**Bluetooth Vulnerability Research (EvilSmurf)**

Kelly-Ann Downer, Kaitlyn Malone, Josh Minick, Vi Nguyen, Jack Raymond

**Overview:**

As Bluetooth technologies become more popular, the vulnerabilities within Bluetooth also rise significantly. These vulnerabilities make the systems and devices more exploitable and put confidential data at risk. There are two types of authentications when it comes to pairing, which are legacy authentication procedures and secure connection procedures. These processes allow the two Bluetooth devices to securely pair with one another and establish a secure connection between the two devices for future uses. However, an attacker can insert themselves into the system, pretending to be one of the pairing devices and manipulate the system connection once they get in. This project, our team is exploiting the known vulnerabilities in the old systems, finding patches, and analyzing them for future mitigation.

The sponsor that our team is working with is Lockheed Martin (LM). LM is one of the biggest aerospace and security companies in the world and was created in 1995. LM works with private companies and organizations on defense and security projects. LM also has contracts with the government to build aircraft and spacecrafts for the military. LM is an international company that employs thousands of people who are working to ensure the company is operating properly through their use of extensive enterprise networks and information technology solutions.

**Operations:**

This project is split into three primary phases: 1) Vulnerability Exploitation, 2) Automated Vulnerability Remediation, and 3) Vulnerability Mitigation and Testing. In the first phase, vulnerability exploitation, the team was asked to exploit two Bluetooth vulnerabilities. First, two Common Vulnerabilities and Exposures (CVEs) were found and exploited successfully. Next, we reproduced the results and documented our findings. In the second phase, automated vulnerability remediation, the team is tasked with creating and documenting an automated tool. This tool is expected to read a device and determine any vulnerabilities it might have, as well as provide mitigations or patches to help secure the device. Lastly, in the third and final phase, vulnerability mitigation and testing, the team will patch the previously exploited vulnerabilities and create a mitigation plan that will ensure more efficient remediation in case of a repeat event.

**Design:**

The product delivered to the sponsor, Lockheed Martin, will be two automated vulnerability detection and remediation systems. These systems will scan a given device for vulnerabilities, patch the device if it is susceptible, and rerun the scan to verify that the device has been fixed. Both systems will use python and shell scripting languages.

The product addressing the Bad Karma vulnerability will check whether a given Linux system is using a kernel version between 4.8 and 5.9. If so, the program will notify the user that the device is vulnerable and will ask whether to update the device. If the user responds yes, the system will install a newer, stable kernel version and reboot to apply the changes.

The product addressing the Crackle exploit will identify whether a nearby Bluetooth device is susceptible by determining whether the device is using both Link Layer encryption and Bluetooth Low Energy Legacy pairing. If a device is susceptible, the user will be notified and given various recommendations on how to best secure the device.

**Implementation:**

To gain a better understanding of the project, the team spent time researching Bluetooth vulnerabilities in the Linux environment for the first month and a half of the semester. Our search led us to the Bad Karma Bleedingtooth exploit which affects Linux kernel versions 4.8 through 5.9. This vulnerability when executed causes the victim’s kernel to panic, thereby crashing the device’s Bluetooth services. Any new or existing Bluetooth connections with the device will become unresponsive, resulting in a denial of service. The team then met up frequently to perform the exploit. A model of the exploit was done using a Linux environment on the RasberryPi OS 32-bit system, headphones connected via Bluetooth, and the proof-of-concept code which can be found [here](https://github.com/google/security-research/security/advisories/GHSA-h637-c88j-47wq). Compiling and executing the code caused the music that was being played on the system to be cut off and the Bluetooth disabled.

The second exploit was Crackle, which decrypted Bluetooth Low Energy packets. The demonstration of the attack was not successful due to issues encountered and time limitations. When the two exploits were completed, two documents were created to explain the steps taken to attack the system and how the exploit affects the vulnerable systems. The team also engaged the sponsor throughout the process with weekly meetings to provide updates on the project and incorporate any suggestions. Regular meetings were also set up with the team’s Mentor to provide great support and suggestions to improve the quality of the content being produced.

**Verification and Validation:**

To ensure these vulnerabilities cannot be exploited, we are developing a program to scan a network for devices with specific vulnerabilities. If these devices are detected, the program will trigger an alert along with remediation recommendations. A second program is then run to complete the fixes ensuring the device will no longer be vulnerable. Lastly, the vulnerability scanning program is run again to ensure the devices are patched successfully.