CPSC 525/625: Principles of Information Security (F19)
Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

UNIVERSITY OF CALGARY

Name: _____ UCID: _____

Assignment 01

Due 2019-09-30 @ 11:59

1. **[20 marks total]** Spend *at least 25 minutes* and *at most 35 minutes* thinking about and formulating your responses to the following five sub-questions. Provide as many responses as you can think of (in 30-ish minutes), but don't worry if you can only think of a few.

   Background: You are presumably familiar with webmail services (e.g., Gmail, Hotmail, Yahoo! Mail, and so on). Webmail services are generally free – users can go to their preferred service provider and create a webmail account. They can then access their webmail account from a browser anywhere around the world, and often from their phones as well. These webmail systems benefit users, who now have a free email account; they benefit the providers in various ways that depend on those providers' business models.

   (a) **[4 marks]** When considering the design of a webmail system, what do you think the *assets* should be? The assets you mention do not need to all be assets to same party—different actors may have different assets, so make it clear which actors will view each kind of asset as an asset.

   (b) **[4 marks]** Who are primary *adversaries*, and what might their *goals* be?

   (c) **[4 marks]** How do you think someone might go about trying to attack the webmail system or its users? That is, what do you think the *threats* are?

   (d) **[4 marks]** How do you think someone might go about trying to leverage the webmail system to implement attacks or defenses affecting other systems.

   (e) **[4 marks]** Given all of the above, what do you think are the most important security concerns for webmail systems?

Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

UNIVERSITY OF CALGARY

Name: _____ UCID: _____

Security review [40 marks]

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. Your response should be 1.5–2 pages (11pt, single spaced, preferably typeset in LaTeX) 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 (like Amazon Echo) 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 to read. For example, use bulleted lists whenever possible. E.g., list each asset as its own entry in a bulleted list.