IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor 6.252

Volume 2, Issue 1, July 2022

Survey of Security Issues with Virtual Assistant Technology

Chirag Liladhar Nehete[1] and Prof. Divakar Jha[2]
Student, Department of MCA[1]
Mentor, Department of MCA[2]
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Today, virtual voice-assistants are used for manifold purposes. Besides their promising potential, many users are concerned about their privacy and what happens to the data recorded by the voice assistant. Relating the well-known privacy utility trade-off, we found out that not the price of a voice assistant is the most important factor for its acceptance, but privacy. Nevertheless, the acceptance of voice assistance and the decision to use a voice assistant always depends on a combination of different factors, of which privacy seems to be most important.*

Keywords: Virtual Private Voice Assistants, Security Risks, Privacy, Threat, Vulnerabilities

I. INTRODUCTION

Every voice assistant has inherent privacy issues. It's the nature of the game of collecting data, particularly biometric data like voice data. Because while the end-user may not realize it, the only way a voice assistant is useful for the developer is when you're able to review the voice data you collect, either through software, human review, or a combination of the two. From the consumer perspective, the issues associated with voice assistants are two-fold. First, the consumer is worried about "who is listening." In these cases, those who use voice assistants must be transparent about how the data gets used and who gets to hear it. The second issue is one of security. Voice assistants only "listen" in the background until called upon, but they still collect huge amounts of data, which will only be compounded by the number of available applications for voice assistants in the growth of users. Hundreds of millions of people already use voice assistants, which means the amount of data they generate is already staggering. What's more, the keyword trigger designed to 'activate' the voice assistant can be sensitive, which means people can accidently engage the assistant and inadvertently record huge amounts of sensitive data. Transparency and privacy come together again because the data created by voice assistants is increasingly personal. Smart assistants don't only collect data created through voice interactions, which can be virtually limitless. They also integrate with apps and other devices .Virtual Private voice assistants (VPVA's) are a new technology whose acceptability, privacy concerns, security Risks, vulnerabilities [1] [2] [2] have been researched on, but missing on the recent advancements, illustration of Security risks, Check point's research, and the certain measures users can take to minimize security issues related to the VPVA's.

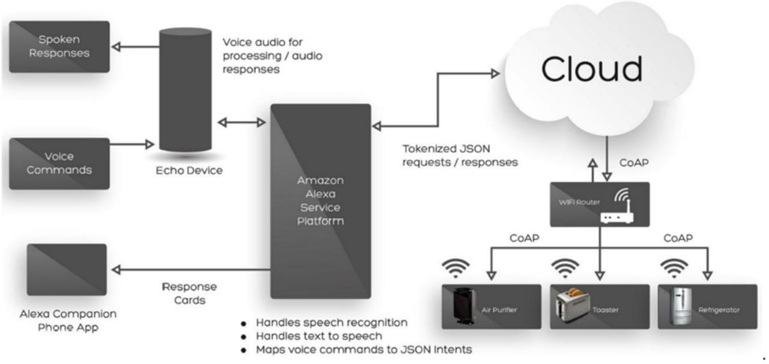
Spoken Responses
Voice Commands
Echo Device
Voice audio for processing / audio responses
Cloud
Amazon Alexa Service Platform
Tokenized JSON requests / responses
CoAP
WiFi Router
CoAP
CoAP
Air Purifier
Toaster
Refrigerator
Alexa Companion Phone App
Response Cards
Handles speech recognition
Handles text to speech
Maps voice commands to JSON Intents

Figure 1. Architecture of a voice assistant (Alexa) (https://www.faststreamtech.com/blog/amazon-alexa-integrated-withiot-ecosystem-service/). (access on 10 February 2021) [6].

DOI 10.48175/568

In 2019, the Daily Telegraph reported that Amazon employees were listening to Alexa users' audio—including that which was recorded accidentally at a rate of up to 1000 recordings per day [4]. As well as concerns about snooping by the VA, there are several privacy and security concerns around the information that VA companies store on their servers. The software application on the VA device is only a client the bulk of the assistant's work is done on a remote server, and every transaction and recording is kept by the VA company [5].

An example request might follow these steps:

1. The VA client—the 'Echo Device' in the diagram—is always listening for a spoken 'wake word'; only when this is heard does any recording take place.
2. The recording of the user's request is sent to Amazon's service platform where the speech is turned into text by speech recognition, and natural language processing is used to translate that text into machine-readable instructions.
3. The recording and its text translation are sent to cloud storage, where they are kept.
4. The service platform generates a voice recording response which is played to the user via a loudspeaker in the VA client. The request might activate a 'skill'—a software extension—to play music via streaming service Spotify, for example.
5. Further skills offer integration with IoT devices around the home; these can be controlled by messages sent from the service platform, via the Cloud.
6. A companion smartphone app can see responses sent by the service platform; some smartphones can also act like a fully-featured client.

As with any distributed computing system, there are several technologies used. The endpoint of the system with which the user interacts, shown here as the Echo device, commonly takes the form of a dedicated smart speaker—a computer-driven by a powerful 32-bit ARM Cortex CPU. In addition, these speakers support WiFi, Bluetooth, and have internal memory and storage [7].

II. LITERATURE REVIEW

This survey tried to provide the adaptability, recent advancements, privacy concerns, Security Risks with multiple demonstrations, surprisingly how still issues such as "Electronically Produced Speeches" can wake up a device, which could possibly lead to a massive threat affecting multiple user simultaneously, and different types of security threats and vulnerabilities analysis that can be observed in every phase of the VPVA process, and also tried to include the demonstration of Checkpoint's (Cybersecurity solution company) [8] Research on the vulnerability identified in Amazon's Alexa, and finally ending the survey with some actions that could be taken from the user end to minimize the privacy and security issues from the user's end. Hopefully the initial efforts can stimulate further research on the Privacy and Security related concerns on the VPVA devices. In the upcoming work, aiming to cover the authentication schemes, and algorithms that is associated with the process.

It was found that the VA is becoming the target of malicious attacks just as other connected computing devices have been in the past. These attacks show an interesting pattern: they are evolving. For any malicious attack to be effective and dangerous to the end user, it must be simple enough to be carried out by someone who has not made an extensive study of the VA's internal architecture. Furthermore, an attack is made more dangerous by the lack of the need to be proximate to the device. Finally, any attack must be repeatable—if it only works once, in laboratory conditions for example, it poses little threat to the end user. A ready-coded, malicious skill could be exploited remotely by a threat actor with limited knowledge of computer science and it surely, at this point, cannot be long before these attacks are more commonplace.

III. PRIVACY CONCERNS

Virtual Private voice assistant (VPVA) have had widely published privacy related issues. It could be the data that is being collected or could be the actuality that they reportedly ask the employees or could be the contractors to listen to recordings in order to improvise the accuracy, however it is sensitive information which could be very private are getting leaked via these devices. Virtual Private voice assistant pose complex privacy implications.

The recorded conversations of the Virtual Private voice assistants are stored in the databases. These recorded conversations are saved for an extended period of time could be years or months. Anyone having access to the backend

DOI 10.48175/568

can access the stored voice recordings. Normally, the access to these recordings is limited to the owners of the Virtual Private voice assistant. However, it is to be noted that these group of participants and owners may belong to various groups. However, these conversations which are getting recorded could be done on purpose without the consent of user or by accident. Such recordings might be used at the later stage, and it is a key to identify details such as the user's location, routines, participants of the conversation, and the confidential conversations. Let us consider few instances related to Privacy when using the VPVA.

3.1. Always On, Always Listening

VPVA devices keep listening to all the user conversations while it is waiting for the wake-up word. When a device is always on, it means that it is always listening which leads to security and privacy concerns. Fig 2 illustrates on how an attacker could compromise a Virtual Private voice assistant (VPVA) enabled device through its "Always On, Always Listening" feature, which enables the hacker to monitor all voices and sounds in real time.

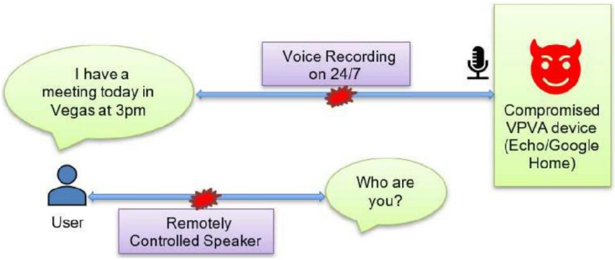
I have a meeting today in Vegas at 3pm
Voice Recording on 24/7
Compromised VPVA device (Echo/Google Home)
User
Remotely Controlled Speaker
Who are you?

Fig 2. Always On, Always Listening

3.2 Compromised Device — Harmful Voice Commands

Fig 3 illustrates an attacker who imitates a user and provide commands which are harmful, For Example, to unlock a smart door and gain access to home which is unauthorized, online shopping without the user's knowledge. Thus, when an attacker who can now access VPVA enabled device will fake the system and make it believe that attacker is the legitimate user and perform all sorts of criminal acts.

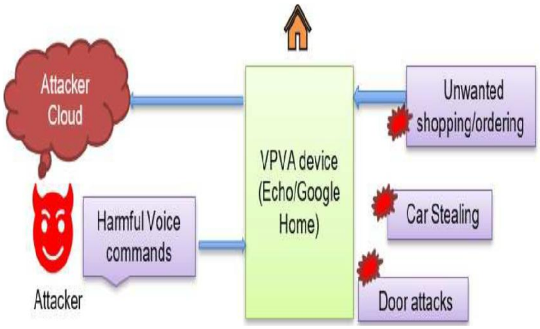

Fig. 3. Compromised Device – Harmful Voice Command

3.3 Weak Authentication — Speech/Voice Authentication

Voice authentication in Virtual Private Voice Assistants can be considered to be one of the weak authentication types. For example, verification of the speaker via voice authentication in Google is called to be voice match [9] and in Amazon it is called to be voice profiles [10]. By default, these mechanisms are not enabled, users have to firstly notice that there is such a feature and then it is completely on the user to get it activated or not to. Even though these kinds of features are activated, attackers can easily collect the electronical voice sample of the lawful user and fool the system [11][12].
Voice samples collection is easily available to the public and it is a painless task to the attacker to obtain it. Passwords can be very easily altered if they are compromised whereas it is a known fact that it is very difficult to replace the characteristic of a human voice.

DOI 10.48175/568

Voice Authentication without External Device

As discussed in this paper, VA user authentication is a concern, as with any other service that collects user data. A VA collects substantial amounts of personal data, as demonstrated in the forensics-focussed works studied in this paper. Several novel methods for authenticating a user to their device were presented in the primary studies. However, each used an external device to provide a form of two-factor authentication, which makes the resultant solution cumbersome and complicated for the user. An interesting future research direction could address this challenge by focusing on biometric voice analysis as a means of authenticating the user, rather than relying on an external device.

IV. CONCLUSION

This survey tried to provide the adaptability, recent advancements, privacy concerns, Security Risks with multiple demonstrations, surprisingly how still issues such as “Electronically Produced Speeches” can wake up a device, which could possibly lead to a massive threat affecting multiple user simultaneously, and different types of security threats and vulnerabilities analysis that can be observed in every phase of the VPVA process, and also tried to include the demonstration of Checkpoint’s (Cybersecurity solution company) [8] Research on the vulnerability identified in Amazon’s Alexa, and finally ending the survey with some actions that could be taken from the user end to minimize the privacy and security issues from the user’s end. Hopefully the initial efforts can stimulate further research on the Privacy and Security related concerns on the VPVA devices. In the upcoming work, aiming to cover the authentication schemes, and algorithms that is associated with the process.

There were several emerging security and privacy concerns, security and privacy concerns do affect users adoption of VAs and adoption of a particular model of VA. This paper provides and overview of many kind of security and privacy issues with virtual assistant technology. In this report of privacy issues a voice authentication or a speech recognition has to be integrated so that the assistant can be access by the users voice only, and also multi factor authorization of the user will be integrated.

REFERENCES

[1]. “Amazon Alexa virtual assistant bug fixed after cybersecurity firm discovered vulnerabilities.” https://www.8newsnow.com/news/localnews/amazon-alexa-virtual-assistant-security-bug-fixed-aftercybersecurity-firm-discovered-vulnerabilities/ [Online; last accessed 5-Nov-2020]

[2]. N. Zhang, X. Mi, X. F, X. Wang, Y. Tian, and F. Qian, “Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems,” 2019 IEEE Symposium on Security and Privacy.

[3]. H. Hyunji Chung, Michaela Iorga and Jeffrey Voas. NIST, Sangjin Lee, Korea University, “Alexa, Can I Trust You?”, The IEEE Computer Society 2017

[4]. Cook, J. Amazon employees listen in to thousands of customer Alexa recordings. 2019. Available online: https://www.telegraph.co.uk/technology/2019/04/11/amazon-employees-listen-thousands-customer-alexa-recordings/ (accessed on 25 March 2020).

[5]. Chung, H.; Park, J.; Lee, S. Digital forensic approaches for Amazon Alexa ecosystem. Digit. Investig. 2017, 22, S15–S25. [CrossRef]

[6]. Siebra, C.; Correia, W.; Penha, M.; Macedo, J.; Quintino, J.; Anjos, M.; Florentin, F.; da Silva, F.Q.B.; Santos, A.L.M. Virtual assistants for mobile interaction: A review from the accessibility perspective. In Proceedings of the 30th Australian Conference on Computer-Human Interaction, Melbourne, Australia, 4–7 December 2018; pp. 568–571.

[7]. Amazon Alexa Integrated with IoT Ecosystem Service. Available online: https://www.faststr eamtech.com/blog/amazon-alexaintegrated-with-iot-ecosystem-service/ (accessed on 22 February 2021).

[8]. Dikla Barda, Roman Zaikin, Yaara Shriki, “Keeping the gate locked on your IoT devices: Vulnerabilities found on Amazon’s Alexa.” https://research.checkpoint.com/2020/amazons-alexa-hacked/ [Online;last accessed 1-December-2020].

[9]. Carlini, N., Mishra, P., Vaidya, T., Zhang, Y., Sherr, M., Shields, C., Wagner, D., Zhou, W.: “Hidden Voice Commands.” In: Proceedings of the 25th USENIX Security Symposium (2016)

DOI 10.48175/568

[10]. "Amazon 2017 About Alexa Voice Profiles", https://www.amazon.com/gp/help/customer/display.html?nodeId=202199440. [Online; last accessed 8-November-2020].

[11]. JIDE S. EDU, JOSE M. SUCH, GUILLERMO SUAREZ-TANGIL,"Smart Home Personal Assistants: A Security and Privacy Review ACMComputer. Survey.", Vol. 1, No. 1, Article. Publication date: August 2020

[12]. Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Hennenfent, Joshua Mason, Adam Bates, and Michael Bailey.2018. "Skill Squatting Attacks on Amazon Alexa". In 27th USENIX Security Symposium