CSE 484 - Homework 3 (Winter 2021)

This homework is focused on a variety of topics from the last ~third of the quarter. It is designed to give you exposure to some security/privacy related tools, and to prompt you to revisit and think deeply about the ethics questions from Homework 1.

Overview

- **Due Date:** Monday, March 8th, 2020 at 11:59pm
- **Group or Individual:** Individual
- **How to Submit:** Submit a PDF via Canvas
- **Total Points:** 30 points across 3 parts

Part 1: Web Privacy Settings (10 points)

Experiment with the privacy/anti-tracking settings in a browser you *don't usually use*. For this assignment, pick one of the 4 major web browsers (Edge, Safari, Chrome, Firefox) that is **not** your regularly used web browser. Once you have installed it, look for what settings you can find around anti-tracking, and privacy (in regular and incognito/private/etc modes.) Common settings include 3rd party cookie disabling, all cookie disabling, 'enhanced privacy', etc. Try turning on most/all of them, and visit three websites (e.g. www.cnn.com, www.facebook.com, canvas, etc.). You'll want to compare the experience of visiting and using these with privacy settings on, and off.

What to Submit:

1. **(3 points):** Briefly describe (a few sentences) or sketch how third-party tracking allows advertisers or others to track users across multiple sites.
2. **(1 point):** Which browser did you try?
3. **(3 points):** What privacy settings did you find? (Describe not only the name, but what you believe to be the technical effect of at least 3 settings)
4. **(3 points):** What behaviors differed for each of the 3 pages you visited? Did some pages work differently than expected? Did any features stop working with extra privacy settings enabled?

Part 2: Code-and-Data (10 points)

Over and over again in this course we've seen that an adversary wins when they can cause *data* to be considered *code*. This was the case with binary exploits (e.g. putting data on the stack that was actually shellcode and later interpreted as such), as well as the case with multiple types of web exploits (where data was either interpreted as JavaScript or as an SQL statement).

While far from the only exploitation pattern, it is a consistent one.

Why is this a consistent pattern?

1. **(3 points):** Pick one of the cases we've seen in the course. Why do you believe this particular problem arose, and kept happening?
2. **(7 points):** Why is 'data-as-code' a consistent bug across so many different systems? (Consider if this is a problem because of attacker strategy, the way we build hardware, software, or something else entirely! Feel free to include new examples) (Expected 250-350 words)

Part 3: Revisiting Your Ethics Questions (10 points)

Ethics is often domain specific, created by the practices, beliefs, and advocacy of domain experts. In this way, ethics in computer security (as it is in many other technology domains) is currently in-the-making. As future professionals, *your* practices, beliefs, and advocacy will help contribute to our understanding of computer security ethics. *You* are already computer security ethicists!

Throughout the quarter, we have been collecting questions about computer security ethics through homework and in-class activities. For this assignment, you will gain experience acting as a computer security professional by answering one of these questions.

Please ***choose one of the following*** ethics questions to address in your answer:

1. When, if ever, should a government be able to ban a technology or application? For example, under what circumstances should a government be able to mandate that app stores remove a specific application?
2. Who should be held responsible for problematic activities that occur on platforms (e.g., encrypted messaging platforms, social media platforms, Tor)?
3. Should university-based research on computer vision techniques that enable "deep fakes" be stopped or paused?
4. How should companies be held accountable when security breaches occur or privacy violations come to light?
5. Under what circumstances should a government require companies to provide or build in backdoor access to encrypted technologies for law enforcement purposes?
6. Should homeowners be allowed to set up cameras that record what happens in a public space visible from their property?
7. Should parents have a right to monitor their children's use of technology? Alternatively (or additionally), should employers have a right to monitor their employees' use of technology?

To help justify your answer, we ask you to revisit the same ethical framework that you considered in Homework 1. Repeating those links here:

- Menlo report, which connects computer security ethics to research ethics.
- Capabilities framework, which foregrounds global well-being, justice, and development.
- Manifest-no, which emphasizes refusal of historically harmful data regimes.

There are not necessarily correct/incorrect answers to ethical questions. Rather than trying to create a perfect “right” answer, focus on interpreting and applying your given ethics framework. Though the questions above may be framed as yes/no questions (“should…?”), **it is very likely that your answer will involve “it depends” -- you probably want to discuss under which circumstances something should or should not be done, rather than simply being able to answer “yes” or “no”.**

Your response should:

- **(1 point)** Note explicitly which ethical framework you used (it should be the same one you used in Homework 1);
- **(1 point)** Note explicitly which question you are answering (from the list above);
- **(1 points)** Be 350-450 words long;
- **(7 points)** Try to use the assigned ethical framework to explain your response.

There are no right or wrong answers, but some answers are better justified than others. All responses that thoughtfully engage with the question will receive full credit. Responses that are hard to understand, vague, or overly simplistic (these are not simple questions!) will receive partial credit.