CS Capstone Progress Report

December 4, 2016

Security for Robotics

Prepared for

Oregon State University

Vedanth Narayanan _____ _____
Signature *Date*

Prepared by

Group 50

RoboSec

Emily Longman _____ _____
Signature *Date*

Zach Rogers _____ _____
Signature *Date*

Dominic Giacoppe _____ _____
Signature *Date*

Abstract

In drones and other networked robotics there is a broad array of security vulnerabilities that can be leveraged in an attack. We will evaluate the ROS to find as many of these security holes as we can and document them. The different vulnerabilities found will be categorized into malware, sensor hacks, network and control channel attacks, and physical breaches. For some of these exploits we may be able to implement solutions, which will also be documented. These findings and any solutions will be added to an ongoing academic effort to make robotics more secure.

Contents

1 Introduction

Over the course of the past ten weeks our group went from first being chosen for this project to having created a complete outline of our research and possessing our hardware. We started with the task of creating a research project to investigate the security of devices running ROS, specifically drones. The overall purpose of the project is to gather data on the vulnerabilities and their failures when exploited, from a variety of areas. Having a list of possible exploits and a ranking of how catastrophic their failures would be has academic worth of its own, but a secondary goal is to find patches for any successful attacks. If those patches are viable they could hopefully be submitted to the SROS project, which is working to make a more secure version ROS. We've done a lot of work to make the best plan for this research, laying out different assigned steps over the weeks.

2 Weekly Summaries

2.1 Week 0-3

The first few weeks of this course were spent analyzing which projects we wanted, who we would be working with, and how we wanted to initially approach our given problem. It was somewhat of an adjustment period to the course and the next nine months. The calm before the storm essentially. These weeks also provided us with an opportunity to prepare for all the technical writing and research we were about to do. We also got some input from some research professors, which helped us to refine the goals of the project.

2.2 Week 4

During this week we continued our work on getting the project better defined and potentially revising our problem statement. We also got to have a great meeting with Rakesh, our security professor and Vee's advisor, and Jesse, a crypto expert, who gave us some really cool professional insight into what we could potentially focus on. We know that we'll be making threat models to design our approach, based on Adam Shostack's textbook on them. [1] We've mostly confirmed that we're using ROS at this point, and we have some ideas about ways to attack it, but nothing has really been solidified yet. Being that we are using ROS though, we do already have some vulnerabilities that we can look at, as ROS has some out of the box. We gained the hope to be able to contribute to the SROS project, but we weren't sure it will be usable for us.

2.3 Week 5

This week we finished up our revised Problem Statement document, and also spent a lot of time trying to work out our requirements document to get our first draft submitted. We were able to meet briefly with our client to check in and make sure everyone was on the same page with regards to the requirements document. After finishing up some formatting and polishing it came together well.

2.4 Week 6

Despite our solid first draft we still scrambled to pull together our final version of the requirements document, mainly because it was a little bit unnatural for a research project. There was still so much ambiguity that it seemed like we were pulling at straws and making wild guesses as to what we need. As for the hardware we do now actually have our drones but we need to do some surgery on them and re-solder a component on one of the PixHawk boards that Sam broke.

2.5 Week 7

This week we made some rough sections for the tech review, but it was really difficult for us to figure out enough of them that make sense to do a tech review on. The majority of our project is based around the research lifestyle and ROS, but outside of that we didn't have a ton to talk about. We hoped to have a more specific view of what we were doing that we could come back to and better define.

2.6 Week 8

Things were a bit of a struggle this week and not a lot got done. Two of us were sick, so it was mostly just each person trying to finish their tech doc sections. A lot of other classes got chaotic this week too, so we were definitely not as focused as we needed to be.

2.7 Week 9

This week was a short one with the holiday, and was spent trying to catch up on the tech doc that two of us failed to complete by the deadline. We talked with both professors about it and they had useful pointers, but it still seemed like such a stretch when writing it. We met to discuss how we are going to finish the tech doc, along with further debating some technical aspects of the project, most specifically for me whether or not we will be using SROS or not, and if our board can support the latest version of ROS. We were also starting to think about the design doc coming up the next week and the end of term assignments.

2.8 Week 10

This was the last week of classes and we focused quite a lot of our effort into making the best design document we could. We were all happy with the outcome, and it was probably the most useful of the documents we wrote written this term. It would have been nice to have a little more time to add a better literature review section per Kirsten's suggestion, but we can still add those to our revision at the beginning of next term.

3 Retrospective

Positives	Deltas	Actions
Met with and now have useful contacts for our research	Work to meet more often with Vee and others	Create a standing schedule for meetings
Created useful documents we can reference later	Apply inevitable changes to documents as they happen	Update documents
Got our hardware and were able to familiarize ourselves with it	Exchange components on hardware	Take off and return extraneous components, get ours in working order, and attach them
Established Slack as our main communication line	Need to discuss bettering our communication at times	Meet about expectations and how we can work together on achieving the best communication

4 Conclusion

As a whole this term went well. Our group has not had any significant issues with cooperation and sharing of duties, just a few personal failures. We have had excellent input from both the teaching staff and some outside experts on where to start and how we might proceed. We were able to outline our research design and also familiarize ourselves with the hardware we will most likely be using.

Over the break we intend to do a good deal of literature studying, looking for articles on topics relating to ours and trying to nail down the best places from which to attack. We will also be making our preliminary threat models, which are crucial to being able to actually start accruing data. Come the start of winter term, we plan to go over those threat models with superiors and revise them as necessary. Lastly we want to get the drones as close to set up as we can, so that we'll be able to begin testing as soon as possible. All the assignments this term gave us a fantastic starting point from which we will be able to achieve this.

References

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