CS 4820 – Fall 2022

Wireless and Mobile Security

Lab #3

Due: 10/21 11:30PM

In the class, we learned about Bluetooth protocol. In this lab, you will sniff Bluetooth traffic with both your phone and the provided antennas. You will also crack the sample Bluetooth packet with the tool.

For this lab, you are welcome to work as a team (team of 2) or by yourself. Each team (if you are working as a team) should aim to sniff Bluetooth traffic while the Bluetooth setting of the other person's phone is on/discoverable and display that.

Steps and Procedures:

a. Download 'nRF Connect' to your phone and run it to see available Bluetooth devices nearby. List them and explain at least 2 of the devices you see (you may know or investigate/make a logical guess about it).
b. Use the Bluetooth antenna to sniff the Bluetooth traffic around you. You can use ubertooth (https://ubertooth.readthedocs.io/en/latest/capturing_BLE_Wireshark.html) for this purpose and the provided Bluetooth antenna. You should do technical analysis of the packets captured (about 10 packets of your choice), such as SCAN_REQ/SCAN_RSP packets matches, etc.
c. Using the crackle tool and the samples posted on its github page, follow the same procedures to crack the Bluetooth capture. Please check the following github page to see how to do it and obtain the sample capture files: https://github.com/mikeryan/crackle

Report Submission:

Explain step-by-step how you do each task. Please provide all the screenshots to display your work and write the report in a way that it can be used as tutorial for others.

Extra Credit

1. (+20) Use crackle to crack your own Bluetooth capture rather than the one provided on github.