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

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

Overview

- **Due Date:** April 3rd, 11:59pm
- **Group or Individual:** Individual or group of 2. We encourage having a partner, since discussing these questions helps you think about them.
- **How to Submit:** Submit one PDF containing both parts of the assignment to Gradescope. Make sure that names and UWNetIDs are at the top and that you mark your submission as counting for both of you if partnered.
- **Late Days:** The usual late day policy applies (5 late days for the quarter). **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 two 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.

Part 1: Ethical Analysis

Background

In the computer security field, questions of ethics and morality often arise. For generations, philosophers have considered moral questions and have provided guidance on how to make morally right or morally justified decisions. Unsurprisingly, this has not resulted in a universal definition of "right" or "good". For this assignment, you will have the opportunity to exercise two different approaches to ethical reasoning.

Before You Begin

Before you begin this assignment, you should:

- Watch this (< 14 minute) video on ethical frameworks and computer security: https://www.youtube.com/watch?v=HVRRL9Ky6Eo&ab_channel=USENIX

Optional:

- Read this short article on ethical frameworks and computer security: https://www.usenix.org/publications/loginonline/computer-security-research-moral-dilemmas-and-ethical-frameworks
- Read this longer article on ethical frameworks and computer security: https://securityethics.cs.washington.edu/ComputerSecurityTrolleyProblems.pdf

The Assignment: Analyzing Several Scenarios

In this assignment, you will analyze several scenarios using both "classic" consequentialist (utilitarian) and (Kantian) deontological ethics. These traditions have evolved over many years, and you are *not* expected to know all the details of all these frameworks. Neither is a clear-cut and mechanical framework you can apply, and encompasses many different strains of related thought. Your goal should be to understand the broad concepts of each framework (as described in the "Before You Begin" materials) which will allow you to make reasonable judgments from that perspective.

If you are unsure about how to approach the analysis, the optional readings contain analyses of similar scenarios (see section 5.4 of the longer optional reading which analyzes Scenario C.)

Note: Do not assume that your answer is wrong if you find that both analyses lead to the same conclusion. The important part of this assignment is learning how to consider ethical questions using multiple perspectives. Analyses under two different frameworks may come to the same conclusion, just for different reasons.

Scenario D1: Vulnerability Disclosure (Base Case)

Consider the following scenario: researchers have discovered a vulnerability in a product that can be patched and in which the vulnerable company is believed to be responsible.

Context:

- Researchers discover a vulnerability in Company D's product; the researchers must decide whether or not to disclose the vulnerability to Company D before their research paper is published.
- Once Company D makes the decision to fix the vulnerability, it will take them six months to complete the process and release a patch.
- Once adversaries learn about the vulnerability, it will take them three months to weaponize the vulnerability, after which an exploit will be deployed.
- Once the adversaries begin using the exploit in the wild, each of Company D's users are at risk of losing 25% of their retirement savings; there is no way for users to move their retirement savings into other systems (they are locked into using Company D's product); Company D has ten million users; 15% of users will be impacted during each month of vulnerability (until the system is patched).
- The researchers were originally inspired by monitoring chatter on underground forums; given that chatter, the researchers believe that adversaries will discover the vulnerability in nine months and deploy an exploit in one year.
- The researchers believe that Company D will be responsible: Company D will immediately begin working on a patch after a private vulnerability disclosure and will not entangle the researchers in a legal battle aimed at preventing the publication of the research paper. Further, the researchers are confident that the entirety of their research process was legal.
- The researchers are all tenured full professors who, from a career perspective, do not need a publication.
- The publication program committee has no stated preference on what the authors do; they trust authors to make the right decision.

The choice for the researchers:

- *Disclose the vulnerability to Company D and wait six months before publishing their paper:* Since Company D is believed to be responsible, the company will immediately begin working on a patch. Six months later, after the patch is deployed, the researchers can publish their paper and Company D's users will be secure against the vulnerability.
- *Do not disclose the vulnerability to Company D before publishing their paper:* Once the paper is published (month zero), adversaries will start to weaponize the vulnerability and the company will start working on a patch. Adversaries will deploy their exploit after three months (month three); the patch will be deployed after six months (month six); this

situation leaves *three months* in which Company D's users are actively being exploited (months four, five, and six).

Now, answer these questions:

- **Question 1a.** From a consequentialist (utilitarian) perspective, provide an analysis of what decision the researchers should make, and the reasoning behind that decision.
- **Question 1b.** From a (Kantian) deontological perspective, provide an analysis of what decision the researchers should make, and the reasoning behind that decision.

Scenario D2: Vulnerability Disclosure (Legal Threat)

Context: Equivalent to the scenario in Scenario D1 except the company is not a responsible actor, and will entangle researchers in a legal battle as well as not actively work on a patch:

- Company D is known to be highly litigious. If the researchers disclose the vulnerability first to Company D, the researchers will be drawn into a legal battle and be unable to publicly discuss their findings and the vulnerability for at least three years.
- This legal battle will happen even though the researchers are confident that the entirety of their research process was legal.
- Company D is known to not take computer security seriously unless there is an incident or public pressure. A private vulnerability disclosure to Company D will not cause it to begin working on defenses; it will only begin working on defenses after the vulnerability is actively exploited or there is public pressure.
- The researchers do not fear legal action against themselves if they were to publish their paper before sharing the vulnerability with the company.

The choice for the researchers: Equivalent to Scenario D2 except:

- *Disclose the vulnerability to Company D before publishing their paper and become entangled in a legal battle:* The researchers will not be able to publish their findings for at least three years. Adversaries will manifest in one year, after which Company D will begin working on a patch, which would not be released for another six months. This situation leaves *six months* in which Company D's users are actively being exploited (months thirteen to eighteen).

Now, answer these questions:

- **Question 2a.** From a consequentialist (utilitarian) perspective, provide an analysis of what decision the researchers should make, and the reasoning behind that decision.
- **Question 2b.** From a (Kantian) deontological perspective, provide an analysis of what decision the researchers should make, and the reasoning behind that decision.

And Lastly:

- **Question 3:** Provide a list of all references and communicants, per policy.

Part 2: Security Reviews

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. You should reflect deeply on the technology that you're discussing.

The 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 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.