Consideration of Security Threats for Identification System in Internet of Things

Daewon Kim, Jeongnyeo Kim, and Yongsung Jeon
Information Security Research Department
Electronics and Telecommunications Research Institute
Daejeon, Korea
emails: {dwkim77, jnkim, ysjeon}@etri.re.kr

***Abstract*—During the last years, people have expressed and increased interest towards Internet of Things (IoT) technology. Among various systems in the IoT environment, the identification system has an important role to recognize IoT things. However, current IoT identification systems do not consider security aspects carefully. This paper presents the security threats related to the IoT identification systems.**

Keywords-internet of things; identification; object identifier; security threats.

I. INTRODUCTION

Things, which are constructing the Internet of Things (IoT) environment, can have various physical communication modules, such as ZigBee, Bluetooth, and so on [1]. The IoT environment needs higher level identification systems than physical module-level to recognize things and to communicate with each other. This is the role of the IoT identification system.

Current IoT identification systems are primarily focusing on interworking, interoperability, scalability, distributability, and performance, and they do not consider security aspects carefully [2], [4]. Therefore, researches related to IoT identification security are required to mitigate security threats due to vulnerable identification management.

The nature of security problems related to the IoT identification is that it can be applied to authentication and authorization. As the purpose of our paper, we describes the details related to the security threats of IoT identification, and our challenge is to classify and analyze the sufficient contents of predictable threats for the secure implementation of identification system.

The rest of the paper is organized as follows. In Section 2, we describe the IoT environment, the necessity and role of IoT identification system, and the features of IoT identification. In Section 3, for the IoT identification system, we present the security threat, vulnerability, threat action, threat purpose, and threat result. Finally, we conclude the paper in Section 4.

II. IOT IDENTIFICATION SYSTEM

In this section, as the background to list the security threats of IoT identification system, we will describe the IoT environment, the necessity and role of the IoT identification system, and the features of IoT identification.

A. IoT Environment

IoT environment is the environment in which Internet-connected physical and logical devices are interworked and interoperated. The interworking means that various devices can exchange information among them, and the interoperating means that various devices can use services mutually. The interoperating devices are in a common IoT platform, and if many IoT platforms can exchange information among them, a huge IoT environment is constructed.

B. The Necessity and Role of IoT Identification System

Even in a common IoT platform, there are various physical communication modules, and it is sure that a huge IoT environment includes even more, and more diverse, physical modules. Therefore, some identification methods, which are independent on physical layer communication, are required to recognize various IoT things and to communicate with each other. It is the reason for the necessity of IoT identification system.

The normal role of identification systems is to control identification information to identify physical and logical objects. Therefore, the identification information of IoT identification system has a role to identify physical and logical objects in the IoT environment.

C. Features of IoT Identification

In the communication environment including various physical modules, for the exact and smooth communication, the IoT identification system and information needs to have the following features.

- From top-level things to bottom, unique identifiers are allocated to identify all things. In the sub-areas under the things with unique identifiers, independent identifiers can be allocated only for the sub-areas.
- Identification system and information are independent on various physical communication methods.
- IoT identification system manages naming information to identify each thing.
- IoT identification system manages addressing information to find routes for things.
- IoT identification system manages discovery information to find the naming and addressing information that traces the mobility of things.

 ISBN: 978-1-61208-512-8

- IoT identification system has a life cycle including generation, registration, searching, deletion, and so on.

III. SECURITY THREATS OF IOT IDENTIFICATION SYSTEM

In this section, based on the background of Section 2, for IoT identification system and information we will present security threat (ST), identification threat (IT), and the threat description (TD) including vulnerability, threat action, threat purpose, and threat result. Among various identification pieces of information, in this paper, we focus on device identification such as Object IDentifier (OID) [3].

- **ST: Device Malfunction, IT: Damaged Identification Information**

TD: It can occur when identification system and information are vulnerable to the unauthenticated and unauthorized accesses. It is possible to miswrite and delete identification information. The threat purpose is to cause internal service troubles to vulnerable devices and systems.

- **ST: Out of Service Request, IT: Tampered Identification Information**

TD: It can occur when identification system and information are vulnerable to the unauthenticated and unauthorized accesses, and cache poisoning. It is possible to change the identification information to that of the attacker. The threat purpose is to cause external service request troubles to vulnerable devices and systems. Since this is tampering with the identification information for connection to remote servers, service requests may fail due to wrong destination.

- **ST: Denial of Service Attack, IT: Tampered Identification Information**

TD: It can occur when identification system and information are vulnerable to the unauthenticated and unauthorized accesses, and cache poisoning. It is possible to change the identification information to that of the attacker. Similar to tampering with the information for identifying destination devices, this may cause denial of service attacks to the tampered destination devices.

- **ST: Information Leakage, IT: Tampered Identification Information**

TD: It can occur when identification system and information are vulnerable to the unauthenticated and unauthorized accesses and cache poisoning. It is possible to change the identification information to that of the attacker. Similar to tampering with the information for identifying destination devices, critical information can be leaked to the devices compromised by attackers.

- **ST: Illegal Service Access, IT: Counterfeited Identification Information**

TD: It can occur when identification system and information are vulnerable to the unauthenticated and unauthorized accesses, and sniffing. After the device identification information is exposed to attackers, they can use the counterfeited identification information. As illegally gaining the identification information from vulnerable devices and systems, attackers can illegally access critical services granted to legal users and devices.

- **ST: Illegal High Authority Access, IT: Counterfeited Identification Information**

TD: It can occur when identification system and information are vulnerable to the unauthenticated and unauthorized accesses, and sniffing. After the device identification information is exposed to attackers, they can use the counterfeited identification information. As illegally gaining the identification information from vulnerable devices and systems, attackers can illegally access critical resources through high authority, such as the administrator.

- **ST: Information Eavesdropping, IT: Counterfeited Identification Information**

TD: It can occur when identification system and information are vulnerable to the unauthenticated and unauthorized accesses, and sniffing. After the device identification information is exposed to attackers, they can use the counterfeit identification information. As illegally gaining the identification information from vulnerable devices and systems, attackers can eavesdrop messages in the communication area of the attacker device disguised through the counterfeit identification information.

IV. CONCLUSIONS

Identification is a very important component in IoT environment. However, current IoT researches do not consider security aspects related to the identification carefully. In this paper, we described IoT environment, the necessity and role of IoT identification system, and the features of IoT identification. Based on the background information, we presented security threat, identification threat, and the threat description including vulnerability, threat action, threat purpose, and threat result.

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] D. Katusic, et al., "Universal Identification Scheme in Machine-to-Machine Systems," Proc. of 12th International Conference on Telecommunications (ConTEL), pp. 71-78, 2013.

[2] European Research Cluster on The Internet of Things, "EU-China Joint White Paper on Internet-of-Things Identification,-" European Commission-Information Society and Media, Nov. 2014. [Online]. Available from: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_EU-China_IoT_Identification_Final.pdf 2016.05.18.

[3] International Telecommunication Union, "Information technology - Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree," ITU-T X.660, July 2011.

[4] oneM2M-TS-0003, "oneM2M Security Solutions Technical Specification," V1.4.2, Mar 2016.

 ISBN: 978-1-61208-512-8