CPSC 525/625: Principles of Computer Security (F23)
Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

UNIVERSITY OF CALGARY

Name: _____ UCID: _____

Assignment #1

Due 2023-10-06 @ 23:59 MST

1 Assets, vulnerabilities, threats, & controls [26 points]

Background: You are presumably familiar with social media platforms (e.g., Facebook, Snapchat, Reddit, Tumblr, LinkedIn, and so on). In case you are not, here's how the first paragraph of the Wikipedia article on social media (as of mid-afternoon on 2022-09-18) describes them:

> "Social media [platforms] are interactive technologies that facilitate the creation and sharing of information, ideas, interests, and other forms of expression through virtual communities and networks. While challenges to the definition of social media arise due to the variety of stand-alone and built-in social media services currently available, there are some common features:
>
> 1. Social media are interactive Web 2.0 Internet-based applications.
> 2. User-generated content—such as text posts or comments, digital photos or videos, and data generated through all online interactions—is the lifeblood of social media.
> 3. Users create service-specific profiles for the website or app that are designed and maintained by the social media organization.
> 4. Social media helps the development of online social networks by connecting a user's profile with those of other individuals or groups.
>
> The term social in regard to media suggests that platforms are user-centric and enable communal activity. As such, social media can be viewed as online facilitators or enhancers of human networks—webs of individuals who enhance social connectivity."

Social media platforms are generally free to use—users simply visit a webpage or launch a smartphone app to create a free account, which they can subsequently access from a browser or smartphone app anywhere around the world. Such services benefit users, who can use them to forge personal relationships; connect with prospective customers, employees, or employers; access countless pictures of kittens; or otherwise become members of communities they find interesting. They benefit the providers in various ways that depend on those providers' business models.

The task: Spend *at least 30 minutes* and *at most 40 minutes* thinking about and formulating your responses to the following seven sub-questions. Provide as many responses as you can think of (in 35-ish minutes), but don't worry if you can only think of a few per sub-question. The goal here is to get your gears turning, so try thinking outside the box and please try to come up with your own ideas (i.e., **don't ask Google** and **don't discuss your thoughts and ideas with your peers** prior to responding).

The sub-questions: Without further ado,

(a) **[2 point]** Choose a specific social network. It doesn't matter which one you pick; just pick one and record your choice. (While any social network is fine, it does make sense to pick one you're somewhat familiar with!) Also write a few sentences explaining what niche the chosen social network serves/what sort of user experience it offers.

(b) **[4 points]** In the context of the specific social network you chose, what do you think are the most notable *assets*? The assets you mention do not need to all be assets to the same party—different actors may have different assets, so make it clear which actors will view each kind of asset as an asset.

(c) **[4 points]** How do you think someone might go about trying to attack the social network or its users? That is, what do you think the *threats* are? Because different actors may have different assets, the threats you mention do not need to all be threats to the same party. So make it clear which actors will be most affected by each of the threats you list.

(d) **[4 points]** Who are the primary *adversaries* that might target the various threats, and what might their *goals* be? (For example, with regards to threats that involve defacing a website, the adversary might be amateurs or script kiddies doing it for "the lulz"; for threats that could result in the leaking of payment information, the adversary might be organized crime seeking financial gain; for threats that could result in the revelation of trade secrets, the adversary might be economic competitors hoping to gain an unfair competitive advantage; for threats involving the leakage of personal emails, the attacker might be "a 400 lb person" or "somebody from New Jersey" trying to Make America Great Again. Note that you need not limit your response to the example attackers listed in the slides.)

(e) **[4 points]** What are some reasonable *controls* that might help to mitigate the threats you identified?

(f) **[4 points]** How do you think someone might go about trying to leverage the social network to implement attacks or defenses affecting *other* networked systems? That is, are there ways an adversary could use or abuse the infrastructure and functionality of your chosen social network to thwart or launch attacks against "unrelated" systems? (For example, an attacker that compromises a point-of-sale terminal could skim credit card data with which to commit fraud against a credit issuer.)

(g) **[4 points]** Given all of the above, what do you think are the most important security concerns for your chosen social network?

Name: _____ UCID: _____

2 Writing a dumb program [30 points]

Throughout the semester, you will be asked to interact with and attack various *objectively dumb* programs that I have written. For this question, you are asked to write a specific, objectively dumb, program of your own in C. The goal is to get your hands dirty with some low-stakes C programming, figure out how to properly leverage `setuid` and drop privileges when `setuid` is no longer needed, start thinking about how to write code that fails gracefully when provided with malformed inputs, and craft a functioning `Makefile`.

To this end, you are asked to write a short C program called `foo` (implemented in a file called `foo.c`) that is intended to be run with `setuid` privileges so that it can read and write files accessible only to the owner. The program should do the following:

1. Upon starting, print the string "Hello `current_euid` (`current_ruid`)." to `stderr`
2. Attempt to open a file (for both reading and writing)
   (a) the filename (`file_name`) is specified by the first command-line argument
   (b) if no such file exists, then
      i. create the file with permissions `0600` owned by `current_euid` and write a 32-bit integer `0` to that file
   (c) if such a file already exists, then
      i. if file size is not 32 bits, print "You can't foo `file_name`, it's all bar'd!" to `stdout`

   (Note the relevance of the `setuid` privileges at this step)
3. Permanently drop privileges as soon as they are no longer (possibly) needed
4. Read a 32-bit integer `count` from the file, increment it, and then write the incremented `count` over the existing file contents
5. Print "You have foo'd `file_name` a total of `count` times." to `stdout`
6. Print "Farewell `current_euid` (`current_ruid`)." to `stderr`

Your program should fail gracefully if anything – bad or missing arguments, file I/O failures, etc. – goes wrong; that is, rather than segfaulting or behaving unpredictably, your program should calmly explain where the problem was encountered and then terminate cleanly. During testing, we *will* feed your program some malformed inputs and non-sensible environment defaults; see the rubric on D2L for details.

In addition to writing the above `foo.c`, you must also write a basic `Makefile`. The TAs will simply run `make` to compile your code; if that fails to produce a working binary, the TAs will *not* attempt to troubleshoot why.

To facilitate testing the `setuid` *functionality and that you are dropping privilege correctly, we've added a simple program* `/usr/bin/make_setuid` *so that running* `make_setuid foo` *effectively runs* `chown dwight foo; chmod 4555 foo`. *This allows you to run your* `foo` *binary as a* `setuid dwight` *executable.*

To submit your response to this portion, simply copy `foo.c` and `Makefile` to `/submit/your_username/a1` on `pr.iva.cy`. You do not need to submit anything via D2L.

3 Security review [35 points]

For this part of the assignment, you must evaluate the potential security and privacy issues with some new (at least to you) technology, evaluate the severity of those issues, and discuss how future advances might address those security and privacy issues. The technology you select will presumably (but does not have to) involve some sort of networking—e.g., a new network protocol, a toaster with WiFi connectivity, vehicular networks, smart speakers, ride-share services, etc. Your response should be 1.5–2 pages that reflect deeply on the technology that you're discussing. In particular, your response should contain:

- A summary of the technology that you're evaluating. You may choose to evaluate a specific product or a whole 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.
- 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.
- 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 for the TAs to parse. For example, use headings and bulleted lists whenever possible, such as by listing each asset as its own entry in a bulleted list. Full paragraphs often make it harder for the TAs to find the relevant information you are trying to convey.

Note on citations: Research is not required to complete this assignment, but if resources are used, it is important they are properly cited. No specific citation style is required in this course, but enough information must be supplied that the resources used can easily be found by someone else (namely, the TAs).

Name: _____ UCID: _____

4 Dropbox Submission

Your submission to D2L should include:

1. <username>.pdf containing your answers to questions 1 and 3