Security for Robotics - Tech Review

Emily Longman, Zach Rogers, and Dominic Giacoppe

CS461 Capstone

11/28/2016

Emily

Threat Modeling

A key element to the project is being able to accurately find vulnerabilities or identify areas where they are likely to be. One of the best ways to do this in an organized way that can be later referenced is with threat modeling. This method is widely used in industry when producing any sort of software. Many security professionals use it, but anyone can employ its methods. There are a variety of tools and technologies that can be used in threat modeling, which are compared below.

Adam Shostack mentions in his book on threat modeling that [1, p.203] One of the most important tools we can use is a whiteboard. This may not be a true technology but its important to be able to visualize the various modes of possible attack. It's perfect for initial creation of the models as they're sure to go through many changes.

After using whiteboards to create model visualizations though, tools like Visio can be extremely useful for creating a more formal, digital version. The Visio creations can also be easily shared and modified by anyone in the team, which makes distributed work easier. It also serves as a useful reference and record throughout the research process. If the models change at all there will still be a formal record of any previous versions which we used to collect any previous data.

One last and important technology that Adam Shostack mentions is a bug tracking system. Just the issue tracking system in git could work for this, but there's a variety of ways it can be done. What's important is that it includes a definition of the threat, how the team is going about it, the need to test it, the need to validate an assumption, and any possible mitigation found. [1, p.205] It can then be updated as progress is made on that specific exploit, and eventually closed as either completed or a dead end. To get the most out of threat modeling it would be great to employ all of these, but they may not all be viable.

Documentation of Data

The core of the project is the data recorded when trying out different exploits on the system, and for it to be useful it must be recorded thoroughly and consistently. Because there is such a wide variety of methods which will be used to attack the system, the data will be quite varied. As much as it would be wonderful if it were possible to have easily comparable data from all of them, it simply isn't. To combat this what we come up with must be recorded consistently.

An article from Georgia Tech on proper research data documentation gives a few great concepts to focus on. [2] It states that among a number of things, one should record the location, methodology, software used, and any data processing done. For location data this means recording where the data was taken, which for our project might include GPS data when testing with the drones. It could also mean what location within the drone, and within that it could even be as specific as where in the code (if it's a software based exploit). Methodology is possibly the most important one, as it records how the data was generated, the protocol used, or where it came from. Our diverse range of data could actually be somewhat standardized if we meticulously record the methodology used and then later visualize it somehow according to that, most likely in some sort of tree based on categorizations of methodology. Software used ties into this, as it is part of what generates the data points we output. If software is used in manipulating, organizing, or visualizing the data, that would need to be recorded separately. This leads to the last point of data processing, which is also a very important one. If the data is changed in any way while processing it, that absolutely must be recorded, or else the legitimacy of the final conclusions could be ruined. Just like citing any sources used, anything done in the project must be cited for the sake of reproducibility.

While they are options, all of these should be taken into account when starting to actually produce data. The previously stated ideas don't necessarily need to be followed as they are, and there are sure to be problems with them or better options along the way. The main concept here is that research data is precious and sensitive and that integrity needs to be preserved to make our final product something that's academically valuable.

Data of Interest

There is wide variety of data to collect in this project, and that data is different for each class of attack. This makes drawing any overarching final conclusions difficult, as well as defining which exploits are the most severe. One form of data is universal though, and that's the failure mode of each successful attack. 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. 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 mathematically ranked in order of importance. [3]

Employing this method and applying it to all successful exploits found will be immensely helpful in being able to compare completely separate systems. Final conclusion data can be drawn form these and an ultimate ranking of security prioritized vulnerabilities would be an immensely useful product to the community as a whole.

References

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

[2] G. Tech. Document your data. [Online]. Available: http://d7.library.gatech.edu/research-data/documentation

[3] ASQ. Failure mode effects analysis. [Online]. Available: http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html