Assignment 3: Threat Modeling

eSoc 488: Privacy Technology in Context

Due: Tuesday, 02 October 2018

Total Homework/Assignment Points: 125

You are to create a threat model for your final project proposal. Here is a useful example: `https://docs.securedrop.org/en/release-0.9/threat_model/threat_model.html`. *Be warned, they are doing things slightly differently than we do here; however, the thinking evident should be handy.*

Design

1. [10] Clearly specify the high-level, main goal of the project. Ideally, this would be done in one sentence, but as long as it is succinct, a short paragraph is acceptable. Immediately after describing the goal, provide motivation for it: why is it important?
2. [10] Provide a description of the design of the project. Answer these subquestions
   (a) Who uses, sets up, and maintains the system, and what is their role?
   (b) What is the infrastructure is involved? This should include systems, and their connections to each other. You may need to break this description into several sections to provide adequate details about the inner workings of your infrastructure. *Examples: There will be documentation stored on server X, which details how to set up the system. There will be an air-gapped computer that is connected to the rest of the project only via manually-transferred USB drives.*
   (c) What kind of data is stored or seen by the infrastructure and users mentioned above?
3. [5] How does the design of the project serve the goals of the project? List as many potential criticisms as you can, and your response to them. *Example: is the project usable for different kinds of users? It is too weak to be really helpful to people in practice?.*
4. [15] Draw a dataflow diagram for your project.
5. [5] Add trust boundaries to your diagram.
6. [5] Write a caption to explain clearly what your diagram shows (assume this diagram would be included in a paper that includes your design documentation). Walk through the diagram, including all parts.

Assets

7. [15] Write a section called "Assets" which detail what valuable things the system protects from adversaries.
8. [10] What are the additional assets that might be used as stepping stones to getting the primary assets given in the previous question?

Assumptions

9. [12.5] Write a section called "Assumptions." Within this section, include a subsection for "Users" that describes any assumptions made about each of the users mentioned in your design section. *Example assumptions: What do you assume that the user wants? Do you assume that they have legitimate copies of the software that your project relies upon? Do you assume that they follow the protocol you*

specify (that is, do you not protect against the case in which they do not follow the protocol)? And so on.

10. [12.5] Also include a subsection for "Infrastructure" that describes any assumptions made about each of the systems listed in the design section above. *Example assumptions: That a computer runs some piece of software correctly, that a system is not compromised by malware, that the security assumptions of various pieces of software you rely upon hold.*

Attacks

11. [12.5] Add a new section called "Attacks." Create a subsection called "attackers" and describe the classes of attackers which your system is designed to defend against. For each class, specify what attackers could do, given different abilities, to compromise the assets you have listed above. *Example: A network attacker who can monitor the entire network could do identify the sender of a document (a listed asset being sender anonymity), and a network attacker who could just observe the link between the database and the web server could read the contents of the query, violating confidentiality. An attacker with physical access to an administrator's computer could seize the system (system availability, avoiding denial of service being an asset), and an attacker with physical access to a database server could provide bad responses to queries (response integrity being an asset). And so on.*

12. [12.5] Add another subsection called "attack scenarios." Reference different features of your design specifically and describe as many attacks against them as you can imagine. *Your system uses passwords hashed using SHA-512 (what we saw in the last assignment). Point out the possibility of a dictionary attack, or the use of rainbow tables.*