Are We Secure in the Internet of Things Era?

P. Gowri Prasad *

*** Librarian**
Shah & Anchor Kutchhi Engineering College,
Mumbai, Maharashtra, India

QR Code

Abstract: - *There is a rapid influx of Internet of Things devices in our daily life. This has raised several privacy and security challenges. This paper addresses some of them and the remedial measures to be taken.*

Keywords: Internet of things, Security, Privacy, IoT, Intrusion Detection Systems, Library

Introduction

The rapid expansion of Internet of things (IoT) devices in the last few years, ranging from body sensors and wearable devices to home appliances and industrial monitoring sensors, has driven the evolution of various computing paradigms such as pervasive and ubiquitous computing, mobile crowd sensing, edge computing, as well as the emergence of diverse applications and services. (Wang, Zhang & Taleb, 2017). The era of Internet of Things (IoT) is characterized by an environment in which we live in an ecosystem consisting of billions of smart, connected computing devices (Ray & Jin, 2017).

In spite of the technological and societal benefits and economic potentials of IoT, security and privacy have become the cause of concern. This hinders the further development and deployment of IoT infrastructures, services, and applications. Security issues can come at different levels, including deployment issues that leave devices unprotected from cyber-attack, functional vulnerabilities in system design or implementation, an altered functionality by some player in the complex supply-chain, or side-channel issues exploitable by physical access to the device. The data collected by these devices have a complex communication path through switches, gateways, routers, and the cloud of servers and datacenters.

Internet of Things in Libraries Internet of things has tremendous scope for use in libraries. Pujar &

Satyanararya (2015) have enumerated the potential uses of IoT in libraries-

Access to library and its resources

Libraries, using a mobile app, may provide a virtual library card to its members, which will enable members to gain access to the library and use its resources.

Collection management

With the integration of RFID tags to library cards, circulation of items and fine collection can be made efficient. The IoT can tell users about overdue books and estimated fine. Smart digital shelves may be able to promote the content based on user's borrowing records and search history on the Internet. IoT will also help in better inventory management and locate misplaced books.

Information literacy

IoT may help libraries in providing a virtual tour of the library. When users visit the particular section, their mobile phone will play a video or audio explaining more about that section and how one can get maximum benefit out of it.

Recommendation service

IoT can use the patron's data to suggest customized recommendations, using real time data, based on the history of their borrowings. IoT would be able to inform the user about new arrivals in his or her subject.

Location based services

With IoT enabled mobile device user would be able to get directions for stacks.

Appliances management

IoT may help libraries and their users in better management of available appliances thus saving the energy costs. Using an IoT enabled mobile phones user should be able to control the lighting, air conditioning, Wi-Fi etc.

Internet of Things Architecture

The Security structure in IoT can be divided into three layers, which are the perception layer, the network layer, and the application layer. (Chahid, Benabdellah and Azizi, 2017).

A) Perception layer -When the data is collected, the mode of transmission of the information is basically the transmission of the wireless network. The signals are displayed in the public place. If effective protective measures are lacking, the signals will be monitored, intercepted and disturbed easily. Most detection devices are deployed at unsupervised monitoring sites. Attackers can easily access, control or physically damage equipment.

Following types of attacks are possible in the perception layer-

I) Attacks on the tags

Cloning- Unique identifier of RFID tag is cloned to replicate the tag.

Spoofing- In this an adversary impersonates a valid RFID tag to gain its privileges

II) Reader attacks

Impersonation- adversaries may easily counterfeit the identification of a legitimate reader in order to elicit sensitive information or modality data on RFID tags.

Eavesdropping- An unauthorized individual uses an antenna in order to record

communications between legitimate RFID tags and readers. This type of attacks can be performed in both directions: tag to reader and reader to tag.

III) Network Protocol Attacks

Malicious users can use flaws in the operating system and network protocols in order to launch attacks and compromise the back-end infrastructure.

B) Network layer- the network layer exists on the internet or on the existing communication network. Some types of attacks on this layer are as follows-

The gateway node: The gateway node is a sensitive element, it is easily controlled by the attackers. It can leak all information, including the group communication key, the corresponding key, radio key etc., and threatens the security of the entire network.

False node and malicious data: Attackers add a node to the system, and enter the wrong code or data. They stop transmitting real data. The sleep of the limited node of energy is refused. They consume valuable node energy, and potentially control or destroy the entire network.

DoS: DoS attack is the most well-known attack in Wireless Sensor Network (WSN) and Internet. It causes loss of network resources and renders the service unavailable.

Sync: The attackers analyze the execution time of the encryption algorithm in order to obtain more information about the hacking method to be used.

Routing: The user can create routing loops, cause or resist transmission of the network, extend or shorten the source path, form error messages, increase the number of end-to-end delay, etc.

Replay: To obtain the confidence of the system to attack, the attacker launches a packet received by the destination host. It is mainly used in the processing of authentication, destruction and certification validation.

SCA: Time consuming, energy consumption or electromagnetic radiation are the key information used by an attacker to tag encryption devices, and they are also called data leaks.

C) Application layer – This depends upon the type of device. It runs customized codes for end users. Some of the common things are

Authentication: Different applications have different users; each application will have a large number of users. In order to prevent illegal user intervention, there should be effective authentication technology. Spam and the identification and processing of malicious information should also be considered.

Data Protection and Recovery: Communication data involves the confidentiality of users. Data protection mechanism and data processing algorithm are not perfect, and it can result in data loss and damage.

Ability to process mass data: Due to a large number of nodes, an enormous amount of data transmission, and complex environment, once the data processing capacity and adaptability cannot meet the requirements; it will lead to interruption and loss of data.

Security Measures for Internet of Things

Security is one of the most important components of IoT system. Product or service providers should ensure proper security by making the patches available as soon as any vulnerability is detected. Products are prone to new kinds of attacks no matter how the providers had paid attentions to their product's security at the development phase. Product providers and consumers should pay more costs on security during its operation periods.(Koo & Kim, 2017)

These steps are to be followed-

***Firstly*,** Having awareness about the value of privacy, and strong policy requiring higher security standard could be the solution. A punitive fine can compensate the differences of expected financial loss between business areas. To maintain strong security policy over whole IoT system, various system components should comply with it and prevent vulnerable areas by punitive financial penalty on its business owners if they fail to follow proper guidelines.

Secondly, the security standards required by law or regulations should be continuously maintained to complement to the higher-level security.

Pishva (2016) has illustrated a few common attacks and their solution

1 User Impersonation

Threat -Impersonation using password.

Solution – Introduce a certificate mechanism.

2 Device Impersonation

Threat -Impersonation of a device using its faulty certificate.

Solution – Introduce a certificate mechanism.

3 Service Interruptions.

Threat - Distributed Denial of Service (DDOS).

Solution- Control through network and access mechanism to outside world.

4 Data Alteration

Threat- Data alteration of transmitted or stored data.

Solution- Introduce access control and certificate mechanism

5 Worm/Virus Infections.

Threat- Infiltration and/or damaging of a computer system.

Solution- Use virus protection software and prepare to handle new vulnerabilities

6 Phishing/Pharming.

Threat- Impersonation of user's destination.

Solution- Consider using SSL to assure genuineness of displayed sites.

7 Data Wiretapping.

Threat- Information leakage through wiretapping.

Solution- Protect communication via IPSEC, SSL/TLS.

8 Firmware Alterations.

Threat- Replacing of firmware at will.

Solution- Use physical access control for update procedure.

9 OS/Software Vulnerability.

Threat- Launching of worms and attacks using such vulnerabilities.

Solution- Educate R&D people on security and conduct product test.

Some steps which were proposed for Internet of things security model are (Moganedi & Mtsweni, 2017):

a. Device Protection: Only trusted and authentic programming code or logic should be executed on the device. This can be achieved by following software development best practices in order to deploy trusted and authentic code. The devices should have the ability to be remotely managed in order to enhance on the remote vulnerability remediation.

b. Device Boot: Devices which require being configured should enforce booting for the very first time and prompt the user to change the default security settings. IoT should also provide an auto-update mechanism for device's firmware and/or software to counter any recently discovered vulnerability at the hardware level.

c. Authentication: The IoT devices will be communicating with other devices. Therefore, authentication is vital to ensure that the device in use is only communicating with known and trusted devices. Authentication process should be established every time the devices is making a connection to other devices.

d. Communication: Interconnected devices should provide a trustworthy communication. IoT allows simultaneous connection of the devices and the communication causes an increase in data traffic. Confidentiality and integrity of the data during communication should be established and maintained. This means authentication and data encryption should be integrated for secure communication purposes.

e. Device Monitoring and Reporting: Each device runs numerous applications that collect data about the device and the user. A privacy policy should be available to the users disclosing the type of data that is collected by the device and how it is processed and, where and how the data is stored before the user can use the device. This will also create security awareness for the user prior to using the device.

f. Personal Data Protection: A lot of personal data in collected by the IoT devices. Personal data should be protected during data transmission and in storage by encrypting the data using generally accepted security standards with regard to encryption.

g. Data Transmission Security: This requires the network layer for data transmission to be secured from attacks such as DDoS, eavesdropping and other external interference or monitoring. Employing two-layer encryption mechanism to encrypt data on the device level with the Base Encryption Layer (BEL) before transmitting the data to the cloud storage, and performing the second encryption at the cloud storage level with a Surface Encryption Layer (SEL).

h. Intrusion Detection Systems: (IDS) can be used for monitoring malicious activity.

This table consists of some of the existing IDS.

Intrusion Detection System(IDS)	Attacks targeted	Limitations
SVELTE	Sybil and Clone attack	False alarms in testing and need improvement in true positive rate
RIDES	Intrusion detection in NS2	Doesn't match real-time requirements. Need automation
Specification based IDS	Rank attack and local repair attack	Resource constrained nature of IoT is disturbed
NIDS	UDP flood attack	Tested with only UDP flooding
DEMO	DoS detection	Complicated environment of IDS

(Source- Security in Internet of things...Adat & Gupta, 2017)

Conclusion

We are engulfed by Internet of things devices these days. They have potential uses in libraries as well. Though they are extremely useful, there exists some security and privacy concerns. This paper has discussed about IoT architecture, various ways in which the security can be compromised and the possible solutions.

References

1. Adat, V., & Gupta, B. B. (2017). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, 1-19.
2. Chahid, Y., Benabdellah, M., & Azizi, A. (2017, April). Internet of things security. In *Wireless Technologies, Embedded and Intelligent Systems (WITS), 2017 International Conference on* (pp. 1-6). IEEE.
3. Koo, C., & Kim, J. (2017). Enforcing high-level security policies for Internet of Things. *The Journal of Supercomputing*, 1-9.
4. Moganedi, S. & Mtsweni, J. (2017). Beyond the convenience of the internet of things: security and privacy concerns in *IST-Africa Conference Proceedings*, pp 1-10
5. Pishva, D. (2017, February). Internet of Things: Security and privacy issues and possible solution. In *Advanced Communication Technology (ICACT), 2017 19th International Conference on* (pp. 797-808). IEEE.
6. Pujar, S. M., & Satyanarayana, K. V. (2015). Internet of Things and libraries. *Annals of Library and Information Studies (ALIS)*, *62*(3), 186-190.
7. Ray, S., & Jin, Y. (2017). Guest Editorial: Security Challenges in the IoT Regime. *Journal of Hardware and Systems Security*, 1-1.
8. Wang, H., Zhang, Z., & Taleb, T. (2017). Special Issue on Security and Privacy of IoT. *World Wide Web*, 1-6.