Security for Robotics - Tech Review

Emily Longman, Zach Rogers, and Dominic Giacoppe

CS461 Capstone

11/28/2016

Emily

Threat Modeling

A key element to our 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 I am going to be comparing.

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

After using whiteboards to create our 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 our models change at all we'll still have 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 we can do it. What's important is that it includes a definition of the threat, how we're going about it, the need to test it, the need to validate an assumption, and any possible mitigation we have. [**?**, p.205] We can then update this as we make progress on that specific exploit, and eventually close it 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 our project is the data that we record 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 ways we will attempt to attack the system, the data will also be quite varied. As much as I wish it were possible to have easily comparable data from all of them, it simply isn't possible. To combat this we have to try to at least document what we come up with consistently.

An article from Georgia Tech on proper research data documentation gives a few great concepts to focus on. [1] 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 we used software in manipulating, organizing, or visualizing the data though we would need to record that separately. This leads to the last point of data processing, which is also a very important one. If we change the data in any way to process it we absolutely must record that, or else the legitimacy of the final data could be ruined. Just like citing any sources we use, we have to cite anything that we do for the sake of reproducibility.

While they are options, all of these should be taken into account when we start to actually produce data. We don't necessarily need to follow the previously stated ideas as they are, and we're sure to find problems with them or better options along the way. The main concept here is that research data is precious and sensitive and we need to do our best to make our final product something that's academically valuable.

References

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