International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 03 | Mar -2020 ISSN: 2582-3930

Overview of Security Issues in Voice First Devices

Bollampally Rohit Bhargav

Department of Information Technology, Anurag Group of Institutions

---

ABSTRACT -Information is the critical asset that needs to be secured and protected from unauthorized accesses. With rapid technological advancements happening around the world there has been a significant rise in interest and usage of voice first devices which are designed with minimal security features. Amazon, Google, Microsoft are the companies that opened their platforms for developer driven extensions to build voice-based systems. The main focus of this research is to describe the potential security and privacy issues of voice first devices which are now prevalent in many houses around the world.

1. INTRODUCTION

Voice first platforms primarily interact through voice and then are open for extension by third party developers. When a banks Interactive Voice Response (IVR) system is compared to what a user can do on the Amazon Echo the options on the Echo are limitless. Instead we can have a more natural conversation.

Voice first devices can not only perform built in functions, they can also buy products and can search the web or they can take help of the apps created specifically for the platform- "Skills" in Alex parlance.

Skills are the voice enabled apps that developers can create for service that allow users to interact with their own device. Amazon provides a platform in creating these apps in the form of Alexa skills kit interface.

2. ANATOMY OF VOICE FIRST DEVICES

To fully perceive the privacy of user information, we've got to investigate and perceive the anatomy of voice initial devices. However information flows from the user to the assorted platforms. Could this can facilitate in recognizing at that points the user's data may leaked which might result in serious exploit.The voice initial device streams the user's speech to the platform, that successively performs language Undersatnding (NLU). Then the speech passes the nowstructured information to the fulfilment, that is developer created code that contains logic. The fulfilment builds the response into a structured format and reverses the method. The response goes back to the platform and also the platform transforms the text to speech. Speech to information and information to speech once more. With the ever-increasing quality of voice enabled devices, customers are getting more aware and terrified of their privacy doubtless being in danger to malicious hackers.

3. PRIMARY SECURITY AND PRIVACY GOALS

In order to have efficient security for voice first devices, we must be aware of primary security goals as follows

3.1 CONFIDENTIALITY

Confidentiality is an important security feature with voice first devices. Sensitive data such as conversations, payment details, personal details must be hidden from unauthorized entities.

3.2 INTEGRITY

In order to provide reliable services to users, integrity is a mandatory security property. It is the trustworthiness of data or resources in the prevention of unauthorized use.

3.3 AVAILABILITY

A user must be capable of accessing services anytime, whenever needed. It should provide assurance that the system responsible for processing information are accessible when required.

4. POTENTIAL ATTACKS

There are many risks involving as there are points of vulnerabilities that intruders can easily setup and access

4.1 WIRETAPPING

Using voice first platforms allows intruders to easily tamper with the device maliciously to their needs such as for packet sniffing, accessing stored recordings of the conversations.

4.2 EAVESDROPPING

Malicious intruders can make use of voice first devices for unauthorized interception of user's conversations without their consent.

4.3 UNAUTHORIZED TRANSACTIONS USING SKILLS

The malicious intruders can hijack and tamper with how users may interact with their skills and thereby making unauthorized transactions using bank account details of the legitimate user.

4.4 PORT BASED ATTACKS

As voice first devices make use of ports for interaction and communication these ports might be subject to attacks from intruders which helps them in gaining access to the device

4.5 DENIAL OF SERVICE ATTACKS

Intruders can perform denial of service attacks on voice first devices. As voice first devices make use of wireless routers to access internet, intruders can send large number of packets by hacking these wireless routers to voice first devices which may reboot these devices or might completely destroy them.

5. INDUSTRIAL RESEARCH AND REPORTS

A report from EY the future of privacy forum provides information about the privacy implications concerning microphone enabled devices. The report talks about the developments in speech recognition technology and also about the availability of these devices. The report also showcases the legal issues that surround these kinds of devices and how these violate federal wiretapping laws.

There are several blogposts from people who work in cybersecurity, detailing security flaws in Amazon echo device. The writer manages to intercept the package being sent over HTTP which makes programs such as Wireshark to obtain image files.

Google also has a security bulletin for the operating system which releases a list of critical vulnerabilities.

6. PREVENTION AND COUNTER MEASURES

The attacks on voice first devices can be prevented by following few policies and procedures.

6.1 ENCRYPTION AND DECRYPTION ALGORITHMS

Using encryption and decryption algorithms we can prevent wiretapping and Eavesdropping as the data passing through the network will be encrypted and the intruder cannot tamper with that data.

6.2 TWO FACTOR AUTHENTICATIONS

Using two factor authentications helps in preventing unauthorized bank transactions. Usage of voice recognition and one-time passwords for transactions related to purchase helps in overcoming this type of skills-based attacks.

6.3 SECURE PORTS

Ports are the main areas where intruders try to enter and make use of them. Using secure ports for communication is the best way to overcome port-based attacks.

7. CONCLUSION

The rise in the usage of voice first devices has increased the awareness of several privacy issues among users and developers. Upon researching on these issues, there are several sources of potential exploits and vulnerabilities available for voice first devices.

This brief overview of security issues within voice first devices and with the increase in popularity of speech recognition technology, it would not be surprising to have new and more complex security problems appearing in future.

REFERENCES

1. Dustin A. Coates, Voice Applications for Alexa and Google Assistant.
2. A. Alhadlaq, Privacy in Amazon Alexa Skills Ecosystem, in PETS, 2015.
3. Stacey Gray, Always on: Privacy Implications of Microphone-Enabled Devices.