Security Issues on Smarthome in IoT Environment

Seokung Yoon[1], Haeryong Park[1], and Hyeong Seon Yoo[2]

[1] Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa, 138-950, Seoul, Korea
[2] Inha University
100 Inharo, Nam-gu, Incheon, 402-751, Korea
{seokung,hrpark}@kisa.or.kr, hsyoo@inha.ac.kr

Abstract. Smarthome as one of IoT(Internet of Things) services is growing more and more interested. Due to the development of mobile network, proliferation of smartphones and increasing of interest for personal safety, many enterprises enter the smartphone market. However, incidents could happen because they provide their services without considering security. This paper analyzes security vulnerabilities of smarthome and proposes countermeasures.

Keywords: Smarthome, Security, IoT.

1 Introduction

Smarthome means smart life environment based on human that enables the convenience for people, promotion of welfare, and safety of life [1]. Due to rapid development of IT technology and diffusion of broadband Internet connection, digital devices could get IP addresses to communicate each others. As many service providers launch various smarthome based services, smarhome becomes one of representative services in IoT (Internet of Things). Smarthome services market from under $2 billion worldwide in 2012 to $10.9 billion by 2017 according to a new report from NextMarket Insights [2].

In smarthome environment, all home devices are connected via Internet. By doing so, many supplementary services are provided and they make our living much more convenient. However the more home devices are linked, the more security flaws are revealed. There exists only few security flaws when home devices are operated independently. Nowadays home devices are accessible via Internet anywhere and at any time, many security experts warned they could be used as attacking tool. Recently there was an example that smart TVs and refrigerators infected by malicious codes sent the bulk of spam mails. Because smarthome devices are tightly coupled with real life, incidents could lead to extensive damage. Therefore it is important to analyze the possible security vulnerabilities and prepare countermeasures in smarthome.

We briefly look into smarthome in Section 2. Section 3 analyzes the possible security attack scenarios and proposes countermeasures. Lastly, Section 4 discusses the study result.

James J. (Jong Hyuk) Park et al. (eds.), *Computer Science and Its Applications*,
Lecture Notes in Electrical Engineering 330, DOI: 10.1007/978-3-662-45402-2_97

2 Smarthome

According to the development of smart devices and network technology, all devices in the home are connected each other through Internet. As appetite for safety is expected to pick up, many companies are getting into the smarthome market. In korea, three major carriers (KT, LG, SKT) already launched value-added services based on smarthome. Security companies and manufacturers also provided smarthome services in their own way. Because most companies do not consider the security in their services, they have been exposed to the security vulnerabilities.

Smarthome consists of 4 parts: smart devices, home network. home gateway and service platform as shown in Fig. 1. In smarthome system, many devices are connected and shared their information via home network. Therefore, there exists home gateway to control the information flows among smart devices and connect external network. Service platform is normally located in service providers, it could be used for delivering various services to home devices.

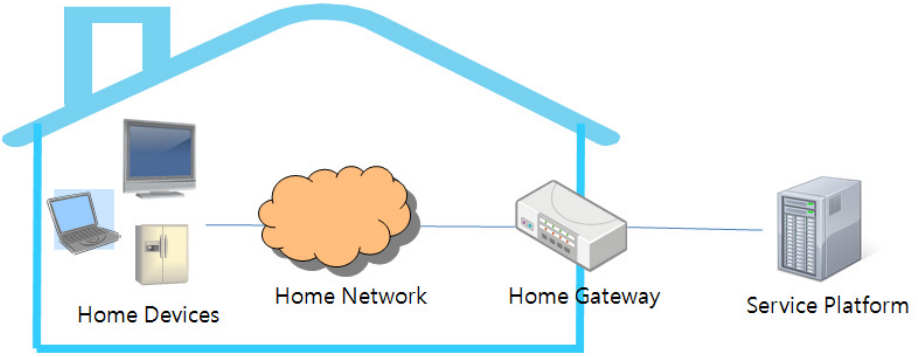

Fig. 1. Constitution of smarthome

As mentioned previously, smarthome services are vulnerable to cyber attack because most service provider don't consider the security in the initial stage. According to the recent report, Hackers have successfully compromised smart televisions, routers, and even smart refrigerators to carry out a series of spam email attacks [3]. The possible security threats in smarthome are eavesdropping, DDoS (Distributed Denial of Service), information leakage, and so on [4-5]. These could be happened from smarthome components. Smart devices and home gateway are threatened with malicious codes and home network also under threat by unauthorized access. Contents from service platform are exposed to eavesdropping or falsification. The possible security threats happened in smarthome are shown in Fig. 2.

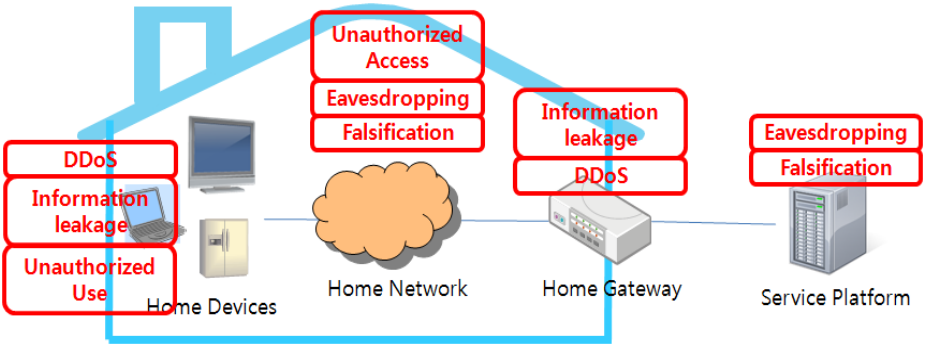

Fig. 2. Possbile security threats in smarthome

3 Attack Scenarios and Countermeasures

In section 2, we briefly looked into possible security threats in smarthome. Becuase smarthome system is very closely tied everyone's daily lives, it is dangerous for people in case of cyber incidents. In this section, we describe some attack scenarios and propose countermeasures.

3.1 Trespass

When the smart doorlock would be infected by malicious codes or hacked by security flaws, attacker could trespass on his/her home without destroying a doorway as shown in Fig. 3. This threat could cause the loss of life and property. To protect this attack, password of smart devices could change frequently and hard to infer. Authentication and access control also have to be applied.

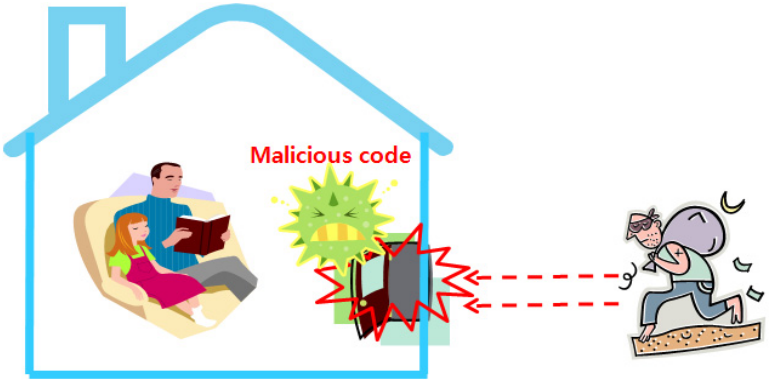

Fig. 3. An example of trespass by hacking a doorlock

3.2 Monitoring and Personal Information Leakage

One of the purposes to use smarthome is safety. Therefore, there are many sensors for fire watch, housebreaking, baby monitoring, etc. If these are hacked by malicious codes, attackers could monitor inside the home around the clock as shown in Fig. 4. Even if sensors are not infected directly, they could be under control when other devices were infected. By doing this, they could get sensitive personal information and trespass when empty. To protect this attack, data encryption between sensors and gateway has to be applied. It is also important to use authentication for detecting and blocking unauthorized devices and adopt anti-virus product.

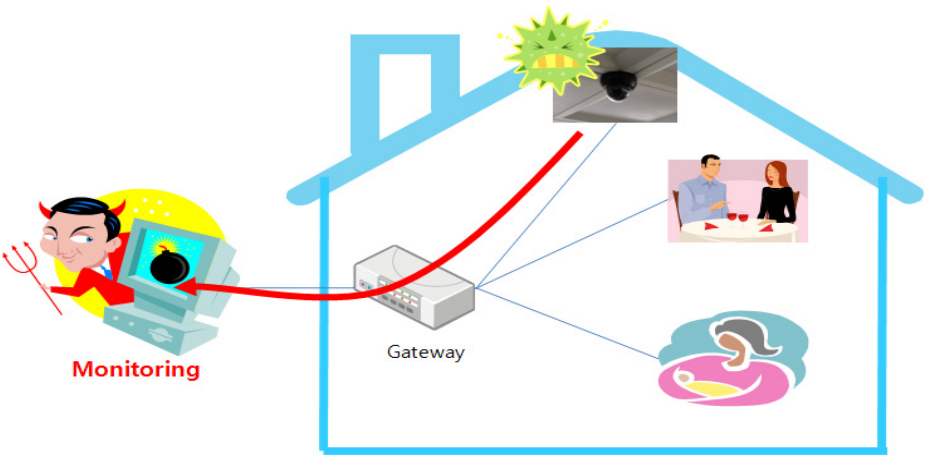

Fig. 4. An example of monitoring

3.3 DoS/DDoS

Attackers access smarthome network illegally and send messages such as RTS(Request to Send)/CTS(Clear to Send) to smart devices in bulk. They also infect a target device using malicious codes and perform dos attack to a target device or other devices in smarthome network as shown in Fig. 5. Smart devices are not working because of depleting their resources when they receive such attack messages. To protect this attack, it is important to use authentication for detecting and blocking unauthorized devices. Security techniques such as rate limiting, null0 routing have be applied to home gateway.

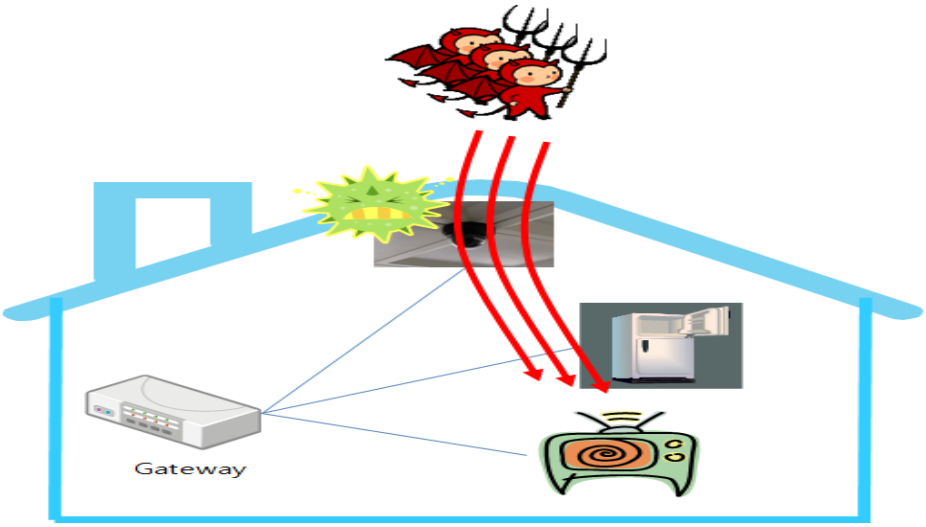

Fig. 5. An example of DoS/DDoS

3.4 Falsification

When smart devices communicate application server, attacker could gather packets by manipulating routing table in gateway as shown in Fig. 6. Even if SSL(Secure Socket Layer) technique is applied, attackers could detour by forged certificate. By doing this, they could falsify the contents or leak confidential information. To protect this attack, SSL technique with proper authentication has to be applied to smarthome components. It is also important for blocking unauthorized devices to access smarthome network.

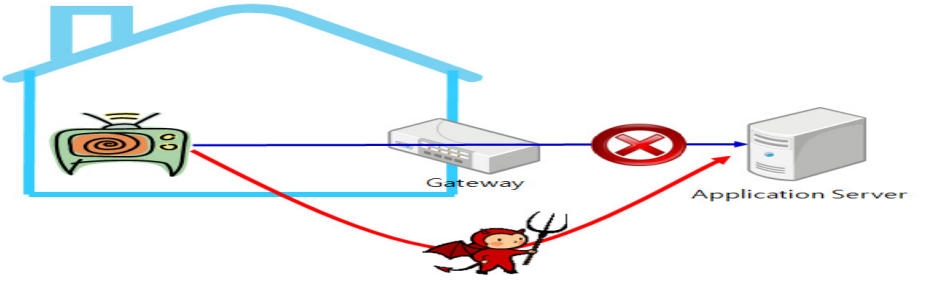

Fig. 6. An example of falsification

4 Conclusion

Smarthome as one of IoT(Internet of Things) services is growing more and more interested. Therefore it is important to consider security aspects before it is activated.

This paper analyzes the possible attack scenarios in smarthome and proposes countermeasures. The use of complicated passwords, various security functions, information security awareness raising have to be applied when providing smarhome services. Proposed countermeasures are carefully reviewed and adopted by security policy. With this study, companies could provide various smarthome application safely and people could use them at easy.

Acknowledgments. This research was supported by the ICT Standardization program of MISP(The Ministry of Science, ICT & Future Planning)

References

1. Korea Association of Smart Home, http://www.kashi.or.kr/html/smarthome_001.html
2. NextMarket Insights, http://nextmarket.co/products/smarthome
3. Techlicious blog, http://www.techlicious.com/blog/report-smart-home-appliances-hacked-to-send-spam/
4. Erzen, R.: Review of main security threats in Smart Home networks (2012)
5. Information-technology Promotion Agency (Japan), 2010 Smart Home Appliance Security (2011)