Security Considerations Based on Classification of IoT Device Capabilities

Seungyong Yoon, Jeongnyeo Kim, Yongsung Jeon
Mobile Security Research Section
Electronics and Telecommunications Research Institute
Daejeon, Rep. of Korea
e-mail: syyoon@etri.re.kr, jnkim@etri.re.kr, ysjeon@etri.re.kr

Abstract— **In the Internet of Things (IoT) environment, the various types of IoT devices, from tiny and lightweight devices to powerful smart devices, are connected to send and receive information to and from each other. We need to define different security requirements of IoT devices, depending on the functionality, capabilities, and characteristics. In this paper, we analyze security threats and vulnerabilities of IoT devices, and propose the security requirements based on classification of IoT device capabilities.**

Keywords-IoT; security; classification.

I. Introduction

With the rapid growth of IoT market, security threats and vulnerabilities of IoT devices, having a variety of types and performance, are increased by being interconnected with the network. Therefore, IoT devices need to be provided with various security features for responding to security threats such as hacking and exploitation. Most existing IoT devices are available for the CPU and memory resources are limited, such as lightweight devices, so low-power and lightweight security mechanism are essential. In addition, IoT devices should be able to prevent malfunction or stop due to the malicious code, and should be able to prevent information leakage from physical theft or loss.

In this paper, we analyze security threats and vulnerabilities of various IoT devices, and propose security requirements in order to prevent confidentiality, integrity and availability, for example, access control, device authentication, data integrity, anti-virus, secure storage, security updates, and so on. Also, we classify IoT devices into four categories depending on their capabilities and propose security requirements for each class of IoT devices.

The rest of this paper is organized as follows. Section II gives an overview of related work and provides a discussion of our contribution. Section III describes security threats analysis and security requirements of IoT devices. Section IV proposes security requirements based on classification of IoT device capabilities, followed by conclusion in Section V.

II. Related Work

IoT devices can be classified according to various criteria. They can be classified by functionality and type [1], classified based on the type of data handled [2], and classified according to the degree of resource constraint [3]. Many researches have been performed for the security function required of such IoT devices [4][5][6] and classification mechanism for IoT devices to determine their capability to support security mechanisms of different degrees [7].

III. Security Threats Analsysis and Security Requirements of IoT Devices

IoT devices are exposed to a variety of security threats and vulnerabilities. Hackers who launch attacks using these vulnerabilities exhibit malicious behaviors. Typical security threats and vulnerabilities of IoT devices include unauthorized access, loss or theft, physical destruction, information leakage, illegal data modification, and denial of service attacks.

TABLE I. Security threats and vulnerabilities of IoT devices

Categories	Security threats	Security vulnerabilities
Confidentiality	Eavesdropping, Man-in-the-middle attack, Illegal message modification, Sniffing	Sensitive data(privacy) leak
	Zombie devices, Distributed Denial of Service (DDoS) attacks, Phishing, Pharming	User data leak, Secondary damage caused by malware infection
	Attacks using web interface vulnerabilities	Data and device takeover
	Illegal firmware update, Hardware interface and flash memory physical takeover	Root privilege takeover
	Replication through the device unique identifying information leakage and change	Data and device replication
Integrity	Eavesdropping, Man-in-the-middle attack, Illegal message modification	Sensitive data(privacy) leak
	Attacks of interfaces and system vulnerabilities through illegal intrusion and access	Firmware and operating system permissions takeover
Availability	Software malware infection	malfunction
	Physical removal and destruction, Unusual installation attempt	Data and device takeover
	Persistent attempted access attack, Denial of service attack	System operation and malfunction
	Lost or stolen, installation and disposal	Data and device takeover

	Network platform smishing attack	Malware infection
	Network platform screen capture attack	Sustainable security error
Authentication/ Authorization	Unauthorized user access and unauthorized devices access	Privilege takeover, Illegal access, Data leak
	Device replication, alteration, appropriation	Data and device takeover

The openness of IoT platform accelerates interworking between heterogeneous devices, and the variety of security threats is increasing. In addition, three elements of information security which consist of confidentiality, integrity, and availability are increasing the possibility of infringement. From these threats, we present the security requirements to keep the IoT devices safe.

A. *Confidentiality*

- [Transmitted message encryption] Messages transmitted between IoT devices are to be transmitted in encrypted format to prevent illegal sniffing or eavesdropping.
- [Malware response] IoT devices should provide the ability to detect and defend against malware infections and external hacker attacks, such as worms and viruses to prevent information leakage.
- [Data encryption] IoT devices should encrypt sensitive data such as private information and cryptographic key, and securely process and store these data to prevent information leakage.
- [Tamper resistance] IoT devices should provide tamper resistance function to ensure the safety and reliability from physical attacks.
- [Device ID management] IoT device should have unique device identification information and safely handled so as not to leak outside or to change illegally.

B. *Integrity*

- [Data integrity] IoT device should provide data integrity verification function to prevent forgery of data.
- [Platform integrity] IoT devices should provide platform integrity verification function of system-level such as firmware and operating system.
- [Secure booting] When power is first introduced to the device, IoT devices should provide secure booting function to ensure the reliability of the device through authenticity and integrity of the software on the device.

C. *Availability*

- [Logging] IoT device should provide the appropriate log function for the user, the system, the security event.
- [State Information Transmission] IoT device should provide a periodic keep-alive message or device state information transmission function for prevention from physical removal/destruction and abnormal installation attempt.
- [External attack response] IoT device should provide the capability to respond to external attacks, such as denial of service attacks and persistent connection attempt attack.
- [Security monitoring/management] IoT devices should provide security monitoring and management capabilities to respond adequately if lost or stolen, installation and disposal, etc.
- [Security patch] IoT device should provide a safe and secure software update and patch function.
- [Security policy setting] IoT device should provide the capability to securely set an appropriate security policy on the various types of devices.
- [Software safety] IoT devices should ensure software safety, with features such as appropriate module separation or removal, and access restrictions, despite a software failure or malfunction due to malware infections.

D. *Authentication/Authorization*

- [User authentication] IoT device should provide a user authentication function to block the access of unauthorized users.
- [Device authentication] IoT device should provide a device authentication function in order to block the access of illegal device.
- [Password management] IoT device sets the secure and robust password, and should provide the periodic update feature.
- [Mutual authentication] IoT device should provide a mutual authentication between the devices to establish secure, autonomous communication environment.
- [Authority control] IoT device should provide the authority control functions, such as ownership control for preventing information leakage and privacy protection.
- [Access control] IoT device should provide a access control function to block the access of unauthorized users and devices.
- [Identification information verification] IoT device should provide the unique device identification information verification function for preventing device replication, alteration, and appropriation.

IV. Security Requirements based on Classification of IoT Device Capabilities

International Telecommunication Union (ITU) classified into four different types of IoT devices according to type and functionality as follows: data-carrying device, data-capturing device, sensing and actuating device, and general device [1]. In this paper, however, we classify IoT devices in four classes, depending on their capabilities.

Class 0 devices are very constrained devices, such as compact, lightweight, and low-power sensors. Due to the constrained in memory and processing capability, they do not participate in Internet communication in a secure way. These devices usually communicate with the help of proxies or gateways.

Because of constrained resource and processing capabilities, Class 1 devices cannot easily communicate with other devices employing a full protocol stack, such as HyperText Transfer Protocol (HTTP) and Transport Layer Security (TLS). They use a protocol stack for specifically designed for IoT device with constraints, such as Constrained Application Protocol (CoAP). Device examples include a blood glucose meter or a thermostat that is based on 8-bit or 16-bit processors. It is possible to communicate with other devices without the help of a gateway.

TABLE II. SECURITY REQUIREMENTS ACCORDING TO IOT DEVICES CAPABILITIES

Categories	Security Requirements	Class 0	Class 1	Class 2	Class 3
Confidentiality	Message encryption		√	√	√
	Malware response				√
	Data encryption		√	√	√
	Tamper resistance			√	√
	Device ID management	√	√	√	√
Integrity	Data integrity		√	√	√
	Platform integrity			√	√
	Secure booting			√	√
Availability	Logging			√	√
	State Info. Transmission	√	√	√	√
	External attack response				√
	Security monitoring			√	√
	Security patch			√	√
	Security policy			√	√
	Software safety		√	√	√
Authentication/ Authorization	User authentication		√	√	√
	Device authentication		√	√	√
	Password management		√	√	√
	Access control		√	√	√
	Device ID verification			√	√

Class 2 devices can be supported in the existing communication protocol stack, or that are less constrained. Examples include an IP camera or a smart meter that is based on 32-bit processors. However, these devices also can benefit from using low-power and lightweight protocol, and from consuming less bandwidth.

Class 3 device example is a smartphone or a tablet beyond class 2. They can use existing protocols without any changes or modifications. However, these devices can still be constrained by a limited power supply.

Table II presents the security requirements according to IoT device classification. It can be easily utilized as a security guideline to apply to various IoT devices.

V. CONCLUSION

IoT devices are always exposed to security threats, such as loss or theft, information leakage, and data forgery. In this paper, we analyzed security threats and vulnerabilities for IoT devices, and proposed security requirements based on classification of IoT device capabilities. By presenting with the applicable security requirements in the various classes of IoT devices, we are expected to contribute to improving security of IoT devices.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (B0190-16-2032, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices).

REFERENCES

[1] ITU-T Y.2060, Overview of the Internet of Things, 2012.6.

[2] Imagination Technologies Limited, White Paper, Internet of Things – Opportunities for device differentiation, 2015.2.

[3] IETF RFC7228, Terminology for Constrained-Node Networks, 2015.4.

[4] Wind River, White Paper, Security in the Internet of Things, 2015.1.

[5] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things”, IEEE Computer, Vol.44, pp.51-58, 2011

[6] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)”, Proc. International Conference on Network Security and Applications (CNSA 2010), Springer-Verlag Berlin Heidelberg, pp. 420-429, 2010

[7] V. J. Jincy and S. Sundararajan, “Classification Mechanism for IoT Devices towards Creating a Security Framework”, In Intelligent Distributed Computing, Springer International Publishing, pp. 265-277, 2015