Security Considerations for Secure and Trustworthy Smart Home System in the IoT Environment

Jin-Hee Han, YongSung Jeon
Mobile Security Research Section
Cyber Security System Research Department
Electronics and Telecommunications Research Institute
Daejeon, Republic of Korea
e-mail: {hanjh, ysjeon}@etri.re.kr

JeongNyeo Kim
Cyber Security System Research Department
Cyber Security Research Division
Electronics and Telecommunications Research Institute
Daejeon, Republic of Korea
e-mail: jnkim@etri.re.kr

***Abstract*— Recently, smart home appliances and wearable devices have been developed through many companies. Most devices can be interacted with various sensors, have communication function to connect the internet by themselves. Those devices will provide a wide range of services to users through a mutual exchange of information. However, due to the nature of the IoT environment, the appropriate security functions for secure and trustworthy smart home service should be applied extensively because the security threats will be increased and impact of security threats is likely to be expanded. Therefore, in this paper, we describe specifically the security requirements of the components that make up the smart home system.**

***Keywords*— security, requirements, smart home system, IoT**

I. INTRODUCTION

Along with the growth of the smartphone, a large number of embedded devices have been developed to provide various services. Especially, the smart home, smart city, smart health care and smart car services have been receiving the spotlight throughout the society in recent years. For this reason, various sensors, small embedded devices and home appliances have been studied and developed continuously through several companies, universities and research institutions. And then they have been gradually intellectualized in order to provide smart services to the users [1][2].

However, an increment phenomenon of a user privacy data leakage and security vulnerability should not be overlooked in the IoT (Internet of Things) environment. A number of significant research needs, including security and privacy, for future IoT systems is described in [3] and the general definitions for the main security aspects within the IoT domain was depicted in [4]. If the service infrastructure is designed without considering predictable security flaws, user privacy data leakage, social infrastructure paralysis, and economic losses as well as a risk of human life as a severe cases can be occurred by the attacks of outsiders with malicious purpose.

To establish the service infrastructure that provides security features, it is necessary to define the appropriate security features required for each component that make up the service infrastructure [5]. In addition, various services require a different security issue that is suitable for individual characteristics [6]. For example, data (e.g. user's privacy data) security is essential to the intelligent transportation service and intelligent medical service, while authentication scheme is more important in the case of smart city and intelligent farm services. Therefore, we should carefully scrutinize the security requirements and necessity for a specific IoT services.

In this paper we define the security requirements for the smart home service which is emerged as a hot item of major IT companies, and specifically describes a security feature for each component of smart home system in the IoT environment.

The rest of this paper is organized as follows. In Section II, we give some overview of the smart home system. Section III describes the security requirements of the smart home service. Section IV addresses the security functions for the components (smart home device, home gateway, and home server) that make up the smart home system. Finally, Section V concludes this paper with a summary and future works.

II. SMART HOME SYSTEM

In general, smart home system can be configured as shown in Figure 1. As shown in Figure 1, smart home system consists of largely three components, home server, home gateway, and smart home devices. First, the home server provides storage, integration and distribution function of the information collected from various media in the home as a kind of computer device.

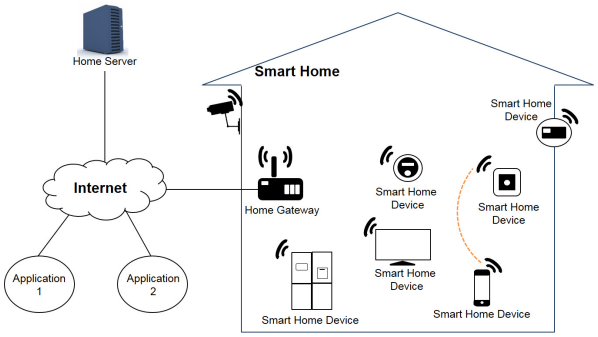

Figure 1. Smart Home System

Next, the home gateway performs a relay function, or inter-connect function between the subscriber access network and a

wired/wireless home network. Finally, smart home devices can intelligently provide the information exchange function between the devices, and external internet access function [7].

III. SECURITY REQUIREMENTS OF THE SMART HOME SERVICE

Components constituting the smart home system are likely to be exposed highly to a variety of threats from inside or outside because most of them have internet connectivity, unlike the existing home network environment. To cope with the security threats such as malware infections, unauthorized user access, important information disclosure, we should apply the security functions according to the component-specific characteristics of a smart home system.

Table 1 shows the security requirements that are required to provide a secure and trustworthy smart home service. As seen in Table 1 below, we classify the security requirements based on the integrity, confidentiality, availability viewpoint and describe the details.

TABLE I. SECURITY REQUIREMENTS FOR THE SMART HOME SERVICE

category	Security Requirements
Confidentiality	User's privacy data delivered during the smart home devices inter-communication, and the key information used for the encryption algorithm should be managed securely to prevent potential exposure to the outside.
	In case sending the data generated from the smart home device into another device, the transferring data should be converted into cipher text form.
	To prevent the replication and modification by an outsider, Identification information of a smart home device should manage securely.
	Smart home devices should provide a highly secure password setting function and periodic password change functionality.
	Home Gateway must strengthen security through a robust and complex password setting.
Integrity	To maintain the reliability and safety of the smart home device, unauthorized device or user access should not be allowed.
	User's privacy data delivered during the smart home devices inter-communication, and the key information used for the encryption algorithm should not be forged or tampered.
	In case sending the data generated from the smart home device into the outside or another device, data integrity should be provided.
	Through the mutual authentication between devices constituting a smart home service, reliable communication environment must be configured.
Availablity	To respond to security threats such as cyber-attacks and hacking, external attack detection capabilities must be equipped.
	The security features for software update of smart home device must be provided.
	Device security policy settings features that reflect a variety of device characteristics and specifications must be considered.
	In order to grasp a physical status (e.g. theft, loss, add, disposal) of smart home devices correctly, device management system should be provided.
	Periodic status monitoring of a smart home device, and unnecessary remote access blocking should be provided. In addition, if abnormal operation is generated from smart home devices, appropriate response and event history about abnormal behavior should be accompanied.

Security requirements summarized in Table 1 assume some limitations. First, smart home devices (e.g., smart phone, etc.) that can be connected to the internet via a mobile communication network are limited within the case connected to the internet via the home gateway. Also, the security functions of the home server and the home gateway can be performed by any one of the two objects, and it is possible to implement home gateway and home server as a single device in accordance with the system implementation method.

IV. SECURITY FUNCTIONS FOR THE SMART HOME SYSTEM COMPONENTS

Security functions for the smart home system components (i.e. home server, home gateway, and smart home device) are listed in Table 2. The security functions described in Table 2 are the basic security functions to be preferentially applied in the smart home system.

Additionally, we do not consider network security functions and the security features related to a specific service, and also a remote service environment in this paper.

A. Confidentiality

In case of data communication between devices as well as sending data to the outside, the transferring data should be converted into cipher text form. That is, the data confidentiality should be provided.

And, we recommend to use hardware security module to enhance security of device which has a specification capable of providing a security feature by mounting a hardware security module. For example, device identification information can be managed securely by using the hardware security module.

TABLE II. SECURITY FUNCTIONS FOR THE SMART HOME SYSTEM

Component / Security Functions	smart home device	home gateway	home server
Data Confidentiality	√	√	√
Management of Device identification information	√	√	
Strong Password Settings	√	√	
Access Contol	√	√	
Secure Storage of Important Data	√	√	√
Data Integrity	√	√	√
Device-to-Device Authentication	√	√	
External Attack Detection	√	√	
Software Secure Update	√	√	
Security Policy Settings		√	√
Device Management		√	√
Device Control		√	√

To set a strong password, it is preferable to use a password of more than 8 figures composed of numbers, letters, and special characters. In addition, we recommend to use a more secure algorithm than 128 bit encryption algorithm to enhance security.

B. *Integrity*

Low-capacity smart home devices (e.g., tiny sensors and actuators, etc.) and a home server can use the access control function and mutual authentication function provided by the home gateway.

In consideration of the device specification, the critical data (user's privacy data, key information, and access control/ authentication data, etc.) should be stored securely using a hardware security module.

Besides, data integrity should be provided to prevent data from being changed.

C. *Availibility*

To defend cyber-attacks including hacking from the outside, the firmware integrity verification feature should be provided. Also, we recommend the integrity verification function having fast execution speed and ease of implementation for a low-capacity smart device.

In case a secure software update, verification of the software update file and software update server should be provided.

According to the respective characteristics and specifications of the device, we should grant a different security level for each device. And also, suitable security functions such as access control, authentication and encryption algorithm which are applicable to each security level should be provided as a security policy setting function.

V. Conclusions and Future Works

Since a user privacy data leakage, social infrastructure paralysis, and economic losses as well as a risk of human life can be occurred in the IoT environment, we have defined the security requirements for the smart home service which is emerged as a hot item of major IT companies.

In this paper, we specifically proposed the smart home system security requirements reflecting the IoT environmental characteristics. And, the security functions of the components that make up the smart home system was classified and defined according to confidentiality, integrity, and availability.

However, since we consider only the basic security functions for the smart home system, we will analyze additional security functions which are against the security vulnerabilities and the security flaws caused by device-to-device infection as a future work.

In addition, network security functions and the security features related to a specific service (i.e., smart metering service, smart health service, etc.), and also a remote service in the smart home will be defined in the near future.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) [No.R-20150518-001267, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices]

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things: A vision, architectural element, and future directions,” ELSEVIER, Future Gener. Computet. Syst., vol. 29, issue 7, February 2013, pp. 1645-1660

[2] M. Newlin Rajkumar, C. Chatrapathi, and V. Venkatesakumar, “Internet of Things: A vision, technical issues, applications and security,” IPASJ International Journal of Computer Science, vol. 2, issue 8, August 2014, pp. 20-27.

[3] John A. Stankovic, “Research Directions for the Internet of Things,”, IEEE INTERNET OF THINGS JOURNAL, vol. 1, no. 1, February 2014, pp. 3-9.

[4] T. Heer, O. Garcia-Morchon, R. Hummen, S. Keoh, S. Kumar, and K. Wehrle, “Security Challenges in the IP-based Internet of Things,” Wireless Personal Communications Journal, vol. 61, issue 3, September 2011, pp. 527-542.

[5] S. Sicari, A. Rizzardi, L.A. Grieco, and L.A. Grieco, “Security, privacy and trust in Internet of Things: The road ahead,” ELSEVIER, Computer Networks, vol. 76, January 2015, pp. 146–164

[6] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, “A systemic approach for IoT security,” IEEE International Conference on Distributed Computing in Sensor Systems, May 2013, pp. 351-355.

[7] ITU-T X.1111, ‘Framework of security technologies for home network’, February 2007.