**Progress Report Number Two**

**Project Name:**

* REsDR (pronounced ‘reader’)

**Name/Roles of Team Members:**

* Ryan Eslick - Team Leader, Reverse Engineer
* Austin Brown - Signals Engineer
* Hunter Griffin - Technical Writer/Reviewer, Software Engineer
* Carter Church - Spectrum Analyst
* Daniel Bangham - Protocol Expert

**Updated Project Summary/Abstract:**

With the recent growth and utilization of software defined radio technology in commercial products, a greater focus on communication security needs to be upheld. The primary objective of the REsDR project is to develop a streamlined process of radio communication protocol recovery given a black box system. This entails initially having no formal understanding of the device, then reverse engineering its communication processes solely from wireless transmissions emitted by the device. The final goal of this project is to effectively decode and analyze the black box’s emitted binary data to achieve full understanding of the device.

**Current State of Project:**

* All purchased SDRs received and confirmed to be functioning correctly (four total in group).
* Team has been informed that black box device access is likely 1-2 weeks out.
* Continuing to experiment and further knowledge with SDR devices.
* Decoded some key fob signals using Universal Radio Hacker
* Did not receive black box last sprint so wasn’t able to investigate it as planned last sprint
* Waiting on word from Dr.Wells to see if we need to do anything to get the remote access server going, but might not need it now.
* Found tools such as GNU radio, wave converter, iqconvert, DSpectrumGUI, DSDPlus, Matlab/Octave, Universal Radio Hacker, Spektrum

**Major Project Issues/Obstacles Identification and possible solutions:**

*Obstacles)*

1. Lack of technical knowledge on some parameters used in gnu radio device blocks
2. Black box not available yet
3. Limitations imposed by bandwidth capabilities of rtl\_sdr v3 devices (2.8Mhz limit before sample loss occurs)
4. Ensuring auto detect features in tools are trustworthy

*Possible Solutions)*

1. Further research and collaboration amongst group members
2. Black box should be coming to us soon
3. Coordination with Dr. Wells to ensure the signals to be analyzed can be fully captured by our devices
4. Low level analysis of waveform plots and cross referenced with data obtainable from eye diagram plots

**Next Sprint Objectives:**

* Explore more protocols while we wait for the blackbox.
  + Daniel Bangham
  + Hunter Griffin
* Investigate how to load a digitized stream from a file in GNU radio
  + Ryan Eslick
  + Hunter Griffin
* Study modulation and data encoding detection methods
  + Carter Church
  + Austin Brown
* Better understand limitations of our hardware
  + Ryan Eslick
  + Carter Church
* If the blackbox is received, begin investigating it by seeing what signals we can pick up close to and far away to correlate the data to identify novel signal(s)
  + Entire group effort (if applicable)

**Project Effort Log:**

|  |  |
| --- | --- |
| **Team Member** | **Hours Spent on Project** |
| Ryan Eslick | 6 |
| Austin Brown | 4 |
| Hunter Griffin | 5 |
| Carter Church | 5 |
| Daniel Bangham | 4 |