The Internet of Things: Security Challenges and Solutions

Haseeb Farooq
Faculty of Engineering and Informatics
University of Bradford
Bradford, UK
hfarooq7@bradford.ac.uk

Abstract—The Internet of Things (IoT) is the notion of converting everyday objects into smart objects. The purpose of this is to connect the rigid objects we use in our everyday lives to one another to create smart homes, smart cities and smart environments. Objects such as clocks, thermostats, speakers and almost every other electrical object are being equipped with the ability to connect to the internet. This in turn converts the object into a smart object which becomes a part of the internet of things family.

Keywords—Internet of Things, network security, cyber-attacks, information security.

I. Introduction

The current form of the internet of things is present in our personal devices such as smart phones, tables, computers and other smart gadgets. These devices collect data and communicate with one another. On the other hand, the data is also being sent to cloud-based servers where companies that make the products can access the data and use it for their own personal gain. This is the because security issue of the internet of things, privacy [1]. In this report I will be discussing the complex security challenges faced when implementing the internet of things. I will be outlining the positives and negatives of a society that functions using the internet of things. As well as this I will be discussing the solutions and ideas that are designed to counter act the security issues faced.

II. What is the Internet of Things?

The internet of things or commonly known as IoT, is our advancements of having a more connected society. With the recent introduction of 5G network speeds, it is now possible to have almost every electrical device connected to the internet to create 'smart' societies. Devices will constantly be communicating and sharing data to one another in order to complete the tasks they are set and improve efficiency. The internet of things devise work by using sensors that will measure a variable such as, temperature, speed, lighting, noise etc. The data is then sent to secure servers using the internet. The data is then analyzed in an automated process and converted into information that can be visualized and understood. The smart devices we use such as mobile phones or personal computers are then sent this information where they can be monitored and if needed acted upon. The security risk involved is when the internet of things device is sending the data to a server, the data can be intercepted by hackers which can then use the devices for their own illicit purposes. The process of securing these devices are what the security solutions will become, and this report will be discussing these risks and solutions in different internet of things environments [2,3].

III. Internet of Things in Smart Cities

The internet of things can already be seen in modern developed cities. Traffic lights already have sensors to detect vehicles and pedestrians and some are already connected and sharing data. In a smart city where certain lampposts are turned off to save energy, a traffic light can detect and oncoming car and turn on the lamp posts for the corresponding road. A garbage bin could have sensors that let the city council know when it is nearing full capacity. With 5G network speeds there are plans to introduce smart devices all over cities to improve the inhabitant's day to day lives and improve efficiency [4]. Traffic can be monitored with sensors on the road to detect the most congested areas and re-route driverless vehicles to improve the traffic flow. Subway systems in cities can also monitor the amount of people using the subway and predict delays before they happen to reduce and prevent the delay times.

A. Security Risk of an IoT Smart City

Despite the endless positive possibilities associated with smart cities and the internet of things. The main drawbacks are the security risks associated with devices connected to the internet. We currently use devices such as mobile phones and computers that have access to the internet. As we have had these devices for many years, they are very secure and good at preventing cybercrimes from taking place. Our devices are very hard to hack and get accessed by the wrong people, this makes our data and privacy relatively secure. However, implementing the same level of security to objects that are rarely interacted with people has shown the drawbacks of the internet of things.

Having firewalls and anti-virus software is easier to implement on a smart phone than it is on a traffic light or security camera [5]. As smart phones are always being interacted by people, we can often notice or be made aware if there is unauthorized access to our device. Objects on the other hand could be hacked and the admins/owners may never even know of the crime. CCTV in public areas, traffic lights, city lighting could all be compromised and exposed to cybercrime with no real way of detection and prevention. A worst-case scenario could be that criminals could use whole cities as hostages for ransomware attacks by taking control of objects that keep the city running [6,7]. This could include railway systems, road sensors used by driverless cars etc.

B. *Security Solutions for IoT Smart Cities*

As we are closing into the age of internet of things, cyber security organizations have begun to introduce potential solutions to the highlighted issues of the internet of things. One example is by the organization NIST, a US government federal agency. They were tasked to find a cyber security solution for a wireless blood fusion pumps used by hospitals. As they are wireless and part of the internet of things, they were prone to cyber-attacks such as hacks to gain access to the machines. The solution NIST came up with was to add a digital certificate to the pumps. This would limit its communication abilities to only establish contact with its intended servers and nothing else. This same system can be used in smart cities as the initial security phase for the internet of things age [8-10]. Cyber security can be compared to an arms race, the higher and complex the security the higher and complex the cyber-attacks. This initial solution of having digital certificates will eventually be compromised by cyber criminals however provide time to introduce better and more complex security solutions.

IV. Internet of Things in Smart homes

Smart homes are now becoming a reality and which the age of internet of things it is rapidly advancing. Internet of things can be seen in various objects around modern homes, the most recent and prominent being smart home hubs such as Amazons Alexa and Google Home. These devices can connect to all the smart devices around a home in the internet of things environment. The goal Is to have a virtual assistant help in daily lives at home, voice commands and smart phone are the most commons method of communicating the smart home hubs. Objects such as light bulbs, temperature control units and televisions can all be controlled with a simple voice command or a simple touch of a button from your smart phone [11].

A smart fridge can detect what items are placed within the fridge. If certain items are running low, it can send a notification to the homeowner’s smart device to alert them so they can re fill what’s missing. All these devices will communicate by sending data collected by their sensors to a cloud server. The data can then be converted into useful information and sent back to the home occupants’ smart devices. The smart home requires a powerful internet connection because of the addition of internet of things devices, high bandwidth will be necessary. Because of these fewer households can take advantage of smart homes as most of the population will not have access to super high-speed internet connections [12].

Internet service providers will also need to ensure that the connection provided does not drop or fail. This could lead to households ceasing to function because of their heavy reliance on internet access. Manufactures that design and create internet of things devices need to implement contingency plans should the device lose connection to the internet. The most notable being smart door locks, a feature needs to be in place where the door can be unlocked without the internet connection. A code to input or a physical key could be some solutions to this issue.

A. *Security Risk of an IoT Smart Home*

The biggest security risk for a smart home is privacy. As the internet of things allows objects to communicate with each other, they are passing data which can often be private around to on another. An example can be smart security cameras within a home, the camera could potential be hacked, and the hackers could have access to the footage being recorded on the cameras. information such as what time the occupants leave home, what time of day the house is empty and even a layout of the entire home can all help burglars when breaking into homes. Smart locks can be hacked to open doors and once a criminal has access to one device in the home, they can gain access to all the other devices with ease. Another major security risk is the botnet.

Botnets are used to take control of internet of things devices and use them for a hacker’s personal gain. An example is the 2016 attack on the internet server host DYN, the severs were overloaded with fake requests which lead to its downtime. The botnet software was called Mirai and it used hundreds of thousands of devices to participate in the attack. It used a variety of internet of things devices such as webcams, smart bulbs, smart locks and many more. The issue with the smart home devices is that they often have little to no security other than a default username and password to gain access. There is very little hardware memory in the devices to set up firewalls which makes it very easy for hackers to gain access. Hackers only need a single device to access the entire IoT network as the other devices are set to trust and communicate with one another [13].

Internet of things environments make it easy for criminals to set up large scale botnets to cause cyber damage. A big privacy risk highlighted is big corporations having control of your home and know your daily activities and habits. Your information could be sold to advertisers who can target you based on how the smart objects around your home have recorded your activities. Your home may virtually have no privacy at all as a result which is concerning to the wider population, and a factor which opposes the idea of an internet of things smart home [14].

B. *Security Solutions for IoT Smart Homes*

The potential criminal damage that can be caused with vulnerable internet of things devices in a smart home is a very serious threat. One proposed solution is to limit the data recorded by the IoT device. This would make it so that the device only records selective necessary data rather than everything. Encryption is also one of the best solutions, having the data sent back and forth the machine encrypted will ensure that any hackers won’t be able to access them as easily and may deter them due to the resource and time consumption. Having unique default password for each device is also a solution manufactures can take. This will add an extra step for any hacker as they would first need to figure out the password for every device before they can access it, this is a deterrent as it can lower the value of the attack. Ensuring that the devices only act on commands given from a verified logged in user can also help when attackers try and spread the attack from one device to another [15].

V. Other IoT Environments

There are many more internet of things environments instead of the usual smart homes and smart cities. Another environment is the healthcare sector and more specifically biotics. As technology advances so do the healthcare treatments and methods, Internet of things have been predicted to be seen in prosthetic limbs and other biotech's. These synthetic organs can be implemented with chips that use the internet of things environments to allow doctors to monitor their patients more closely. It can aid in keeping doctors updated in any changes and they can be made aware should anything go wrong.

Sensors can let the patient know the status of their biotech, if there functioning correctly or if they need to be seen by a health professional. As with the previous internet of things examples, these new technologies come with their security drawback. NIST, a cyber security company have given the example of a biotic eye in a patient who is blind. If the patient looks at a barcode on a malicious web page, the biotic eye could be given false instructions to allow access to cyber criminals [16]. They could then turn off the eye and use it as a hostage for ransomware related crimes. Although this can be seen as an extreme example, it is still nonetheless a possibility. Hospital equipment will become part of the internet of things environment to improve the health care service provided.

The information given by sensors will aid in monitoring patients on their health issues and provide medical professionals the knowledge the need to prove the healthcare required. However, the internet of things equipment is at risk of being perpetrated by cyber criminals. In the UK the national health service or NHS was struck by a ransomware attack. Computers within hospitals and other medical centers were struck with the ransomware that locked and encrypted valuable information. Patients private details were held hostage as a ransom was demanded in exchange for the information. This type of attack could also affect a hospital within the internet of things environment. The connected devices could be compromised and shutdown, the cyber criminals can then ask for demands just like ransomware in exchange for the equipment to be put back online.

A. IoT Solutions

IT security specialist will have to work closely with the healthcare sector in order to provide adequate security solutions in order to protect patients and health care environments from cybercrime. The security within the healthcare sector must be among the best cyber security solutions. This is because of the type of information's hospitals hold and an ever-reliant Internet of things hospital could be brought to its knees as a result of cybercrime. Encryptions between data as well as ensuring devices only take commands and communicate with authorized users can help in reducing the risk of being a victim of ransomware on a botnet. A network firewall can also be put in place, within the network would include all the internet of things devices and any dating flowing in and out the network will be heavily monitored [17]. This would reduce the chances of attack as anything malicious can be stopped before it enters the internet of things environment. Adding honeypot like internet of things devices could also be proposed as a potential solution. The honeypot device would not need a physical form however it would need to be simulated and added to the IoT environment. Any attempted access or communication to the device would be malicious and can give the cyber security team an indication of a cyber-attack taking place [18]. These honeypot devices can also capture the attack and potentially indicate the origin of the attack and how they managed to breach they networks firewall.

VI. Conclusion

In conclusion the internet of things age is upon us and will become a part of our lives very soon. We will become reliant on the day-to-day interactions with internet of things devices as they will help us improve our lives. We will be living in a new era where technology will be present in all things and we will be reaching new levels of efficiency and productivity. However, our society will become ever more vulnerable due to our dependency on the technology around us. Criminals will look to exploit this dependency to use for their own gain or amusement. Newer modern cybercrime related laws will need to be put in place in order to punish cyber criminals as well as deter others from committing the crimes.

Although there is no current universal architecture used in order to secure internet of things devices, there are in development and IT security professionals around the world are working to research security solutions for this problem. With time the security issues will decrease and increase much like how we see with current internet devices such as personal computers and smart phones. No matter how secure we make our devices hackers will always mange to find a way to crack the security. If corporations and organizations are taking cyber security with the internet of things seriously the damage caused by cybercrime can be minimalized compared to an unsecure cyber society.

References

[1] The National Institute of Standards and Technology (2018). *What is the Internet of Things (IoT) and how can we secure it?* [video] Available at: https://www.nist.gov/video/what-internet-things-iot-and-how-can-we-secure-it [Accessed 1 Dec. 2019].

[2] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[3] U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, "An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[4] Jing, Q., V. Vasilakos, A., Wan, J., Lu, J. and Qiu, D. (2019). *Security of the Internet of Things: perspectives and challenges*. 1st ed. Wireless Netw.

[5] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, "Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat." International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.

[6] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[7] Kouicem, Djamel Eddine & Bouabdallah, Abdelmadjid & Lakhlef, Hicham. (2018). Internet of Things Security: a top-down survey. Computer Networks. 141. 10.1016/j.comnet.2018.03.012.

[8] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[9] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[10] National Audit Office. (2017). *Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO) Report*. [online] Available at: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/ [Accessed 7 Dec. 2019].

[11] I. Ghafir, J. Svoboda, V. Prenosil, "A Survey on Botnet Command and Control Traffic Detection," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 75-80, 2015.

[12] I. Ghafir and V. Prenosil, "Advanced Persistent Threat and Spear Phishing Emails." International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

[13] I. Ghafir, J. Svoboda and V. Prenosil, "Tor-based malware and Tor connection detection," International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-6, 2014.

[14] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[15] I. Ghafir, M. Husak and V. Prenosil, "A Survey on Intrusion Detection and Prevention Systems," IEEE/UREL conference, Zvule, Czech Republic, pp. 10-14, 2014.

[16] J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.

[17] I. Ghafir and V. Prenosil, "DNS query failure and algorithmically generated domain-flux detection," International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-5, 2014.

[18] Wolf, M. and Serpanos, D. (2017). Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. 1st ed. IEEE.