Cybersecurity of IoT Systems - RFID

Dhanushga Lionel
Ontario Tech University
Ontario, Canada
dhanushga.lionel@ontariotechu.net

Abstract

The Internet of Things is a network that allows household/everyday objects to interact and communicate with each other. They can exchange data, allowing these objects to collaborate, and offer better services for the user. This paper examines security issues that arise in IoT systems and subsystems.
Index terms - RFID, Cybersecurity, IoT

Introduction

Imagine a world without the Internet. No Instagram. No Snapchat. No more Facebook, even though no one under 25 uses it. No Youtube. No "...". Without the Internet, the world would be in a dystopian future in the Hunger Games.

The Internet is now less a tool and more a necessity of life. We can now communicate with people who aren't even on Earth. We can share memories with our families who live half a world away with just a click of a button.

The Internet can break or make businesses, both large and small. Some of the biggest companies in the world rely on the Internet to succeed. Companies like Google, Microsoft, … would not exist without the Internet.

Political campaigns are won or lost on the Internet. Almost 75% of Internet users went online to get political news and talk about their candidates during the 2008 campaign, and in 2012, more than a fifth of registered voters announced their candidate on Twitter or Facebook [1].

The Internet of Things, or IoT for short, is the next phase of evolution for the Internet, and ourselves. Now millions of interconnected devices can communicate with each other, all for the goal of bettering the users life.

Cyber Security

While the Internet of Technology continues to expand, so do the security concerns that come with IoT. The fundamental nature of the Internet and IoT is one of interconnectedness. While this is important, this also means that any internet connected resources can be attacked through a number of different methods. This makes cyber security issues paramount when talking about IoT.

An IoT architecture can be represented by 3 layers: application, transport and sensing. A more detailed architecture can be defined with 5 layers, Perception, Network, Middleware, Application, and Business [9]. In this section, 4 main key levels will be discussed, as shown in Figure 1 below. Each layer will be briefly described. Then more detail will be given to particular problems that face each layer, and then what the security is at different layers.

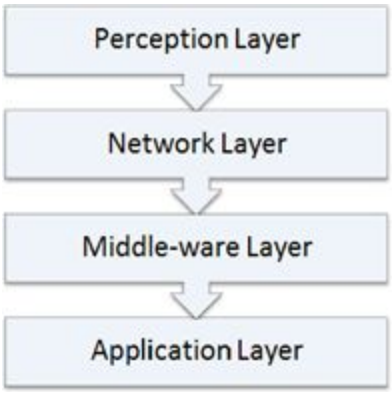

Figure 1: 4 Key Layer Architecture of IoT

1. Perception Layer

Consists of different kinds of data sensors like RFID, barcode and other sensor network. The purpose of the perception layer is to identify

objects, and do something with the data obtained from the sensor.

2. Network Layer

Also known as the 'transmission layer'. It is responsible for securely transferring data from sensory devices to the information processing system.

3. Middleware Layer

This is the service-oriented layer. It makes automated actions based on the processed data results. It also links the IoT system with a database [6].

4. Application Layer

Layer that allows different IoT devices to communicate with each other. For example, smartphones can communicate with a smart door lock to tell it the user is home, and to unlock the door [8].

5. Problems at Perception Layer

There are a number of challenges that plague the perception layer. These include unauthorized access to tags, cloning and spoofing, eavesdropping and replay, DoS and Man-in-the-Middle Attack [2] [5].

5.1 Unauthorized access to tags: RFID systems can be accessed easily, with the data being susceptible to modification, or deletion. This is because a large number of RFID systems do not have proper authentication systems. Due to this, tags can be accessed easily, without authorization [3].

5.2 Cloning and Spoofing: Tags can be easily cloned by duplicating data from the original tag. Due to this, the sensor reader cannot tell the difference between the original and cloned tag [4]. Spoofing is using a cloned tag to gain access to a secured system [5].

5.3 Eavesdropping and Replay: Unauthorized RFID reader can listen to the conversation between the tag and reader, and obtain important and/or confidential data. Replay follows eavesdropping, and is when one part of the communication in an RFID system is recorded, and then replayed later to the receiver to gain access or steam information [5]. Since RFID is wireless, it is very easy for hackers to get any confidential and/or important data from the tag-to-reader, or vice-versa.

5.4 Denial of Service: DoS attacks can happen when a system is jammed through noise interference, radio signal blocking, or removing/disabling RFID tags [5].

5.5 Man-in-the-Middle Attack: Man-in-the-Middle Attack happens during the transmission of a signal. Attacker intercepts for communication between reader and tag, and manipulated information [5].

6.Problems at Network Layer

Issues that face the network layer include sybil attacks, sinkhole attacks, sleep deprivation attacks, malicious code injection, DoS attacks, and man-in-the-middle attacks [2]. DoS and Man-in-the-middle attacks have already been explained in section 1.1.4 and 1.1.5 respectively.

6.1 Sybil Attack: Sybil attack is a type of attack where a node in the network operates multiple identities to gain authority in the system. The main purpose is to gain a majority influence in the network, and carry out dangerous actions [10].

6.2 Sinkhole Attack: This attack makes compromised nodes look attractive to other nodes. Because of this, the data is rerouted to the compromised node. This can also lead to a DoS attack [11].

6.3 Sleep Deprivation Attack: The deployment of sensors, especially in hostile environments makes it vulnerable to battery drainage attacks, because it is hard, if not impossible, to replace the battery of the power of sensor nodes[12]. This type of attack is to keep the nodes awake, resulting in more battery consumption, and as a result the lifetime of the battery is greatly diminished, which causes the nodes to shut down [13].

6.4 Malicious Code injection: Compromised nodes are injected with malicious code, that could result in complete shutdown of network, or even giving full control of network to attacker [14].

7. Problems at Middleware Layer

Types of attacks that haunt the middleware layer include unauthorized access, DoS attacks and malicious insider attacks. DoS attacks have been already explained in section 5.4.

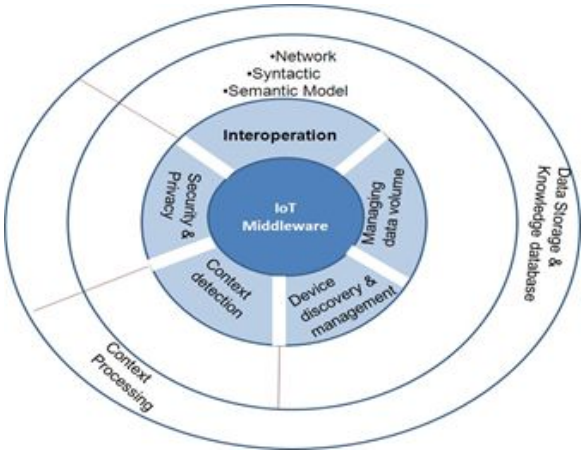

Figure 2: Components of middle-ware layer

7.1 Unauthorized Access: Attackers can get access to the middleware layer. Because the middleware layer has interfaces with application and data, attackers can cause damage to system by forbidding access to much needed services, or deleting existing data.

7.2 Malicious Insider: Malicious insider attack can occur when someone on the inside tampers with the data.

8. Problems at Application Layer

Application layer challenges include malicious code injection, DoS attacks, spear-phishing attacks, and sniffing attacks. Malicious code injection and DoS attacks have been explained in section 6.4 and 5.4 respectively.

8.1 Spear-Phishing Attacks: Is the targeted attempt to steal sensitive information, such as account credentials or financial information. This can be achieved by acquiring personal details about victims such as friends, hometown, employer, location, and online shopping [15]. Attack can then be an email, or message, disguised as coming from a trust-worthy source. When that email is opened, sensitive information from the host device can then be retrieved.

8.2 Sniffing Attacks: Is an attack that can intercept data by capturing network traffic using a sniffer.

9. Security measures at Perception Layer

There are protective measures for the Perception Layer. These include the following:

9.1 Authentication: Devices need to be authenticated before entering the network. Some possible attacks that a simple authentication algorithm can be protected from include brute force attack, collision attack etc.

9.2 Data Privacy: Privacy of data needs to be guaranteed. It can be accomplished by encryption algorithms, which prevents unauthorized access to the sensor data while being collected or forwarded to the network layer.

9.3 Data Integrity: To make sure of no data tampering, each device should have error detection systems, such as checksum, parity bit etc [16].

10. Security measures at Network Layer

These are the protective measures for the Network Layer. These include the following:

10.1 Authentication: With proper authentication methods, and point-to-point encryption, illegal access to sensors is prohibited.

10.2 Data Confidentiality: Data confidentiality can be ensured by preventing illegitimate access of nodes network layer. Point-to-point encryption can also be utilized. This makes data confidential.

10.3 Data Integrity: Data integrity can be ensured by using cryptographic hash functions, which ensures that data is not tampered with.

10.4 Data Privacy: Safety control mechanism can monitor the network layer for any intrusion.

11. Security measures at Middleware Layer

These are the protective measures for the Middleware Layer. These include the following:

11.1 Authentication: Similar to authentication process at other layers.

11.2 Intrusion Detection: Intrusion detection techniques provide solutions for various security threats by generating alarm for each individual suspicious activity in the system.

11.3 Data Fragmentation: data is fragmented and stored on various servers. This allows for minimum data exposure in case of a leak.

12. Security measures at Application Layer

These are the protective measures for the Application Layer. These include the following:

12.1 User validation: User needs to be valid to use the system. This prevents security breach, that can cause data stealing or unauthorized access.

12.2 Firewalls: Authentication password and encryption method can break. Therefore a firewall should be used to monitor traffic.

12.3 Risk Assessment: Risk assessment detects threats to the system.

Conclusion

In conclusion, there are a lot of issues Presented with the use of RFID and a plethora of solutions. Each issue offers a different and complex way of looking into things. The security Exploits are developed and used by intelligent individuals that have a high understanding of the system. This allows for the development of new methods and ideologies behind it.

With each security issue we are able to find a solution depending on the needs. This would suggest that we are keeping up with each security concern by being able to

engineer solutions. Even with evolving security ideals and new technologies claiming to solve old problem it is still important to keep up with the current security threats.

Future technologies

[18] first proposed a concept of ownership transfer of an RFID with a suggested protocol. This required both parties to be in agreement with a trusted middleman. Furthermore, there is no guarantee of protection against denial of service attacks.

[17] Has offered improvements on the subject with a transfer protocol based on bitwise operation (PSU-TOTP) is proposed. With the further use of the FLAG recording system, the analysis shows that the proposed protocol meets the security requirements for the tag ownership transfer.

[19] Offers a wide variety of new solutions and analyses of current problems in the RFID platform. It is widely believed that offering new improved protocols would allow for a much better security outcome on most bases.

For most detailed security implementation, a new type of protocol is suggested with good reason. It is often proven over time that some solutions were great at a given time and they do not withstand the test of time. Thus, some companies have implemented new protocols and change significant sections in order to work with the ever-growing use of RFID technology.

As for thoughts on the future subject, it would be important to hear each security warning and judge based on a cost and danger level weather changes should be made or not.

References

[1] Dewey, C. (2014, March 12). 36 ways the Web has changed us. The Washington Post. Retrieved from https://www.washingtonpost.com/news/arts-and-entertainment/wp/2014/03/12/36-ways-the-web-has-changed-us/

[2] U.farooq, M., Waseem, M., Khairi, A., & Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111(7), 1–6. doi: 10.5120/19547-1280

[3] Al-Sudani, A. R., Zhou, W., Liu, B., Almansoori, A., & Yang, M. (2018). Detecting Unauthorized RFID Tag Carrier for Secure Access Control to a Smart Building . International Journal of Applied Engineering Research, 13(1), 749–760. Retrieved from https://www.ripublication.com/ijaer18/ijaerv13n1_103.pdf

[4] Kamaludin, H., Mahdin, H., & Abawajy, J. H. (2018). Clone tag detection in distributed RFID systems. Plos One, 13(3). doi: 10.1371/journal.pone.0193951

[5] Smiley, S. (2018, March 27). 7 Types of Security Attacks on RFID Systems. Retrieved November 12, 2019, from https://blog.atlasrfidstore.com/7-types-security-attacks-rfid-systems.

[6] Bandyopadhyay, Soma & Sengupta, Munmun & Maiti, Souvik & Dutta, Subhajit. (2011). Role Of Middleware For Internet Of Things: A Study. International Journal of Computer Science & Engineering Survey. 2. 10.5121/ijcses.2011.2307.

[7] M. B. Yassein, M. Q. Shatnawi and D. Al-zoubi, "Application layer protocols for the Internet of Things: A survey," *2016 International Conference on Engineering & MIS (ICEMIS)*, Agadir, 2016, pp. 1-4. doi: 10.1109/ICEMIS.2016.7745303
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7745303&isnumber=7745290

[8] Application Layer Protocol Analysis & the Internet of Things. (n.d.). Retrieved November 12, 2019, from https://study.com/academy/lesson/application-layer-protocol-analysis-the-internet-of-things.html

[9] Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018, September 13). Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends. Retrieved November 18, 2019, from https://www.hindawi.com/journals/wcmc/2018/5349894/.

[10] HoodaCheck, P., & Hooda, P. (2019, January 10). Sybil Attack. Retrieved November 18, 2019, from https://www.geeksforgeeks.org/sybil-attack/.

[11] Baskar, R., Raja, P. C. K., Joseph, C., & Reji, M. (2017, March). Sinkhole Attack in Wireless Sensor Networks-Performance Analysis and Detection Methods. Retrieved November 18, 2019, from http://www.indjst.org/index.php/indjst/article/view/90904.

[12] Bhattasali, T., Chaki, R., & Sanyal, S. (2012, March 1). Sleep Deprivation Attack Detection in Wireless Sensor Network. Retrieved November 18, 2019, from https://arxiv.org/abs/1203.0231.

[13] Pirretti, M., Zhu, S., Vijaykrishnan, N., Mcdaniel, P., Kandemir, M., & Brooks, R. (2006). The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. International Journal of Distributed Sensor Networks, 2(3), 267–287. doi: 10.1080/15501320600642718

[14] Muscat, I. (2019, July 1). What is Code Injection. Retrieved November 18, 2019, from https://www.acunetix.com/blog/articles/code-injection/.

[15] What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing. (2019, October 24). Retrieved November 18, 2019, from https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing.

[16] Aziz, Tariq, and Ehsan-Ul Haq. "Security Challenges Facing IoT Layers and Its Protective Measures." International Journal of Computer Applications, vol. 179, no. 27, 2018, pp. 31–35., doi:10.5120/ijca2018916607.

[17]J.-Q. Wang, "Provable Secure for the Ultra-lightweight RFID Tag Ownership Transfer Protocol in the Context of IoT Commerce," International Journal of Network Security, pp. 12–23, Jan. 2020.

[18] D. Molnar, A. Soppera and D. Wagner, "A scalable, delegatable pseudonym protocol enabling ownership transfer of rfid tags[A]," in 12th International Workshop on Selec

[19] A. Tewari and B. B. Gupta, "An Analysis of Provable Security Frameworks for RFID Security," Handbook of Computer Networks and Cyber Security, pp. 635–651, 2020.