Oregon State University
College of Engineering

CS Capstone Midterm Progress Report

February 17, 2017

Security for Robotics

Prepared for

Oregon State University

Vedanth Narayanan

Prepared by

Group 50

RoboSec

Emily Longman
Zach Rogers
Dominic Giacoppe

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 Overview

In the first six weeks of winter term our group has continued on our research path, along with getting the drone fully online. We've developed new ROS packages to use for testing and made some decisions about the scope of our research. Specifically we have more or less abandoned SROS as a component of our project and are focusing purely on ROS itself due to a lack of movement in SROS. We've all made headway in our respective branches of research, following what we found most promising in our threat models. The drones have given us a good deal of bugs to take care of before we can test our exploits on the actual hardware without fear of it affecting our data, but we can move on with VMs in the mean time. Data is being accrued, waiting for analysis in a couple short months, and each week we broaden that dataset.

2 Weekly Summaries

2.1 Week 1

Over break we each individually did some work on the project. The portion Emily worked on was creating our threat models, which we need to use to complete our research iterations this term. This week she added in some of the sources that Dominic and Zach found over break to finish fleshing them out and finalizing them. We are all also going to get the hardware fully functional this week so that we can begin testing as soon as possible. We met as a group to discuss our project but still needed to meet with Vee and our TA.

2.2 Week 2

This week we made headway with the hardware, getting the pieces we aren't using taken off of the drones and Zach getting ROS installed on both the boards so that they're ready to go. We got the threat models finished up and published, but there's discussion of changing their layout so they may get more tuning this coming week. In finishing them we've amassed more pages and articles we can use, so we have even more to go off. We also got to meet with Jon this week so we have a better idea of what's ahead of us this term, as well as get his input on where we are in the project. we think we're all hoping to get a lot done this coming week. Dominic started working with Vee to create a malicious ROS package for testing purposes, and we have one most of the way there but are running into some compile dependency issues about graphics drivers. We're also making one separately that will be a fair bit less complex.

2.3 Week 3

A lot got done this week, just as we had hoped it would. We met up three or four times and worked together on getting the boards set up with the operating system, getting some malware packages from Dominic set up for testing, and getting the hardware ready to go. For the hardware we got everything returned to Kevin that we weren't using, a battery for one of the drones, and everything put in its place. Zach finally got Ubuntu ARM running on the BeagleBones, along with a working install of ROS! It took two all nighters to work through some issues, but everything finally fell into place. We just need to hook up the boards now and they should be working. We're just making sure that they'll interface correctly with the PixHawks first, since that's been giving us a bit of trouble. In the mean time though we all have an installation of ROS on our computers so we can do some research and testing without having to use the physical drones.

2.4 Week 4

Week four was somehow yet another productive one. While Emily spent the majority of it sick in bed, she was still able to work on some sensor spoofing ideas. We researched the topic more thoroughly and were able to find some pretty great sources. The other two also continued to get work done on their respective research sections. Zach got ArduPilot compiled on the Beagle Bone Blacks, but we needed to setup the PWM connections on the drone to actually test if this worked. This process took several hours for each BBB. We also had class for the first time in a while, which gave us some good pointers for what to expect in the next couple weeks, and how we should prepare for them. Early next week we would be working on the rewrite of the tech doc, which would soon be due.

2.5 Week 5

With the looming deadline of midterm check-in, this week involved a lot of reassessments of our documentation. We each planned out what we would need to revise in our respective sections and prepared for our additional progress documentation. At the same time we continued to put work into our research, with Zach focusing on perfecting the drone communication, Dominic making more malware packages, and Emily continued honing her research on sensor spoofing, waiting to test it on the fully functional drone. With midterms on top of it, the next week was bound to be just a flurry of writing and editing, probably with little research getting done.

2.6 Week 6

This week, as expected, was spent almost exclusively updating our documentation and making the changes necessary. we've finished creating the OneNote document and have also made the new progress report docs. We've all added changes and edited our video. We reused parts of the video from last term that didn't change, and added in more current updates. Next week we can finally be done with all this writing and be back on the research cycle.

3 Conclusion

Significant progress has been made and we have plenty more of it ahead of us. Our collection of OS exploit packages continues to grow, the communication of the drone is being refined, and research results are looking promising. We plan to continue our efforts to exploit as many vulnerabilities as possible all the way through to Expo. We will have a variety of data from which to draw meaningful conclusions and provide the world more insight into the security flaws of ROS.