SECURITY FOR ROBOTICS

Researching Vulnerabilities in the Robotic Operating System

Why is this Important?

THE PROBLEM WITH ROS

The Robotic Operating System (ROS) has a lot of problems from a security standpoint due to being middleware. Middleware does not typically focus on security because it needs to be lightweight.

Without any specific security measures taken, there is room for all manner of attacks. To try to tackle them, the vulnerabilities were broken into three categories:

1. Those affecting the confidentiality of data
2. Those affecting the integrity of data
3. Those affecting the availability of data

CREATION OF A THREAT MODEL

A threat model was created to visualize the three categories. It serves as a roadmap for the research and can be looked back on at any time. The model below in Figure 1 is organized as a tree, with the three main branches being the three components of the CIA triad (Confidentiality, Integrity, and Availability). This way one can look at our threat model, decide if their concern is one of confidentiality, integrity, or availability, then examine the vulnerabilities in that category.

Not every area from the threat model was successful, some were not possible to breach, but it's still good to acknowledge that they are still likely targets.

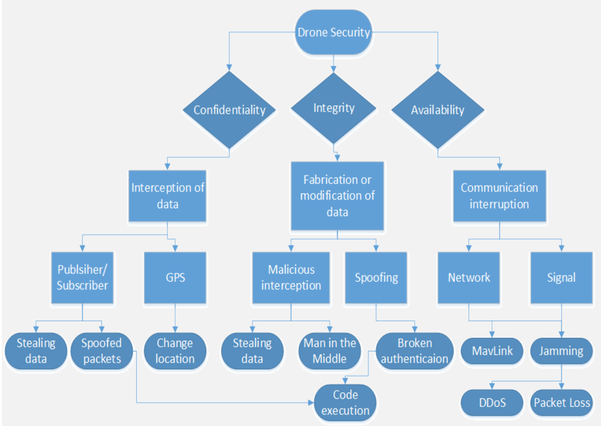


Figure 1: The three pathways of ROS vulnerabilities and how they can be exploited

RESEARCH DESIGN

The project aims to find exploits for whichever vulnerabilities seem most the most open. This means first doing some research to locate the best starting points. Because each exploit is unique it is difficult to draw final conclusions as well as define which exploits are the most severe.

Failure Mode Effects Analysis (FMEA) is a procedure used in a variety of fields which creates an empirical system for testing and logging any failures, which can be applied to all of our attacks. Somewhat akin to risk analysis, FMEA involves defining severity, occurrence, and detection rating scales, usually from 1 to 10. After these scales have been defined one can use them to calculate a risk priority number (RPN) and a criticality number with which the found failures can be ranked in order of importance. You can see this represented in figure 2 below.

As for the sort of exploits created in this project, there was a variety of paths covered. Some examples of these attacks are:

- Man in the Middle
- Spoofing
- Broken Authentication
- Denial of Service
- Resource Consumption
- Data Stealing

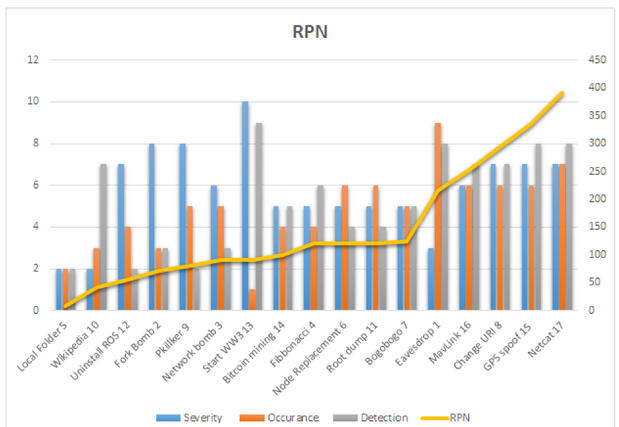
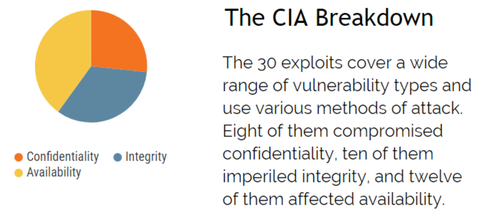


Figure 2: This chart shows that the RPN is a more meaningful number than the others alone

NOTABLE PROOF OF CONCEPTS

- Lack of Authentication
  - Remote control over ROS
  - Package Installation
- Process Communication (Publisher/Subscriber Model)
  - Fuzzing of Subscribers
  - Data Capture of Publishers
    - ROS Bag Replay Attack
  - Sensor Spoofing
- Denial of Service
  - Bogo Sorting
  - Bitcoin Mining

The Exploits **30** Total



The CIA Breakdown

The 30 exploits cover a wide range of vulnerability types and use various methods of attack. Eight of them compromised confidentiality, ten of them imperiled integrity, and twelve of them affected availability.

Figure 3: View at a glance of which areas of security our work affects

OUR FINDINGS

Just as suspected, ROS has wide range of vulnerabilities that this project exploits with a success rate of nearly 100%. Most of these exploits involved either entering the system via the publisher/subscriber system that ROS uses to communicate, or demonstrated what malicious actions could take place on the system once inside. In figure 3 above is a visualization summing up the numbers in our research.

We also found that our project evolved as we went along. We had initially intended to do more hardware based attacks, but they proved to be too cumbersome and difficult to generalize. There are also a board range of physical attacks ranging anywhere from an EMP type gun to an eagle taking down an airborne drone.

The Team:

WHO WE ARE

We are a group of students interested in cybersecurity, guided by our client's graduate research project.

Team Members:

Emily Longman
longmane@oregonstate.edu

Dominic Giacoppe
giacopped@oregonstate.edu

Zach Rogers
rogersza@oregonstate.edu

WHERE IT GOES FROM HERE

We hope that this research will be continued and expanded upon not only by our client in his thesis, but also by other members of the security and robotics communities. The more that is done in this field, the better all future robotics can be, without being a huge security threat.

Client:

Vedanth Narayanan
narayave@oregonstate.edu

Oregon State UNIVERSITY