CS 4820 – Fall 2022

Wireless and Mobile Security

Lab #4

Due: 10/21 11:30PM

In class we discussed a methodology to reverse engineering a radio signal from a radio-enabled device. In this lab, you will realize such task with the SDRs provided.

Steps and Procedures:

First identify the frequency of the signal by making use of the FCC ID database at //www.fcc.gov/oet/ea/fccid
Determine a specific frequency by examining the signal in a spectrum analyzer such as inspectrum (https://github.com/miek/inspectrum) or audacity (https://manual.audacityteam.org/index.html).
After capturing some sample trac we further examined the signal to determine the modulation of the signal such as AM, FM, PSK, or GFSK
After determining the modulation, attempt to uncover the encoding scheme such as NRZ or Manchester
Finally, examine the signal as an alternate representation such as binary, decimal, hexadecimal, or ascii format to understand the underlying protocol

Lab Objectives
Working with a team of up to four students, you will reverse engineer a radio-enabled device RC car. All students will be provided with SDR dongle that can intercept radio signals.

Report Submission
You must produce a report discussing your understanding of the frequency, modulation, encoding, and protocol for the signal. You should also include any signal captures and gnuradio companion (grc) files that your team made to process the signal.

Extra Credit
1. (+10) Develop a gnuradio companion file to control the device you analyzed. Note, your gnuradio companion file may use a previously captured signal to execute a replay attack from a previous signal capture.