Bluetooth LE Security | Jacob Schwartz Cybersecurity Major

Faculty Advisor: Joshua White

SUNY POLYTECHNIC INSTITUTE
COLLEGE OF ENGINEERING

INTRODUCTION

Throughout our daily lives, Bluetooth LE is utilized in countless devices ranging from wireless headphones to things you wouldn't expect like Internet of things devices, cameras, printers, and miscellaneous computer peripherals all utilize Bluetooth LE in some way so the question I pose is how secure is Bluetooth LE given its wide use.

Bluetooth LE EXPLAINED

Bluetooth LE (low energy) is a wireless communication technology that allows devices to communicate with each other over short distances. It is also sometimes referred to as Bluetooth Smart this works by creating a wireless connection between two devices, a master and a slave. The master device initiates the connection and controls the communication between the two devices. The slave device responds to the master device's requests and sends data back as needed.

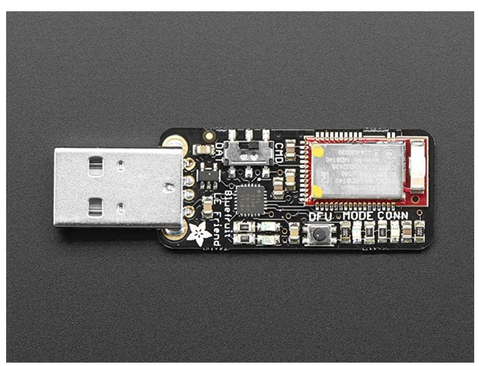
PROCESSES

To test how Secure Bluetooth LE can be a very simple and straightforward method is used, with an Adafruit Bluetooth LE sniffer and Wireshark I'm able to sniff the Bluetooth LE communication between devices. The setup for this project boils down to:

- Installing Wireshark
- Installing drivers for the Adafruit sniffer and Wireshark
- Installing python3 and pyserial for the Adafruit sniffer

PROCESS FOR CONDUCTING EXPERIMENT

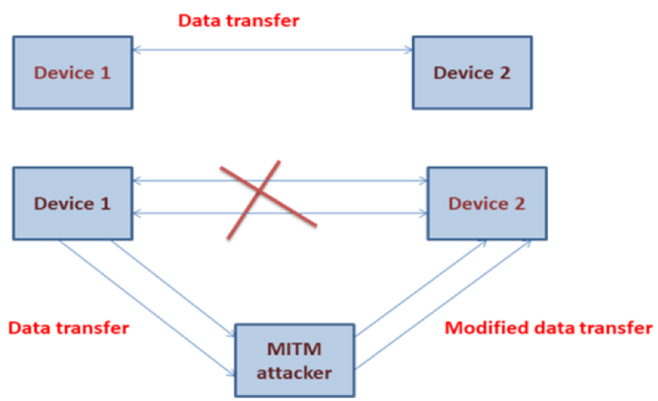
I used Wireshark for 5 minutes throughout each building on the SUNY Poly campus with the goal of demonstrating the variety of devices that utilize Bluetooth LE in a public setting and to see what kind of data I could get from sniffing in a public setting



RESULTS

Throughout the 5 Wireshark traces, there are a wide variety of devices that have Bluetooth communications captured specifically, what is captured are the series of Bluetooth LE communication packets between master and slave devices. There's a huge problem with having access to this data, as you can perform

- Device identification with MAC addresses
- Data interception because some of the packets may have login credentials or personal data
- Replay attacks because you have communication data between devices, you can store and reissue the communication later for malicious purposes. And as an extension of this, you can also do malware injection by inserting malicious code during the replay attack.



CONCLUSION

Even with using an extremely simple and straightforward method of Bluetooth sniffing data and devices are still at risk even with minimal data, the risk compounds on itself, if you can identify the device, you can do data interception, and if you can do that you can do replay attacks into malware injection which ultimately boils down to a Man in the Middle Attack

REFERENCES

1.https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf
2.https://us.norton.com/blog/mobile/bluetooth-security#
3.https://www.makeuseof.com/what-is-ble-bluetooth-low-energy/
4.https://novelbits.io/deep-dive-ble-packets-events/
5. https://developer.qualcomm.com/hardware/qca4020-qca4024/learning-resources/enforcing-security-between-ble-supported-devices