**IoT Device Security Guide Trend and Analysis Research**

Seul-Ki Han , Ye-na Lee , Myuhng-Joo Kim

1Dept. of Information Security, Seoul Women’s UniversityCenter Address Here

Seoul Women’s Univ.,  Gongneung 2(i)-dong, Nowon-gu, Seoul 139-774, KOREA

cocoq@swu.ac.kr, yena22222@swu.ac.kr , mjkim@swu.ac.kr

**Abstract**

**Demand for IoT devices is increasing, and the need for security of IoT devices handling important information of users is also increasing. As a result, various domestic and foreign organizations are conducting active research on IoT security, and security guidelines specialized for IoT are presented. However, the current IoT security guidelines have limitations that are not categorized according to the characteristics of IoT.**

**Therefore, in this paper, we analyze the limitations of existing IoT security guidelines and suggests ways to improve them.**

Keywords-component; formatting; style; styling; insert (key words)Internet of Things(IoT), security guidelines, security evaluation model

**I. Introduction**

Since 2014, IoT (Internet of Things) has received attention from the next generation of IT technology. IoT is used in a variety of fields including home network, public safety, health care, medical care, and manufacturing.

TABLE I. IoT Filed of use [1]

|  |  |
| --- | --- |
| IoT Service field | Contents |
| Home Care | Intelligent Housing Management, Smart Home Service |
| Health Care | Taxi wireless payment ,Health information transmission, Healthcare applications |
| Agriculture and Industry | Smart Factory, Real-time crop monitoring, Crop yield management |
| Car | smart car, Unmanned car,Vehicle remote management |
| traffic | National road monitoring, Taxi wireless payment |

 Global market forecasting company Gartner, ABI Research etc. predicts more than 25 billion IoT devices will be connected in 2020. Thus, as the demand of IoT increases, the need for security of IoT devices collecting various important information of users is steadily increasing. As a result, various international organizations are conducting active research on things' Internet security, and present different standards for it. However, current IoT security guidelines are based on the existing security system, and most of them are comprehensive.

Therefore, it is difficult to apply it properly to IoT devices with various constraints such as energy, processor, and hardware. Therefore, in this paper, we analyze the limitations of the characteristics of IoT devices and that of the IoT security guideline based on sensing, communication, network, and service interface technologies, which are the three components of IoT technology. In addition, IOT device security check are presented and concluded in order to properly apply security to various IoT devices.

TABLE I. IoT Technical components [2]

|  |  |
| --- | --- |
| Technical area | Main Content |
| Sensing technology  | · Measurement of environmental changes in Environment around things such as temperature and humidity· Detecting human behavior such as location and facial expression· Re-processing ~~the~~ collected Information |
| telecommunication and network technology | · Identification of things through IoT such as RFID· Wi-Fi, Bluetooth, 4G / LTE etc. Network connection |
| Service interface technology | · Visibility of Web services, mobile applications, etc. · Application service technology |

**II. Main subject**

The IoT equipment is designed to maintain minimum performance according to the weight saving and low cost characteristics[2].

Also, since the IoT environment has changed in the cyber environment as a conventional PC and mobile, not only the existing security threat but also a new security vulnerability depending on the IoT environment may occur. Additional security requirements according to characteristics are required[3][4].

As a result, various international organizations and organizations such as OTA, OWASP, GSMA, IoT Security Alliance, etc. study and present standard guidelines for IoT security from different viewpoints.

However, current security guidelines include many of the common security requirements that compose IoT,

Also, we handle comprehensive security without considering the characteristics of each IoT device, and it is difficult to utilize it as a practical guide for applying appropriate security to IoT devices [5].

In order to complement these limitations, the method proposed in this paper is as follows.

1. Classify IoT equipment by application field.

2. We reclassify IoT devices classified by usage category
according to hardware performance based on IoT technical elements, sensing, communication, network, service interface technology area.

3. Analyze the existing security guidelines, delete duplicate
items, then present and create detailed security check items by IoT devices based on this.

Fig. 1 IoT Device Security Certificate

**III. Conclusion**

In this paper, we propose a method of deriving more specific security authentication items of IoT equipment in IoT environment by analyzing the limitations of existing IoT security guidelines and requirements based on IoT features.

In the method proposed in this paper, it is easy to grasp the security requirements of IoT equipments separated by each field and performance at a glance. Utilizing the research method presented in this paper, it can be utilized as an index to evaluate the security of IoT equipment by the manufacturer who manufactures IoT equipment and the user who use it.

As a future research topic, we plan to practically apply it to IoT equipment currently being used by using the method proposed in this paper.

**Acknowledgment**

"This research was supported by the MIST(Ministry of Science and ICT), Korea, under the National Program for Excellence in SW supervised by the IITP(Institute for Information & communications Technology Promotion)"(2016-0-00022)

**References**

[1] Si-Jung Kim and Do-Eun Cho, "Technology Trends for IOT Security," The Korea Contents Association Review, Vol. 13, No. 1, pp. 31~35, March 2015

1. Yong-Sik Jung and Jae-Sang Cha , "IoT Standard for device security check", The Journal of The Korean Institute of Communication Sciences, Vol. 34, No. 2, pp. 27~33, Jan 2017.
2. Hyung-Jin Mun, Gwang-Houn Choi and Yooncheol Hwang, “Countermeasure to Underlying Security Threats in IoT communication”, Vol. 6, No 2,pp. 37-44, June 2016.
3. Dong-Hyuk Lee and Nam-Je Park, "IoT Product Security Certification and Security Maintenance Plan", The Journal of The Korean Institute of Communication Sciences, Vol. 33, No. 12, pp. 28~34, November 2016.
4. IoT Security Alliance,“IoT Common Security Guide”, 2016