Asian Journal of Basic Science & Research
Volume 3, Issue 2, Pages 01-09, April-June 2021

IoT Hacking: Cyber Security Point of View

Kshitij Pawar[1], C. Ambhika[2] & C. Murukesh[3]

[1,2]SRM Institute of Science and Technology, Chennai & [3]Velammal Engineering College, Chennai.

DOI: http://doi.org/10.38177/AJBSR.2021.3201

Article Received: 27 January 2021 *Article Accepted: 24 April 2021* *Article Published: 10 May 2021*

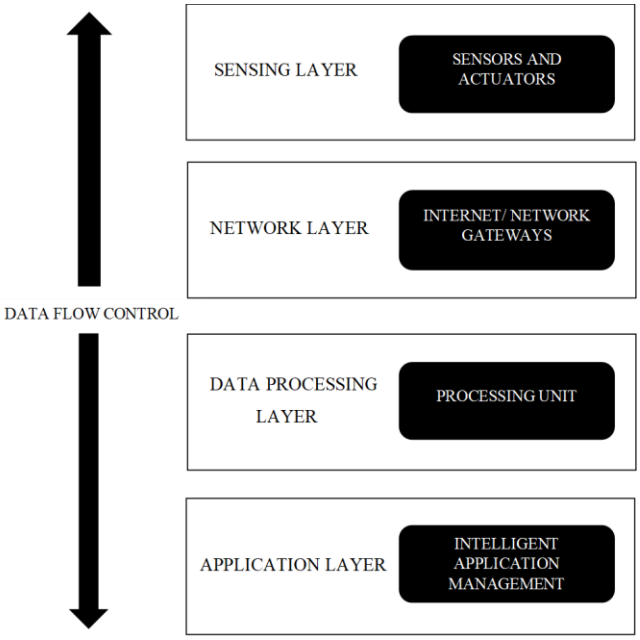
ABSTRACT

With the introduction of Internet of things (IoT) into our lives, it has been simplified to a greater extent. Being able to communicate over the network without any direct communication with human and computer or human and human, On the other hand, threats to the network of Internet of Things has also increased. Certain exploits and vulnerabilities have emerged since the development of Internet of Things. The most common vulnerability arises due to the firmware version of the IoT device. It is difficult to identify as well as update the device firmware version. Due to this incapability, it becomes easier to hack an IoT device. This paper identifies the current issues and provide with the latest solutions to secure IoT devices against attackers constantly trying to penetrate the network.

Keywords: *Internet of things, Exploit, Firmware, Penetrate, Vulnerability.*

1. Introduction

With the increase in use of IOT devices connected to the internet this will result in more use of IOT applications e.g. smart homes, smart devices health monitoring devices etc. will be widely available to the people all over the world. Thus, the industry will see a growth on an average of 21% per year between 2017 and 2025. As of this result 14 billion IOT devices will be in use by 2025 [1]. Each device associated with internet is assigned with a different IP address. With the rapid growth in use of IOT devices comes a great risk of getting hacked or the entire network to be comprised from different kind of attacks. Industry has experienced such attacks previously, these attacks include brute force, DDoS, some many more attacks [2].



Some examples from the previous years include the Mirai malware, specially known for its ability to use common username and passwords to access the IoT devices. Since getting access to an individual IoT device will not be

much helpful, so the attackers combine millions of IoT devices making them a collection of bots also be referred as botnet further used to perform a distributed denial of service attack on major networks [3]. One attack took place dated October 21st, 2016 on the DYN, company which provides domain name services to the major companies like Netflix, GitHub etc. The main problem with the IoT device security is that most of these devices are running default passwords. Cui et al found that 13% of the devices were accounted for default root passwords which were about 540,000. Webcams, routers, printers, etc. web pages were found for managing these devices, showing us how easily these webpages could be brute forced to get the id and passwords [4]. Shodan and Censys known popularly for IoT device search engine also displaying the exploits in the particular type of IoT device. However, the level of detail of device information obtained from search engines is very rough and estimated.

The fine-grained firmware identification method was found out by Li et al. Initially the file system of the firmware was analyzed, and then through reverse analysis the extracted firmware is compared with the present web file of the IoT device to identify the current firmware version [5]. Due to the abridgement of security adaptations in the current firmware of IoT devices, a new and more secure dashboard is required to set up to find out the security controls to avoid attacks on IoT environment.

2. Security Challenges in Internet of Things

Today's IoT interface face a lot of threats whether it be in physical form or attack on a network. These attacks could be on personal Wi-Fi network, or a smart car also could be on a smart TV. These devices face continuous risk. The open architecture makes security of IoT devices even more challenging. There are some properties which can lead to security challenges faced by IoT devices like embedded device used, scale and diversity stated by Iqbal et al [6].

Table 1. TLSD and Specific Attacks

Top Level Security Domain	Domains
Architecture	Perception layer
	Application Layer
	Network Layer
Threat Vector	Communication Attacks
	Physical Attacks
	Application/Software attacks

IoT devices have a unique architecture which are the layers. IoT devices are consists of three different operation layers naming perception layer, application layer and network layer. Each Layer has its own functionality so each possess a different threat. Since each layer is connected for functioning, to secure the higher layers the lower or the consecutive layers needs to be secured.

2.1 Perception Layer

This layer senses and gathers some of the physical parameters or identifies presence of other smart objects in the environment. Each IoT node performs functions which require data to be collected. Perception layer makes use of different sensors such as the Zigbee, RFID and many other sensors.

Since a lot of data is taken as input this data could be malicious or could possess a threat so perception layer should be secured. The type of security which could be placed in the perception are cryptographic elements [7].

2.2 Application Layer

The application layer full fills the goals of Internet of Things which is to ensure that between two different objects with different application a reliable connection is established, which involves providing services and determines a set of protocols for message transmission on the application layer.

Devices nowadays are adopting the terminology Internet of things, with this change in the connection, different protocols are needed to avoid device to vulnerable. Since the communication taking place between the end user and the application layer is direct each consists of their own application layer set of rules. Some challenges like identity authentication verification and data accessibility permissions are cause for concern.

2.3 Network Layer

The network layer in IoT performs and also is involved in the transmission of data. Similar to the security challenges faced by TCP/IP model IoT network infrastructure face the same issues.

The security problems involve TCP sequence number prediction, protocol fuzzing, malicious node injection DoS attack, Man-in- the- middle attack, exploit attacks etc.

Table 2. Comparison of threats and risk levels in IoT architecture

Perception layer	**Application layer**	**Network layer**
Tag cloning	Malicious code injection	Distributed-Denial-of-Service
Information leakage	Denial-of-service attack	Man-in-The-Middle
Eavesdropping	Phishing attack	Storage attack
De-synchronization attack	Sniffing attack	Exploit attack
	Risk Level	
High	Medium	Medium to low

3. Understanding the Attacks

3.1 Communication Attacks

As the name indicates communication attacks are done over the network where the particular IoT device is working. This involves numerous attacks some of them are DoS, Distributed DoS (DDoS), spoofing, SQL injection, Man-in-the-middle and flooding.

3.1.1 Dos and DDoS

DoS attack is attack where the attacker floods the network server with traffic until the target cannot access system or cannot respond [9]. DoS attacks can also be classified in two types Smurf Attack and SYN flood.

DDoS attack occurs when multiple machines operate together to perform attack on a target. This attack makes use of botnets collectively known as collection of bot networks.

Solutions:

- (DoS)
  - Block the origin IP address, further escalating to the ISP Level.
  - Several tools exist which detect flood attacks and further prevent them.
- (DDoS)
  - Ingress/Egress filtering [10]
  - Martian address filtering [11]
  - Honeypots
  - Load balancing

3.1.2 SQL Injection

SQL injection is a penetration technique performed by attacker, inserts a SQL statement through the webpage's input fields to access the resources. Attacker can also use the SQL injection to bring down the whole database of the website. Injecting of a SQL can result in the execution of administrative operations, also modify the database [12]. The purpose of attack maybe extracting data, modifying data, bypassing authentication etc.

Solutions:

- WAVES – Tool to test websites for SQL injections [13].
- SAFELI – Used to identify SQL vulnerabilities [14].
- CANDID – Used to modify web applications which make use of program transformation in java.

3.2 Physical Attacks

Majority of IoT devices communicate directly with the environment, with the use of physical objects like temperature sensors, smart grid, heartbeat sensors etc. These devices not only communicate with the environment

bur also monitor and execute tasks and coordinate decisions [15]. Due to the deployment of tremendous number of physical objects into the internet, Internet of Things (IoT) face a lot of consequences [16]. Being bounded to humans closely and their environment a smallest of vulnerability could lead to a major financial loss.

3.2.1 Object replication attacks

In this attack attacker add a malicious physical object to the network which would redirect the flow of data to the desired network. This type of attack could result in huge drop in the network performance. This object can further lead to performance deterioration, corruption even redirecting the received packets to desired machine and extracting the secret keys.

Solutions:

- Split Manufacturing – Used to hide the design intent to enhance the security of Integrated Chip [21].
- Hardware security module (HSM) – Used to increase the authenticity by providing each device with different electronic identity [18].
- Trusted platform module (TPM) – A microprocessor embedded with advance cryptographic functionalities [19].
- Roots of Trust (RoT) – Computer's operating system trusts this source of cryptographic system [20].

3.2.2 Social engineering

This attack involves physically modifying the users of IoT system in order to extract sensitive data.

Solutions:

- Artificial Intelligence – using artificial intelligence to detect social engineering attacks can be very helpful for a network or a IoT device.
- Honeypot – It is a system to trap the attackers and analyze there working behavior. Honeybot is specially used for attacks based on the social media [22].

3.2.3 Side channel attack

To protect the data of IoT devices they are integrated with some security mechanisms such as encryption to protect sensitive data. Some examples are power and time analysis attack [23].

Solution:

- Randomizing the intermediate data is the simplest approach to render the hypothetical leakage value collections [24].

3.3 Application/Software Attacks

Application based or the software-based attacks are the most powerful attacks vectors and the most efficient ones, as the data extracted from this attack is not raw instead the data being stored in the database. While dealing with IoT

software we mostly make use of API's and web applications [25]. As there are more possibilities of threats this software vector should be secured.

3.3.1 Brute force attack

This attack forces a list of passwords to the webpage on the login page, this attack involves guessing passwords. In brief, BFA is a password experiment that uses mix of possible ASCII characters in isolation or in combinations. The Brute force attack is divided into two classes insider and outsider [26, 27, 28].

Solutions:

- SSH port forwarding – This functionality forwards the ports between client and server through an encrypted connection [29].
- IP tables – It filters out the packet by header fields like IP, TCP, UDP and ICMP. Depending upon the packets number of different actions could be taken [30].

3.3.2 Cross site scripting

This also one of the types of code injection, analogous to the SQL injection cross site scripting (XSS), makes use of malicious scripts to execute into web interface of the victim which is originated from the attacker and is sent back by making use of the web application.

This attack alters the victim to other webpage further making the victim engage in a Distributed Denial of Service or steal the victim's current running session.

Solutions:

- Enhanced XSS Guard algorithm – E_XSS Guard scans the webpage source with the provided whitelisted and black listed scripts [31].
- Pattern filtering – This approach uses technique by filtering out the insecure keywords, character encaping and some common words in XSS payload.
- Concolic testing – Used to detect any XSS vulnerability. This technique is followed by selective instrumentation for runtime XSS detection.

4. Conclusion

Due to the introduction of the concept IoT in the last few years has drawn attention of many hackers. Due to this several security attacks took place over the years, still many of the issues are not resolved and for some the way to bypass the vulnerability has not been found.

This paper makes the best effort to classify the vulnerabilities present in the current scenario and the solutions to secure IoT devices and the networks. IoT developers with the intention to develop a secure IoT system can consent this paper for the current threats and the solutions to avoid them.

By taking the necessary security measures IoT system could be improved in the future

Declarations

Source of Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The authors declare no competing financial, professional and personal interests.

Consent to participate

Not Applicable

Consent for publication

We declare that we consented for the publication of this research work.

Availability of data and material

Authors are willing to share data and material according to the relevant needs.

References

[1] gsmaintelligence.com.

[2] businessinsider.com.

[3] www.digikey.com/en/maker/blogs/2019/5-leading-iot-security-breaches-and-what-we-can-learn- from-them.

[4] A. Cui, S. J. Stolfo, "A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan," in Proceedings of the 26th Annual Computer Security Applications.

[5] Q. Li, X. Feng, H. Wang, Z. Li, L. Sun,2018, "Towards Fine-grained Fingerprinting of Firmware in Online Embedded Devices," in IEEE INFOCOM 2018-IEEE Conference on Computer Communications, pp. 2537-2545. Conference (ACSAC '10), pp. 97-106, 2010.

[6] A. Iqbal, R. Saleem, and M. Suryani, 2016, "Internet of Things (IOT): ongoing Security Challenges and Risks," International Journal of Computer Science and Information Security, vol. 14, pp. 671.

[7] Yang, Y., Wu, L., Yin, G., Lifie, L., & Hongbin, Z. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal, 1250-1258.

[8] Muneer Bani Yassein, Mohammed Q. Shatnawi, Dua' Al-zoubi Application Layer Protocols for the Internet of Things: A Survey.

[9] https://www.us-cert.gov/ncas/tips/ST04-015.

[10] Senie D and Ferguson P. Network ingress filtering: defeating denial of service attacks which employ IPsource address spoofing. Network, 1998, https://dl.acm.org/citation.cfm?id=RFC2267.

[11] Baker F. Requirements for IP version 4 routers, 1995, https://datatracker.ietf.org/doc/rfc1812/.

[12] Fabrizio Monticelli, 2018, PhD SQL Prevent Thesis, University of British Columbia(UBC) Vancouver, Canada.

[13] Yao Wen Huang, Fang Yu, Christian Hang, Chung Hung Tsai, D. T. Lee, Sy YenKuo,2005, "A Testing Framework for Web Application Security Assessment", Journal of Computer Networks, Volume: 48 Issue: 5, Pages: 739-761.

[14] Xiang Fu, Kai Qian,2008, SAFELI–SQL Injection Scanner Using Symbolic Execution. Proceedings of the 2008 workshop on Testing, analysis, and verification of web services and applications. pp 34-39: ACM.

[15] J. Pike, 2014, "Internet of Things - Standards for Things,".

[16] F. Da Costa, 2013, "Rethinking the Internet of Things: A scalable approach to connecting everything." Apress Open, p. 185.

[17] J. Sen, 2009, "A Survey on Wireless Sensor Network Security," International Journal of Communication Networks and Information Security (IJCNIS), vol. 1, no. 2.

[18] https://hsm.utimaco.com/solutions/applications/key-injection/.

[19] Bajikar, S, 2002, Trusted Platform Module (TPM) Based Security on Notebook PC White Paper; Mobile Platforms Group Intel Corporation: Santa Clara, CA, USA.

[20] https://www.synopsys.com/designwareip/technicalbulletin/understandinhardware-roots-of-trust-2017q4.html.

[21] Li, H.; Liu, Q.; Zhang, J, 2016, A Survey of Hardware Trojan Threat and Defense. Integ. J. 55, 426–437.

[22] Jin, X. et. al. (2011). A Data Mining-Based Spam Detection System for Social Media Networks. International Conference on Very Large Data Bases (VLDB). August, Seattle, WA. 1458-1461.

[23] A. Mohsen Nia and N. K. Jha, 2016, "A Comprehensive Study of Security of Internet-of-Things," IEEE Transactions on Emerging Topics in Computing, vol. PP, no. 99.

[24] Jean-Sébastien Coron, 2002 "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems," in Proc. 1st Int. Workshop, CHES'99 Worcester, MA, USA, vol. 1717, pp. 292-302.

[25] B. Dorsemaine, J. P. Gaulier, J. P. Wary, N. Kheir and P. Urien, "A new approach to investigate IoT threats based on a four layer model," 2016 13th International Conference on New Technologies for Distributed Systems (NOTERE), Paris, 2016, pp. 1-6.

[26] J. Jang-Jaccard and S. Nepal,2014, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, Vol. 80, no. 5, pp. 973–993.

[27] M. GhasemiGol, A. Ghaemi-Bafghi, and H. Takabi,2016, "A comprehensive approach for network attack forecasting," Computers & Security, vol.58, pp. 83–105.

[28] S. Zeadally and A. Flowers, 2014, "Cyberwar: the what, when, why, and how [commentary]," IEEE Technology and Society Magazine, vol. 33, no. 3, pp. 14–21.

[29] Ramsbrock, D.; Berthier, R. and Cukier, M. 2007. "Profiling Attacker Behavior Following SSH Compromises", in Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp.119- 124.

[30] Mukosaka, S. and Koike, H. 2007 "Integrated visualization system for monitoring security in large-scale local area network", Asia-Pacific Symposium on Visualization, 0: 41–44, 2007.

[31] M. James Stephen, P.V.G.D. Prasad Reddy, Ch. Demudu Naidu, Ch. Rajesh, "Prevention of Cross Site Scripting with E-Guard Algorithm".