A Survey of IoT Security Infrastructure for Business and Cities

Luke Walker
Manchester Metropolitan University
luke.walker3@stu.mmu.ac.uk

Louis Kelly
Manchester Metropolitan University
louis.kelly@stu.mmu.ac.uk

October 27, 2020

Abstract

There has been an incredibly massive boom in terms of IoT connected devices in recent years, mainly due to the rapid adoption of high-speed internet, cloud computing and big data. Cheap electronic devices are now taking over our homes, businesses and cities with the promise that boring and uninteresting tasks can now be completely automated by machines. There has been a general positive reception to these developments, however some security professionals warn that this could be a completely new era for cyber attacks. Within this paper we will discuss the current IoT landscape, critically analyse already existing solutions to IoT security and present our own ideas around how IoT can be re-imagined into a helpful and secure computer system.

I. Introduction

In the modern world, Internet of Things (IoT) devices are generally small, low powered internet connected devices that enable users to connect objects, such as light bulbs or CCTV cameras to the internet for the purpose of simplicity and ease of access. The role of IoT is to identify and discover new information, create decisive creative solutions, provide automation and anticipate future affairs. The goal is to provide end users with smart services where specific activities can be used anytime and anywhere. Additionally, IoT has grown to become a predominant part of smart technology and continues to strengthen the many benefits to human life. [1]

IoT offers numerous benefits to organizations. Most modern enterprises are already leveraging IoT to automate and simplify many of their daily tasks. Connected devices are being integrated into existing and evolving business processes. The industrial Internet of Things focuses on automation - not just to lower operating costs but also to increase productivity, improve business processes, enhance customer experience, expand to new markets, and generate additional revenue streams. Industrial IoT is all about being well-informed to make timely and better decisions. It can help organizations shift from the traditional way of selling hardware or software to selling all-inclusive solutions - products equipped with sensors and wireless communications to generate valuable data.

With the explosive growth of IoT devices in our cities and businesses, many mission critical job roles are being replaced by machines. Unsafe and dangerous work can now be achieved with intricate IoT machines, reducing the amount of accidents in the workplace. With the rise of these IoT systems increases the threat from traditional cyber attacks, along with newly posed threats.

IoT devices have a reputation in the media for poor programming etiquette within their software packages and along with poor application design these computer systems have become a massive target for hacktivists, state sponsored actors and cyber crime gangs. Within the ever-growing use of smart devices, poor and vulnerable code has snuck its way into healthcare,

nuclear power and military missile silos, with devastating consequences. The societal opinion on IoT devices doesn't stop us from lining our streets, our homes and businesses in the latest smart gadgets and in this paper, we shall perform an ad-hoc analysis on proposed solutions to this largely growing issue around smart devices. It is our responsibility as computer scientists to analyse and protect our information systems from attack.

II. Classification Proposal

The chosen classification for this survey paper is primarily focused on three main types of attacks associated with the IoT infrastructure. These three attacks have been chosen specifically for this survey paper to help prevent the effects of successful cyber attacks upon businesses and smart cities. While the threat towards smart cities are minimal in this current age due to the small adoption rate of smart technologies, research must be conducted to ensure that our cities remain secure when the proffer of these technologies occur. With the rapid adoption of 5G wireless technology, smart cities are becoming more surreal. There is already a growing number of cyber security threats within businesses, as new office buildings move to adopting IoT enabled devices. These devices are usually connected to corporate LAN's and usually aren't placed under the same monitoring conditions as employee computer systems which offer easy access points for attackers to exploit and break into company LAN's. This paper will investigate the current threats facing IoT security infrastructures along with an analysis into defense mechanisms and unresolved problems and difficulties we as computer scientists will face. Below is the proposed classification model.

Table 1: *Classification Model*

Threat	Eavesdropping	DDoS	Malware
Vector	Network	Network/Physical	Network
Attack Complexity	Low	Low	Medium
Confidentiality Impact	High	None	High
Integrity Impact	High	None	High
Availability Impact	Low	High	High

III. Current threats facing IoT Security

The threats facing IoT are continuously on the rise as the development of IoT technology is rapidly changing and expanding. The emergence of IoT has led to the industry finding it difficult to keep on top of the current threats facing IoT. As more devices are introduced, convivence tends to overwhelm the thought of potential security threats that already exist within IoT technology. Businesses are becoming more reliant on IoT technology in terms of cost efficiency and convivence rather than the security protection that the technology has to offer.

i. Eavesdropping

Eavesdropping is currently another threat facing the security of IoT. Eavesdropping occurs when an attacker is able to listen to the data transmissions exchanged between two or more devices over a network. In relation to IoT, an attacker remotely uses the same process however the only difference is that the attacker can either receive audio and video transmissions or other related sensitive information [2]. An example of a successful eavesdropping attack on IoT would be when Reuben Paul, attended a cybersecurity conference and demonstrated a live attack on a Bluetooth enabled teddy bear. Reuben was able to succeed with his attack due to the vulnerabilities in the Link Layer Protocol and the Link Manager Protocol. When the teddy bear was connected to both Wi-Fi and Bluetooth, the transmission to receive and send data was enabled. After performing a scan, he was able to obtain the device number, listen and record the transmission of audio from the integrated microphone [3].

ii. Denial of Service Attacks

Overall, IoT devices generally communicate via radio access technologies located in the physical layer. Additionally, the wireless link is very prone to the approach of Denial of Service attacks caused by either jamming or signal distortion. As there is no general solution to the avoidance of DoS attacks, proven techniques such as spread spectrum can be used to mitigate against wireless jamming [2]. Overall, existing approaches require a large amount of processing which most existing IoT devices will not have. In order to propose correct solutions, the use of monitoring traffic needs to be implemented however this only operates on layers higher than the physical layer. Alternatively, IoT devices can be utilized as a source for Distributed Denial of Service attacks. With the lack of authentication, countless amounts of devices with vulnerable username/password pairs can be used to serve as part of a botnet to perform a successful DDoS attack. A clear demonstration of this would be the Stuxnet attack in 2010. Iran's Natanz uranium enrichment facility was the target of a DDoS attack which deployed a botnet of over 600,000 IoT devices causing centrifuges to burn out [4].

IV. Trends within IoT Security

Within Computer Security generally there has been a massive push by governments and professionals to make sure systems are secure for users. This gigantic push has started to inform the public on how they can keep their data secure, for example, using password managers, 2 factor authentication and malware protection is now an extremely common practise. Arguabily the industry that's been missed is IoT, with cheap software and hardware being massed produced for the western market, software vulnerabilities are prevelent within the IoT devices of today. Within a paper written by M. Radovan et al, he discusses the need for support of the confidentiality, integrity and availability triange between devices within his own study of IoT security trends [5]. Arguabily, this point is fully developed, but with low powered IoT devices being produced for cheap in easten markets, suppliers and companies are not implementing hardware that's fast enough to keep up with secure standards of encryption, within their own research and development, security costs time and money and therefore mass produced insecure devices are finding their ways into mission critical environments, such as hospitals, power stations and nuclear weapon programs [6]. This becomes an issue for Cities and Businesses wanting to implement smart devices into their workflow. Systems such as SCADA, or supervisory control and data acquisition systems are usually used to connect industrial devices to a network, these are key, mission critical devices within most businesses and manufacturing plants, therefore the security of these devices, especially since the Stuxnet hack, has been looked into a lot more rather than everyday IoT such as Amazon Alexa. Companies need to be more aware of what is publically accessible on their interanet due to services such as Shodan.io and Censys.io making it extremely easy for malicious attackers to preform reconnaissance on IT networks.

V. Defence Mechanisms

IoT devices mainly interact with the internet or other controller devices over Bluetooth, WiFi or Ethernet. This section will delve into the discussion of defense mechanisms of these protocols, and underlying protocols such as Zigbee. Defensive solutions to mitigate Bluetooth threats are significantly different compared to defensive solutions in relation to the vulnerabilities of other network protocols, depending on the device and the programming practises that have been taken when writing the software, it has been known that vulnerabilities can be found in the Bluetooth stack of devices, some which require no authentication and give the attacker full control over the device (Usually called Remote Code Execution). Patches for software versions are generally used to prevent ongoing/recently

found vulnerabilities in computer systems however, some no name IoT manufacturers will not push updates for devices which are considered old or obsolete, this can leave serious vulnerabilities, such as no click remote code execution issues unpatched forever. If this sort of device is connected to the world wide web, it makes for an extremely easy access point for attackers. Only device manufacturers can develop such upgrades/patches usually, therefore users cannot develop their own patches to the system firmware and therefore it is inevitable that Bluetooth devices with these characteristics will remain vulnerable to attacks. Whilst there is no guarantee of security, there are countermeasures that exist and can be utilized to safeguard the Bluetooth communications, examples of these are baked right into the Bluetooth standard and include things such as PIN authentication when connecting new devices together.

On the other hand, we have WiFi. An extremely common protocol which uses many security standards to make sure traffic between the router and the connected device isn't compromised in transit. WiFi, when used in WPA/WPA2 or even WEP mode, encrypts all data traveling to and from the router which makes packet sniffing and man in the middling these connections completely impossible. The attacks that mainly threaten IoT security in regards to WiFi are rogue access points, if an attacker can transmit a WiFi signal, using the same SSID as what the IoT device is usually connected to. There is a possibility that the IoT device will connect to the attackers wifi access point instead of the secure one. The attacker can then use tools such as SSLStrip to see what data is being passed over the wifi network from the IoT device. This wouldn't usually be a problem, however if the device isn't recieving updates, as mentioned in the Bluetooth section, it could be an easy step towards fully compromising the IoT device, for example, if the device is checking or downloading an update binary, the attacker controlling the rogue WiFi access point could potentially deliver a malicious update binary instead. The attack theoretically discussed here can be protected against with basic hash checking on the IoT device itself, however from our research presented in this paper it should be known that most IoT devices don't have the hardware capabilities to do basic encryption.

VI. Unresolved problems and Difficulties

In this section, we will discuss the unresolved problems and difficulties that currently face IoT security. As mentioned previously within this paper, IoT security is arguabily down to the manufacture to implement secure products for the market. However, on the flip side, with the deployment of IoT devices within mission critical operations, it should also be down to the business or government to make sure that the technology is safe. Dr. K Tabassum et al said in his paper "Security Issues and Challenges in IoT" [7, "it can be achieved through planning at the beginning, since if the security is considered in the initial stage it can solve substantial IoT security issues"]. While I agree with this statement, depending on the vendor of the product, this might not be the case. If an IoT product for business, eg: CCTV for security is developed, the company developing the application code that will power the system might have a completely different definition of security when compared to another company or individual's opinion. Research has been conducted to outline the current security threats and vulnerabilities within IoT and the lack of implemented security standards associated within the development of IoT. M.Radovan and B.Glub mention in their research paper [8, "But in the future, we will have to address this problem further by moving to a more systematic approach to IoT security."] Here, both authors have addressed the issue that IoT security needs to be considered in the future, however, throughout the paper no ideas or mitigation strategies have been suggested to

futureproof the security of IoT. Additionally, both authors have mentioned a wide variety of the current security trends in IoT and have suggested counter measures in prevention of the current threats towards IoT. Additional research has been done within using blockchain as a potential security standard within IoT devices/networks. Minhaj Ahmad Khan et al stated in his paper "IoT Security: Review, blockchain solutions, and open challenges" [9, "blockchain based on smart contracts is expected to play a major role in managing, controlling, and most importantly securing IoT devices."]. The basic idea behind his research is to utilize blockchain, due to the encryption and other security features that it implements. While this is a good idea, and the implementation of the project already exists, it may prove to be extremely difficult to get device manufacturers on board, since it's a very time and cost consuming idea, a better idea might be to implement a similar technology to blockchain which inherits it's encryption algorithms, which is the main point that's pushed within this research. While on the topic of blockchain, research has also been developed within the Machine learning and Artificial intelligence community. Liang Xiao et al, of Xiamen University, create a paper discussing the use of machine learning and AI to secure IoT devices. The idea behind the research presented in the paper [10], is using AI to create machine learning models around when devices are accessed and used, with the idea being that a IoT device will learn what hours of the day its normally used and then therefore only allow the use of the device at these given times. Another approach is to train a machine learning algorithm which classifies what malware looks like, so, therefore when a device is potentially exposed to malware, the machine learning algorithm produces a test to see if the file being executing acts like malware or not. Both of these ideas are extremely futuristic, and something that could be used in the future, however in the current day and age it's extremely CPU and GPU intensive to run machine learning and AI. With most IoT devices being low powered, this idea is not applicable to the current day and age, but copuld be implemented into smart cities within the coming years. Research in relation to Bluetooth vulnerabilities and types of attacks have been illustrated by Angela M et al [11]. In depth descriptions of the types of attacks associated with Bluetooth have been detailed, providing explanations with examples for each attack "During the hack, continuous device inquiries for visible Bluetooth devices are conducted by running cwscanner script" Here, the authors have specifically gone into detail of how one of the attacks is performed. Alternatively, the research conducted has only focused on Bluetooth and research hasn't been expanded in relation to other versions of Bluetooth such as BLE which has a number of different vulnerabilities. A well-presented structure and an overview of security aspects for different IoT technologies have been illustrated by Ivan C et al [12] and have focused primarily on the perception layer "This chapter will present the security features of each layer of the IoT architecture with the focus on perception layer specific to the IoT environment." In addition, some descriptions of the types of threats related to the technologies haven't been mentioned. Furthermore, explanations of protection methods have been detailed efficiently. Finally, we would like to touch on the topic of 5G and the security concepts that have been developed around this new internet protocol. In a paper by B. Seok [13, "Secure D2D Communication for 5G IoT Network Based on Lightweight Cryptography"]. B. Seok, et al goes into details about a basic and lightweight cryptography standard that can be impliemented in relation to D2D networking with 5G. D2D networking is usually used in vehicles, such as the Tesla brand of cars to allow them to communicate with the owners smartphone over a network connection, this enables features such as Web browsing on the internal computer system and also allows the Tesla to automatically update it's software versions. The point put across in this paper

is to make sure that there is a cryptographic wrapper around network transmissions to ensure data integrity when communicating with vehicles. This paper suggests using an Elliptic curve encryption algorithm, with a 128-256 bit key. Suggested algorithms include Diffie-Hellman and ECDSA. This is a good idea, however the application code running these algorithms needs to be easy to use for the public. The public will not like it if they have to manually mess around getting the encryption keys setup, additionally the software inside the car needs to be stable, as if the memory chips holding the encryption algorithms short or break, the owner will no longer be able to communicate to his car remotely and the additional network features that are provided by the 5G protocol will no longer work.

Our paper now proposes an interesting concept, can a standard for securing IoT devices be developed similar to ISO 27001?

By proposing a standard of security for IoT devices, similar to other standards that already exist within other areas of IT security, will in theory reduce the number of malicious actors using IoT devices around the globe for the threats already mentioned in this paper. For example, the Mirai botnet, which was active in 2017, used a bruteforcing mechanism, along with an internet scanner to remotely take over IoT devices. Many other similar botnets already exist and are still in use today, however the weakpoint in the chain is default Admin credientials for the control panel of these devices. [14, "the bot then performs a dictionary attack over Telnet using a set of hard-coded credentials"]. Theoretically, if the standard included using random, 8-16-character passwords, the Mirai botnet and its clones wouldn't exist in todays enviroment on such a large scale.

Secondly, this paper proposes new secure programming practises. This suggestion can easily tie in within the compliance standard as suggested above, however the main aim here is to make sure that code which is running on these IoT devices, wether that be in the local takeaway, or in an extremely dangerous enviroment such as hospitals intensive care unit is arguabily secure. When we talk about arguabily securing devices, it is defined as writing secure programming code, weather that be C or PHP which doesn't introduce any vulnerabilities into the product from poor programming ettiqute. Examples of this might be making sure that bruteforcing secure panel logins isn't possible via rate limiting or making sure user controllable data inputs are sanatized. This would dramatically reduce the attack surface for IoT devices.

Thirdly, and finally, this paper also proposes that governments and organizations related to security need to do more in regards to informing the public about the IoT devices they are purchasing in stores, wether that be for home or business, the public need to be able to make an informed choice which has been backed up by professionals on the safe devices to buy. This helps prevent people from becoming victims of Cyber attacks, which in this day and age can result in serious fines and penalties. For example if a business buys some new IoT thermostats for the office, and they're insecurely programmed and a malicious entity breaks into these devices and manages to exfil sensitive data from the company, it is quite possible under European law that a GDPR fine will be presented to them. The National cyber security center for the UK is currently doing an excelent job at providing and sharing knowledge and advice around which IoT products are safe to buy and how the public can secure these devices further. However, this needs to be a worldwide share of data and not just localised to the UK. We firmly believe that with knowledge around security of these IoT devices, the landscape that has been presented in the media related to IoT devices being completely insecure will start to fade away, and people do listen when it comes to security in general; 2 Factor

authentication and password managers are now quite commonplace throughout the developed world, which has been constantly suggested and mentioned within the media.

VII. Conclusion

The growth of IoT is everlasting as the advancement of technology is increasing significantly as the future develops. Businesses and consumers are becoming more reliant on this technology as it offers cost efficiency, ease of access, automation and security. In the modern world, individuals and organisations are so indulged by the convenience that IoT offers that not enough research has been evaluated to express the importance of the security risks associated with IoT. As smart cities are on the verge of development, it is crucial that research is conducted to future proof the inventible threats that IoT technology will face. Because the development of this technology is ceaseless, once the development of smart cities starts, the overwhelming number of new devices being introduced will drastically affect the security of IoT and will become more difficult to remain in control. This survey paper has outlined the current threats facing IoT followed by the current trends within IoT security and has presented new solutions to issues discussed within this paper.

References

[1] Selvaprasanth Pallakku and Sathiyanathan N. A brief study on iot applications. *Journal of Scientific Research and Development*, 4:23–27, 01 2020.

[2] Congyingzi Zhang and Robert Green. Communication security in internet of thing: Preventive measure and avoid ddos attack over iot network. In *Proceedings of the 18th Symposium on Communications and Networking*, CNS '15, page 8–15, San Diego, CA, USA, 2015. Society for Computer Simulation International.

[3] Mark Samuals. With teddy bear bluetooth hack, 11-year-old proves iot security is no child's play. *https://securityintelligence.com/news/with-teddy-bear-bluetooth-hack-11-year-old-proves-iot-security-is-no-childs-play/*, 2017.

[4] Marie Baezner and Patrice Robin. Stuxnet. 02 2018.

[5] M. Radovan and B. Golub. Trends in iot security. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1302–1308, 2017.

[6] Dorothy Denning. Stuxnet: What has changed? *Future Internet*, 4:672–687, 12 2012.

[7] K. Tabassum, A. Ibrahim, and S. A. El Rahman. Security issues and challenges in iot. In *2019 International Conference on Computer and Information Sciences (ICCIS)*, pages 1–5, 2019.

[8] Mihael Radovan and Boris Golub. Trends in iot security. pages 1302–1308, 05 2017.

[9] Minhaj Ahmad Khan and Khaled Salah. Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395 – 411, 2018.

[10] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu. Iot security techniques based on machine learning: How do iot devices use ai to enhance security? *IEEE Signal Processing Magazine*, 35(5):41–49, 2018.

[11] Angela Lonzetta, Peter Cope, Joseph Campbell, Bassam Mohd, and Thaier Hayajneh. Security vulnerabilities in bluetooth technology as used in iot. *Journal of Sensor and Actuator Networks*, 7(3):28, Jul 2018.

[12] Ivan Cvitić, Miroslav Vujić, and Sinisa Husnjak. Classification of security risks in the iot environment. 10 2015.

[13] Byoungjin Seok, Jose Costa Sapalo Sicato, Tcydenova Erzhena, Canshou Xuan, Yi Pan, and Jong Hyuk Park. Secure d2d communication for 5g iot network based on lightweight cryptography. *Applied Sciences*, 10(1):217, Dec 2019.

[14] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim. An in-depth analysis of the mirai botnet. In *2017 International Conference on Software Security and Assurance (ICSSA)*, pages 6–12, 2017.