or phishing
Privacy Breach	The adversary can infer private information from other sources such as meta data and traffic analysis
Buffer Overflow	Subvert the function of a privileged program so that the attacker can take control of that program, and if the program is sufficiently privileged, thence control the host
SQL Injection	A code injection technique, used to attack data-driven applications, exploit a security vulnerability in an application's software, allow attackers to spoof identity, tamper with existing data, cause repudiation issues.

VI. Engaging the smart city

The term Smart City has been more precisely specified as Infrastructure, Water, Lighting, Security and HVAC. However, those cities that have deployed IoT to enable a Smart City have brought all the data together into a single big data instance and will allow developers to leverage the pool of data. The Smart City is used to imply one focus, yet when asked for details everyone will agree its formed from many parts such as mobility, public services (including schools), Health and utilities (grid, energy, water, waste) in the dream of building out a whole city as smart [17]. The Smart City address the establishment of the root of trust by devices and establish a secure connection to the cloud is a significant, but end-to-end secure. The integrity of the whole chain of sea of devices into the cloud analytics engine, where the devices have secure boot, signed binary executables and initially establish a secure channel of communication such that the source of data has high integrity and high availability.

Figure 3: Smart city elements

The smart cities elements can include:

- **Transportation**

Capturing data from traffic flow, rail schedules and status, flights departures and arrivals, bus status and self-driving along with ticketing and informing travellers.

- **Airports**

Trials have been ongoing to count footfall into airport toilets to understand whether the cleaning crew are likely required. Bathroom service companies are developing smart soap dispensers, video capable hand dryers and toilet roll monitoring. Tracked luggage, intelligent lighting, passenger travel patterns, intelligent advertising.

- **Rail**

Companies like Cubic Transportation, the operator of the TfL transport network have bought Serco's road traffic information system. They have devices known as gates, others as station computers and also ticket machines (PoM's) for the rail and bus services, and are planning to add road to enable intelligent travel, a real IoT application bringing related but unconnected data together to provide additional business value.

- **Traffic**

There are several systems out there that count traffic flow and feed into navigation systems to enable the driver to make an informed decision to follow the revised routing. Locating parking, managing traffic lights, recommending switching to rail in times of high congestion.

- **Automotive**

Several automotive companies and others are researching self-drive cars and some are forecasting that it will not be long before car ownership is a thing of the past. The challenge will be the autonomy will need to be on board as the communication

channel needs to avoid being the single point of failure. However, traffic flow information from the traffic system will need to be directed into the communications network4. Variable speed limit gantries would be replaced by intelligent vehicle behaviour, lane changes minimized and traffic flow and traffic speed optimized.

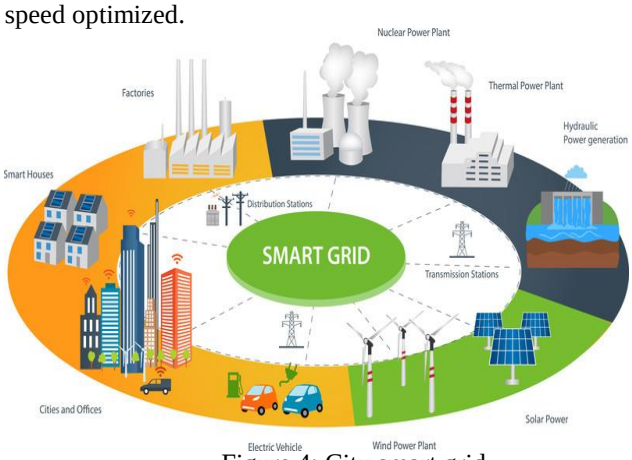

Figure 4: City smart grid

VII. Commercial Utilities

The IoT is a suite of technologies and associated business processes that imbues devices of all types with an ability to communicate information about their status to other systems, creating the chance to evaluate and act on this new source of information. Thanks to the IoT, the energy usage become more efficient, which will help to relieve some of the stress on energy demand. The common IoT commercial utilities are:

- **Electricity**

Demand Side Management, such as that being developed under the EU project "Real Value"5 is enabling the energy provider to manage the energy storage at the energy user's property. The Shetland trial6 has shown that providing consumers with a room temperature management by the energy provider is valuable, particularly where renewables are in use. Intelligent lighting7 enabling commercial premises to install adaptive lighting which leverages not only motion detection (occupancy) but also daylight farming to reduce the energy demand, and can also provide temperature, humidity, CO, CO2, NO, NO2 and hence provide environmental quality and utilization information to the site manager [15].

- **Public Utilities**

The management of public bins, consumer's bins, commercial bins along with street lighting that monitors the street, perhaps monitoring parking bays and car park usage.

- **Waste Management**

Instrumenting containers, whether they are street bins or larger, is enabling informed waste management. Examples include Helsinki and Enevo OneCollect where the use of smart routing to manage collection waste is saving time, money and resources.

- **Street Lighting**

Taking already smart lighting and connecting them to form intelligent lighting can establish lux (light intensity) as a service rather than lighting, establish connectivity to other items by providing IoT access points. Additionally, the street light is a perfect place to add additional instrumentation for instance to determine temperature, humidity, pollution, pedestrians, vehicles, parking.

- **Education**

The smart education changes the learner's learning style as learning happens through multiple devices and is not limited to paper and traditional classroom learning. It allows for learning to be tailored to the requirements and abilities of the learner. This can significantly enhance the interest and engagement levels of the students that learn through these environments.

- **Government**

The government needs to play a role in the development of the IoT, not just to create and execute on strong policies to foster innovation but also to provide a sense of security to our citizens when they are confronted with security issues. Some government organizations have cited budget costs or other higher priorities as the reasons to not currently engage in the IoT.

- **Parking**

Coupling parking bay sensors and ANPR into a central service that can notify either a mobile device or the in-car navigation is already deployed in many towns. The driver is directed to the parking place, the system knows when they are parked and for how long and hence automatically charges on leaving. The Smart City takes these live data control loops (data causes response) from multiple services, and applies a collective intelligence. For example, the traveller may arrive into the city by car and due to pollution levels from traffic congestion be advised the journey to the parking place identified near their destination that selecting an alternative, nearer parking space and using the underground train will be cheaper and less expensive. However, such joined up, live data based analytics comes with some significant security, data integrity challenges. To combine data sources and formulate a decision with live data, will require a root of trust not only for the data that is the prime active source, but for all the secondary data that is being utilized to formulate the recommended, or taken, course of action [16].

VIII. The connected Individual

It is clear that each of us, in one way or another is very closely a part of the Internet of things and security or data breaches can affect us in many different connected ways. People will soon be wearing electronic devices and many are already wearing trackable heart implants. This area of biomedicine is likely to grow in the future. A recent article in Wired indicates that pacemakers are vulnerable to malicious hacking. However, on a daily basis as the diagram below shows how the individual is

affected via IoT on a grand scale on a daily basis without being aware of their own health and security.

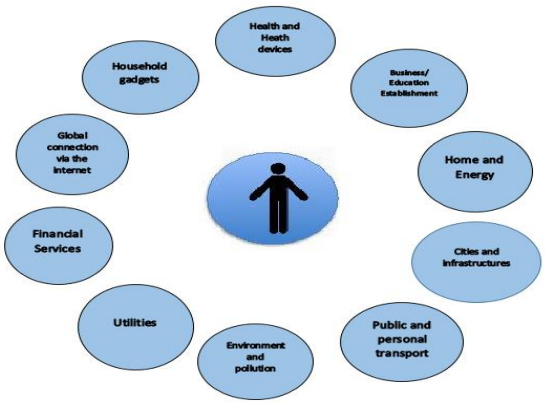

Figure 5. The connected individual of the IoT

IX. Building trust using blockchain

The concept of trust and integrity is reflected in our daily lives. The trust of close family, the determination that data being used to make decisions is not only from a trusted source but has also maintained integrity ensures decisions have checks and balances in their formation. The bitcoin invention required such security, integrity and from this developed the blockchain database. The mechanism to determine the data, from all data sources needing to be part of the analytics, is from a root of trust, has maintained its integrity and is time bound and its history locked in a public ledger (or blocks) where copies are held in the community, the city if you like [15]. In the world of the "things", there are mechanisms to determine root of trust, including trusted boot, signed executables, white-list security and SSL/TLS encryption and, an aspect of past behaviour included in the edge management [16].

X. Conclusions

IoT represents a modern approach where boundaries between real and digital domains are progressively eliminated by changing over consistently every physical device to smart object ready to provide smart services. These services are getting more opportunities in different life domains but at the same time rising new challenges specifically in security. The Consumer-facing segment of the IoT has been termed "a train wreck" but advice is available from security professionals that are building out the recommendations that consumer companies can adopt. The IoT Security Foundation have this area identified and there is building consensus that an "approved by" mark, much like CE, UL or "BS kite" is required to provide the consumer with a level of confidence regarding the security of IoT. While Smart Cities are referred to as if a singular entity, they are in-fact a collection of smaller systems that have their own value delivered through a sensor-control loop. The very nature that a Smart City is bringing together live data from multiple feeds and then making decisions based on the collected information is its vulnerability. Regarding Smart City, we suggest it's no longer about the devices but the whole system. The broad set of sensors and the broad set of controls would suggest that applying analytics to the breadth.

Our recommendation is that the next area to focus is the Smart City, as it rather than just thinking about the devices its thinking about the whole system and the challenges that a security vulnerability in a connected city could provide. The single point of failure, where a breach would impact, potentially the whole city.

References

[1] R. Shanbhag and R. Shankarmani, "Architecture for Internet of Things to minimize human intervention," *2015 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2015*, pp. 2348–2353, 2015.

[2] K. Ashton, "That 'Internet of Things' Thing," *RFiD J.*, p. 4986, 2009.

[3] G. Joshi and S. Kim, "Survey, Nomenclature and Comparison of Reader Anti-Collision Protocols in RFID," *IETE Tech. Rev.*, vol. 25, no. 5, p. 285, 2013.

[4] ITU, "The Internet of Things," *Itu Internet Rep. 2005*, p. 212, 2005.

[5] ITU, "Overview of the Internet of things," *Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model.*, p. 22, 2012.

[6] P. Guillemin and P. Friess, "Internet of Things Strategic Research Roadmap," *Eur. Comm. Inf. Soc. Media, Luxemb.*, 2009.

[7] D. Evans, "The Internet of Things - How the Next Evolution of the Internet is Changing Everything," *CISCO white Pap.*, no. April, pp. 1–11, 2011.

[8] H. Gusmeroli, S., Haller, S., *Vision and challenges for realizing the internet of things*, vol. 1, no. APRIL. 2009.

[9] M. S. A. Carlo, "An Overview of Privacy and Security Issues in the Internet of Things," *McKinsey Q.*, vol. 2, p. 6, 2013.

[10] T. Greene, "Largest DDoS attack ever delivered by botnet of hijacked IoT devices," 2016. [Online]. Available: http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html. [Accessed: 28-Nov-2016].

[11] Thor Olavsrud, "11 Steps Attackers Took to Crack Target," 2016. [Online]. Available: http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html. [Accessed: 26-Nov-2016].

[12] CORY DOCTOROW, "Two hackers are selling DDoS attacks," 2016. [Online]. Available: https://boingboing.net/2016/11/28/two-hackers-are-selling-ddos-a.html. [Accessed: 28-Nov-2016].

[13] A. W. Atamli and A. Martin, "Threat-Based Security Analysis for the Internet of Things," *2014 Int. Work. Secur. Internet Things*, pp. 35–43, 2014.

[14] F. A. Teixeira *et al.*, "Defending Code from the Internet of Things against Buffer Overflow," *2014 Brazilian Symp. Comput. Networks Distrib. Syst.*, pp. 293–301,

2014.
[15] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, 2016.
[16] Enrico Camerinelli, “How I Explained Blockchain to My Grandmother,” 2016. [Online]. Available: https://www.finextra.com/blogposting/12378/how-i-explained-blockchain-to-my-grandmother. [Accessed: 22-Nov-2016].