COMP 8047 Project Test Plan

[COMP 8037 – Major Project Test Plan]

[Eric Wu – A00961904]

[2021/04/08]

Environment Setup

Devices used:

- Two Kali Linux machine
- one smartphone
- one Bluetooth earbud

Some of the test cases require a Bluetooth dual-mode device (supports both BR/EDR and BLE). The two kali Linux machine by default runs Bluetooth in dual mode. To make the smartphone simulate a dual-mode device, we will install an external app that can open a GATT server. The app is called “BLE Tool”, and can be found on the google app store.

The assumption of this test plan is that all the devices involved must have the Bluetooth address known beforehand. One of the Kali Linux machines will act as the attacking machine.

Test Cases & result

*custom tool: an exploit tool developed for this project. Refer to the user manual for details

Case #	Description	Tool	pass/fail criteria	status
1	* Verify that the exploit can be executed on a Kali Linux based system	● Kali Linux	Pass if the exploits can be executed on the system	passed
2	* Verify that the DoS attack can disrupt the existing connection on the target Bluetooth device. Both the smartphone and Earbud are paired and connected prior to the start of this test.	● Kali Linux ● earbud ● smartphone ● custom tool ● Wireshark	Pass if two conditions are met. First, on the smartphone display, it should show that the device gets disconnected from the Bluetooth earbud. Second, the Wireshark packet capture should show that the Bluetooth connection gets terminated by the target device (Ear Bud).	passed
3	Check the HCI info on the attacking machine, and run a Bluetooth scan on the smartphone. * Verify that the machine running the exploits can spoof the identity of the legitimate Bluetooth client.	● Kali Linux ● earbud ● smartphone ● btmgmt ● hcitool ● Wireshark ● custom tool	Pass if three conditions are met. First, the HCI info display on the attacking machine should have both address and device name match with the Bluetooth client (earbud). Second, on the smartphone display, the Bluetooth client	passed

			name should appear as one of the results Third, on the smartphone display. when attempt to pair with Bluetooth client, the Wireshark running on then attacking machine should show capture connection request from the smartphone	
4	Pair and connect both smartphone and earbud. ***** Verify that the machine running the exploits successfully steals the Bluetooth session shared by the earbud and smartphone	● Kali Linux ● earbud ● smartphone ● Wireshark ● custom tool	Pass if two conditions are met. First, run hcitool with the “con” option. The list of connections displayed should include the address of both the smartphone and earbud. Second, the packet captured on the attacking machine should have packets that show “connection response - Success” from both smartphone and earbud.	passed
5	Play any audio on the legitimate Bluetooth host. ***** Verify that the attacking machine can receive the audio stream intended for the Bluetooth client.	● Wireshark ● Kali Linux ● Any audio source	Pass if two conditions are met. First, the audio stream on the attacking machine matches with the one sent from the Bluetooth host.	passed

			Second, Wireshark running on an attacking machine shows incoming traffic from the Bluetooth host.	
6	Verify that the exploit is capable of overwriting the long-term key generated from the legitimate Bluetooth host	● `Kali Linux (x2)` ● custom tool ● `hciconfig (Linux command)`	Compare the LTK on the Bluetooth client (victim) with the fake one generated from the attacker’s machine. Pass if same, fail otherwise	passed