CSE 484 / CSE M 584 - Homework 3 (Autumn 2020)

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:** Friday, December 4, 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 Tracking (10 points)

Experiment with an anti-tracking browser add-on, such as Ghostery, Lightbeam, or Privacy Badger. Pick three websites (e.g., www.cnn.com, www.facebook.com, and www.weather.com -- though you may pick any sites), visit them with the add-on installed, and report on what you find. If you don't want to install this in a browser you personally use, you can use a different browser, or a browser inside a Virtual Machine.

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 add-on did you try?
3. **(6 points):** Include a screenshot of the add-on's output for each of the 3 pages you tested. How many trackers did you find on each page?

Part 2: Password Security (10 points)

Below we give you the entry for a password stored on a Linux machine. The password is weak. *Your goal:* find the password.

To do this, we recommend using either john or hashcat. We strongly recommend using Linux for this question. (Use attu or a VM if you don't have a native Linux). You can likely install John the Ripper from the repository using apt-get or yum. The Linux package name is most likely john, e.g., for Ubuntu, run "sudo apt-get install john".

Or, you can download john (**John the Ripper 1.9.0 core release**, from the link above) and build it from source (**you will have to use this option if you are using attu; during build specify the architecture as linux-x86-64,** i.e., *make clean linux-x86-64*). We have verified that these instructions work on attu!

Here is the password entry, from a Linux machine (this should all be one line, without a line

break or spacing in between):

```
charizard:$6$vgk.6o3T$gPX6Sm4CNvu.4fUQi08IvBZEmO1aeemnkDWdGboK7qV54N2eVVetkIf
5ifPeQcWVJ/93LByKyIraRILs02AvC0:18585:0:99999:7:::
```

What to Submit:

1. **(8 points)** The password
2. **(1 point)** What tool you used to crack the password
3. **(1 point)** Approximately how long it took the tool you used to crack the password

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.