Defcon 27 Badge NFMI- replay attack
Hacking the badge using Software Define Radio

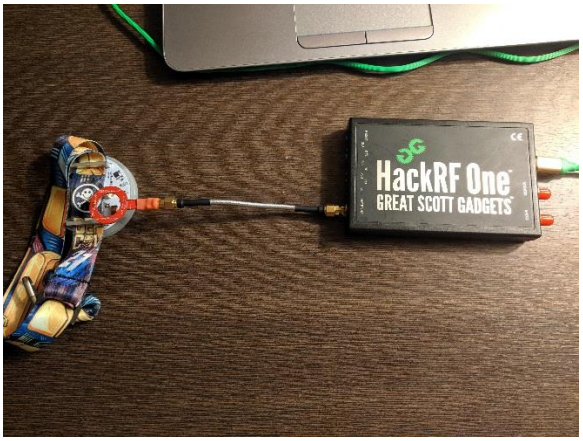
Team Members

Wohlford, Malm, Nelson

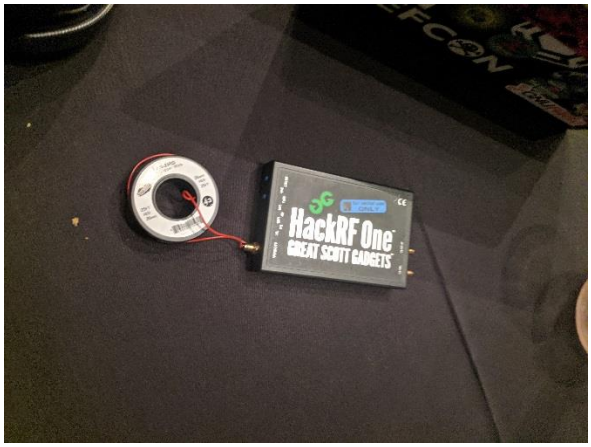
What we used

- Laptop running Ubuntu 19.x
- GNU Radio / GNU Radio Companion
- HackRF One SDR ($330 in the Vendor Village)
- RF Explorer H-Loop Near field Antenna part number RFEAN25 ($40 in the Vendor Village)
    - Or small spool of wire plugged into the HackRF One (less than $10)

NFMI source signal is approximately 10.25MHz to 10.9MHz



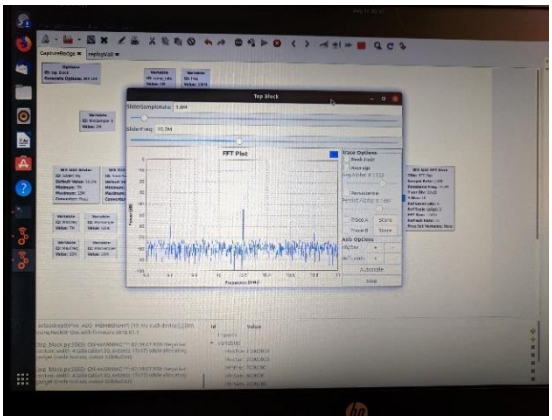
2 Our RFEAN25 antenna



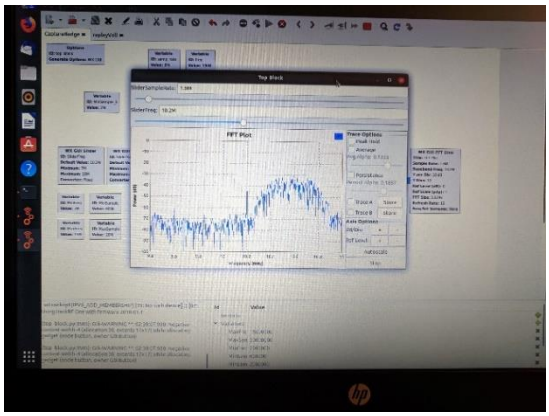
1 Another groups' successful loop antenna

Capture: Settings in GNU Radio Companion

1. Osmocom source
    a. Frequency: set to 10.2MHz
    b. Sample Rate: set to 1.6M



3 View of no active transmission



4 Badge actively transmitting

Replay: Settings in GNU Radio Companion

1. File source data with throttle
    a. Sample Rate 1.6M
2. Multiply throttled data by generated Signal
    a. Sample Rate 1.6m
    b. Consine: -350kHz
3. Low Pass Filter
    a. Cutoff Frequency: 185kHz
4. Multiply filtered data by Generated Signal
    a. Sample Rate 1.6m
    b. Consine: 350kHz
5. Multiply the broadcast signal (to amplify for retransmission)
    a. Value 50
6. Osmocom sink
    a. Sample Rate: 1.6M
    b. Frequency 10.2MHz