State of Internet of Things (IoT) Security Attacks, Vulnerabilities and Solutions

Daisy T. Endencio-Robles[1], Rosslin John Robles[1*]

[1]University of San Agustin, Philippines

dendencio@usa.edu.ph, rjrobles@usa.edu.ph

Abstract

Internet of things (IoT) security is the technology area concerned with safeguarding networks and connected devices in the internet of things (IoT). IoT involves adding internet connectivity to a system of mechanical and digital machines, interrelated computing devices, animals, people and/or objects. Each "thing" is provided a unique identifier and the ability to automatically transfer data over a network. Allowing devices to connect to the internet opens them up to a number of serious vulnerabilities if they are not properly protected. In this paper, we discuss the different attacks and vulnerabilities which is classified by layer in the architechture. We also proposed solutions to mitigate and counter these attacks and vulnerabilities.

Keywords: Internet of Things, Network Security, Cybersecurity, Smart Home

Introduction

The internet of things, or IoT, is a system of interrelated mechanical and digital machines, interrelated computing devices, animals, people and/or objects that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-computer or human-to-human interaction. The internet of things has been highlighted as a new growth engine of the ICT industry. [1] It was 20 years ago that the term „things of Internet" was first used, when Kevin Ashton of P&G mentioned that the IoT mounted with RFID and sensors would be built in 1999. It was more than 150 years ago when the communication between men was done via telephone. To the exclusion of communication other than the simple communication and internet, network devices have made a direction long ago for the Internet to go smoothly and to allow men to communicate with each other through various routing protocols. The internet of things means the Internet environment of generating, sharing, mutually collecting, and using information by allowing all the things, such as animal, people, around things, data, etc., to be connected to wireless and wired networks. [2]

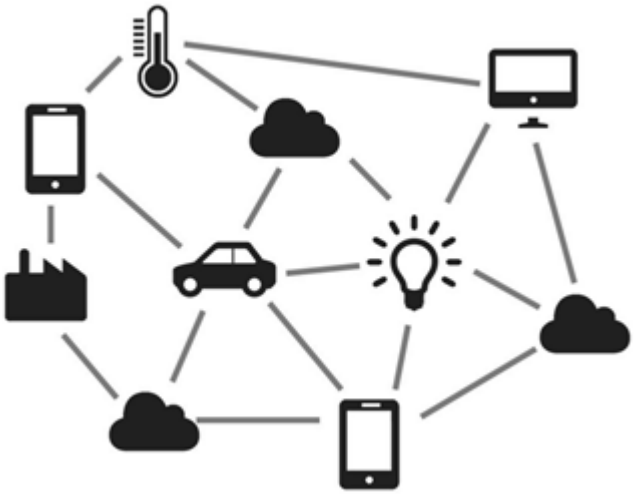

Figure 1. Internet of things (IoT) Overview

One application of internet of things is in Smart homes. Smart homes connect all the devices and appliances in your home so they can communicate with each other and with you. [3] Anything in your home that uses

electricity can be put on the home network and at your command. Whether you give that command by remote control or computer, voice, the home reacts. Most applications relate to lighting, home security, home theater and entertainment and thermostat regulation. [3]

In the next sections, The Promise of Internet of Things (IoT), Internet of Things (IoT) Architechture, Internet of Things (IoT) Security Attacks/Vulnerabilities and the Proposed Solutions and Discussions.

The Promise of Internet of Things (IoT)

Internet of Things (IoT) has garnered alot of media attention for good reason. The advantages of connecting devices using real-time analysis to improve procedures and processes seems nearly limitless. By at least one estimation, only about 10% of a company's data is effectively used. [4] As the Internet of Things(IoT) and other data-based technologies improve, that number should rise dramatically. Businesses leveraging the IoT should garner great advantage. [4]

An example given by Becker in [4] was the Wastewater treatment which is one modern example of IoT-inspired improvements. The advances in Wastewater enabled by IoT technology are fascinating and also great for the environment. [4]

Today the process of calibrating wastewater treatment levels is on firmer analytical ground. This can be attributed, in part, to the Internet of Things (IoT). Businesses can deploy sensors that report real-time data. This data concerns variables such as pH value, temperature, and flow. This information is then relayed to a platform (such as SAP HANA) where regression techniques are applied. The end result equals accurate predictions of midterm chemical oxygen demand (COD) values. [4]

By utilyzing accurate predictive data into their processes, companies can ensure they stay within regulatory dictates. This, in turn, lowers exposure to fines and penalties. By using IoT technology, companies protect against the possibility of a major pollution event. Should projected pollution levels be too high, alerts are immediately issued. Mitigating steps can then be taken. [4]

Internet of Things (IoT) Architecture

Internet of Things (IoT) is typically structured into 3 Layers, [5]; the Application Layer, the Network Layer, and the Physical Layer, as shown in the following Figure.

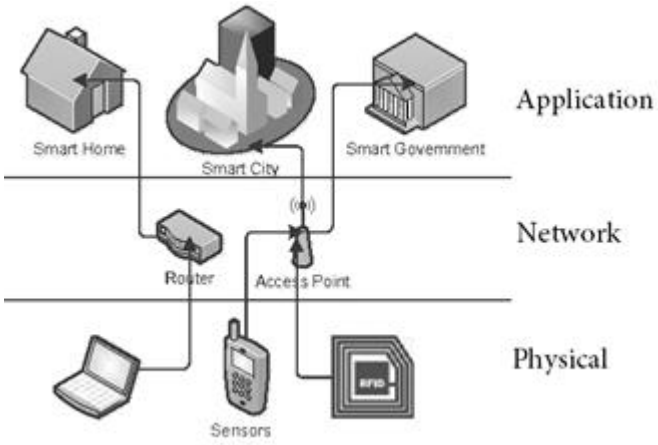

Figure 2. Internet of things (IoT) Architecture

Application Layer

The Application Layer is service-oriented [6], which ensures the same type of service among the connected devices. It can store data into a database providing storage capabilities to the collected data. Also, just like its name suggests, it facilitates ways for these devices to communicate outside of the device-oriented system with the use of different kind of applications depending on the needs of the users [7]; e.g., Smart Transportation, Smart Home, eHealth, Smart Objects etc. [8]

Network Layer

Just like any other Network Layer model this one includes network interfaces, network management, communication channels, information maintenance, and intelligent processing, and is mainly responsible for the communication and connectivity of all the devices in IoT system through the help of multiple communication protocols [8][9][10][11]. It is within this layer that the gathered information from the Physical Layer are transmitted to any specific information processing system within the network using Wireless Sensors [12] or to an outside network through existing communication infrastructures like the Internet or a Mobile Network. Each device in an Internet of Things (IoT) system usually sends its information with the use of wireless sensors. These are small sensors, with limited processing and computing power for lower power consumption. The data received from the sensors are processed, transmitted wirelessly, and presented to the end user. So the network layer aggregates and combines communications from different devices and provides the ability to route communications to any specific device usually via a gateway [8][13].

Physical Layer

The bottom layer of the architecture is basically the layer responsible for the interconnected devices and its main purpose is to provide service discovery and perform device identification. These devices can be of various types [3], but in order to be considered as IoT devices they need to utilize communication technology that allow them to connect to one another either directly or indirectly using the Internet like a Raspberry Pi with a Wi-Fi connection, a Bluetooth connection, the Arduino with Ethernet connection, and a low power radio connection. [8]

Each device needs to have a unique tag that allows it to connect successfully to the network. Ideally, Universally Unique identifiers (UUID) [14] should be used for different objects throughout the Internet that should be burnt onto the device; they are typically part of the System-on-Chip or provided by a secondary chip [15]. Currently a device can be coupled with a data sensor device like an RFID or any other sensor network device [16] with a unique ID for the main purpose of identifying it as a unique object. [8]

Internet of Things (IoT) Security Vulnerabilities

There have been many advances in the research field of Internet of Things [17], however there are still some open challenges that needs to be addressed for the ubiquity of this technology. In this section some of the threats in each architectural layer that needs special attention are presented.

Table 1. Internet of Things (IoT) Security Attacks

Physical Layer	Network Layer	Application Layer
Eavesdropping	Denial-of-Service (DoS) Attack	
RF Jamming	Malicious Code Injection	
Spoofing	Sinkhole Attack	Sniffing Attack
Unauthorized Access to the Tags	Sybil Attack	Spear-Phishing Attack
Tag Cloning	Denial of Sleep Attack	
	Man-in-the-Middle Attack	

Physical Layer Challenges

Physical layer consists of different sensor technologies like RFID which are exposed to the following threats:

Eavesdropping

Because of the wireless characteristics of the RFID it becomes very easy for the attacker to sniff out the confidential information like passwords or any other data flowing from [20] [21] tag-to-reader or reader-to-tag which makes it vulnerable because the attacker can make it to use in despicable ways [22].

RF Jamming

RFID tags can also be compromised by kind of a DoS attack in which communication through RF signals is disrupted with an excess of noise signals [22].

Spoofing

Spoofing is when an attacker is able to listen in on network traffic and identify the MAC address of a computer with network privileges and broadcasts fake information to the RFID systems and makes it to assume its originality falsely which makes it appearing from the original source [23]. This way attacker gets full access to the system making it vulnerable. [21]

Unauthorized Access to the Tags

Due to the lack of proper authentication mechanism in a large number of RFID systems, tags can be accessed by someone without authorization. The attacker cannot just read the data but the data can be modified or even deleted as well [18].

Tag Cloning

Since tags are deployed on different objects which are visible and their data can be read and modified with some hacking techniques therefore they can be easily captured by any cybercriminal who can create a replica of the tag and hence compromising it in a way that the reader cannot distinguish between the original and the compromised tag [19].

Network Layer Challenges

Network layer consists of the Wireless Sensor Network (WSN) which transmits the data from the sensor to its destination with reliability. The related security issues are discussed below:

Sinkhole Attack

Sinkhole attack is a type of attack were compromised node tries to attract network traffic by advertise its fake routing update. One of the impacts of sinkhole attack is that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information. [24].

Sybil Attack

Sybil is a kind of attack in which the attacker manipulates the node to present multiple identities for a single node due to which a considerable part of the system can be compromised resulting in false information about the redundancy [23].

Denial of Sleep Attack

The sensor nodes in the Wireless Sensor Network are powered with batteries with not so good lifetime so the nodes are bound to follow the sleep routines to extend their lifetime. Denial of Sleep is the kind of attack which keeps the nodes awake, resulting in more battery consumption and as a result battery lifetime is minimized which causes the nodes to shut down [25].

Man-in-the-Middle Attack

This is a form of Eavesdropping in which target of the attack is the communication channel dueto which the unauthorized party can monitor or control all the private communications between the two parties hideously. [28]. The attacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack". [21]

Denial of Service (DoS) Attack

The kind of attack in which the network is flooded with a useless lot of traffic by an attacker, resulting in a resource exhaustion of the targeted system due to which the network becomes unavailable to the users [21] [26].

Malicious code injection

This is a serious kind of attack in which an attacker compromises a node to inject malicious code into the system which could even result in a complete shutdown of the network or in the worst case, the attacker can get a full control of the network [27].

Application Layer Challenges

The related security issues of the Application layer are described below:

Denial-of-Service (DoS) Attack

DoS attacks nowadays have become sophisticated, it offers a smoke screen to carry outattacks to breach the defensive system and hence data privacy of the user, while deceiving the victim into believing that the actual attack is happening somewhere else. A Denial-of-Service attack (DoS) occurs when an attacker continually

bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. [21]

Malicious Code Injection

An attacker can leverage the attack on the system from end-user with some hacking techniques that allows the attacker to inject any kind of malicious code into the system to steal some kind of data from the user. [21]

Sniffing Attack

An attacker can force an attack on the system by introducing a sniffer application into the system, which could gain network information resulting in corruption of the system [21].

Spear-Phishing Attack

It is an email spoofing attack in which victim, a high value person, is lured into opening the email through which the adversary gains access to the credentials of that victim and then by a pretense retrieves more sensitive information.

Solution and Discussion

The following table shows the different Attacks or Vulnerabilities in different layers and the presented solutions:

Table 2. The IoT attacks and preventions/solutions

Layer	Attack/Vulnerability	Solutions
Physical Layer	Eavesdropping	Apply encryption on all the devices that perform communication.
	RF Jamming	RF Jammer executes by entering jamming messages in the wireless network. Transmission of jamming messages can be prevented by cryptanalysis and steganography techniques.
	Spoofing	To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack.
	Unauthorized Access to the Tags	Tags can be protected from illegal access by unscrupulous readers through the authentication procedures of the APF systems.
	Tag Cloning	To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack.
Network Layer	Sinkhole Attack	Analyze data consistency and network flow information.

	Sybil Attack		Use of artificial intelligence to recognise fake account patterns.
	Denial of Sleep Attack		Workload should be distributed among the components according to their capacity to avoid complete exhaustion of battery power.
	Man-in-the-Middle Attack		Apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission.
	Denial of Service (DoS) Attack	Malicious code injection	Apply cryptographic techniques to ensure security of network.
Application Layer			Apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage.
	Sniffing Attack		Connect to trusted networks. Encrypt all the traffic that leaves your system.
	Spear-Phishing Attack		Scan all inbound email to spot indicators in the message header, domain information and message content that may indicate a message is suspicious.

There are different vulnerabilities in the Physical Layer such as Eavesdropping, RF Jamming, Spoofing, Unauthorized Access to the Tags, Tag Cloning. These can be prevented by applying encryption on all the devices that perform communication. RF Jammer executes by entering jamming messages in the wireless network. Transmissionof jammingmessages canbe preventedbycryptanalysis andsteganographytechniques. [29] To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack. Tags can be protected from illegal access by unscrupulous readers through the authentication procedures of the APF systems. To avoid from spoofing and cloning attacks, apply identity-based authentication protocols. Physically unclonable function is a countermeasure for cloning attack.The network layers are also susceptible to attacks such as Sinkhole Attack, Sybil Attack Denial of Sleep Attack, Man-in-the-Middle Attack, Denial of Service (DoS) Attack and Malicious code injection which can be prevented by analysing data consistency and network flow information. Use of artificial intelligence to recognise fake account patterns. Workload should be distributed among the components according to their capacity to avoid complete exhaustion of battery power. Apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission. Cryptographic techniques be applied in both network and application layers to ensure security of network and apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage. To secure the application layer, Connect only to trusted networks. Encrypt all the traffic that leaves your system. Scan all inbound email to spot indicators in the message header, domain information and message content that may indicate a message is suspicious.

Conclusions

The Internet of things (IoT) is the network of different devices such as vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data. Since almost anyone can connect to the network, important data can be accessed on devices can be vulnerable to attackers. In this paper, we define the different vulnerabilities and attacks. These vulnerabilities and attacks are classified by layers and a prevention/solution scheme is presented. On different layers, applying cryptographic techniques should be used to ensure security of network.

References

1. Young-Mo Kang, Mi-Ran Han, Kyeong-Seok Han and Jong-Bae Kim, "A Study on the Internet of Things (IoT) Applications", International Journal of Software Engineering and Its Applications, Vol. 9, No. 9 (2015), pp. 117-126, ISSN: 1738-9984, DOI: 10.14257/ijseia.2015.9.9.10
2. Kevin Ashton, "That Internet of things thing", URL: http://www.rfidjournal.com/articles/view?4986 Accessed: September 2018
3. Rosslin John Robles, Tai-hoon Kim, "A Review on Security in Smart Home Development", International Journal of Advanced Science and Technology, Vol. 15, February, 2010, pp13-22
4. Alfred Becker, "The Promise Of The IoT: Go Green With Greater Efficiency", Digitalist Magazine, URL: https://www.digitalistmag.com/iot/2018/01/23/promise-of-iot-go-green-with-greater-efficiency-05790019 Accessed: September 2018
5. Song Y. (2013) Security in Internet of Things, KTH Information and Communication Technology, Stockholm: Master of Science Thesis
6. R. Khan, S. U. Khan, R. Zaheer, and S. Khan "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges." In FIT, pp. 257-260. 2012.
7. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29, no. 7 (2013): 1645-1660.
8. Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi, "Internet of Things: Security Vulnerabilities and Challenges", Conference Paper, July 2015, DOI: 10.1109/ISCC.2015.7405513
9. X Yang, Z Li, Z Geng, and H Zhang, "A Multi-layer Security Model for Internet of Things." In Internet of Things, pp. 388-393. Springer Berlin Heidelberg, 2012.
10. U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks." In Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on, pp. 791-798. IEEE, 2008.
11. Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP).", 2014
12. J. Yick, B. Mukherjee, and D. Ghosal. "Wireless sensor network survey." Computer networks 52, no. 12 (2008): 2292-2330
13. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29, no. 7 (2013): 1645-1660
14. P. J. Leach, M. Mealling, and R. Salz, "A universally unique identifier (uuid) urn namespace." (2005)
15. Z. Song, A. A. Cárdenas, and R. Masuoka, "Semantic middleware for the Internet of Things." In IoT. 2010
16. Y. Zhang, "Technology Framework of the Internet of Things and its Application." In Electrical and Control Engineering (ICECE), 2011 International Conference on, pp. 4109-4112. IEEE, 2011

17. M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications, Volume 111 - No. 7, February 2015, ISSN: 0975-8887

18. Mr. Ravi Uttarkar and Prof. Raj Kulkarni, "Internet of Things: Architecture and Security," in International Journal of Computer Application, Volume 3, Issue 4, 2014

19. Mike Burmester and Breno de Medeiros, "RFID Security: Attacks, Countermeasures and Challenges."

20. Benjamin Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, 2011

21. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "",Wireless Network Security: Vulnerabilities, Threats and Countermeasures, International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, July, 2008

22. Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, "Classification of RFID Attacks."

23. Lan Li, "Study on Security Architecture in the Internet of Things," in International Conference on Measurement, Information and Control (MIC), 2012 [19] John R. Douceur, "The Sybil Attack," in Peer-to-Peer Systems - IPTPS, 2002, pp. 251-260

24. Nadeem AHmed, Salil S. Kanhere and Sanjay Jha, "The Holes Problem in Wireless Sensor Network: A Survey," in Mobile Computing and Communications Review, Volume 1, Number 2

25. Tapalina Bhattasali, Rituparna Chaki and Sugata Sanyal, "Denial of Sleep Attack Detection in Wireless Sensor Network," in International Journal of Computer Applications, Volume 40, Number 15, 2012

26. G. Padmavathi, Mrs. D. Shanmugapriya, "A survey of ATtacks, Security Mechanisms and Challenges in Wireless Sensor Networks," in International Journal of Computer Science and Information Security, Volume 4, Number 1, 2009

27. Priyanka S. Fulare and Nikita Chavhan, "False Data Detection in Wireless Sensor Network with Secure Communication," in International Journal of Smart Sensors and AdHoc Networks (IJSSAN), Volume-1, Issue-1, 2011

28. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges," in International Journal of Computer Science and Information Technology & Security (IJCSITS).

29. Neha Thakur, Aruna Sankaralingam, "Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555, Vol. 3, No.2, April 2013