Requirements Document DRAFT

Security for Robotics

Emily Longman, Zach Rogers, and Dominic Giacoppe

CS461 Capstone

10/28/2016

Introduction

Purpose:

To define the requirements and deliverables for (team name)'s capstone project to our sponsor, Vedanth Narayanan.

Scope:

We are to find security vulnerabilities in ROS/SROS, document these vulnerabilities, and if possible, produce patches for anything we find. Any patches produced will be submitted to the ROS project. Our testing will be focused around ROS/SROS running on a drone, and we will see if we can compromise that drone based on our findings.

Definitions:

- Vulnerability: Any exploitable piece of code or system that would allow unauthorized users to interact with/-damage/control the system, especially in a malicious manner.
- ROS: Robot Operating system, as found at link
- SROS: Secure ROS; a project based on ROS with the goal of implementing various security standards.

Overall

Perspective:

All software developed by (Team name) should have 2 objectives: 1. Fixing a specific, known vulnerability in ROS/SROS 2. Be lightweight enough that the implementation doesn't drastically affect the overall operation of the robot. Ideally, any code produced would be later incorporated into ROS itself, and not an external layer or program.

Software Interfaces:

As we are looking for vulnerabilities in ROS, all code produced must be compatible with it or integrated into it. The version of ROS we will be using is TBD.

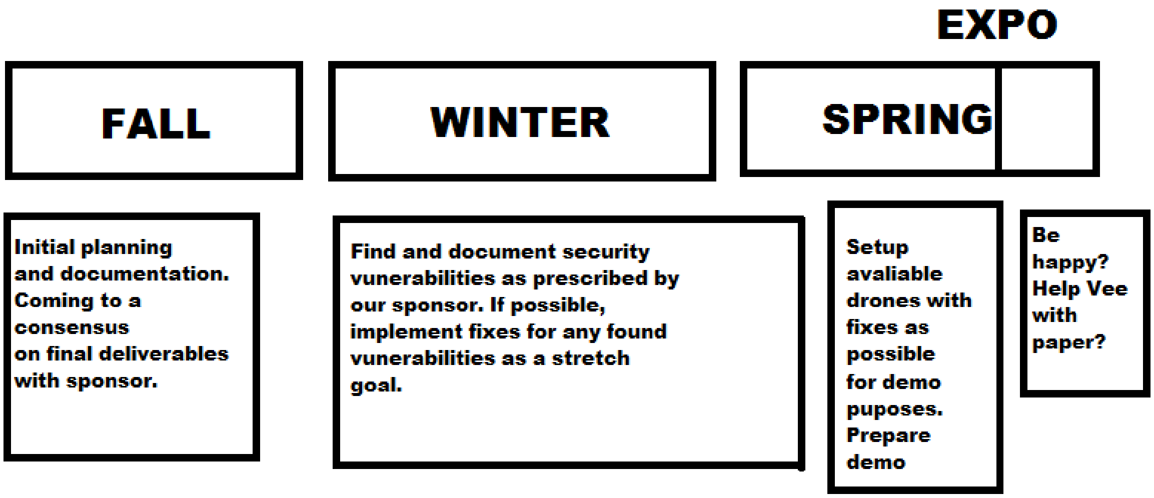
Communications Protocol:

ROS uses 2 major forms of communication. Internally, ROS has the publisher subscriber system, which works basically like a socket system. Publishers export data, and anyone who subscribes to that publisher receives the data, with no limit to the number of subscribers or any authentication on who can subscribe. There is also normally some sort of wireless/wired connection to a base station, which controls the starting and stopping of the robot. These generally take the form of a standard LAN connection, although with extra effort more complicated setups are possible. (SOURCE)

Specific Requirements:

As previously stated, at the moment (Team Name) is in the process of finding specific vulnerabilities. When we do find one, we will produce documentation outlining at least but not limited to: Our operating environment, the type of attack, the particular system/piece of code attacked, the success rate of the attack, the result of the attack, and the potential fix to prevent the attack.

Gantt Chart:



Initial planning and documentation. Coming to a consensus on final deliverables with sponsor.

Find and document security vunerabilities as prescribed by our sponsor. If possible, implement fixes for any found vunerabilities as a stretch goal.

Setup avaliable drones with fixes as possible for demo puposes. Prepare demo

Be happy? Help Vee with paper?

Figure 1: Gantt Chart

References

[1] A. Shostack, *Threat Modeling, Designing for Security.* Indianapolis, Indiana: John Wiley and Sons, Inc, 2014.