Hunter Griffin

Ryan Eslick

Austin Brown

Carter Church

Daniel Bangham

**SDR Reverse Engineering Marketing Requirements**

For our Senior Design project, our group has decided to reverse engineer an instructor-provided black box device. This project will be titled “REsDR,” an acronym intended to be pronounced like “Reader”. This stands for “Reverse Engineering Software Defined Radio”.

Our team has devised a four step approach to our project. These steps consist of first determining the base frequency of our given black box. Next, we plan to determine modulation. After completing these two steps, we will determine the transmission encoding of our black box. Finally, after completing all of the aforementioned steps, we will begin to analyze actual binary data to get a better understanding of how our device communicates.

In our initial step, we will analyze our device’s wireless transmissions to determine its operating frequency through spectral analysis. This is necessary as it will provide us with the frequency range that we should dial our own software defined radio to. When our software defined radio is adjusted to this range we can receive data transmitted by the black box.

In our “determining modulation” step, we will analyze the aforementioned frequency ranges determined in our initial step. In this analysis, we will determine the modulation that is being utilized by our black box device such as frequency shift keying, amplitude shift keying, or quadrature amplitude modulation. Completion of this step will get us closer to being able to decipher the binary data being output by the black box.

Next, our “determining encoding” step, we plan to utilize the information gained in steps one and two to get a better understanding of the format that our black box is transmitting data with. Completion of these three steps will finally get us to the point where we can begin to view and understand the actual binary data emitted by our black box.

Once all other steps have been completed, our final step will consist of receiving the actual binary data output by our black box device. We plan to utilize this emitted data to gain a complete understanding of what our black box is and what it intends to accomplish. This step will include documenting all outputs for all potential inputs, creating diagrams based on this understanding, and writing a final project report in which we will include all technical specifications of our black box device. Upon completion of this step, our team should have a complete understanding of the given black box device and all potential interactions with it.

One requirement of our software defined radio reverse engineering project is to be provided a device that operates within the receivable range of our group’s already owned software defined radios. At this time, we believe this range to be between 25MHz and 1750MHz. If we were provided a device outside of this range, our process would be identical to its current state however we would require additional hardware that could receive signals over or under our current operating frequency range. To our knowledge, hardware that could receive signals outside of this general range is likely more expensive than our current hardware. At this time, our team believes that this is our only instructor-driven requirement.

In summary, our team will receive a black box device provided by our instructor. Our team will fully analyze this device to determine the frequency range within which it operates, the device’s encoding, and finally its modulation. With this information, we will begin to analyze the device itself including providing inputs and monitoring all output data. After our analysis is complete, we plan to prepare formal documentation of our findings in the form of a technical report and submit this to our instructor prior to the end of the term.