Hunter Griffin

Ryan Eslick

Austin Brown

Carter Church

Daniel Bangham

**SDR Reverse Engineering Project Summary**

With the recent growth and utilization of software defined radio technology in commercial products, a greater focus on communication security needs to be upheld. In this project we will be exposing the vulnerability of intercepting communication protocols by recovering the system of rules that allow two or more systems to communicate. With these rules recovered outside malicious individuals could subvert proper communication for their own benefit.

The main objective of this project is to show how communication protocol recovery is possible from a black box system. This entails having no formal understanding of the device and reverse engineering the communication process solely from wireless transmissions made by the device.

Our group's general approach to recovering the communication protocol of the black box system will be to first determine the base frequency of the system under testing. Then we need to determine the modulation of the system. Next, we need to determine the encoding method used on the tested system. Finally we will analyze the binary data to recover the communication protocol.