OREGON STATE UNIVERSITY POLICY EXEMPTION REQUEST

REQUEST TO INTERCEPT RF COMMUNICATIONS ON UNIVERSITY PROPERTY FOR THE PURPOSE OF EVALUATING DRONE SECURITY

CS SENIOR CAPSTONE GROUP #50 - SECURITY FOR ROBOTICS

ZACH ROGERS, EMILY LONGMAN, DOMINIC GIACOPPE, VEDANTH NARAYANAN

9 MARCH 2017

DRAFT

Background:

Our senior project capstone group is evaluating the security of the Robotic Operating System (ROS). We are specifically focusing on identifying and exploiting vulnerabilities with ROS running on a drone. One aspect we are looking to explore is exploiting the methods of communication our drone uses. The drone in question has two communication channels:

- 2.4 Ghz frequency primary communication channel, used by the drone's controller to fly the drone.
- 900 Mhz frequency telemetry communication channel, used by the drone for MAVlink communications.

In order to explore possible vulnerabilities within the drone's method of RF communications, we need to openly intercept wireless communications on the 2.4 Ghz and 900 Mhz frequencies.

Impact:

Openly intercepting wireless communications on the 2.4 Ghz frequency will not only intercept our drone's communication, but will also intercept any nearby WiFi communications through access points operating on 2.4 Ghz. We are only interested in information pertaining to our communications between the drone and the drone controller. In the event that additional communications are intercepted on the 2.4 Ghz frequency, that data will be removed from our logs.

With regards to intercepting communications on the 900 Mhz frequency, we will intercept our drone's MAVLink communications, as well as anything else operating on the 900 Mhz frequency nearby. At this time, we are not aware of any university systems using the 900 Mhz frequency.

Procedure:

We will be using a Software Defined Radio (SDR) which will allow us to receive and transmit data on the 900 Mhz frequency. We will also be using a 2.4 Ghz wireless radio, running in promiscuous mode, which will allow us to intercept and transmit 2.4 Ghz data.

We plan to analyze intercepted data in real time using Wireshark, GNU Radio, and any other software tools that will allow us to process the data we intercept. Data that we collect will be logged, so we can perform more in-depth analysis.

When possible, we will apply filters to Wireshark and other tools, so that only our drone's communications are logged. In the event that this is not possible, or if data slips past our applied filters, we will try to remove any and all data that is not related to our drone's communications.

Goals:

Intercepting data on the 2.4 Ghz and 900 Mhz frequencies, we hope to reverse engineer our drone's method of communication. Reverse engineering the communication protocols our drone uses will allow us to identify, document, and exploit any vulnerabilities we may come across. Being able to assess the communication attack vector in this fashion will go a long way towards our project goal of documenting current security vulnerabilities effecting drones, and other robotic devices using ROS.

Communications is a huge part of our overall drone threat model that we are exploring, and anything that we can find out with regards to this attack vector will be incredibly beneficial for our research.