INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 11, Issue 12, (2021) E-ISSN: 2222-6990

Security Analysis And Feasibility of Smart Entrance System in Smart Home Applications

Rizzo Mungka Anak Rechie, Amir Firdaus bin Saib, Lucyantie Mazalan and Yusnani Mohd Yussoff

Faculty of Electrical Engineering, Universiti Teknologi MARA Shah Alam,
40450 Shah Alam, Selangor
Email: yusna233@uitm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v11-i12/12005 DOI:10.6007/IJARBSS/v11-i12/12005

Published Date: 28 December 2021

Abstract

Technology advancement, especially in the area of Internet of Things has enabled many high-end applications to be developed. The complexity of the applications will continue to grow with the coming of 5G technology. The technology has improved our life. However, there are many security issues that exist together with the advancement. This paper first discussed on the security issues focusing on IoT and Home Digital Voice Assistant (HDVA) applications. Outcome from the study shows an alarming security issue. To prevent one of the security issues, a Secure Smart Entrance system is designed and implemented using Alexa; a type of home device voice assistant, Raspberry Pi and RFID. The developed system is designed and implemented to study and validate the vulnerability issues in the IoT applications that utilize HDVA devices. The analysis on the energy consumption and feasibility of the Secure Smart Entrance System using HDVA is presented in this paper. The results show an acceptable amount of energy and is therefore suitable for future IoT related applications. Further study will focus on the security analysis using the developed system.

Keywords: Amazon Echo, Alexa, RFID, Raspberry Pi 3.

Introduction

In recent years, more and more Home Digital Voice Assistant (HDVA) devices are deployed at home. Examples of (HDVAs) are Amazon Echo, Google Home, Philips Hue and few more. These devices connect to the home electronic appliances and become an intelligent personal assistant service, which responds to their name.

For Amazon Echo Dot, commonly called as Alexa and it can be used to control smart home or smart office. The basic function of Alexa is to turn on the light, play music and to give news update. Alexa's task can be further added by the owner, to control other appliances and to become a talking companion.

Few smart home projects that utilize voice assistant such as Alexa, Google Home, Vivint Smart Home and Simplesafe (Home, 2016; Garcia, 2020). In these systems, the HDVA have been used to give feedback from the user command or questions regarding the house, temperature and few basic home appliances needs.

Strategic Analytics' research indicates that the use HDVA will exponentially increase with a total of 15.1M devices in 2020 (Watkins, 2017). In China, household penetration for smart home applications was estimated around 8% in 2019. It is predicted to reach nearly US46 Million by the year 2026 (Newswire, 2020).

The Alexa services on the other hand offer users more than 10,000 skills (Alexa voice services) to be explored (Barret, 2017). Besides smart homes, HDVA can also be used in the office, schools and much more. Smart Entrance System is one of the promising solutions that can use HDVA. However, proper security features are needed to ensure only authenticated users are allowed to enter the premises. Currently, Alexa or any HDVA takes any voice from any person as long as the word usage is correct. This may cause serious security issues. Paper presented by Xinyu et. al. discusses the insecurity issues in HDVA (Singh *et. al.*, 2015).

This paper first discusses the security issues in the smart home. Types of threats and vulnerabilities exist in smart home are presented and discussed. Following that, the development of a test bed of a Smart Entrance System or SES that utilizes Alexa and Amazon services are presented. The test bed consists of an Alexa, Raspberry Pi as the controller, RFID for authentication and LCD for display purposes. User information will be stored and Alexa should be able to identify and validate the authenticity of the user that logs in to the premises. The test bed was set up for the purpose of security analysis. However, in this paper, an analysis on the feasibility of the smart home system in term of energy consumption are presented.

The following sections discuss the possible threats and vulnerability issues in HDVA for smart homes. Section III presents the methodology involved, followed by results and discussion. Finally, a conclusion is presented at the end of the paper.

Vulnerabilities and Threats

Threats and vulnerabilities of smart home come from various sources. With the increase in technologies, attack to smart home devices can be done easily. Further, limited knowledge of the homeowners on the connected devices increases the possibility of being attack. The following sections discuss some of the security issues on few wi-fi network implementations.

One of the vulnerabilities exists in the smart home network is through a gateway. A simulation study conducted by a group of researcher using few network analysis tools such as Wireshark, Can & Able and network Miner based on Kampung WiFi network has shown the vulnerability of the gateway that enables attackers to further conduct another attack such as brute-force and identify open ports on the network (Fahmy *et. al.*, 2012).

Advanced Metering Infrastructure (AMI) is an application that integrated with available Home Area Network (HAN). Paper presented by presents an analysis of attacks due to the integration of AMI and HAN (Namboodiri, *et. al.,* 2014). The AMI has the ability to control any

home appliances that can operate at a given time to achieve load balancing. In turn, the smart meter is able to communicate with all appliances connected at the property it is monitoring and able to control the power used by the appliances through switching. Possible attacks presented in the paper towards the HAN are jamming attack, equipment impersonation, replay attack and nonrepudiation.

A video surveillance system or commonly called closed-circuit television (CCTV) is another source of vulnerabilities in smart home devices (Costin, 2016). Factory password, expired firmware is one of the vulnerabilities issues. The types of attacks in CCTV are visual layer attack, covert channels attack, denial of service and jamming attack. The visual layer attack is an attack that takes advantage of the imaginary semantics and image recognition. The video surveillance system (VSS) can also be infected with a malicious malware via firmware update over USB port or over web interface. Following this, the malicious component could blur pre-programmed faces or car plates that give an advantage for the attacker to precede their attack towards a premise with a dysfunctional VSS.

Another source of vulnerabilities is cloud servers and IoT devices that are used to remote control and to monitor the home. With this in mind, as the smart home systems grow in popularity and the mobile apps for home control are increasing in demand, the security challenges are growing too in return (Ruiz *et. al.,* 2018). Mobile apps are directly exposed to the public network, which makes it one of the vulnerable points for the smart home system. Therefore, the encryption for outbound and inbound of sensitive data flows in and out of the app is very crucial. Particularly, the flows and the destination of data which in most cases are cloud, play an important role due to the sensitivity of the personal data to be leaked out.

The current trend of smart home devices is Home Digital Voice Assistant or HDVA. A study conducted by shows that, available HDVA takes commands from any source of voice input and reacts to it (Lei *et. al.,* 2018). This opens a door for the attacker to breach the house through a fake order attack. In this situation, the HDVA may be triggered by a breached Bluetooth speaker inside the house or by a breached smart TV that plays a sound or video to give commands to the HDVA device. The researcher proposed an authentication system to be added to the system to allow only authenticated users can activate the HDVA.

Based on William Hack, Amazon Echo is vulnerable, and can be taken advantage of (Haack *et. al.,* 2017). The common attack to be used on a voice assistant device is the sound attack. Other than that, Amazon Echo is lacking in terms of single factor authentication. The Amazon Echo will accept command from any user without knowing if it is the main user or not. Through man in the middle attack, attackers can sniff the packet and extract the information in the network. Besides, attackers can also conduct a replay attack on Amazon Echo. This will lead to duplicate order delivery.

Dain Overstreet in his paper proves that, the Amazon Echo is vulnerable to the denial of service attack (Overstreet *et. al.,* 2019). The Amazon Echo can be compromised with this attack by other device applications. The malicious applications, on the other device will be able to attack the Amazon Echo wirelessly. In this case, to make this attack work, the other vulnerable part of the system is the router connected to the Amazon Echo. The router has an important role in internet device's safety in terms of network.

According to Raphael Leong et.al, the Amazon Alexa is vulnerable to the skills set part (Leong, 2018). The skill set is mostly made by other developers, the attack is by making the Amazon Alexa command almost similar to the third-party developers and direct the Amazon Alexa to run a malicious activity on a malicious site. By that, the device security will be breached through the web application.

Ike Clinton et.al, stated that the HDVA device is also vulnerable to hardware reverse engineering attack (Clinton *et. al.,* 2016). The JTAG pinout hardware of the Amazon Echo can be compromised and be fully controlled. Other than that, the SD card attached to the Amazon Echo also can be compromised.

Addition to this, as stated by Abdulaziz Alhadlaq, the Amazon Alexa skill ecosystem are mostly does not have any privacy policy, and this can be taken advantage of for private data breaching (Alhadlaq *et. al.,* 2015). Following this, the skill set without any linking account which is by means are not made by Amazon are totalling 8967 skills sets, which is very vulnerable to attack without any awareness from the Amazon.

Next, based on Wenrui Diao, the voice assistant specifically Google Voice Assistant can be exploited by a malware app that is installed inside a mobile phone (Diao *et. al.,* 2014). The main concept is very clear, it stated that the main attack is the sound attack towards the voice assistant. The malicious app VoicEmployer is being installed on a mobile phone, then the app will run a sound attack through the phone speaker that will activate the phone voice assistant. The attack can make the voice assistant to dial a malicious number.

Following this, Nan Zhang had identified the voice squatting and the voice mitigating attack towards a virtual assistant, such as Amazon Alexa and Google Assistant (Zhang *et. al.,* 2019). The voice squatting attack is an attack that impersonates the voice command, such as “go there” and “go they”. The attack will use the squatted command to run a malicious activity towards the voice assistant. Addition to this, the voice masquerading attack is an attack that pretend to run a command but stealing the user information during the process.

In addition to this, Huan Feng had developed a continuous authentication for voice assistant called VAuth at a Google Voice Assistant (Feng *et. al.,* 2017). The VAuth consists of two components, the first one will be a wearable device with an accelerometer mounted. The second one is the extended voice assistant that authenticates the user with the right wearable device for it to work. The reason for this is for the wearable device is a legitimate user, the voice assistant will only receive voice input from the legitimate user.

Finally, for the insecurity of the voice assistant, Geumhwan Cho had identified the vulnerabilities of the voice assistant applications using a threat model (Cho *et. al.,* 2019). The threat model used is the STRIDE and DREAD, which represent spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privileges, damage potential, reproducibility, exploitability, affected users and discoverability. The attack consists of microphone spoofing, tampering by human voice to activate the voice assistant and launching a denial of service attack from a microphone to the voice assistant, flooding it with sound signals. By that, an attack towards a voice assistant may compromise towards the information disclosure, which results in no information confidentiality.

To summarize, smart home network is susceptible to network attacks due to the various vulnerabilities that exist in the devices. Demand on embedded security features on smart home devices is therefore undeniable. By limiting the number of vulnerabilities, number of successful attacks can therefore be reduced. Table 1 below tabulates and summarize the studies on IoT applications and the security issues.

TABLE 1:
Comparison of Smart Home Vulnerability

Ref.	**HVDA Used**	**Smart Home**			**Vuln.**			**Attacks**		**Solution**
			Router	Apps	SFA	PPBC	Hrd.	Sound	Network	
Haack *et. al.,* 2017	Amazon Echo	Yes	Yes	No	Yes	No	-	Yes	MITM Packet info Replaying Web App. API	Improved SFA during orders
Overstreet *et. al.,* 2019	Amazon Echo	Yes	Yes	Yes	-	-	-	-	DoS	-
Leong, 2018	Amazon Alexa	Yes	-	Yes	-	-	-	Yes	Respiratory data Skill data set	-
Clinton *et. al.,* 2016	Amazon Echo	Yes	-	-	-	-	Yes	eMMC SD card pinout JTAG	-	-
Alhadlaq *et. al.,* 2015	Amazon Alexa	Yes	-	Yes	-	-	-	-	Skill data set	-
Diao *et. al.,* 2014	Google Voice Assistanr	No	-	Yes	Yes	-	-	Yes	VoicEmployer	-
Zhang *et. al.,* 2019	Amazon Alexa Google Assistant	No	-	Yes	-	-	-	Yes	VSA VMA	-
Feng *et. al.,* 2017	Google Now	Yes	-	Yes	Yes	No	No	VAuth	VAuth	Authentication ring
Cho *et. al.,* 2019	Any	Yes	No	Yes	Yes	No	No	Microphone	DoS Spoofing Sniffing	-

SFA: Single Factor Authentication
PPBC: Physical Based Control
Vuln.: Vulnerabilities
Hrd.: Hardware
VSA: Voice squatting attack

VMA: Voice masquerading attack

Methodology

This section presents the methodology for this project. In general, the work can be divided into two parts, which are test bed and software development.

Figure 1 explains the overall functionality of the SES (Smart Entrance System) procedure. In this system, Alexa will only be activated by authenticated user who has successfully entered the area.

In specific, when the user taps their ID cards on the RFID reader, the data will be added into the MySQL server. After that, the data will be stored inside the database. If the data are available in the database, authentication will be successful. Authenticated user will have to call Alexa by calling its name. Alexa will then wait for user further instruction to respond. In this project, Alexa will give personal details of the successful user to lab owner or anybody who requested.

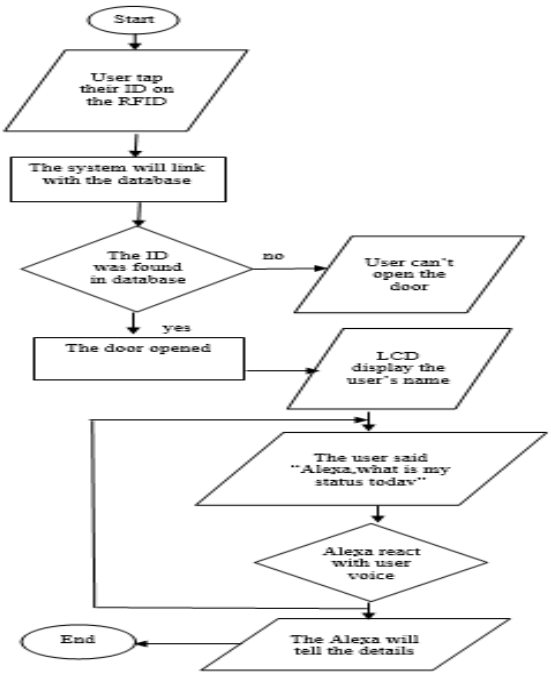

Fig. 1: Flowchart of the process

Figure 2 depicts the overall view of a complete SES system. The test bed developed is for the purpose of analyzing threats and vulnerabilities on the smart system that utilize HDVA. The microcontroller used for this project is Raspberry Pi 3 which has been used to control the operation of all activities. RFID is used as a reader and sensor to detect the card and send the data to the database. The controller is provided with a power supply to make it operate efficiently. The Alexa and the LCD are the output of the system. The LCD will display the user's details and Alexa will respond to the user's voice.

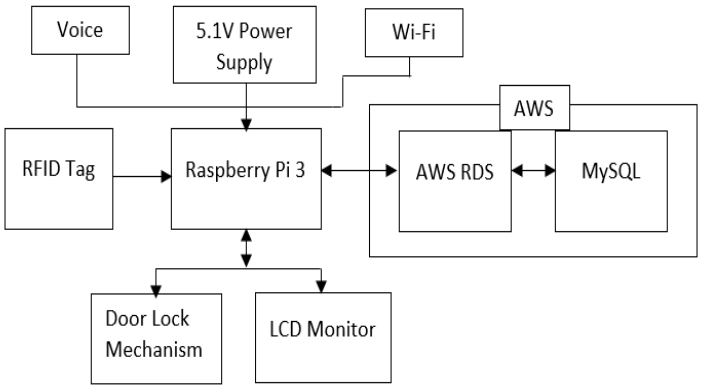

Fig. 2: Block Diagram of the SES

The above section presents the flowchart and block diagram of the developed testbed of smart home using Alexa as the HDVA devices. The input of the system is RFID card that is uniquely assigned to dedicated user. The card number is stored in the database for authentication purposes. Successful user will be able to activate the Alexa and performed other functions that have been preconfigured in the AWS services. Two AWS services are used which are AWS Relational Database Service and MySQL. Communication from Alexa to AWS is through WiFi connection available in the Raspberry Pi 3 that function as a controller in this smart home system.

Energy consumption is one of the important elements in home appliances. Consideration on low energy applications is very essential to ensure low emission of carbon footprint to the world. To ensure this, analysis on the energy consumption of Alexa is conducted using the formula as stated in eq (1).

$$E(kWh/day) = P(W) \times t(h/day) / 1000(W/kW)$$

eq (1)

Following section will discuss the outcome from the energy analysis. Security analysis on the developed system will only be discussed in the next article.

Results and Discussion

In this section, the result presented will focus on the energy analysis of the developed SES. The objective of the analysis is to look at the feasibility of the smart system in term of energy consumption. Table 2 tabulates the energy consumes by each process. Electronic devices involved are Alexa and raspberry Pi. The energy consume by Alexa varies depending on its mode. The highest energy is during playing music at high volume.

In this analysis, the energy calculated for Alexa is during mode idle, listening and basic reaction. This analysis assumes that, most of the time, Alexa will be in idle state and at very minimum time being in listening and basic reaction mode. Therefore, the energy consumed will be lower than the total energy for the three modes plus Raspberry Pi energy; which is 10.368 watts. This low energy has suggested the feasibility of the smart home system using HDVA device.

Table 2:
Analysis on Power Consumption for Alexa and Raspberry Pi

Device	Mode	Power usage (watts) in 1 hour	Power in 24 hours	Energy (kwh) Per day	Energy (kwh) Per month
Alexa	**Idle**	2.8	67.2	0.0672	2.016
	Listening	3.6	86.4	0.0864	2.592
	Playing music (low volume)	2.8	67.2	0.0672	2.016
	Playing music (medium volume)	3.0	72	0.072	2.16
	Playing music (high volume)	7.0	168	0.168	5.04
	Basic reaction	4.0	96	0.096	2.88
Ras-pi		4.0	96	0.096	2.88

The energy E in kilowatt-hours (kWh) per day is equal to the power P in watts (W) times number of usage hours per day t divided by 1000 watts per kilowatt.

With this in mind, the result shows that the implementation of the SES (Smart Entrance System) into the smart home is feasible for home use purposes as the additional security features does not affect much of the power consumption when it is at idle despite the SES system is attached and running. This low energy has suggested the feasibility of the developed system.

Conclusion

As a conclusion, the first part of the paper shows a demand on security enhancement for smart home applications. Vulnerabilities or weaknesses in the HDVA and other smart home devices need to be identified and mitigated to avoid security problems to users. To enable further studies on smart home vulnerabilities and attacks, a testbed of a smart home system using HDVA is implemented. Energy analysis on the system was conducted and the results shows the feasibility of the smart home system in term of energy consumption. Further studies will look into vulnerabilities and successful attacks that exist in this test bed. Following that, a mitigation technique will be proposed to enhance the security features in the smart home network that utilize HDVA.

References

Alhadlaq, A., Tang, J., Almaymoni, M., & Korolova, A. (2015). Privacy in the Amazon Alexa skills ecosystem. Star, 217(11).

Barrett, B. (2017). Amazon Alexa Hits 10,000 Skills. Retrieved from https://www.wired.com/2017/02/amazon-alexa-hits-10000-skills-plenty-room-grow/

Cho, G., Choi, J., Kim, H., Hyun, S., & Ryoo, J. (2018, August). Threat modeling and analysis of voice assistant applications. In International Workshop on Information Security Applications (pp. 197-209). Springer, Cham.

Clinton, I., Cook, L., & Banik, S. (2016). A survey of various methods for analyzing the amazon echo. The Citadel, The Military College of South Carolina.

Costin, A. (2016). Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In Proceedings of the 6th international workshop on trustworthy embedded devices (pp. 45-54).

Diao, W., Liu, X., Zhou, Z., & Zhang, K. (2014). Your voice assistant is mine: How to abuse speakers to steal information and control your phone. In Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (pp. 63-74).

Fahmy, S., Nasir, A., & Shamsuddin, N. (2012). Wireless network attack: Raising the awareness of Kampung WiFi residents. In 2012 International Conference on Computer & Information Science (ICCIS) (Vol. 2, pp. 736-740). IEEE.

Feng, H., Fawaz, K., & Shin, K. G. (2017). Continuous authentication for voice assistants. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (pp. 343-355).

Garcia, A. (2020). Best Home Security Systems that Work with Alexa. Retrieved from https://www.safehome.org/security-systems/best/alexa/.

Haack, W., Severance, M., Wallace, M., & Wohlwend, J. (2017). Security analysis of the amazon echo. Allen Institute for Artificial Intelligence, 11.

Home, V. S. (2016). Vivint Smart Home Launches Integration with Amazon Echo to Create Comprehensive, Voice-Controlled Smart Homes. Retrieved from https://www.vivint.com/company/newsroom/press/vivint-and-amazon-echo.

Lei, X., Tu, G. H., Liu, A. X., Li, C. Y., & Xie, T. (2018). The insecurity of home digital voice assistants-vulnerabilities, attacks and countermeasures. In 2018 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE.

Leong, R. (2018). Analyzing the privacy attack landscape for amazon alexa devices. Imperial College London, Tech. Rep.

Namboodiri, V., Aravinthan, V., Mohapatra, S. N., Karimi, B., & Jewell, W. (2013). Toward a secure wireless-based home area network for metering in smart grids. IEEE Systems Journal, 8(2), 509-520.

Newswire, P. R. (2020). China's Smart Home Market, Forecast to 2026 - Policies, Initiatives, and IoT Driving Smart Homes. Retrieved from https://finance.yahoo.com/news/chinas-smart-home-market-forecast-174500282.html

Overstreet, D., Wimmer, H., & Haddad, R. J. (2019). Penetration Testing of the Amazon Echo Digital Voice Assistant Using a Denial-of-Service Attack. In 2019 SoutheastCon (pp. 1-6). IEEE.

Ruiz, E., Avelar, R., & Wang, X. (2018, May). Protecting remote controlling apps of smart-home-oriented IOT devices. In Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings (pp. 212-213).

Singh, M., Khan, M. A., Singh, V., Patil, A., & Wadar, S. (2015). Attendance management system. In 2015 2nd International Conference on Electronics and Communication Systems (ICECS) (pp. 418-422). IEEE.

Watkins, D. (2017). Strategy Analytics: Amazon, Google to Ship Nearly 3 Million Digital Voice Assistant Devices in 2017. Retrieved from https://www.prnewswire.com/news-releases/strategy-analytics-amazon-google-to-ship-nearly-3-million-digital-voice-assistant-devices-in-2017-300339381.html.

Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., & Qian, F. (2019). Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. In 2019 IEEE Symposium on Security and Privacy (SP) (pp. 1381-1396). IEEE.