SE-4930: Developing Secure Software

Lab 5: Threat Modeling

Due by 23:00 January 14, 2013

Introduction

The battle for software security starts with an effective analysis of the threats facing a system. We have two options: knowing the threats and trying to mitigate them, and ignoring the threats and living in ignorance. The first is the better path; the latter is the more common path until recently.

In this lab, you will be working as an interdisciplinary team to model the threats against your system.

Step 0 – Watch the videos

Prior to lab, watch the 2 videos. The first video introduces the Microsoft Threat modeling game. The second video introduces the Microsoft threat modeling tool.

Step 1 – Sketching Your System

The first step to perform Threat modeling is to identify the structure of your system. Construct a data flow diagram which represents the pieces of your system and the communications between system components. This does not have to be formal. It can be done on a whiteboard or a sheet of paper. Try to be neat, but do not necessarily aim for perfection.

Step

Step 2 – Installing the Tools

For this exercise, the Microsoft Security Development Lifecycle Threat Modeling Tool will be used to construct a model of the threats which exist to a software application. This application is freely available from Microsoft at http://www.microsoft.com/en-us/download/details.aspx?id=2955. This tool requires Visio 2007, which should be available on your university laptop.

Step 3 – Understanding how the tool works

The Microsoft MSDN provides a tutorial on how to use the tool and how to enter items into the system. This article is available at http://msdn.microsoft.com/en-us/magazine/dd347831.aspx. *Read through this article and understand what the tools are capable of doing and how to use them.*

It is probably best if each individual does this exercise before the team tries the activity.

Step 4 – Model your System

Now, it is time for you to model your system. Perfect knowledge is not to be expected, as you do not necessarily have a complete understanding of the architecture of your systems. However, use your best guess if you are dealing with an unfamiliar system.

Once the diagrams have been created, analyze the model for threat vulnerabilities and describe how you believe the threat may be mitigated. If a threat is clearly not present, mark it as such. Complete the analysis of the project, and generate a report.

Deliverables

Each team shall submit a report in pdf format with the following information

1. *Title Page* - Name of all team members, course, and date details.
2. *Project Summary* - Summarize to the best of your ability in a paragraph or two the purpose for the given software application, what it does, and why someone would use the software.
3. *Threat Model* - Include a report generated from the modeling tool of the threat model. This is automatically generated by the tool and can simply be pasted into your word document as generated. Make certain it includes both the threats model analysis. Note that for some threats, you may have multiple instances of the same threat and the mitigation may be the same for each one.
4. *Things gone right / Things gone wrong* - Discuss the things which went well with this lab, as well as the problems you had, either with the tools, the process, etc.
5. *Conclusions* - What have you learned from this experience