RUTGERS

WINLAB | Wireless Information Network Laboratory

IoT Red Team

Infiltrating an Internet of Things system

Adithya Rao Alkankara, Ashton Sopher, Daniel Chong, Joseph Shenouda, Justin Wang, Rishika Sakhuja, Samuel Minkin

Objective

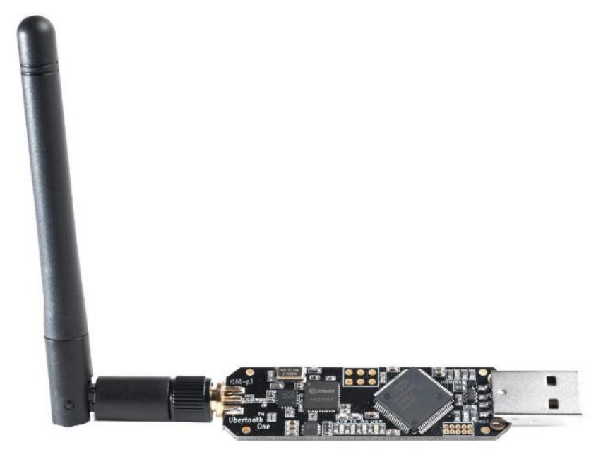
Our ultimate goal is to “attack” the IoT framework created by the Blue Team.

IoT stands for Internet of Things. An IoT system is a network of devices connected by a wireless communication protocol (ex. zigbee, z-wave, Bluetooth).

There are three different kinds of attacks that we attempted:

Sniffing: reading data that is being sent
Jamming: preventing data from being sent
Spoofing: intercepting and editing data

Hardware



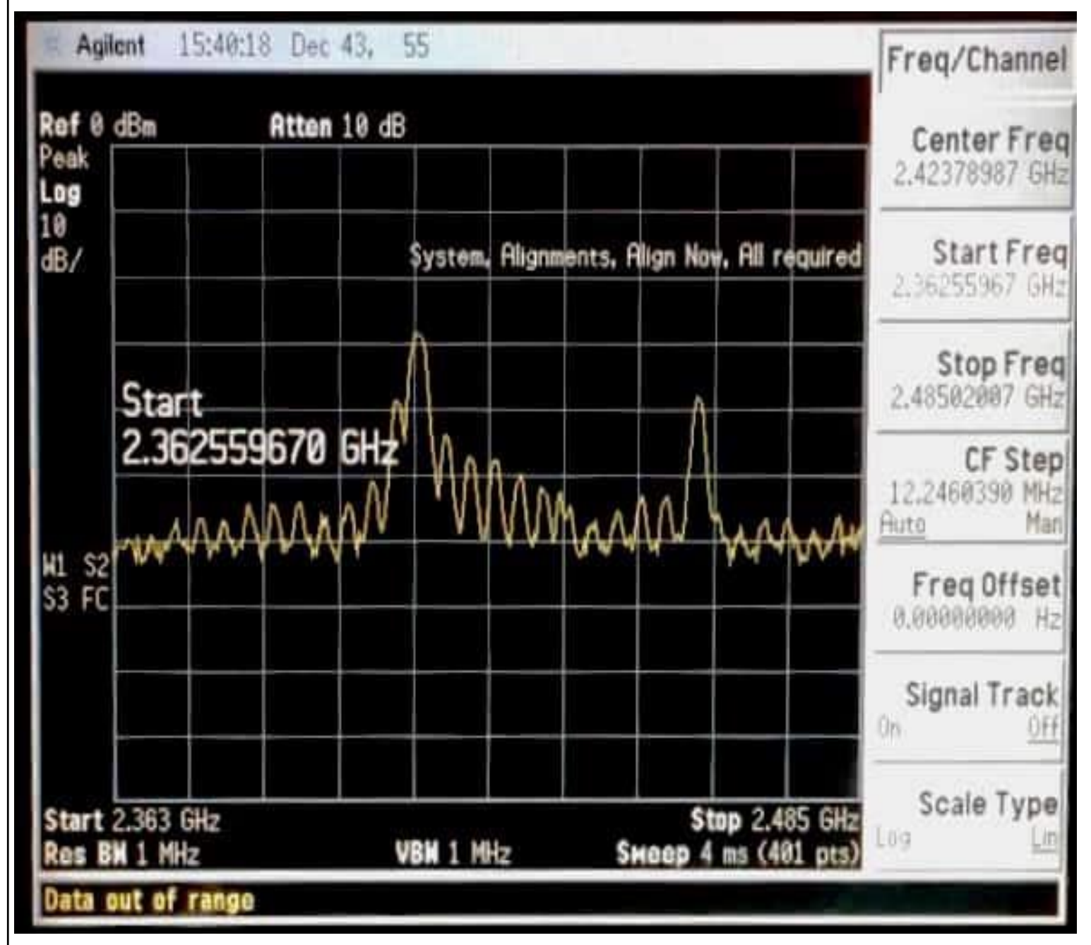
Ubertooth one

USRP x300

E4405B ESA-E Spectrum Analyzer

Attacks

Sniffing
We used the Ubertooth One and Wireshark, a packet analyzer used for network troubleshooting to capture Bluetooth Low Energy packets

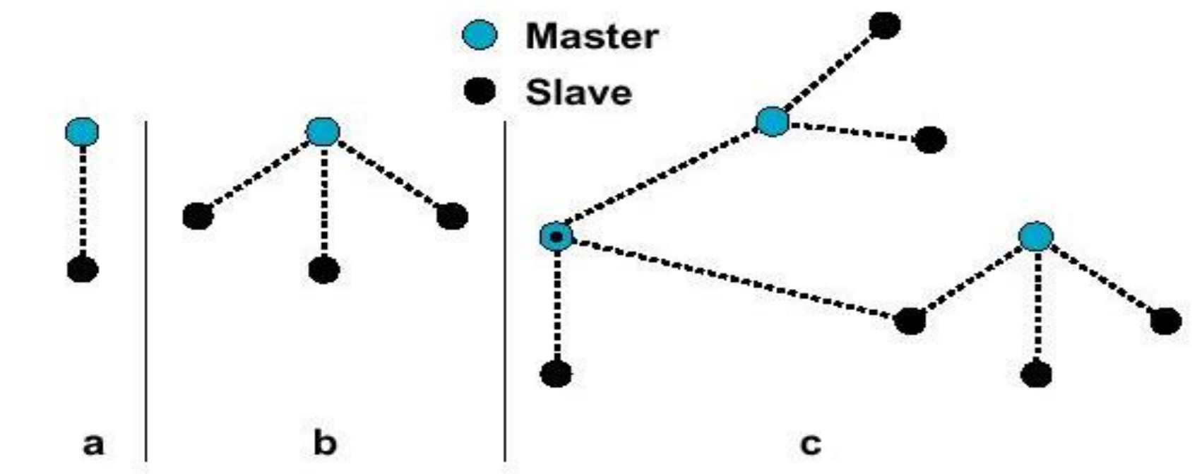


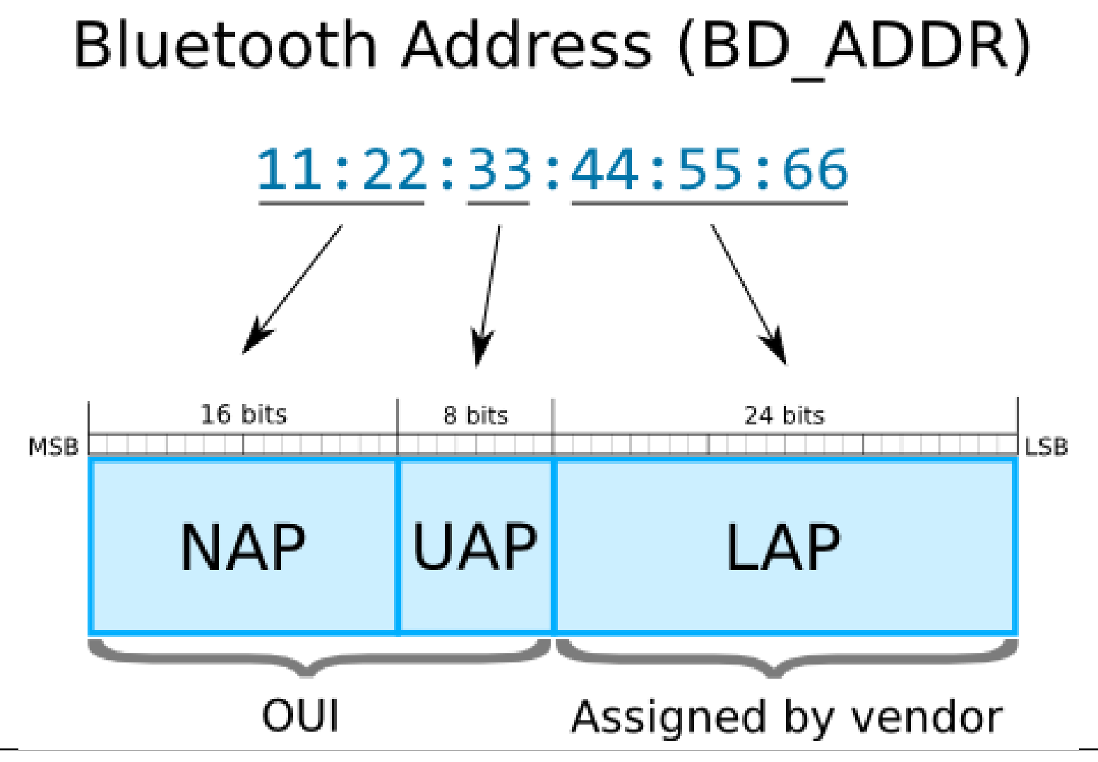
Jamming
We used a Software Defined Radio Peripheral (USRP x300) to generate signals in the same frequency range as Bluetooth to jam their data. To jam Bluetooth we had to generate a signal with a bandwidth wide enough to cover all frequencies that Bluetooth hops along.

Spoofing
Our approach was to create a copy of Blue Team’s sensor and then break their connection with the real sensor, in the hopes that, when they try to reconnect, they will unwittingly connect to our fake version of the sensor. We would also connect our own devices to the real sensor, thus establishing a man-in-the-middle attack in which we forward all traffic both ways so no one is aware of any issue with the connection, but at the same time we can read all the data being transmitted and subtly change certain information, all without Blue Team being aware that there is any issue.

Bluetooth

- Bluetooth works in a piconet topology with one master and up to seven slaves.
- The protocol transmits over the 2.4 GHz band, but uses frequency hopping to constantly switch between 79 unique frequencies within the band.
- All Bluetooth devices come with a Bluetooth address (BD_ADDR), a unique 48-bit identifier.
- BD_ADDR is split into 3 parts, the most important being the 24 bit Lower Address Part (LAP) which uniquely identifies the Bluetooth device in every transmission.





Conclusion

We were able to successfully carry two out of the three attacks we had planned to accomplish. In the future we hope to find a way to successfully spoof data to the Bluetooth devices. One of the main challenges we came across in this project was simply the lack of documentation and resources for penetrating Bluetooth, especially Bluetooth Low Energy.

WINLAB