THINK INDIA JOURNAL

ISSN: 0971-1260

Vol-22-Issue-3-July-2019

Virtual Personal Assistant Security: A retrospect

Nagma Chowdhury[1], ShivaliChopra[2*], Mohit Arora[3]

School of Computer Science and Engineering

Lovely Professional University, Phagwara, Punjab, India

[1]nagmachowdhury2808@gmail.com, [2]shivali.19259@lpu.co.in,[3]mohit.15980@lpu.co.in,

* Corresponding author

Abstract

Virtual personal assistants (VPAs) today rely mainly on the voice commands for communicating with the devices (e.g., Amazon Alexa and Google Assistants).The increased usage of the VPA program, which permits a third party to promulgate a feature of the network and can thus be used to distribute the malicious skills to the general public when communicating with smart speakers like Google Home and Amazon Alexa, is the latest authentication challenge for the user from the VPA platform to the user.This makes the VPA systems more prone to vulnerabilities as there is no such strong encryption for it. This paper shows the review of various attacks performed on a VPA system to exploit its vulnerability and described the basic VPA structure.

Keywords: Virtual Personal Assistant, Masquerading, Voice Squatting, En-route profiling

1. Introduction

People nowadays have the ability to interact with each other to provide some useful services, including smart devices, smartphones and IoT devices in general. In such a case, using Artificial Intelligence and Machine Learning to understand the world itself and the needs of its occupants, smart environments can be built[12].

The understanding of natural communication between humans and machines is one of the aims of Artificial Intelligence (AI). VPA systems, also known as interactive voice systems, have been the fastest budding area of Artificial Intelligence in recent years[8]. There are many organizations who own their own virtual personal assistants such as Microsoft's Cortana, Amazon Alexa, Apple's Siri, Facebook's M and Google Assistant[20].While designing and developing their systems, these organizations used different approaches. Depending on the specification and its sophistication, there are many approaches used to model the VPAs.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

VPA systems are smart agents that can help users through spoken interactions to complete tasks more efficiently. In addition, spoken dialog systems are built into several devices such as smartphones, smart TVs, and car navigation.VPA systems can also serve a wide range of industry, education, state, healthcare, and entertainment applications[25].

Modernistic VPA systems are primarily delineated to be voice-controlled. Shielding these VPAs is challenging because of the lack of emphatic means of authenticating the users involved throughout the noisy and open voice channel. Previous research indicates that the attackers can produce vulnerable voice commands or inaudible ultrasound to target voice recognition systems[9]. Such kind of attacks are impersonating the accredited user to theVPAsystem, as there is no protection to accredit the user to the system. Another authentication problem is the advent of the VPA ecosystem: it makes it challenging for the client arbitrate whether the client is using the right skill of the VPA which he wants to use. The issue arises that an attacker can promulgate malicious third-party skills when a user either knowingly or unknowingly triggers a vulnerable skill due to misunderstanding the system [11]. The enemy could therefore, impersonate the user with a correct skill or the VPA. The failure to authenticate the user's authentication on the Voice Channel makes this attack possible, which leads to a realistic threat in our research.

2. Background and Related Work

VetonKepuska et al. introduced a new model of Virtual Personal Assistants, which is designed to interact with a human being with a consistent structure. The system used both input and output streams to communicate with speeches, graphics, videos, gestures and other modes. The VPA could also be used by certain applications such as the knowledge base, image / video recognition, language recognition and gesture recognition to improve user's communication with computers. In addition, the proposed system enabled users to have lengthy conversations using the extensive knowledge base dialog. The platform can be used in various tasks such as academic, robots, medical and cars, mobility systems, control safety access, and home automation. It can help in various applications such as customer response and service agent, online shopping, training or education, ticket booking, facilitating purchases, travel information, data enquiry, counselling, etc[1].

Rongjunchen Zhang et al. proposed a smart Vaspy attack targeting VPAs on smartphones. The voice commands can be manipulated by the attacker to trigger the VPA and initiate a few attacks with the new attack, including sending fake messages or emails, leaking private

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

information and calling arbitrary numbers. Inside the Vaspy is designed an Attacking Environment Sensing module to pick an appropriate amount of attacking voice and time allowing the attack unnoticed by the users. They built a prototype spyware for Vaspy and evaluating it on different Android phones with participants across different Vaspy[15].

Nan Zhang et al. reported the first security analysis of VPA ecosystems. The attacks of voice squatting and masquerading was explained through which an attacker canharnessvoice assistant systems to steal crucial information from users. Its serves as a threat to the device. To minimize the danger, they built an information scanner and tested it against the market for Google and Amazon, which results to a discovery of a large number of already reported VPA skills at risk and problem names, suggesting that millions of VPA users could already encounter the attacks[3].

Xinyu Lei et al. studied Google Home and Amazon Alexa to establish a number of security vulnerabilities in HDVAs. In order to secure HDVA services, they proposed a physical presence,a further factor of authentication.
Only when a person is physically present in the vicinity can the HDVA app recognize voice c ommands. Therefore, they developed a solution called the VSB button to detect physical presence. They modelled and tested the prototype on an Alexa phone. Their results demonstrated that VS Button was able to detect accurately both in the laboratory and in the real world[6].

George W. Clark et al. checked the efficacy of an adversarial software attack on a dynamic environment of the ML rule for a physical robotic device. This was achieved through the construction of an environment that simulates a city street grid and the development of JAV, a tiny robot capable of acting as an autonomous vehicle. The attack was successful in diverting JAV from a learned route to a false location [2].

RoumenTrifonov et al. described a project related to the application of AI methods to increase computer network's security. A feasibility study of the various methods of AI has proved an equally effective method which cannot be identified at all levels of cyber intelligence. While a Multi-Agent System has been selected and tested for Recurrent Neural Networks, Tactical Cyber Threats Intelligence[4].

Koosha Sadeghi et al. suggested a theoretical method to change the parameters of ML in order to be safe from attacks while maintaining high accuracy. The model seeks the optimal

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

parameter set by defining a new function that looks after ML's accuracy test results and its protection against attacks[5].

V. Kanimozhi et al. imposed a dataset, which contained both real-time and current attacks, the proposed system can be expanded to detect all remaining groups of attacks. The system used an artificial intelligence technology training application optimization which is based on the central processing unitand the optimization can be easily modified by other systems such as the open source tensor flow from Google[7].

Sagar B.S et al. addressed the need to build cybersecurity skills and how the use of machine learning algorithms and artificial neural networks can mean AI to improve skills. They discussed AI is a research area designed to simulate human behaviour and intelligence, to protect networks more effectively and reliably.These technologies provide better good flexibility, decision support and better accuracy, leading to better results[10].

3. Virtual Personal Assistant

A Virtual Personal Assistant system was developed on the android platform that demonstrates the use of voice commands using natural language processing. Using the mailing and calendar, users were able to mail and build their reminders using voice command.VPA system based on the IOT operates by connecting simple appliances to it, and the appliances have been successfully controlled via the internet[28]. VPA system can track the sensor data such as fuel, light, motion sensors, temperatures[18]. The system allows to switch on the lights when it gets dark. It also helps a user to maintain its various tasks on his device through voice like making reminders, making calls, searching anything, opening an app, getting an information, etc. Everybody needs to know Watson, Siri, Google Now or Cortana or any of the virtual fictional assistants[19]. Such real-life virtual assistants are not as smart as the Jarvis of Ironman, but their intended purpose is essentially the same, artificial intelligence powered voice computing. Ask a question, get your answer.

A unique feature of the VPA system is that everyone forgets traditional interfaces like the tactile display and uses less (to change the volume or mute) buttons that give users a hands-free experience. In other words, you're only supposed to give commands through voice[16]. The VPA system uses a circular microphone array which is designed to pickup audio at 360-degree and also uses other technologies like beam forming to capture the voice. This allows the user to speak from anywhere in the room to get a response from the device quickly.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

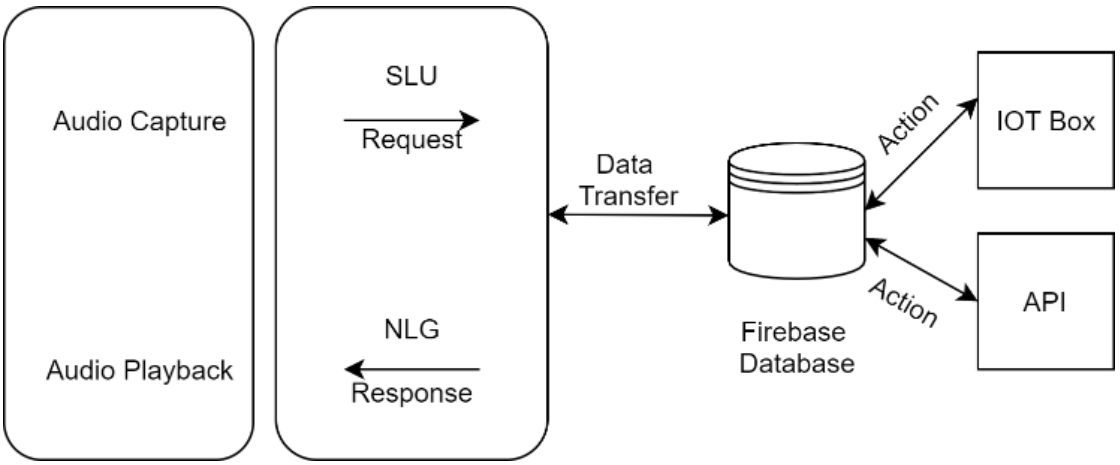

Fig 1 Basic VPA structure

A third-party skill is basically a web service hosted by its creator and registered with the VPA service provider (Amazon or Google)[25]. When a user uses the wake-word to invoke a VPA device, the device captures its voice and sends this command to the cloud of the VPA service provider. The device recognizes the voice record in text, detects the skill to be invoked and then provides the text along with the timeline, the device status and another metadata as an on-demand for the web services of the expertise[26]. The skill does not receive voice recordings bit it will receive requests in text format. In response, the service provides an answer, the text content of which is translated to the cloud voice and played to the client via the phone, either in plaintext or as Speech Synthesis Markup Language (SSML) format. SSML also provides the ability to attach audio files to improve the response that both Amazon and Google support.

4. Attacks On VPA

Some VPA follow a continuously listening system that takes continuous voice commands to provide user comfort. Sometimes before speaking commands, users do not need to press a button on VPA devices. Because of the openness of voice channels, such great comfort can expose the VPA to security threats. Therefore, we believe that special consideration should be given to the VPA protection[20].

A. Voice Squatting Attack

By voice squatting, the ability to attack and fake the VUI to gather information that the user shares only with the system. Some skill requires the user to provide private information to do their job. For example, to book a ticket the system needs your private credentials like name, address, phone number, etc.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

These skills could lead to serious leaks if the attacker can impersonate the skill. A skill asserted falsely can lead to a Phishing attack by giving wrong details to the user by voice commands: e.g., fake phone number or website[22]. Through its card system, this can even be achieved on Amazon Alexa: Alexa provides a skill to add a home card if the user needs, which is shown on smartphone or web browser via Amazon's companion app, to assist with voice communication. Home card makes it easy for users to access information that is hard to remember and stored in the activity history.

Today's VPA's longest string match strategy can easily be exploited by voice squatting attack. About 60 per cent of Google Home and Alexa users use the word “please” to start a skill and 26 per cent of them add “me” to the name of the skill. So, the opponent can register skills like “Capital One Please” to impersonate “Capital One”.

B. Voice Masquerading Attack

Unconscious of the capabilities and behaviors of a VPA system could lead users to voice masquerading attacks. The system owner thinks the previous (malicious) software is no longer functioning, but the app still listens to incoming commands. The two such skills which can impersonate a skill to give out personal information to the user or eavesdrop a conversation are:

i. In-communication skill switch

Skill switching is supported during interactions by the VPA system with the help of skill switch common, which may lead to give control to the target skill to impersonate the other skill. That would likely result in leaking the crucial information to the impersonated skill, which should only be shared with the target skill. This effort to masquerade was opportunistic.

Google Assistant does have a protection to this impersonification of the skills. By speaking “Sure, here is,” it launches a skill along with the name of the skill and a special earcon, and the termination of the skill with another earcon. In addition, the VPA speaks to the user in a distinctive accent to distinguish it from the skills.

ii. Faking termination

Google Assistant and Alexa advocate autonomous termination of skills, which enables a skill to end itself. There is a shouldEndSession field in the object. A capacity ends after the answer by setting it to true[27].

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

A session can be kept alive by speaking “goodbye” or staying silent to impersonate the ending of a skill. Both Google Assistant and Alexa returns a re-prompt through skill when the VPA receives no user's voice command within a timing period.

An attack skill may be masquerading as the VPA service recommending certain malicious skills to the user or the user's legitimate abilities may share crucial data. These skills are falsified to imitate the original skills. The silent audio response and fake termination leads the opponent to eavesdrop on the user's conversation till the user continues to talk during the waiting period.

C. Weak Signal-factor Authentication

The VPA device only understands the voice commands which are a type of password like voice words. The voice mechanism does not consider the users's authenticity, it just recognizes the semantics of the voice word command. Therefore, an attacker can easily access the device if they know the voice command.

A VPA device can always accept a correct authentication word, regardless of where the voice goes. It also embraces voice controls from different machines, such as laptop and desktop computer systems, music / audio players (such as MP3 players, the Bluetooth speakers and home theatres), mobile devices (smartphones and tablets). And it also accepts orders from a range of computers[14].

D. No Physical Based Access Control

The voice services of VPA are designed to provide a user to give voice command in a certain range. The system cannot acknowledge voice commands, since there is no physical presence-based access control. It works for all sounds which achieve 60dB or higher sound pressure (SPL). There are therefore malicious voice commands from an adversary outside the owner's room or a speaker device to the Alexa device[23].

E. Insecure Access Control

By speaking its names (e.g.' My Door') and commands (e.g.,' Open'), VPA owners can control smart devices enabled by VPA. Most providers are permitted to substitute the default device names, but they are not generally required. As all the voice commands are accepted by the cloud from VPA, VPA devices can trigger security threats to them. The unclear control of access can exacerbate the damage caused by the vulnerabilities of VPA[14].

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

F. Proof-of-concepts Attack

Without the close interference of the enemy, VPA apps can be misused to get fake voice commands. Remember that our attack cases are used to target victims, but not particular victims, marked by the malware as vulnerable. Although the proportion of potential victims to all VPA owners is small, these victims are not only at risk of unintended injury, but also the other owners. An indoor sound system located in the same room can be used for sounds on an VPA device without being present nearby.

The opponent could find potential victims, using smartphone malware with no root permission, who have been using VPA devices or / and VPA-enabled smart devices. Since both VPA and the intelligent devices have a Wi-Fi connection, the malware will search the home Wi-Fi network with which its smartphone host detects whether or not it exists.

G. Weak Payment Authentication

The VPA system supports online ordering more and more. Proper security controls are difficult to use. For example, the ability to set a 4-digit PIN for purchases can be used by users of Amazon Alexa. This option is not activated by default at the time of writing[29]. Even if this option is allowed, it is vulnerable because of the poor implementation of the lockout. This is because, before a order system lockout, Alexa requires two PIN checks, after which the user has to restart the order process. Nevertheless, the number of times a client may try to order after each lockout is not limited. Despite this, vendors have tried in the ordering process to introduce alternative countermeasures against violence. It creates problems for consumers who often do not search or recognize their phones or emails[24].

H. Always On, Always Listening

As mentioned, the speaker is constantly listening to the user statements while awaiting the word awakening. The constant listening and listening to a device present important concerns about security and privacy[13]. Accidentally, the assistants will be recorded with the word "wake-up" or other phonetically similar words.

As a result, any subsequent conversation is uploaded to the Internet. This problem can lead to the leakage of sensitive information of the user to the attacker. This can harness the device security as it can be easily accessible by the attacker and the attacker can use them harm the other connected devices.This feature has recently accidentally recorded a private

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

conversation of a couple and randomly sent to Echo. This example shows that their voice data is not fully controlled by the user.

I. En-route Profiling

Traffic analysis is a good example of an En-route profiling method. A user profile can be used with traffic analysis. An attacker can use En-route profiling in particular to deduce the presence of a user. This can be used further for more specialized attacks. In-route profiling attacks can be carried out even with the encryption of network traffic[13]. While hiding techniques can be used to avoid these attacks, they have not been used in VPA. In this case, a deceptive or moral Internet service provider would be the most likely foe.

J. Profiling by the Third-Party Developers

VPA is incorporated into the expertise of third parties to develop their capacities as part of steps to provide omnipresent interaction. Such collaboration includes the exchange of important information between the SPA process and expertise of third parties. Skills from third parties include access to information from users such as location, mobile number, email address, names, computer addresses, payment details and many others, that users must agree to use the skills[17].

5. Conclusion

This paper explains the security analysis of the Virtual Personal Assistant systems, its basic structure. Further describing the various attacks and security issues in the VPA systems. It brings together the attacks that are possible on the VPA system to exploit the system and get through the authentication. In other applications, a new VPAs system can be used, including education support, medical assistance, vehicle and robotics, systems with disabilities, automation at home and security access control. Another challenge for authentication arises from the emergence of the VPA ecosystem: the user also finds it difficult to determine whether they actually talk about the right skill and VPA as they expect. The question is that the skills market contributes to. The approved user is affected by these attacks to the voice-controlled system, as no protection is given for the user's authentication.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

REFERENCES

[1] Kepuska, V., &Bohouta, G. (2018). Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home). 2018 IEEE 8th Annual Computing and Communication Workshop and Conference, CCWC 2018, 2018-January(c), 99–103.

[2] Clark, G., Doran, M., & Glisson, W. (2018). A Malicious Attack on the Machine Learning Policy of a Robotic System. Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, (Ml), 516–521.

[3] 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. Proceedings - IEEE Symposium on Security and Privacy, 2019-May, 1381–1396.

[4] Trifonov, R., Nakov, O., &Mladenov, V. (2019). Artificial intelligence in cyber threats intelligence. 2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018, 1–4.

[5] Sadeghi, K., Banerjee, A., & Gupta, S. K. S. (2019). An Analytical Framework for Security-Tuning of Artificial Intelligence Applications under Attack. Proceedings - 2019 IEEE International Conference on Artificial Intelligence Testing, AITest 2019, 111–118.

[6] 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. 2018 IEEE Conference on Communications and Network Security, CNS 2018, 1–9.

[7] Kanimozhi, V., & Prem Jacob, T. (2019). Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing, ICCSP 2019, 33–36.

[8] Dekate, A., Kulkarni, C., &Killedar, R. (2016). Study of Voice Controlled Personal Assistant Device. International Journal of Computer Trends and Technology, 42(1), 42–46.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[9] Falco, G., Viswanathan, A., Caldera, C., &Shrobe, H. (2018). A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities. IEEE Access, 6, 48360–48373.

[10] Sagar, B. S., Niranjan, S., Kashyap, N., & Sachin, D. N. (2019). Providing cyber security using artificial intelligence - A survey. Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019, (Iccmc), 717–720.

[11] Khor, J. H., Ismail, W., Younis, M. I., Sulaiman, M. K., & Rahman, M. G. (2011). Security problems in an RFID system. Wireless Personal Communications, 59(1), 17–26.

[12] Gaglio, S., Lo Re, G., Morana, M., &Ruocco, C. (2019). Smart assistance for students and people living in a campus. Proceedings - 2019 IEEE International Conference on Smart Computing, SMARTCOMP 2019, 132–137.

[13] Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2019). Smart Home Personal Assistants: A Security and Privacy Review. (March).

[14] Thompson, S., Giles, N., Li, Y., Gharib, H., & Nguyen, T. D. (2007). Using AI and semantic web technologies to attack process complexity in open systems. Knowledge-Based Systems, 20(2), 152–159.

[15] Zhang, R., Chen, X., Wen, S., Zheng, X., & Din, Y. (2019). Using AI to Attack VA: A Stealthy Spyware against Voice Assistances in Smart Phones. IEEE Access, 7, 1–1.

[16] Y. Nung, A. Celikyilmaz.Deep Learning for Dialogue Systems. Deep Dialogue.

[17] G. Bohouta and V. Z Kepuska. 2017. Improving Wake-Up-Word and General Speech Recognition Systems. 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress.

[18] SIKDER, A. K., AKSU, H., AND ULUAGAC, A. S. 6thsense: A contextaware sensor-based attack detector for smart devices. In 26th USENIX Security Symposium (USENIX Security 17) (Vancouver, BC, 2017).

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[19] Vaidya, T., Zhang, Y., Sherr, M., AND Shields, C. Cocaine noodles: Exploiting the gap between human and machine speech recognition. In 9th USENIX Workshop on Offensive Technologies (WOOT 15) (Washington, D.C., 2015).

[20] Khan, M. T., Huo, X., LI, Z., AND Kanich, C. Every second counts: Quantifying the negative externalities of cybercrime via typosquatting. In 2015 IEEE Symposium on Security and Privacy (2015).

[21] N. Carlini, P. Mishra, T. Vaidya, Y. Zhang, M. Sherr, C. Shields, D. Wagner, and W. Zhou, "Hidden voice commands," in USENIX Security, 2016.

[22] M. Kunz, K. Kasper, H. Reininger, M. M¨obius, and J. Ohms, "Continuous speaker verification in realtime." in BIOSIG, 2011

[23] DIAO, W., LIU, X., ZHOU, Z., AND ZHANG, K. 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 (2014).

[24] D. Watkins, "Strategy analytics: Amazon, google to ship nearly 3 million digital voice assistant devices in 2017,"

[25] Selma Dilek, HuseyinCakir and Mustafa Aydin "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," Int. J. Artif. Intell. Appl., vol. 6, no. 1, pp. 21–39, 2015.

[26] RanjeevMittu&Willliam F. Lawless, "Human Factors in Cybersecurity and the Role for AI," in Foundations of Autonomy and Its (Cyber) Threats: From Individuals to Interdependence: Papers from the 2015 AAAI Spring Symposium, 2015, pp. 39–43.

[27] ArockiaPanimalar.S, GiriPai.U, Salman Khan.K, "Artificial Intelligence Techniques for Cyber Security," Int. Res. J. Eng. Technol., vol. 5, no. 3, pp. 122–124, 2018.

[28] M. Baloul, E. Cherrier, and C. Rosenberger, "Challenge-based speaker recognition for mobile authentication," in BIOSIG, 2012.