CSE 484 / M584 Homework 1: Threat Modeling

1 Due Dates

- Wednesday April 23rd, 11:59pm

Handin Via Gradescope, submit a PDF. See Deliverables.

Groups

- Individual only.

Grading

Points

- 1 point per question.

This is an individual assignment, but you are welcome to discuss the ideas with others. If you want to talk in-depth with a friend, you must choose *meaningfully different* products to evaluate. That way you can discuss the actual threat modeling, but complete the assignment independently. Do not share a complete or partial writeup with anyone else in the class.

2 Before you start

Remind yourself of the threat modeling exercises we've done in class so far. You will need to use the same conceptual tools you used to think of concrete adversaries and adversarial objectives here.

3 Overview

3.1 Background

They say that one of the best ways to learn a foreign language is to immerse yourself in it. If you want to learn French, move to France. This assignment is designed to give you an opportunity to develop a "Security Mindset" and to think about related ethical issues in computer security settings.

Cultivating this "security mindset" is a key goal of this course. We want you to learn to think about security and related ethical issues during non-course related activities, such as when you're reading news articles, talking with friends about current events, or when you're reading the description of a new product. Thinking about security will no longer be a chore relegated to the time you spend in lecture, on assigned readings, on homework assignments, or on labs. You may even start thinking about security while you're out walking your dog, eating breakfast, at the gym, or watching a movie. In short, you will start thinking like a seasoned security professional.

Your goal with the security review assignment is to evaluate the potential security and privacy issues with new technologies, evaluate the severity of those issues, and discuss how those technologies might address those security and privacy issues. These assignments should reflect deeply on the technology that you're discussing.

3.2 Setup

Decide on a technology or product you want to do a security analysis of. If you are going to discuss this with classmates, make sure you all choose completely different products or technologies.

You may choose to evaluate a specific product (like the Miracle Foo) or a class of products with some common goal (like the set of all implantable medical devices). Do not choose a technology or product we've already discussed in detail in class (e.g. Microsoft Recall.)

4 Deliverables

You should submit a PDF or plaintext file to Gradescope. The exact format is not important, but it must contain:

- Your UW NetID
- Your name
- A writeup covering all of the material listed below in "Questions".

Please make your submissions easy to read, while still writing them as prose with complete sentences. We encourage using bulleted lists whenever possible. For example, a list where each asset as its own entry in a bulleted list.

Estimated effort. Include an estimated number of hours you spent on this assignment.

5 Questions

For each of these, make sure your writeup clearly indicates where it is answered.

1. **Summary of the product or technology.**
   This summary should be at a high level, around one or two paragraphs in length. State the aspects of the technology that are relevant to your observations below. If you need to make assumptions about a product, then it is extremely important that you state what those assumptions are. To elaborate on the latter, if you end up making assumptions about a product like the Miracle Foo, then you are not studying the Miracle Foo but "something like the Miracle Foo", and you need to make that extremely clear in your review.

2. **At least two stakeholder-benefit pairs for the technology.**
   Before considering security (i.e., considering the system as operating as intended), give at least two stakeholder-benefit pairs. Each pair consists of the naming of a stakeholder and how they might benefit from this technology. The stakeholder-benefit pairs may have the same stakeholder listed twice, or each pair might have a different stakeholder.

3. **At least two stakeholder-harm pairs for the technology.**
   Before considering security (i.e., considering the system as operating as intended), give at least two stakeholder-harm pairs. Each pair consists of the naming of a stakeholder and how they might be harmed by this technology. The stakeholder-harm pairs may have the same stakeholder listed twice, or each pair might have a different stakeholder.

4. **At least two assets a corresponding security goals.**
   Explain why the security goals are important. You should produce around one or two sentences per asset/goal.

5. **At least two possible threats.**
   A threat is defined as an action by an adversary aimed at compromising an asset. Give an example adversary for each threat. You should have around one or two sentences per threat/adversary. "Compromise" will depend on the asset, and may mean theft, destruction, denial of access, or even just misbehavior.

6. **At least two potential weaknesses.**
   Again, justify your answer using one or two sentences per weakness. For the purposes of these security reviews, you don't need to fully verify whether these potential weaknesses are also actual weaknesses. (You may find some overlap with your answer here and your answer to the bullet above.)

7. **Potential defenses.**
   Describe potential defenses that the system could use or might already be using to address the potential weaknesses you identified in the previous bullet.

8. **Evaluate the risks associated with your assets, threats, and weaknesses.**
   Informally, how serious do you think these combinations of assets, threats, and potential weaknesses are? Are they likely to happen with these adversaries?

9. **Conclusions.**
   Provide some thoughtful reflections on your answers above. Also discuss relevant "bigger picture" issues (ethics, likelihood the technology will evolve, and so on).

6 Notes

Here are some examples of some (very) past security reviews: https://cubist.cs.washington.edu/Security/category/security-reviews/. (The requirements for this assignment changes from year to year, so please pay attention to the specific requirements for this version of the course.)