CSE 484 / 584M (UW CSE Computer Security & Privacy): Homework 2

[Course Homepage: https://courses.cs.washington.edu/courses/cse484/22wi/]

Technologies do not exist in isolation. Technologies exist in the context of people and society. Societies have policies and laws and norms. The people might be the direct users of a technology (a *direct stakeholder*), or they might be impacted by a technology even if they are not the direct users (an *indirect stakeholder*).

Computer security offers one vantage point to thinking about the relationship between technologies and people + society. The reason: in computer security and privacy, we consider adversaries. There are other vantages points, like considering algorithmic bias, but for the purposes of this course we will focus on computer security and privacy.

Homework 2, like Homework 1, is (1) an opportunity to revisit the security mindset, this time with the context of the first portion of the course and with a renewed focus on the relationship between technology and people+society. Additionally, Homework 2 (2) provides an opportunity to spend some time thinking about a technology that might be relevant to your final project (if you wish).

Overview

- **Due Date:** February 22, 11:45 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 2 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 2 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 Person A work on Part 1 and have Person B 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 of 2: Fiction, Technologies, Society, and Security Review

For this assignment, you will begin by reading three pieces of fiction. Two (1st and 2nd) of the stories should be from the book *Telling Stories: On Culturally Responsive Artificial Intelligence* (https://techpolicylab.uw.edu/telling-stories/). The third story (3rd) can be another story from *Telling Stories* or any other story that you find as long as the story explores the relationship between society and technology.

After having read those three stories, please write up and include in your submission:

- **The title, author, and one-sentence summary of the first (1st) story.** Your summary may be longer than one sentence but does not have to be. This must be a story from *Telling Stories*.
- **The title, author, and one-sentence summary of the second (2nd) story.** Your summary may be longer than one sentence but does not have to be. This must be a story from *Telling Stories*.
- **The title, author, and one-sentence summary of the third (3nd) story, and publication information *if* the story not from *Telling Stories*.** Your summary may be longer than one sentence but does not have to be. If you chose a story that is not from *Telling Stories*, please provide publication information (e.g., name of publisher, publication date, URL if the story is online).

Next:

- **Tell us which of the three stories you plan to use for the rest of this part of the assignment.**

Now, given the backdrop of this story, your task is to conduct a security review of that fictionalized technology. It is helpful to conduct this exercise multiple times, especially after having learned more about security. Additionally, please think deeply about the stakeholders that might be involved; the fictional setting may help with this, but do not feel a need to restrict yourself to the fictional setting in the story that you read.

First, describe the technology that you are evaluating:

- **Summary of the technology that you're evaluating.** Summarize the technology that you are evaluating. This is a technology that appears either explicitly or implicitly in the story. Because the technology may be fictionalized, it is okay to make assumptions and define technical details of the technology as you wish. Just make sure to describe the technology.

Next, do the following. The text in the following is identical to the text in Homework 1.

- **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).

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 of 2: What Goes into a Story

Read the Introduction (page 10) of the book *Telling Stories: On Culturally Responsive Artificial Intelligence* (https://techpolicylab.uw.edu/telling-stories/).

(*Optional*: Read the Preface (pages vii to ix) of *Our Reality: A Novella* (https://homes.cs.washington.edu/~yoshi/OurReality/OurReality.pdf). *Reading this is optional, but gives more context into how I was thinking about the role of storytelling in conversations around technology + society*.)

The above writings discuss the value of stories and the criticality of considering the relationship between society and technology.

Read steps 4, 6, and 8 of *Telling Stories* (pages 58-59). These pages mention AI Technologies. *For the purposes of this course, you can consider any technology as long as it has potential computer security and privacy issues*. (Step 4 corresponds to pages 63-68 of Telling Stories. Step 6 corresponds to pages 71-75. Step 8 corresponds to pages 77-81.)

You do not need to write a full story for this assignment! You are only required to work through aspects of creating a story narrative.

Follow Step 4 of Telling Stories, and include the following in your submission:

- **State at least two aspects of culture.** Write at least two aspects of culture that you consider for the backdrop of your story.
    - Note that the *Telling Stories* book, step 4, writes: “Authors initially noted their particular cultural and political environment.” One reason to focus on personal contexts is to avoid accidentally stereotyping or making incorrect assumptions if trying to design for people other than oneself. For the purposes of this course, you can think about personal contexts other than your own, but please be conscientious of the risk of stereotyping. Additionally, if working in a group of more than one person, you may have different personal contexts and hence may have to pick one or a combination. (Many good books relate are relevant to the risk of stereotyping in writing and design, e.g., one I read, with a focus on writing, is Writing the Other, http://www.aqueductpress.com/books/978-1-933500-00-3.php.)
- **State at least two aspects of the political context.** Write at least two aspects of the political context that you consider for the backdrop of your story.
- **State at least three different types of technologies that you might consider for your story.** Each technology description needs to only be one sentence long. Use this to brainstorm before picking the final technology that you wish to study (see the next section, about Step 6).

    - Note that the *Telling Stories* book, step 4, writes: “This first story sheet was intended to help authors situate potential story ideas in their own personal context (or contexts) as well as to prompt thinking around the wider AI landscape.” As noted above, *your technology can be any technology, not just AI*.
- **State at least two stakeholder-benefit pairs for the technology.** 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. As you consider stakeholders, you are encouraged (but not required) to consider the cultural and political backdrop.
- **State at least two stakeholder-harm pairs for the technology.** 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. As you consider stakeholders, you are encouraged (but not required) to consider the cultural and political backdrop.

Next, follow Step 6 of Telling Stories, and include the following in your submission:

- **Summarize the technology that you're considering for your story.** Summarize the technology that you are considering for your story. Because the technology may be fictionalized, it is okay to make assumptions and define technical details of the technology as you wish. Just make sure to describe the technology.
    - Optional: You might consider a technology that you wish to explore in more depth in the final project.
- **State at least two stakeholders or stakeholder groups that are impacted by the technology, and state how they are impacted by the technology.** These could be stakeholders that you considered in the earlier part.
- **State when your story takes place**. This could be a single sentence, or it could be more – it only needs to be clear.
- **State where your story takes place**. This could be a single sentence, or it could be more – it only needs to be clear.
- **Describe what happens in your story**. You do *not* need to write a story. But provide a few bullets (at least three) about what happens in your story. Your story will explore the relationship between society and technology. You will not be graded on the story structure and no assessment will be made of the “quality” of the story. (Aside: different cultures have different story structures.) Use these three bullets to explore the relationship between your chosen technology and people+society through a narrative.

Reread Step 8 of Telling Stories, and think about your answers to Step 8. But there is nothing you need to submit for Step 8.

Lastly:

- **Provide two bullet points of reflection.** Write down at least two reflections on how this exercise might or might not inform how you design or evaluate computing systems in the future.

Please make your submissions easy to read. For example, use bulleted lists whenever possible.