SE4930 Lab 3 - Assets Definition and Abuse Case Definition

Dr. Walter Schilling

Due: 23:59 CDT December 17, 2012

1 Security Goals

To define our approach to security, it is important that we first think about our security goals. What are we trying accomplish with our security, as this will govern how our system evolves. In setting the goals, there are often two pieces to the security equation, namely what we expect of our system and what we expect of our users. In terms of our system, there are certain aspects of security that is expected out of our system. And, there are certain aspects which are expected to be sheltered by our users.

In this first pass, your goal is to set the security goals for the system. What are you trying to achieve with your system and its security?

2 Asset Identification

Determining the security of the system also requires the identification of assets. An asset, by definition, is the object of protection efforts. This may be a component of the system, a piece of data, a process, or the very system itself. Each asset that the system holds may require differing levels of protection, and this protection will need to be designed into the system. Additionally, the level of protection for each asset might be different based on the risk that would be posed by an improper access to that asset.

To complete this task, you will need to identify each asset that you system contains. For each asset, you will need to classify its required confidentiality, integrity, and availability needs. For each classification, you should also include a few statements justifying your decision. There are multiple ways you can accomplish this task, either with a structured layout and a paragraph format or a tabular layout with a paragraph segment in one of the columns for justification.

3 Use and Abuse Case Modeling

Concurrent with asset identification, you will also need to document the use cases for your project. The easiest way to accomplish this is to start by defining the use case diagram. The use case diagram will clearly show the actors who act upon the system as well as what they are permitted to do to the system. A sample use case diagram is given on page 118 of the course textbook. You may find it simpler to start by drawing this diagram on the whiteboard and obtaining general agreement before drawing the diagram electronically using EA or another CASE tool of your choice.

After the use cases have shown on the diagram, you will want to add abuse cases to the diagram as well. The first type of abuse case involves simply taking the existing use cases and defining a user who would try to maliciously use an existing use case. In some cases, this is referred to as an abuser. For consistency, we will show this actor on the right side of the use case diagram and ideally could color them "black" if the tool would support this coloration. Once you have added the abuser to the diagram, then you will need to think about how the various abuses might be mitigated by additional use cases. This will be shown by an arrow going from the mitigation use case back to the threat. Examples of misuse cases can be found online at `http://easyweb.easynet.co.uk/iany/consultancy/misuse_cases_hostile_intent/misuse_cases_hostile_intent.htm` and `http://agile.csc.ncsu.edu/SEMaterials/19_AbuseCases.pdf`. In doing this exercise, you may also notice specific misuse cases that need to be dealt with that may not directly depend on common use cases. These should also be noted.

Once you have drafted the diagram, write a set of abuse case scenarios. Abuse case scenarios follow the same trend as use cases but have a bad or negative outcome associated with them.

4 Time Analysis

Once the team members have completed their work, the spreadsheet shall be updated with effort and allocation.

5 Review of last weeks submission

In addition to this work, the instructor will be meeting with each team to review last weeks submissions.

6 Deliverables

Each team should submit through the course website a pdf with the following

1. A cover page with the project name, team members, date, course, and assignment information
2. A brief introduction as to the scope of this artifact and its purpose within the project development
3. A listing of definitions. This section shall list and define any terms which are being used in a manner specific to this project. For example, there are different security classifications that may be used on this project. This section will define what is meant by those security classifications.
4. A brief overview of the purpose of the project, what its goals are, and what it will accomplish
5. A description of the assets held within the artifact and their security classifications.
6. An abuse case diagram showing the abuse cases and their relation with the use cases.
7. A brief description of each actor in the system as well as each abuser in the system.
8. Abuse case scenarios for each of the abuse cases shown on the diagram.

Each team should also update and submit its spreadsheet with time and effort information included.