Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

Literature Review

A Study of breach attack simulation in smart voice assistants

Jingyi Qin Supervisor: Dr Martin Harrigan

MSc in Cybersecurity, Privacy and Trust

1.Introduction

There are already many tools in the market that are ready to use for breach attack simulation. They can use to simulate a cyber-attack on the organization's network, infrastructure, application and on email. But as smart devices become popular, more smart home devices are implemented with home users. Many of them use smart audio devices like Amazon Echo, and Google Nest to control their smart home devices. Does there any solution that we can use to run the attack simulation on smart audio devices?

In this research, we are focused on creating an attack simulation solution that can use for smart audio devices. The project is to extend Infection Monkey to do the perception layer attack. To do the attack simulation on smart voice assistants to find the weakness of these types of systems in cybersecurity.

Infection Monkey is a tool that currently can general a network map and security report. Also, have ransomware simulation. But not have a feature to run the attack simulation for smart audio devices. So this project is to general a full solution of smart audio device voice attack simulation by using the Infection Monkey.

2. Research Questions

Q1:

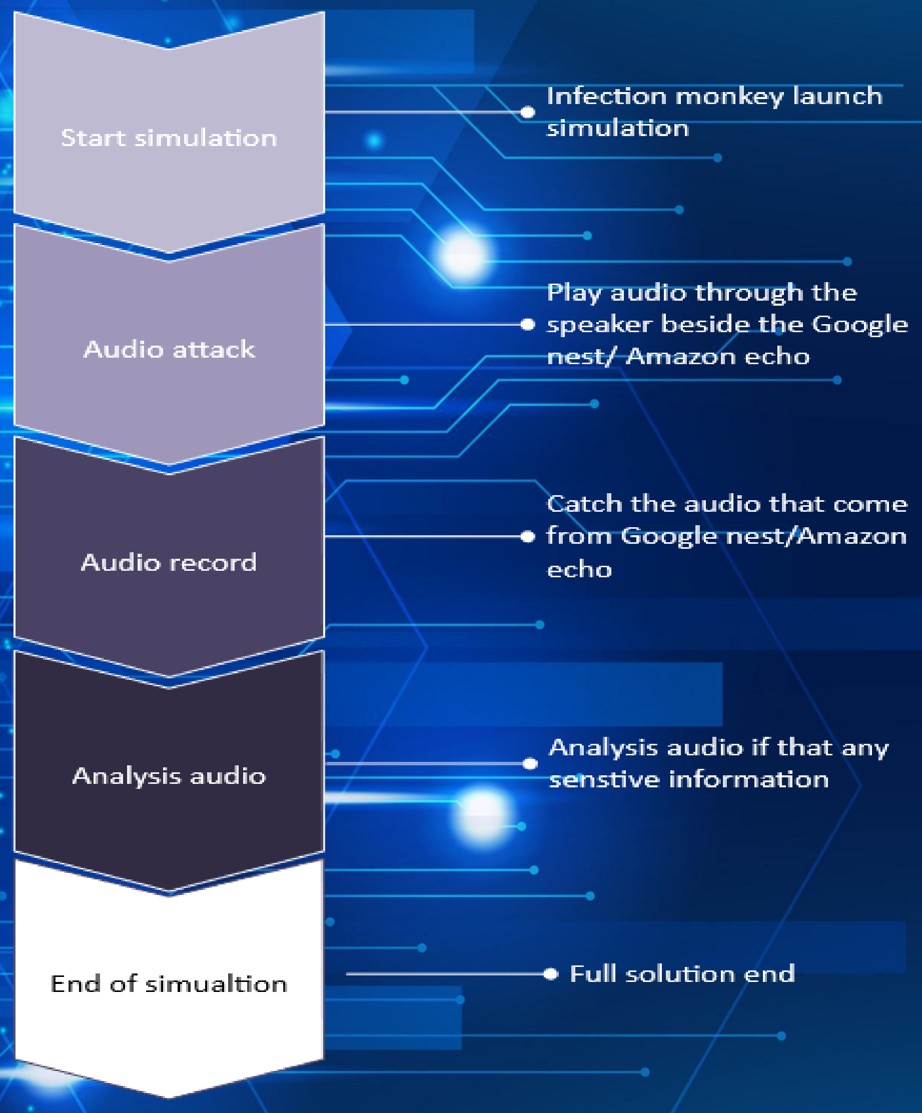
Can we extend Infection Monkey to perform a perception attack on voice control systems such as Google Nest and Amazon Alexa?

Q2:

Can we exploit any (un)known vulnerabilities in Google Nest or Amazon Alexa using this form of attack?

3. Literature Review

- Virtual personal assistants (VPA), also known as smart assistants like Amazon's Alexa and Google's Assistant, are in the spotlight for vulnerabilities to attack. Take, for example, that incident about an Oregon couple's Echo smart speaker inadvertently recording their conversation and sending it to a random contact. *(Umawing, 2018)*
- The voice assistant system attack is the perception layer attacks, it bypass the platform's security policies on Authentication as well as Encryption and data protection *(Wang et al., 2022)*



Start simulation — Infection monkey launch simulation

Audio attack — Play audio through the speaker beside the Google nest/ Amazon echo

Audio record — Catch the audio that come from Google nest/Amazon echo

Analysis audio — Analysis audio if that any senstive information

End of simualtion — Full solution end

Figure 1 Full solution structure

4. Technologies

- **Research target:** Google Nest, Amazon Echo
- **Software:** Infection Monkey

5. Next Steps

- The audio attack simulation for smart audio devices will need to set up a new process and allow simulation. As the simulation need to run automatic and frequency. So, to test the new process work and stable is important.
- The speed of testing is also important, that will affect the time of simulation running. To test the time of simulation and compare to usual tests performed should be consider.