Security Concerns of Internet of Things devices

Niema Attarian
Galway-Mayo Institute of Technology
Computing in Software Development
niema.attarian@gmail.com

***Abstract*—The Internet of Things (IoT) is one of the most vastly expansive and profitable markets in modern times. This technology has improved the quality of life greatly, making day-to-day duties enjoyable and simplistic. It has benefited the population in many ways such as improved healthcare, fitness and leisure. However, with the large dynamic of the Internet of Things comes the issue of privacy and security vulnerabilities.**

The aim of this study was to investigate the the security concerns of the Internet of Things; how it is structured, what type of attacks take place and to what effect they have both personally and financially, and the privacy issues raised in the data protection society we live in today. Also discussed is what measures will be put in place to help protect the consumer to their fullest.

***Index Terms*—Internet of Things; Cyber-Security; Privacy; Attacks**

I. Introduction

The Internet of Things (IoT) has gone from a coined term by Kevin Ashton to one of the most commonly used technologies, in just twenty years. IoT comes in a variety of applications including smart home, medical and healthcare equipment, vehicles, autonomation, smart grids and smart cities [1]. This expansive quality is the main reason why it is set to be one of the most profitable markets available. This is achieved by Radio-frequency identification (RFID), which can automatically identifies and tracks an object; a person, vehicle or animal. In doing so, it can further generate information about specific behaviours of an object, dissect it and act accordingly. This service reeks great benefits to the quality of human life in many forms, however, it sparks the debate on whether the increase in the quality of human life is worth the risk of an individuals security and privacy [1].

This paper is structured as follows. Chapter II will delve into how IoT is structured to create an understanding of how it is then compromised. Chapter III discusses issues regarding IoT; providing examples of attacks that occur, how this effects those on a commercial scale and a personal scale. Chapter IV will discuss how privacy is effected when security is compromised and what has been done to amend it. Finally, Chapter V concludes the paper.

II. How IoT is Structured

To discuss concerns regarding the security of IoT, one must analyse the architecture of IoT. This way, it is more efficient to identify flaws in particular layers where attacks are most common. The architecture of IoT is known to be split up into three layers; Perception layer, Network layer and Application layer [2]. Cloud computing in modern day technology has brought upon a new layer which is considered a support layer. This is said to be located between the perception layer and the network layer. However, only the concrete three layers will be discussed.

A. Perception Layer

The Perception layer is the lowest layer in the architecture of IoT. Also known as the recognition layer, it's main purpose is to collect real-world data and information from real-world objects. Some of this data and information may include, heat, temperature and humidity. This is achieved with the help of sensors and heterogeneous devices such as RFID and Bluetooth [3].

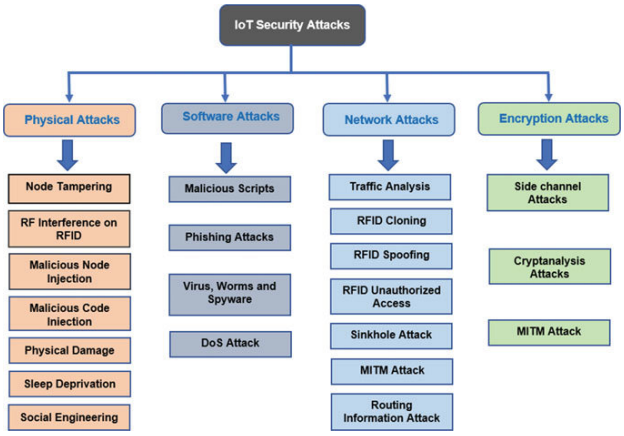
B. Network Layer

The Network Layer one of the most important layers in the IoT architecture. It is known as the brains of the architecture as its purpose is to safely and securely transfer data and information from the Perception layer to the Application layer. It acts like a secure inter-connection between the top and bottom layer [3].

C. Application Layer

The Application Layer is the top layer. This is the layer which is responsible for providing the services for the user. The main purpose of this layer is to bridge the gap between the user and the application which displays relevant information to the user [3].

III. Security Attacks Regarding IoT



Various Security Attacks in the IoT System [4]

A. Physical attack

Physical attacks consist of attacks that are generally hardware orientated. These include Node tampering, RF Interface, Node Jamming, Malicious Node Adware, Physical Damage, Social Engineering, Sleep Deprivation attack and Malicious code attacks (Injection).

1) Node Tampering: This includes an attacker who physically alters or removes a node from a network. In doing this, sensitive information can be obtained such as an encryption key [5] [6].

2) RF Interference on RFID: This involves a denial of service by an external radio frequency. Radio frequency is the main communication method for RFID's [5].

3) Malicious Node Injection: In this attack, a modified node is injected in between two existing nodes. This nodes identity and location has been spoofed and this leads to data being passed through [5] [7].

4) Malicious Code (Injection): Malicious Code Injection attacks are similar to Malicious node injection in the sense that code is injected into a system which allows the attacker to gain access and obtain or change data.

5) Physical Damage: This attack involves an attacker physically harming a system which in turn results in a DoS [5].

6) Sleep Deprivation: The goal in this attack is to simply over-power the system that in turn, shuts down the nodes [5].

7) Social Engineering: This attack involves the attacker to influence and manipulate the user to gain access of their system and obtain sensitive information [5].

B. Network Attack

Network attacks focus more on the network of the IoT system. This includes attacks such as Traffic Analysis Attacks, RFID Spoofing, RFID Cloning, RFID Unauthorised Access, Sinkhole Attack, Man in the Middle Attacks (MITM), Denial of Service (DoS), Routing Information attacks and Sybil Attacks.

1) Traffic Analysis: This network attack involves an interference in traffic of a system. Eavesdropping methods are used to surmise the traffic pattern. Once this is achieved, it can locate strategic nodes. The dangers of this is that DoS attacks can be performed with this information [5] [8]

2) RFID Cloning: The act of RFID Cloning is the copying or duplicating an RFID tag. Practise has proven that this method is not costly and is very do-able considering the number of writable and re-usable tags available. An example of this is a passport. They are susceptible to cloning and can bypass the network in many different ways [9].

3) RFID Spoofing: RFID Spoofing is similar to cloning, however unlike cloning, it is not a a direct copy of the RFID tag. In this case, the attacker would adapt a valid and working RFID tag to gain its original privileges. This could allow attackers to gain access to anything that the original tag had access to [9].

4) Sinkhole Attack: A Sinkhole Attack involves an attacker attempting to draw as much traffic their way as possible. This is achieved by using unfaithful routing to attract nodes around them. In-turn, data is changed, rearranged or withheld as some of it may not be forwarded on. This attack is known commonly in many-to-one types of communication [10].

5) MITM Attack: A Man in the middle attack is a real-time attack where the attacker intercepts any communication in-between two active nodes. Eavesdropping methods are used to obtain sensitive information [5].

6) Routing Information Attack: Routing Information Attacks involves an attacker attracting all nodes around them to go towards them. An example of this is a Black Hole attack. In this instance, the attacker sends out fake routing information (via malicious nodes) claiming it has the optimum resources causing good nodes to route data through it. In turn, this malicious node(s) forwards data from the good nodes [11].

C. Software Attack

Software Attacks include software such as worms or viruses which compromise a system. These attacks include Malicious scripts, Worms, Viruses and Spyware, Phishing Attacks and DoS Attacks.

1) Malicious Scripts: Malicious Scripts are known to be fragments of code scattered and hidden in a a trusted website. The purpose of these scripts are to cause harm to a user who is unaware of the script as they believe they are entering a trusted website. Also, malicious scripts in a website can also target business. They can cause breaches in companies and many financial and valuable data can be collected causing great financial harm to both a business and a consumer.

2) Phishing attacks: Phishing attacks are one of the quickest growing threats to global security. Although phishing attacks can be listed under physical attacks via social engineering, a user is also susceptible to these attacks through forged links asking for their information. These links trick the user into believing they are entering information into a link or page from a reputable business [12].

3) Virus, Worms and Spyware: Virus, Worm and Spyware attacks can be some of the most detrimental attacks to both a user and a business.

- Viruses come in thousands of ways and have been growing since the late 1980's, early 1990's, ever since personal computers began entering homes and business [13]. Viruses can infect a system through many means (email, network, files etc.). It's fundamental purpose is to attach itself to as many programs in a system as possible and to remain undetected. The main goal of a virus is to steal valuable information and possibly gain admin control.
- Worms on the other-hand follow more destructive means to achieve its goals. Worms replicate themselves in a system using all the systems resources causing system failure [13].
- Spyware has been a more growing problem in the security of IoT. This involves means of controlling a users smart home remotely. An attacker could turn on a camera or

microphone in a device and begin listening and watching the victim without their knowledge. This can lead to cases of blackmail, privacy invasion and theft of important financial information.

4) DoS Attacks: This attack involves preventing the user from accessing their service. This is often achieved by the attacker overloading a server by sending a stream of request messages that contain any number of invalid return address.

D. Encryption Attack

1) Side-Channel Attacks: Side-Channel Attacks refer to the attacks from gathered information of an implementation of a system. Common examples of this is software bugs. These implementations tend to have 'leakage' of information which lead to attacks. These attacks compare observations of side channel leakage, this can be anything from increased noise to execution time, to the judgement of the leakage [14].

2) Cryptanalysis Attacks: Cryptanalysis Attacks refer to a number of cryptographic attacks of a system. Some of these include cipher-text only attacks, known plain-text attacks, chosen plain-text attacks and chosen cipher-text attacks. These types of attacks can be very technical and some take time, but can be very effective to achieve their goal. One example is chosen cipher-text attack. It is considered to be the strongest attack out of the listed cryptanalysis attacks [15]. This attack is carried out by sending the target a cipher-text of the attackers choice. This then returns a corresponding plain-text. It is here where the attacker will attempt to decipher the text in order to achieve their goal.

3) MITM Attack: Man-in-the-middle attacks are similar to the ones mentioned above in the Network Attacks. It involves an attacker intercepting communication between two parties and relaying the information back to themself. Eavesdropping methods are used to obtain and decipher the information presented.

IV. Privacy

In today's society with the advancement of technology, privacy plays an enormous factor in how humans go about their lives. Privacy has become more pronounced in recent years, especially with the strict enforcement of the General Data Protect Rule (GDPR) by the European Union (EU). Privacy and security run hand in hand in the sense that if the security of a persons device is compromised, it is most likely that their privacy is too.

A common system that has been mentioned in this paper is RFID. There have been many privacy issues surrounding RFID systems. A major issue being that the leaking of personal information. This pertains to the case of reusing tags. Anyone can read the information stored on the tag relating to the previous possessor of said tags without their knowledge or consent. This is a huge issue, especially pertaining to the GDPR laws set by the EU [16].

There have been suggested fixes to this data protection issue, one of which entails tags with re-writable memory. Not only does this help with cost and scalability, this scheme can help improve the security and privacy of the public. Also, another scheme put into place is that of the "anonymous-ID-scheme". This scheme incorporates an encrypted ID in the tag. To put into motion, the response to a readers request involves encrypted ID from the server to the reader. This helps rectifies the problem of leakage as any leakage of consumer data is encrypted [16].

V. Conclusion

In conclusion, it is evident that the Internet of Things is a thriving market and has not yet reached its peak. It can be expanded into an endless number of fields and will become second nature to human life in years to come. It is, however, clear that before the IoT can reach its full potential, it must first address and fix many of the outlining issues with security and privacy. With privacy being a large focus point in our lives today, the technology behind IoT must tighten and improve their security as to help progress the privacy of their consumers. In all, although there remains the concerns with the security of the Internet of Things, it is clear that it is here to stay and will continue benefiting the world.

References

[1] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[2] X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in *2012 2nd international conference on consumer electronics, communications and networks (CECNet)*. IEEE, 2012, pp. 1282–1285.

[3] M. Bilal, "A review of internet of things architecture, technologies and analysis smartphone-based attacks against 3d printers," *arXiv preprint arXiv:1708.04560*, 2017.

[4] H. F. Atlam and G. B. Wills, "Iot security, privacy, safety and ethics," in *Digital Twin Technologies and Smart Cities*. Springer, 2020, pp. 123–149.

[5] J. Deogirikar and A. Vidhate, "Security attacks in iot: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017, pp. 32–37.

[6] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Mobility and cooperation to thwart node capture attacks in manets," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 945943, 2009.

[7] A. Atassi, N. Sayegh, I. Elhajj, A. Chehab, and A. Kayssi, "Malicious node detection in wireless sensor networks," in *2013 27th International Conference on Advanced Information Networking and Applications Workshops*. IEEE, 2013, pp. 456–461.

[8] X. Luo, X. Ji, and M.-S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in *2010 International Conference on Information Science and Applications*. IEEE, 2010, pp. 1–6.

[9] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of rfid attacks," *Gen*, vol. 15693, p. 14443, 2010.

[10] E. C. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," in *2006 IEEE International Conference on Communications*, vol. 8. IEEE, 2006, pp. 3383–3389.

[11] P. Goyal, V. Parmar, and R. Rishi, "Manet: vulnerabilities, challenges, attacks, application," *IJCEM International Journal of Computational Engineering & Management*, vol. 11, no. 2011, pp. 32–37, 2011.

[12] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3629–3654, 2017.

[13] U. Mishra, "An introduction to computer viruses," *Available at SSRN 1916631*, 2010.

[14] K. Tiri, "Side-channel attack pitfalls," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 15–20.

[15] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *Proceedings of the twenty-second annual ACM symposium on Theory of computing*. Citeseer, 1990, pp. 427–437.

[16] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Rfid privacy issues and technical challenges," *Communications of the ACM*, vol. 48, no. 9, pp. 66–71, 2005.