Winter Term Progress Report

Emily Longman, Group 50, Security for Robotics

March 22, 2017

Introduction

In what seems like a flash Winter Term is coming to an end and this project has come a long way. After painstaking planning and documentation in the previous term, all that work actually got underway. Because this is a research project the main goals were simply to make significant progress in ROS vulnerability and exploitation studies. This meant reading articles, studying code, creating exploit packages, and collecting data from trials. I specifically focused on exploiting the hardware of the drone, creating and maintaining threat models, documenting collected data, and forming metrics for analysis. All of these progressed this term.

Individual Portions

The there portions I am specifically responsible for are: threat models, documentation of data, and forming metrics. As stated above I've also informally taken on the hardware portion of our research, which is one of the three designations from the threat models I created. The other two are operating system exploits and communication channel exploits. Documentation of data meant designing a way to track any and all data collected in the most uniform way possible. The metric creation was similar, which involved expanding upon and testing out the FEMA method proposed previously.

Progress and Problems

Problems are inevitable on every project, and this one has certainly had its fair share of them. Coming into this term there was a lot to be done, but few major setbacks. The drone needed to become functional, ROS needed to be built properly, and the threat models needed to be created, and the research just generally needed to get underway. As with most things though, discussing and planning a task is always easier than actually implementing it.

Throughout this entire term the drone has proven itself to be persnickety at best. As soon as one problem was solved, three more would arise. Even now at the end of this term the drone is still not in perfect working order, despite our best efforts. However, it is very close. Had there been more time to devote to it in these busy final weeks, it may have finally been successful. To remedy this continued work on it is planned for spring break.

Thankfully the trouble with the drone hasn't hindered the research from continuing. I created three threat models at the beginning of the term, denoting three separate sectors of drone security that would be researched, one going to each member of the team. All of these could still be researched, first just by finding more preexisting data, and also by running any exploits that were created on a ROS install on a laptop. This meant that vulnerabilities could still be tested, data could still be gathered, and the project as whole could still progress.

I've worked hard on researching the hardware attacks on ROS, which has yielded a number of interesting papers, a good deal of raw data, and a handful of code exploits. Another one of my specific responsibilities was to create a standardized data storage system, which I implemented in the form of a layered spreadsheet. It allows each researcher to have their own page and organize their results in the best way possible, but allows everyone to see how the others are doing it and match them as best as possible. As planned, this will make it easier for the final analysis of the findings. The FEMA system that was laid out in the previous term is fitting well so far. I've been able to apply the ratings to all my findings and the others have been encouraged to do so as well.

The brunt of the evaluation will happen next term when the majority of the data is available, but so far the results have been very promising. I specifically have been able to exploit two separate areas of the drone hardware, and the others have been successful across the board as well. As of now a vulnerability that cannot be exploited has yet to be found. Some have been difficult, but all have been relatively trivial to break. This completely supports the initial hypothesis and purpose of the project, which was to illustrate just how lacking the security is within ROS. I have plans and preliminary work for even more hardware exploits, and as more data is gathered I can hone my analysis metrics to create refined final results.

Evaluation

Retrospective

Positives	Deltas	Actions
Met and worked together as a group twice a week	Get some input from security experts	Meet with Rakesh and Jesse
Gathered a lot of research information and sources	Be better about documenting data in the shared space	Keep everyone accountable for weekly data updates
Learned from a lot of hands on work with ROS	Strive to work together as a team even more often	Write more code so as to have more tangible deliverables

Conclusion

With the solid foundation of research that has been laid this term, next term is just about continuation and extrapolation. The truly fun part comes next term, when I get to do statistical analysis on everything that has been gathered and create meaningful graphics for the poster. Putting together this data of interest and drawing meaning from it is the final deliverable for which I am responsible. Assuming this is done thoroughly, consolidating everything into the final packet should be trivial. I hope to make it resemble a true research paper as much as possible. The more data there is to put into it the better.