CSE 484 / 584M (UW CSE Computer Security & Privacy): Homework 1

This homework is focused on helping you develop the security mindset. **It has two parts**: a security review and an ethics journal entry.

Overview

- **Due Date:** January 13, 4:30 pm
- **Group or Individual:** Groups up to three people. We will not require that you work in groups for this assignment, but we strongly encourage it, since discussing these questions helps you think about them. **Important for grading purposes: Join a Canvas Homework 1 group even if you are submitting individually (you will see why this is necessary below).**
- **How to Submit:** Submit one PDF containing both parts of the assignment to Canvas. Join a Homework 1 group on Canvas, and then only one person needs to submit. Make sure that the names and UWNetIDs of all contributors are at the top of each page of each PDF that you submit.
- **Late Days:** The usual late day policy applies (5 late days for the quarter, of which 3 may be used on a single assignment). **Please note in the header of your submission how many late days you are using.**

A Note on Group Work

You may do this assignment in groups of up to three people. In fact, you are encouraged to work in groups. But if you work in a group, please do not do something like: Have Alice work on Part 1 and have Bob work on Part 2 and then put both names on both submissions. Instead, please all work collaboratively on all parts of the assignment. There is a lot of value in actually discussing these topics with other people.

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.

It is also extremely important for a computer security practitioner (and actually all computer scientists) to be aware of the broader contextual and ethical issues surrounding technology. Technologies don't exist in isolation, but rather as one small aspect of a larger ecosystem consisting of people, ethics, cultural differences, politics, law, and so on. For example, encryption involves many more abstract mathematical questions but also intersects with questions of how people use technology (e.g., whether technology creators are correctly using encryption libraries) as well as societal and ethical questions (e.g., who should have access to encryption technologies and under what circumstances). Alongside a technical “security mindset”, this assignment (and later assignments in the course) are designed to help you cultivate the habit of thinking about the associated “bigger picture” and ethical issues.

Part 1: Security Review

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.

Each security review should contain:

- **Summary of the technology that you're evaluating.** 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). 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.
- **State 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.
- **State 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.

- **State at least two assets and, for each asset, a corresponding security goal.** Explain why the security goals are important. You should produce around one or two sentences per asset/goal.
- **State at least two possible threats, where 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.
- **State 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.)
- **State 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.
- **Evaluate the risks associated with the assets, threats, and potential weaknesses that you describe.** Informally, how serious do you think these combinations of assets, threats, and potential weaknesses are?
- **Conclusions.** Provide some thoughtful reflections on your answers above. Also discuss relevant "bigger picture" issues (ethics, likelihood the technology will evolve, and so on).

There are some excellent examples of past security reviews here. (The requirements for this assignment changes from year to year, so please pay attention to the specific requirements for this version of the course. Also, unlike previous years, you will not be required to post your security reviews on the forum.)

Please make your submissions easy to read. For example, use bulleted lists whenever possible. For example, list each asset as its own entry in a bulleted list.

Part 2: Ethics Journal Entry

This part of the assignment will ask you to choose and describe a computer security related technology (~100 words), identify relevant stakeholders and who holds power over the technology (~200 words), and use an ethical framework to create 3 to 5 ethics questions you have about this technology (~200 words).

(a) Select and Describe a Computer Security Related Technology

First, select and describe a “computer security related technology”. For this assignment, “computer security related technology” has a broad interpretation, and can include software applications (e.g., Signal, or contact tracing apps for COVID-19), hardware or devices (e.g., Ring, or surveillance cameras in hospitals), organizational programs (e.g., Google’s bug bounty program, or the US Department of Homeland Security’s role in election security), policies (e.g.,

Amazon's vulnerability disclosure policy, or the executive order banning TikTok), etc. If you have questions about whether a particular technology is appropriate for this assignment, please reach out to the course staff.

For additional ideas about computer security related technologies, you might scan the following websites:

- KrebsOnSecurity
- SchneierOnSecurity
- Electronic Frontier Foundation's DeepLinks blog
- Wired
- Ars Technica

After selecting your group's computer security technology, you may want to do some brief additional research. What is this technology? What does it do? **Write a summary of your selected computer security technology (~100 words).**

(b) Identify Stakeholders and Power Relationships

Now identify what stakeholders are involved in your computer security related technology, and articulate power relationships between stakeholders. To identify stakeholders and power relationships, you may want to consider questions such as:

- Who creates or deploys the technology?
- Who uses it?
- Who might benefit from it?
- Who might be harmed by it?
- Who has power over the technology (and who does not)?
- Who is responsible for the technology?
- Who might benefit from, or be at risk from, vulnerabilities in the technology?
-

Write a summary of your stakeholder analysis (~200 words).

For instance, using the DHS's Election Security Services as an (incomplete) example, we might say:

- *DHS's Cybersecurity and Infrastructure Security Agency (CISA)* provides election security tools "at no cost" to *state and local officials.*
- *State and local officials* are responsible for both securing elections and asking *CISA* for election security services.
- Vulnerable election technologies put the *security of fair elections*, and by extension *democratic government* at risk.

(c) Develop Ethics Questions

Now, you will create 3-5 ethics questions for your computer security related technology. For our purposes, ethics questions will often start with *"should"*, and frequently occur when computer security needs to call on the rights, responsibilities, or resources of other people.

Returning to our Election Security Services example, we might ask questions like: should state and local officials be the ones to ask for cybersecurity services? Should using cybersecurity tools be mandatory for securing elections?

To help you identify and form ethics questions, we have provided summaries of different ethical frameworks below. Each framework suggests a particular way of thinking about what is right and wrong.

Based on your Canvas Homework 1 group number, please read the following ethical framework summary before developing your questions. The framework you learn about may or may not completely resonate with you, but we hope it will give you some new ways of thinking about your ethics questions in this context.

- **If (group_number % 3 == 0):** Menlo report, which connects computer security ethics to research ethics.
- **If (group_number % 3 == 1):** Capabilities framework, which foregrounds global well-being, justice, and development.
- **If (group_number % 3 == 2):** Manifest-no, which emphasizes refusal of historically harmful data regimes.

Please write down which ethical framework you learned about.

Reflect on your stakeholder analysis and framework together, then **list at least 3-5 ethics questions that you would want to ask a computer security ethicist (~200 words).** Feel free to write your questions as bullet points. You do not need to try to answer the questions; we will continue to discuss ethics throughout the quarter.