Journal of Engineering and Applied Sciences 13 (7): 1804-1812, 2018
ISSN: 1816-949X

Practical Security Considerations of Smart Home via. Vulnerability and Threat Analysis

[1]Sungbum Ahn and [2]Youngsook Lee
[1]Department of Information Security Engineering, University of Science and Technology, Daejeon, Korea
[2]Department of Cyber Security, Howon University, Gunsan, Korea

Abstract: Due to recent development of the "Internet of Things" technology, varieties of smart home industries have entered golden age. Smart home is closely linked to our daily life and therefore, easily exposed to security threats. A smart home is composed of three main components: smart device, network and application. In this study, we analyzed vulnerabilities and security threats regarding component of smart home. Additionally, we suggested applicable security consideration depending on qualitative threat analysis in accordance with possibilities of potential security threats and risk.

Key words: Smart home, vulnerability, security threat, IoT, qualitative, analyzed

INTRODUCTION

Due to the recent development of the "Internet of Things" technology, smart devices are widely used. The demands for smart home services, not restrained by both time and space are exponentially growing. Which are developed with the fusion of existing appliance and ICT (Information and Communications Technologies). Smart home has evolved into a technology that can be provided customized services to meet user's requirements. It adds a variety of sensors and ICT to existing home networks.

Smart home services always have security threats (Harper, 2006). Due to the fact that they are closely associated with Personal information and daily life. Security experts and security companies announced smart home vulnerabilities as a serious problem. As a result, interest in smart home security is increasing.

Globally, a variety of smart home industries have entered golden age. Many companies offer various services to users. To use smart home services safely, users have to follow the safety rules and utilize security solutions that were provided by default. However, user's security awareness is still sketchy and there are no guidelines for smart home services.

MATERIALS AND METHODS

Schema of smart home: Recently, various home appliances are connected to the network. As a result, smart home is emerging as a keyword of smart ecosystem. In particular as the experience and value of users who have already accumulated through smartphones which were personal media devices, began to expand to other devices, the subject of innovation is shifting from smartphones to smart homes. Therefore, the smart home market is growing rapidly, and new services are emerging day by day. In this study, we described the definition of smart home and service type. Additionally, we analyzed the smart home market recent tendency in the globe.

Definition and features of smart home: Smart home is defined as any housing with the electronic home appliances such as TV, air conditioner, radiator, security camera etc., that are connected with each other through the network and exchange date internally. Figure 1 shows general layout of smart home system.

Smart home is composed of the system that can be operated both the inside and outside of the house depending on the user's needs. Throughout the smart home devices, user can control the temperature of the air conditioner and radiator. Also, user can watch the installed security camera in real-time when intruders are detected. Housing installed with such smart home service can be managed freely regardless of user's situation. Additionally, they are more convenient, secure, energy efficient and more easily accessible.

Smart home is composed of the following; a home gateway, a user terminal and smart devices (Yoon *et al*., 2015). Home gateway is a device that allows an access a public communication network for communication among networks in the home where installed smart home services. Home gateway is a device that grants an access to a public communication network in order to ensure inter network communication. User terminal has the function of managing and controlling the smart home devices anytime, anywhere. By using the portable devices such as smart phone, Tablet PC. Smart home devices offer convenience to house holders.

Corresponding Author: Youngsook Lee, Department of Cyber Security, Howon University, Gunsan, Korea

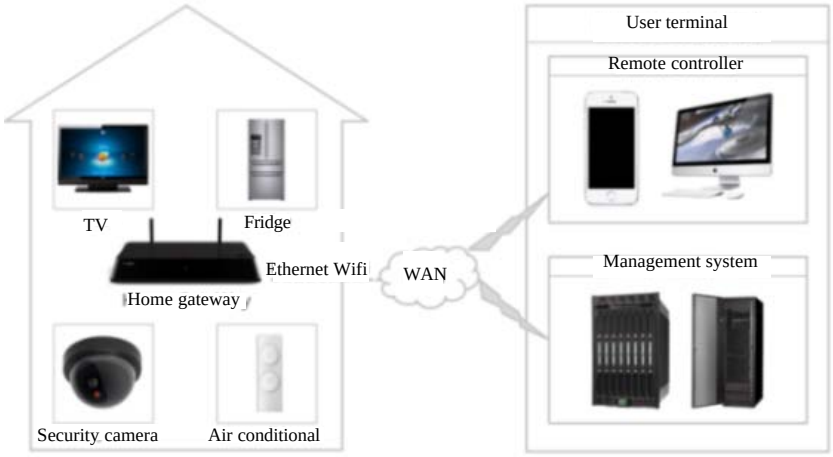

Fig. 1: Components of smart house system

Service type of smart home: Smart home services started when the high-speed internet was widespread. Diverse services are emerging to reflect the demands of comfortable, safe and healthy life. We can classify the smart home services as smart convergence appliance, home automation, smart home security and home health care (Byun *et al*., 2012).

Smart convergence appliance: Smart convergence appliances can remotely check and control the operating status of home appliance connect to network. For example, when devices were out of action, it can understand the cause of any performance itself. Also, it can download firmware updates itself.

Energy management system: Energy management system refers to technology that can automate and remote control home appliance, bulbs, gas facilities in real-life through IT technology. In other word, it can control the housing facilities through connected control devices from outside of house. For example, it can shut off the gas valve by remote control from the outside of the house. Also, it can prevent fire and save energy waste as cut off the power of unnecessary. It can promote a pleasant residential environment by provide appropriate energy consumption for each season.

Home security: Home security refers to services that guarantees the security of the home by the fusion of physical security equipment with ICT (Information and Communications Technologies) technology. The biggest difference from the existing security equipment is that the service user can check and control the security situation inside and outside the house through the remote control device without restriction on the time and space. For example, various sensors installed at home can sense a heat change and motion detection. When an intruder is detected, smart home camera captures the pictures and send an alarm to user's smart phone.

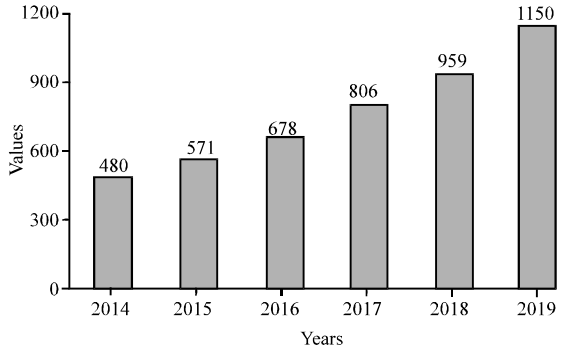

Fig. 2: The global market scale for smart home ($ billions)

Home healthcare: Home healthcare is the service that allows users to receive high quality health care constantly. Throughout the health care services, users can measure and analyze the health condition. Also, the users can receive remote medical services and health care services with measured information.

Smart home market tendency: Smart home has been spotlighted internationally due to the consumer's interests and demands. According to the market research enterprise "Strategy Analytics", the global market for smart home is expected to grow at a CAGR of 19% from $48 billion In 2014 to $115 billion by 2019. Figure 2 shows the global market scale for smart home (Ablondi, 2014).

Table 1: Features and key services of smart home in 3 Korean telecom industry

Variables	SKT	LG U+	KT
Plan	Launching 100 home IoT products	Launching 50 IoT products	Launching 30 IoT products
Feature	IoT open platform services	Various security and safety services	IoT health care focus on IPTV
Key	Control the appliances through the personal assistant platform	Security and safety services such as IoT door lock, gas tap	Check the amount of exercise and provide a customized meals

Especially, US and Western Europe are leading in developing smart home hardware, services and installation. The US market for Smart Home will exceed to grow at a CAGR of 15% from $24 billion in 2016 to $40 billion by 2020. Western Europe is expected to grow at a CAGR of 15% from $10 billion in 2016 to $19 billion by 2020. By 2020, nearly 30% of European homes will have at least one smart home systems.

USA: In the United States, detached house had the largest percentage of residential types. And the crime rate is high and public utility is expensive. To prevent possible issue. The demand for smart home services such as energy management system, security services, etc. are increasing. Therefore, US smart home market is focusing on the services to meet these services. In April of 2013, AT&T launched "Digital Life" home automation and security platform. Starting in 15 cities. Digital life works on a broadband basis using Z-wave technology. Using an open platform, it can be used on other companies' internet networks and offers free compatibility.

Germany: In 2011, digital storm launched "Digital Storm Smart Home". Unlikely US companies, they focus on a comfortable living environment. China: The Chinese smart home market which has the greatest potential in the world, is growing rapidly. According to market research enterprise "Strategy Analytics", The Chinese market for smart home is forecast to grow from 40.3 billion yuan in 2015 to 130 billion yuan in 2018 (7)

South Korea: The Korean telecom industry has stepped into the smart home market beyond the smart phone market. SK Telecom launched an open platform strategy to affiliate with various operators. It can be used in various products and services. LG U+ has the largest subscriber of smart home services in Korea. They currently offer 14 types services but they will expend to 50 different types services. KT which joined the smart home industry in Korea will gradually expend its business based on its subscribers of IPTV. Table 1 shows features and key services of smart home in 3 Korean telecom industry.

RESULTS AND DISCUSSION

Vulnerabilities and threat analysis of smart home: All kinds of security incidents happen due to the proliferation of IoT products and services including smart home. One must firstly internalize security from the design stage, establish a systematic cyber threat response system and the foundation of security for a secure smart home environment. Smart home consists of devices, networks and applications. Devices are appliances convergence with ICT technology. Network components are home server, communication protocol, etc. Lastly, applications can facilitate remote control and management. Applications can also be used on smart phone, Tablet PC and web. As mentioned, there are various factors to compose smart home. There are multitudinous vulnerabilities and security threats. In this chapter, we analyzed potential vulnerabilities and security threats in devices, networks and applications that are a components of smart home (Aloul *et al*., 2012).

Analysis vulnerabilities of smart home: Vulnerabilities that can occur in smart home components can vary greatly. If an attackers abuse these vulnerabilities, it could immediately lead to security infringement accident. Hence, these vulnerabilities should be carefully analyzed in order to create a way to ensure security. In this study, we analyzed vulnerabilities that can occur in smart home components. Table 2 shows possible vulnerabilities, V means vulnerability (Aloul *et al*., 2012; Grobauer *et al*., 2011; Botta *et al*., 2014; Raza *et al*., 2013).

User carelessness: Vulnerabilities related with the user carelessness frequently happened in smart home components. For example, there were physical destruction and loss of smart home devices. There are user's untrusted wireless networks connection and indiscriminate application installation and use. In addition to exploiting vulnerabilities related with smart home, there are vulnerabilities to attack using a social technologic attack.

Wireless network vulnerabilities: There are vulnerabilities related to wireless routers and APs installed in the home to use the smart home service. A malicious attacker who don't have an authority can invade in home wireless network due to a poor management. In addition, when an encryption on communication is not performed, it can lead to information leakage, session interception, data forged or falsified in network communication (Kavitha and Sridharan, 2010).

Unsecured protocols: The communication protocols used in IoT have existing protocols such as Wi-Fi, ZigBee, etc., and optimized protocols for IoT such as CoAP, MQTT, LoRa, BLE (Bluetooth Low Energy). Various communication protocols have sprung up everywhere as

Table 2: Possible vulnerabilities in smart home

Vulnerability	Description
V1; User carelessness	Installing and using untrusted applications
	Connecting to untrusted wireless networks
	Physical destruction, theft and loss
	Ignorance of social the technologic attack
V2; Wireless network vulnerability	Vulnerabilities of the web server, AP, wireless router etc. and insufficient administration
	Unused secure sockets layer
	Man in the middle attack
V3; Unsecured protocols	Vulnerabilities in various communication protocols
V4; execution error	Operations failure and malfunction due to an execution error
V5; Communication error	Malfunction between services due to communication
V6; Structural fault	Information leakage due to centralization of information
	Increased attack targets due to increased numer of networked devices limited performances
V7; Cloud server vulnerability	Unsecured interfaces and APIs
V8; Web application vulnerability	Web vulnerabilities in OWASP TOP 10

emerging IoT devices. Because protocols used in IoT services don't have standard, they have intrinsically various vulnerabilities. For example, DTLS used for security of CoAP protocol is too large in header and frame size, it may cause a speed delay and fragmentation attack as the loss probability increase (Raza *et al*., 2013).

Execution error: Execution error can cause unexpected system crashes or malfunction in devices, networks and applications of smart home. Malicious attacker can take the advantage of system disturbance, system paralysis, malfunction, etc. by executing malicious code. In case of malfunction due to an execution error, threats related with security such as unauthorized, etc. will occur (Aloul *et al*., 2012).

Communication error: Smart home services only came into action through network communication. When networks are unavailable because of an extreme weather condition or a system overload situation, it can cause a communication error. These communication errors expose vulnerabilities that can lead to malfunction such as abnormal termination of smart devices, arbitrary code execution, etc. (Zhang *et al*., 2014).

Structural fault: Unlike smart phone and tablet PC, smart home devices have structural fault that provide hardware capable of minimizing security function considering each role and design. In a smart home device using only simple communication, there are many restrictions on installing and using security software. So, it's easily exposed to security threats. Furthermore, security vulnerabilities will occur due to centralization of the devices in home wireless router (Zhang *et al*., 2014).

Cloud server vulnerability: Various methods for remotely controlling and managing the components of the home network through the home server have been suggested. Cloud-based home control/management, a way to connect devices across the internet to services within a network cloud, can be an effective way of managing resources efficiently. If the intelligent processing part requiring high performance power in control/management is performed in the service on the cloud, the complexity of the management software on the hometerminal can be reduced. While there are many benefits to using a home server with cloud services, there are vulnerabilities related to the use of unsecured Uis and APIs (Grobauer *et al*., 2011; Botta *et al*., 2014).

Web application vulnerability: Smart home services can be used not only on applications such as smart phones but also on the web. According to Symantec's research, in the smart home web application, vulnerabilities have been found in manager web pages such as XSS attack, path traversal, unlimited file uploading (remote code execution) and SQL injection included in OWASP TOP 10. If an unauthorized exploitation of smart home devices is conducted outside the home throughout the web application vulnerabilities, secondary damage is expected to occur. Table 3 shows vulnerabilities related with smart home in OWASP Top 10 (Wichers, 2013; Barcena and Wueest, 2015).

Analysis security threats of smart home: As smart home users increase and smart home devices become more diverse, there are more vulnerable areas and various security threats using vulnerabilities can occur. In this section, we analyzed security threats that can occur in the smart home components. And we conducted qualitative threat analysis in order to possibilities of potential security threats and risk Table 4 shows security threats we analyzed and T means Threats (Wichers, 2013; Zhang *et al*., 2014; Grobauer *et al*., 2011; Atamli and Martin, 2014; Wood and Stankovic, 2002; Botta *et al*., 2014).

Table 3: Vulnerabilities related with smart home in OWASP Top 10

Vulnerabilities	Description
Cross-Site Scripting(XSS)	XSS is an attack that exploits a design vulnerability in a web application and allows an attacker to inject malicious script into a web page. When the Injected malicious scripts are executed on user's computer, the user's cookie and session are extorted. After taking the attacker, the attacker can log in to the web application or control it arbitrarily with the privileges of the user
Path traversal	When user use theargument values forward from the web page as path in that state, it is an attack can that accesses the desired file by manipulating the corresponding argument value. The attacker access the directory that is not open to the user by entering the absolute path of ./or the file in the normal URL
Unlimited file uploading (remote code execution)	Unlimited file uploading attack is an attack in which an attacker uploads a malicious program to a user's system and executes it arbitrarily. This happens when a web application that allows uploading of attachments allows web programs (PHP, JSP, ASP, etc.,) that can execute internal commands. If uploaded malicious program is executed, attackers can remotely control the web application
SQL injection	This is an attack form where SQL is forcefully inserted into web application to cause an unexpected commands or carry out an unapproved identification. Additionally, it can be used to gain a privilege for the attackers to access the data to leak and modulate it

Table 4: Security threats in smart home

Threats	Description	Vulnerabilities
T1; Information leakage	The smart home information can be obtained through the wireless network	V1, V2
	Personal information can be leaked through the malicious code-infected devices	V3, V6 V7, V8
T2; Data forgery alteration	Attackers can intercept the data and then forge and alternate the data	V1, V2 V3, V7, V8
T3; Malfunction	Malfunction of smart devices can occur due to the user's mistake, mechanical problems and attacks	V1, V4
	Malfunction of smart home management devices can occur	V5
T4; Malware	Malfunction can occur due to communication error Malicious code can be transferred	
	Can be used as a spam and denial of service resource Malware can execute the arbitrary code	V1, V2
T5; Attack using firmware update	If the malicious firmware is updated, the control authority may be lost	
	If regular firmware updates are not performed, they may be exposed to zero-day vulnerabilities	V1, V2
T6; Session hijacking	Administrator accounts can be hijacked	
	Access to the session with a man-in-the-middle attack to gain control of the user	V1, V2
T7; Denial of service	The service can be paralyzed by depleting the resources required for the smart home service	V2, V6
T8; Threats using web vulnerabilities	Malicious scripts and SQL statements injected in web applications can lead to illegal authentication, authentication bypass, user cookies and session deception	V8
T9; Threats about unsecured UIs and APIs	Security incidents can occur by exploiting vulnerabilities in the cloud such as authentication bypass and data access	V7
T10; Loss	It can be physically destroyed or lost by user carelessness It may be stolen by an unauthorized intruder	V1

Information leakage: Attackers access user information by exploiting a vulnerability related to wireless networks. And they can leakage the user information. Leaked information may cause the invasion of privacy, medical information and personal information (Atamli and Martin, 2014).

Data forgery, alteration: Smart home users send and receive data at remote location using wireless network. Attackers can forgery and alteration the data by exploiting a vulnerabilities of wireless network. It can cause a malfunction of smart devices (Bagci *et al*., 2013).

Malfunction: Malfunctions of smart home devices, networks, control applications, etc. may occur due to various reasons such as user's mistakes, mechanical defects, communication errors, and the like. Malfunction of devices can lead to another threats such as power overuse, life threatening, etc. (Atamli and Martin, 2014).

Malware: Malware can arbitrarily change or exploit major resources related to smart home. Infected smart home device due to the user carelessness or network vulnerabilities are used as an attack resource such as spreading malicious code and sending spam. According to the research carried out by proofpoint, the malicious

attacks carried on "the internet of things" were 25% more common those targeted in laptop and desktop. For example, smart refrigerators that are infected with malware may control the temperature arbitrarily. It can cause a risk that give the financial loss to user (Zhang *et al*., 2014).

Attack using firmware update: If the authentication process is omitted during the firmware update process, the attacker can update the malicious firmware. In this case, it can lead to a secondary damage such as user information leakage, arbitrary operation of the device, privacy invasion. Also, if security patch is not launched, it could be exposed to 0 day vulnerability attack.

Session hijacking: An attacker can access the session through the man-in-the-middle attack and gain control permission of the user. Also, it can cause a secondary damage by exploiting the obtained session information (Botta *et al*., 2014).

Denial of service attack: Attacker can potentially send a massive number of packets to a smart home device in order to use up all the resource on the system, ultimately paralyzing the system. On the contrast, smart home devices infected with malware can be exposed to massive traffic amplification launched by object bots. Since smart home systems are always connected to the network, it is also under a constant threat of DDoS attack (Wood and Stankovic, 2002).

Threats using web vulnerabilities: Attacks using web vulnerabilities are XSS and SQL injection and XSS. XSS inject malicious script into a web page exploiting design vulnerabilities in web application. SQL injection is forcefully inserting SQL to web application to cause an unexpected commands or carry out an unapproved identification. Additionally, it can be used to gain a privilege for the attackers to access the data to leak and modulate it (Wichers, 2013).

Threats about unsecured UIs and APIs: The cloud service provides various UIs (User Interfaces) and APIs (Application Programming Interfaces) for users and administrators. Through these interfaces, various services such as permission setting, management and monitoring can be used. However, a variety of vulnerabilities of unsecured UIs or APIs can circumvent user authentication or threaten access to inaccessible data (Grobauer *et al*., 2011; Botta *et al*., 2014).

Loss: Wireless APs and smart home devices can be physically destroyed and lost by user carelessness. Especially, when a smart home control terminal is lost or stolen, it may lose overall control authority and lead to secondary damage such as leakage of personal information and invasion of privacy.

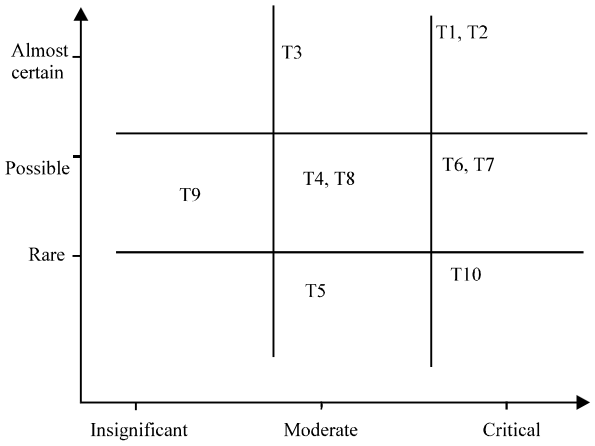

Fig. 3: Components of smart home

Figure 3 presents the result of a qualitative threat analysis that we conducted in order to possibilities of potential security threats and risk (Schreier, 2014). According to analysis result, information leakage and Data forgery/alteration are the biggest threats to Smart Home components. Information leakage from malicious code-infected devices, networks and applications can cause a terrible damage. In addition, data forgery/alteration can cause malfunctions of smart home components which can lead to a secondary damage. Denial of service and session interception are less frequent threats than information leakage but they are expected to equal magnitude if exposed to threats. Threats from malware infections and web vulnerabilities will be frequent and damages will not be small. Lastly, the risk of loss is the lowest but the risk is the highest.

Security consideration of smart home: As the smart home industry is growing rapidly, it is digging into the depths of everyday life. As life becomes easier and more convenient, the interest of smart home is also increasing day by day. Smart home services handle information about residential space from inside and outside the home and help people to live a comfortable and smart life with many useful applications such as energy saving. Smart home services involve the risks about security threats as it directly affects user's privacy, security issues and assets using a secure service is ideal but the security of the hardware and software is not perfect. Therefore, in this chapter, we suggested applicable security consideration about the threats of smart home. Table 5 shows security consideration of smart home (Raza *et al*., 2006; Bagci *et al*., 2013; Lee *et al*., 2014; Kubler *et al*., 2015).

Table 5: Security consideration of smart home

Security policy	Description	Threats
Access control	Monitors unauthorized access to resources and blocks and manages illegal access by unauthorized persons	T1, T2, T5, T7, T10
Firewall	The firewall blocks the unauthorized connection of the device	T4, T6
	Firewall prevents network-related attacks by blocking access to untrusted networks in advance	T7, T8
Authentication	It must be authenticated to use smart home devices/networks/applications	T8, T9,
	Authentication prevents access by unauthorized users	T10
Secure OS	It blocks malicious code transfer and information leakage between devices	
	Blocks information leakage through bind control and potential violation analysis functions	T1, T4, T8
Secure coding	Prevents errors, mistakes and vulnerabilities that occur during the development process	T4, T5, T8
Safety protocols	Block threats using the stabilized IoT protocol	T1, T2
Encryption communication	Use encrypted communication to solve the vulnerabilities of the communication process	
	Ensure the integrity of all data communicating between devices	T2, T6
Firmware update	Security patches through periodic firmware updates. Malicious firmware update blocked through Firmware update including authentication process	T5

Table 6: The function of secure OS

Classification	Threats and vulnerabilities
Server access control	
Server firewall	Access control function by IP and port
Login control	Control login by combination of IP/service/account for operating system login service such as telnet, FTP, SSH
Accounts control	
Account switching control	Controlling account switching by SU command on Linux OS
Delegation of authority control	Delegate permissions for specific accounts to other accounts to allow command execution and file access
Prevention of hacking	
Analysis of potential violations	If a violation of the same type occurs consistently,it is defined as a potential violation and the process is forcibly
Prevention of hacking	Sniffing, DDoS attack detection and blocking
Bind control	Block Illegal Communication Port (TCP)

Access control: Smart home devices detect unauthorized access and block to illegal access by unauthorized person in advance.

Firewall: Firewall can prevent to network attacks in advance by denying access to untrusted networks. Smart home devices have limitations to provide a firewall to the device itself. Therefore, there are a method to prevent an attack from the outside by installing IoT firewall devices (Kubler *et al*., 2015).

Authentication: In Smart home network environment, disguised access of malicious device is possible through the wireless network. To use smart home devices users must be verified as an authorized user. The smart home device must also be authenticated when accessing from the network. Access to unauthorized users can be prevented through the authentication process (Lee *et al*., 2014).

Secure OS: There are restrictions on installing an intrusion detection system and an intrusion prevention system in each home using a smart home device. In order to use Smart Home devices more safely, it is necessary to apply secure OS that can run in embedded OS environment. Secure OS is effective to prevent malicious code transfer, attack and information leakage of infected device through each function of server access control, account control and anti-hacking. Table 6 shows the function of secure OS (Bagci *et al*., 2013).

Secure coding: When developing programs related to smart home, secure coding should be essential. It is a way to prevent malicious attacks by developing to not be inserted the developer's mistake, errors and vulnerabilities during the development process. For example, even if the data is encrypted during communication process through the application of the control device, if there were a bug in the application itself, it is exposed to various threats. Therefore, secure coding should be done to enhance security.

Safety protocols: As new IoT devices emerge, a variety of communication protocols are being used to suit the device specifications and characteristics. For more secure communication, it is necessary to use a verified encryption algorithm and to ensure more stable communication by using an authenticated protocol (Raza *et al*., 2013). Encryption communication. Smart home devices and controlling applications communicate the data with network. Using encrypted communication, it can minimize forge, alter and leakage of exchanged data over the network. cryptographic communication must be applied in order to solve the threats that may occur through the communication process (Kubler *et al*., 2015).

Firmware update: Absolute security does not exist in Smart home devices and controlling applications. Security patches must be done consistently due to a continuously discovered vulnerability. If security patches for vulnerabilities were not done, it will expose to attack such as 0 day attack. Security patches for vulnerabilities should be done through continuous firmware and software updates.

CONCLUSION

In this study, we analyzed the definition and features of smart home which is a type of residential network connected with existing home appliances converge with information and communication technologies. And classified smart home service types. In addition, we analyzed the global market of smart home and analyzed vulnerabilities and security threats that can occur according to the components of smart home. We studied applicable security consideration through qualitative threat analysis in accordance with the probabilities of potential security threats and risks. Because smart home has a close relationship with daily life, security matters will be a very important factor. Security vulnerabilities of smart home are expected to cause many damages such as life, property and personal information. Therefore, Corresponding security technologies for vulnerability analysis of smart home proposed in this study should be applied as essential. We expect that this study will serve as a guideline for building a more secure smart home.

REFERENCES

Ablondi, W., 2014. 2014 Smart home systems and services forecast global total. Strategy Analytics Inc., Newton, Massachusetts. https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/reports/report-detail/2014-smart-home-systems-and-services-forecast-global-total#.WwPsZrg6Fkh

Aloul, F., A.R. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj, 2012. Smart grid security: Threats, vulnerabilities and solutions. Intl. J. Smart Grid Clean Energy, 1: 1-6.

Atamli, A.W. and A . Martin, 2014. Threat-based security analysis for the internet of things. Proceedings of the 2014 International Workshop on Secure Internet of Things (SIoT), September 10, 2014, IEEE, Wroclaw, Poland, ISBN:978-1-4799-7908-0, pp: 35-43.

Bagci, I.E., S. Raza, T. Chung, U. Roedig and T. Voigt, 2013. Combined secure storage and communication for the internet of things. Proceedings of the 10th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks (SECON), June 24-27, 2013, IEEE, New Orleans, Louisiana, USA., ISBN:978-1-4799-0228-6, pp: 523-531.

Barcena, M.B. and C. Wueest, 2015. Insecurity in the Internet of Things. Security Response, Symantec. https://scholar.googleusercontent.com/scholar?q=cache:2r8IEtM10KQJ:scholar.google.com/+Insecurity+in+the+Internet+of+Things&hl=en&as_sdt=0,5

Botta, A., W.D. Donato, V. Persico and A. Pescape, 2014. On the integration of cloud computing and internet of things. Proceedings of the 2014 International Conference on Future Internet of Things and Cloud (FiCloud'14), August 27-29, 2014, IEEE, Barcelona, Spain, ISBN:978-1-4799-4357-9, pp: 23-30.

Byun, J., B. Jeon, J. Noh, Y. Kim and S. Park, 2012. An intelligent self-adjusting sensor for smart home services based on ZigBee communications. Consum. Electron. Trans., 58: 794-802.

Grobauer, B., T. Walloschek and E. Stocker, 2011. Understanding cloud computing vulnerabilities. IEEE Secur. Privacy, 9: 50-57.

Harper, R., 2006. Inside the Smart Home. Springer, Berlin, Germany, ISBN:1-85233-688-9, Pages: 263.

Kavitha, T. and D. Sridharan, 2010. Security vulnerabilities in wireless sensor networks: A survey. J. Inf. Assur. Secur., 5: 31-44.

Kubler, S., K. Framling and A. Buda, 2015. A standardized approach to deal with firewall and mobility policies in the IoT. Pervasive Mob. Comput., 20: 100-114.

Lee, J.Y., W.C. Lin and Y.H. Huang, 2014. A lightweight authentication protocol for internet of things. Proceedings of the 2014 IEEE International Symposium on Next-Generation Electronics (ISNE), May 7-10, 2014, IEEE, Kwei-Shan, Taiwan, ISBN:978-1-4799-4779-9, pp: 1-2.

Raza, S., H. Shafagh, K. Hewage, R. Hummen and T. Voigt, 2013. Lithe: Lightweight secure CoAP for the internet of things. IEEE. Sens. J., 13: 3711-3720.

Schreier, M., 2014. Qualitative Content Analysis. In: The Sage Handbook of Qualitative Data Analysis, Flick, U. (Ed.). Sage, Thousand Oaks, California, pp: 170-183.

Wichers, D., 2013. Owasp top-10 2013. OWASP Foundation, Maryland, USA. https://www.owasp.org/images/1/17/OWASP_Top-10_2013--AppSec_EU_2013_-_Dave_Wichers.pdf

Wood, A.D. and J.A. Stankovic, 2002. Denial of service in sensor networks. IEEE Comput. Mag., 35: 54-62.

Yoon, S., H. Park and H.S. Yoo, 2015. Security Issues on Smarthome in IoT Environment. In: Computer Science and its Applications, Park, J., I. Stojmenovic, H. Jeong and G. Yi (Eds.). Springer, Berlin, Germany, ISBN:978-3-662-45401-5, pp: 691-696.

Zhang, Z.K., M.C.Y. Cho, C.W. Wang, C.W. Hsu and C.K. Chen *et al.*, 2014. IoT security: Ongoing challenges and research opportunities. Proceedings of the 7th IEEE International Conference on Service-Oriented Computing and Applications (SOCA), November 17-19, 2014, IEEE, Matsue, Japan, ISBN:978-1-4799-6833-6, pp: 230-234.