Abstract

Smart Home, also known as Home IoT, refers to the product, service and solution remotely monitoring, controlling and operating domestic devices through the connection to the wireless network with mobile phones and computers. Smart Home has been developed into diverse versions, however its security still owns vulnerability in its device, network and privacy. Considering Smart Home security employs Public network, thus it is relatively more vulnerable than the ones, such as Smart Factory with Private network. Smart Home devised for convenience and safety of lifestyles may result in a disaster in private lives, if its security vulnerability is not resolved. The thesis examines past security threat cases in Smart Home environment, analyzes them in three different aspects – device, network and privacy – then would propose a counter-measure against the threats.

[Keywords] IoT, Smart Home, Hacking, CCTV, Security

1. Introduction

On June 2015, an Internet website exposing 9,187 CCTV videos of 117 countries throughout the world was captured. Among the hacked CCTVs, 344 are installed in South Korea – on public streets, pathways around housing, significant government facilities, tuition centers, hospitals, offices and households. People, who know the website, could monitor the real-time CCTV videos everywhere in the world, and even could record and remotely control them[1]. Furthermore, household electricity charge had become 0 due to hacking on apartment management system of a metropolitan apartment, and another apartment doors had been disabled by the Internet malfunctioning[2]. Picture 1 is the petition content in National Petition Board of the Blue House on February 2019.

Thanks to the advancement of information and communication, and development of connectable devices to the network, development and distribution of distribution of IoT and Smart Home have been accelerated. From domestic electronic devices to security units, and heating or lighting system, various connectable devices to the Internet are devised, thus Smart Home is closely and specifically adhered to daily lives. Smart Home is domestically utilized – the most privately linked to a personal lifestyle – and is continuously being advanced, generating positive influences, however, its security is still vulnerable, and the users are exposed to diverse device, network and privacy threats[3]. If the security vulnerabilities of Smart Home, devised for convenience, life quality increase and safety, are not solved, then a huge disaster may be foreseen. As significance of privacy and safety of Smart Home are being highly raised, the thesis would analyze the security threats and suggest a responsive measure. The thesis consists as followings. Chapter 2 illustrates IoT and Smart Home, then observes Smart Home security threat cases. Chapter 3 analyzes Smart Home threats into device,
network and privacy aspects. Chapter 4 proposes a responsive measure against the threats, then the chapter 5 draws a conclusion.

**Figure 1.** Petition of national.

---

2. Relevant Research

2.1. IOT and smart home

IOT (Internet of Things) is a future Internet, and is an interoperable communication protocol with both physical and virtual identifier[4]. IOT, based on existing wireless communication, is an advanced model over the Internet or the mobile Internet, exchanges data without a human intervention, and processes information. Having no reliance on human control, but exchanging data among things, both Ubiquitous and M2M (Machine to Machine) are similar, however, M2M focuses on communication among things and humans. Therefore, IoT, having the notion of M2M as a basis, has developed into a concept to interoperate with things and all data in both physical and virtual world, by broadening the area into the Internet[4]. Areas of IOT application has expanded from wearable devices, attaching on a body or putting on a watch on the wrist, to home appliances, cooperative system, smart car, smart home and smart city – that is, from micro to macro environment[5].

3 major technologies applied in IoT is sensing, acquiring data from things and surrounding environment, wire or wireless communication and network infrastructure, supporting the connection between things and the Internet, and service interface, converging different technologies to manufacture and process data in accordance with adequacy of each service field and form[3]. <Table 1> is Service case of IOT[6].

Smart Home, also known as Home IOT, refers to product, service and solution which household domestic devices can remotely be monitored, controlled and operated by mobile devices or PC through an Internet interlinks[7]. Smart Home deals with various fields and its boundary has been broadened. Households with Smart Home services integrated home appliances, including TV, air conditioner and refrigerator, energy consumption units, such as water, electricity and cooling or heating, and security devices, - security lock, for example - into a single network, thus its monitoring, control and operation can be performed with no time or spatial restriction[7].

<table>
<thead>
<tr>
<th>Field</th>
<th>Service content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>Intellectual integration service of distributed generators to balance adequate consumption and demand, as well as providing data to power distribution company and customers, by constant measurement on new renewable energy, electrical grid, and electricity and energy consumption.</td>
</tr>
<tr>
<td>Transportation</td>
<td>Application technology to provide innovative service managing different transportation and their system with better safety and convenience by users.</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Real-time integrated processing system reforming and assembling required data in all-process for higher usefulness and application.</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Medical</td>
<td>Establishment of public and personal medical system to improve accessibility of patients and medical teams to medical services via advanced application devices (mobile/smart device, sensor and actuator).</td>
</tr>
<tr>
<td>Public</td>
<td>Establishment of real-time information system to offer higher level of public service and data for civil safety.</td>
</tr>
<tr>
<td>Customer service</td>
<td>Provision of personal customized application service which can interoperate private life and technologies from purchase to entertainment.</td>
</tr>
<tr>
<td>Smart home</td>
<td>Application system relevant to buildings, which their lighting, heating and home appliances can remotely be controlled by smart-phones and mobile devices.</td>
</tr>
<tr>
<td>Finance</td>
<td>Intellectual integrates system that is applicable to various finance markets such as banking, insurance, real estate and loan.</td>
</tr>
</tbody>
</table>

1.2. Smart home security threat cases

Smart Home security, utilizing Public network, is respectively more vulnerable to threats than Smart Factory, using Private network. Followings are Smart Home security threat cases.

Figure 2. Smart home service.

1.2.1. Violation of iron and electric kettle case

An iron and an electric kettle made in China with a spy microchip installed were identified in Russia. Once the device is linked to the wireless network, malignant codes and span mails can be disseminated, and private information collected through tapping may be transmitted via the network. The number of the units identified reached over 30 and would be higher considering unidentified ones. If zombie PCs are produced via malignant codes distributed by the units, the PCs can be utilized for large-scale hacking attacks[3][6].

1.2.2. Violation of vulnerability abuse of thingbots

Thingsbots are the Smart TV, refrigerator and device that are linked to the Internet used for phishing and spam mail transmission due to hacking[8]. In 2016, a large-scale DDoS attack was committed to over 1200 US major agencies, including Twitter, Netflix and The New York Times. Thus, the websites had been disabled. The attacker sent the Mirai malignant code through Thingbots, the code infected IoT devices with their initial ID/PW unchanged by acquiring the administrator access[6][8][9].

1.2.3. Violation of monitor camera case
According to BBC in the United Kingdom, an obscene sound was output from a household monitoring camera designed for toddlers in Texas, the United States, and this was a case of vulnerability abuse of FOSCAM product to produce obscene noise. The case was a violation case of abusing firmware and software weaknesses discovered[6].

1.2.4. Violation of home appliance case

Referring to Proofpoint, a US security company, since 2013 to the early 2014, 750 thousands of phishing and spam mail were transmitted via IoT home appliances such as home networking router, smart TV and refrigerator throughout the world. Attackers abused the mailing function installed in IoT home appliances connected to the Internet and sent phishing and malicious mails. In addition, smart TV was hacked and live-broadcasted inside of an entire household through a camera installed in its home appliance. There were other cases, which order number of TV home shopping has randomly been changed, and collecting and changing significant data such as image, video, sound, credit card number, bank account number and location data — leading to further damages[10].

1.2.5. Privacy infringement case via CCTV

Over 73000 personal CCTVs throughout the world were hacked and broadcasted in real-time. Over 6000 CCTVs hacked were placed in South Korea, which was found to be the second largest in the number of victims in the world. It was, at last, discovered to be an intention of the website operator to emphasize the importance of security, however, the case proved that not only restaurant, café and streets, but also personal privacy may be looked through if one wishes to[6].

2. Smart Home Security Threat

2.1. Device security threat

Attackers disguise unauthorized device into an authorized one, thus can input malignant code into wireless network and counterfeit or falsify data tapped from authorized devices. Smart device with malignant code becomes a zombie device, generating DDoS attack, then other smart devices linked to the same home network with the PC get infected, hence secondary damage occurs. Counterfeiting or falsifying data from authorized device may enable further counterfeiting of device authorization process and outcome, thus inadequate service may be practiced. Furthermore, by tapping data between devices via wireless network, an attacker can capture important data from Smart Home.

2.2. Network security threat

Smart Home, utilizing wireless network, controls home appliances, thus should establish a password to prevent risk of its data being tapped. IP Spoofing is a method to attack system to disguise unauthorized user as an authorized one by pirating the data origin, transferred from internal to external network, threatening Confidentiality of data. The Internet fundamentally is operated based on a client/server structure. User accesses to the central server and received data, the data set is not entirely transferred at once, but by small units segmented, so-called packet. The segregated packets go through several devices till its reception to the user, and the devices may tap and counterfeit the packet content. This is called Man-in-the-Middle attack. Attacker located in-between smart TV and web-server may try unauthorized reading, data counterfeit and falsification attacks by approaching to the data being transmitted.

2.3. Private information-related security threat

As convenience offered by Smart Home, controlling home appliances connected to the wireless Internet, gets enhanced, concerns on privacy violation by hacking and information leakage are growing. As IoT develops, the number of smart devices to collect personal data increased, thus considering the large amount of accumulated private information and its broad application in many directions, growing demand in privacy protection is inevitable[11]. Home appliances for Smart Home collect and store situational data(any human movement inside the housing, room temperature, humidity, lighting
brightness, CCTV, gas valve detection, electricity consumption, absence state and list of home appliances) inside households via attached sensors. Likewise, all devices used for Smart Home can be exposed to security threats – personal information leakage and privacy infringement.

3. Responsive Measure against Smart Home Security Threat

3.1. Measure against device vulnerability

Security issues in devices are access by an unauthorized device, data counterfeit and falsification, and personal information leakage. To cope with such device security threats, first, only authorized device must be allowed for an access to Smart Home network. Cross-certification is executed with all devices used for Smart Home, all users using the devices go through a user authentication. Second, prevent any device access with its integrity damaged via integrity check. Integrity of all data transmitted and received between devices are confirmed by applying one-way hash function. Third, by using the intrusion detection technique for Smart Home service, any device attempting an irregular access is forcibly blocked out. Monitoring Smart Home, detection for any device with irregular action is performed. Fourth, a password is set for all devices as a basic step, then the established password is periodically changed. Fifth, all data transferred to the network is encrypted based on a public-key cryptosystem.

3.2. Measure to ensure network security

To ensure security between networks in Smart Home, devices connected to the network should be trustworthy to each other, tapping by a 3rd party should be prevented during their data transmission, and even if they are exposed to tapping attacks, the attacker must not be able to know the tapped contents. To deal with the network security threats, first, for non-repudiation of data transmission-reception among devices, digital signature or electronic envelop methods are used. Second, for integrity of data being transmitted, one-way hash function is applied, and practice symmetric-key algorithm or public-key cryptosystem to preserve the data confidentiality. To safely perform data encryption, different password key is utilized in each session, and any key, considered significant for the encryption, is distributed in advance and stored in devices.

3.3. Measure for private information protection

Measure to protect personal information stored in Smart Home device as followings. First, authority to access to Smart Home devices must be restricted. By employing various user authentication techniques based on IP, ID and biometrics to users attempting an access to devices, only authorized users can access to the devices. Second, all devices connected to Smart Home should utilize a password. Password is the most basic way to protect privacy. The password should periodically be changed, complicatedly structured, thus its stability must be enhanced. Third, personal information stored in devices should be stored in compliance with public-key cryptosystem. If attackers cannot decrypt the acquired private information from devices, it the data becomes useless. Fourth, access history of users to devices should be kept and managed. Storing and managing the history is to identify any access or action by attackers, attempting an illegal access to devices via counterfeiting as users.

4. Conclusion

Due to development of information and communications and commercialization of smart devices, Smart Home technology and service, using IoT, has more rapidly been developed and distributed. Smart Home enables a wide range of devices – from home appliances to security devices, heating and lighting system – be connected to the Internet, thus human life quality has been enhanced. However, Smart Home security technology is still insufficient, hence individuals and households using Smart Home are being exposed to security threats in many aspects, including device, network and privacy infringement. The thesis observed the actual security threat cases, in terms of Smart Home uses, analyzed any probable security threats in Smart Home.
environment into device, network and private information prevention categories, then suggested their sequent responsive measures.

First, to cope with device security threats, 1. Cross-certification to devices. 2. Blocking any device with damaged integrity. 3. Blocking any irregular access to devices. 4. Set a password. 5. Encryption of all data. are proposed.

Second, to deal with network security threats, 1. Application of digital signature and electronic envelop for non-repudiation of data transmission. 2. Application of one-way hash function to protect data integrity and maintain data confidentiality by using encrypted data. 3. Change the key for encryption at every session, and distribution of significant key in advance. are suggested.

Lastly, to protect private information, 1. Restrict authorities to access device. 2. Manage the password. 3. Full encryption of all data stored in devices. 4. Manage and store all device access history. are proposed.

Smart Home, devised for convenience and constantly being advanced over time, has become an important part of daily lives of human beings. In the light of Smart Home security threats, affecting individuals and households, security has become a necessity, not an option. To enjoy Smart Home and its convenience to the full extent, consistent investment and research on the security should be conducted.

5. References

5.1. Journal articles


5.2. Thesis degree


5.3. Additional references


Author
Lee Jae-young / Semyung University Assistant Processor
B.A. Semyung University
M.A. Semyung University
Ph.D. Chungbuk National University

Research field

Major career
- 2012~2016. Semyung University, Assistant Processor in Department of Liberal Education
- 2016~2019. Semyung University, Assistant Processor in School of Information & Communication Systems
- 2019~ present. Semyung University, Assistant Processor in Department of Liberal Education