CPSC 525/625: Principles of Information Security (F21)
Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

Name: StevenCanon-Almagro UCID: 10155792

Assignment 01

Due 2021-09-30 @ 23:59 AoE

Mocha setup [0 marks – but must get done]

You should have already received an email from mocha with your account information; if not, please log on to Piazza and inform the Instructors ASAP so that we can create an account for you.

Generate a public key, log onto mocha, add your newly generated key to your `authorized_keys` file, and confirm that you can subsequently log on without a password. (You may still need to enter your passphrase, if you set one on your key. That is fine.) You can find the CPSC 329 `tutorial00` worksheet posted alongside this assignment on D2L; it contains relatively detailed instructions on how to generate and install ssh public keys.

In your home directory, you will find a file called `ETHICS`. Open it with your favourite text editor, read it carefully, and then—assuming you agree to be bound by the conditions set forth in the text—replace the string < YOUR_NAME > with, err.. your own name. If you do not feel comfortable agreeing to those terms, then we've got a slight problem and you should reach out to the Instructors via Piazza ASAP.

This first part is not worth any marks, but the remaining sections will be graded only after we verify that the first part is complete.

Name: StevenCanon-Almagro UCID: 10155792

Assets,vulnerabilities, & threats [24 marks]

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.

1. **[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 the same party—different actors may have different assets, so make it clear which actors will view each kind of asset as an asset.

   The assets of this webmail system should be the data that each user is sending. The user would be the most invested in privacy. The data should only be accessible to the user it is intended for. Another asset is the availability of the system. A webmail service should be available to the users and each handle has to be unique to each other. This would be a priority to the developers of the system. Someone shouldn't be able to make a ton of emails and take away all the viable and coherent handles so that when someone wants to create an email they don't have to go with some a long and complex handle. There are two sides of this, if the process is too easy then people will take advantage but if the process is long and confusing then a user might choose to not get a account in the first place.

2. **[4 marks]** Who are primary *adversaries*, and what might their *goals* be?

   Potentially there could be a large amount of adversaries. It all depends on the user and the data that adversary is trying to compromise. Adversaries like troll farms would look to impersonate a user as some joke. Then on the more extreme side we have organized crime where they are using the webmail system to get to the user and all their other information.

3. **[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?

   The best way to go about attacking the system is through the user. Probably by sending them phishing emails to fake pages so they have to log in and give away their password. The threats are the user's personal and/or sensitive information. The user's trust in the system is another threat, if they lose confidence in the system then they will stop using it.

4. **[4 marks]** What are some reasonable *controls* that might help to mitigate the identified threats?

    Having some sort of spam filter for any emails that a user receives letting the user know of the harm. The service could also block users from clicking on any URL unless from a trusted contact. This could eliminate any accidental clicks.

5. **[4 marks]** How do you think someone might go about trying to leverage the webmail system to implement attacks or defenses affecting *other* systems.

    For an attack a webmail system can be used in many ways.Many people reuse passwords so a person could make a fake website of a popular service and then email the URL to a list of many people. Some person may fall for it and try to log into that website and once they have their password they could go around and try to break into other accounts owned by that person. For defenses a service cant defend from those attacks directly, but they can make it so that you need more than just a password to access their service. 2 factor authentication is a great example of this. The service can notify the user when a new sign-in occurred in a new machine. This will notify a user if their account has been compromised and then they can go change their password.

6. **[4 marks]** Given all of the above, what do you think are the most important security concerns for webmail systems?

    The biggest security concern that this system should concern with are the users themselves. Users are not the brightest and they will choose to cut corners whenever they are presented with one. The most important thing this webmail system can do is make sure the user can't compromise themselves or the system by being given too much freedom to do what ever they want with their account.

Name: StevenCanon-Almagro UCID: 10155792

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.

Name: StevenCanon-Almagro

UCID: 10155792

Smart Glasses

We have always looked to make technology portable in order to carry or wear on our person. Sony came out with the Walkman for music on the go, and smart watches allowed us to carry a small screen on our wrist. These are just a few examples of portable examples. The newest trend are smart glasses. Google unveiled Google Glass back in 2013 where they wanted to give an augmented reality experience. Google Glass' OS is based off Android and uses Glassware to optimize the apps its using. Glassware is a company that focuses on adapting apps so that they can work on tablets and phones[2]. The functionality that Google glass offers is[1]:

- Ability to take photos and videos and share them
- Ability to use google search engine when connected to a network
- Have translations directly streamed to the screen
- Write emails and text with voice dictation
- Compatible with Google maps
- Using motions and gestures to control application

Since 2013 there have been some heavy hitters in the smart glasses market. Google, Facebook, and Amazon to just name a few, each with their own take on smart glasses. According to a article on S&P Global there has been a rise in sales in smart glasses, from 76,000 in 2015 to 713,000 in 2019[3]. In 2019 google decided to give google glass another try and in their newest version of the product it has a XRI chip that gives the product the potential to do machine learning and computer vision abilities[1]. With the new spike in interest it is important that consumers get a real good pictures at any security concerns so that they can make an educated purchase. Smart glasses are in a unique position when it comes to security.

1 Assets & Security goals

- Privacy, the biggest asset surrounding smart glasses.
  - The biggest reason why google glass failed to catch on back in 2013. People were rightfully aware and concerned with the recording feature of google glass.
  - The goal of privacy in for smart glasses is to be as transparent as much as possible with any features that could compromise other people's privacy
- User's health
  - Any device that involves a person eyes is a huge health risk and can cause damage to the user and anyone around depending on the situation they are in.
  - A security goal would be to make sure that any app that can be used by the glasses goes through any rigorous vetting and that users use the features at appropriate times.

2 Threats & Adversaries

- A threat could happen where someone could use the camera feature with facial recognition. The user would be the adversary preying upon the public.
- A developer could be the adversary creating a malicious application that would produce bright lights when using their app. this could potentially harm the user's vision.

3 Potential Weaknesses

- If the camera could be used with social media the user would be able to start streaming. More people would be looking at the same thing than are physically present and glasses make it more discrete. A person may not know they are being streamed.
- A user using a malicious app that could seriously harm them, maybe use a bright light or try to induce a seizure.

4 Potential Defenses

- Some smart glasses use an LED to notify the public that the user is recording[4]
  - to add on to this point they can add a sound to go off every couple of seconds when recording so that users don't have to look at the user to know they are being watched.
- The system should have some algorithm to make sure that any app that uses bright lights and colours don't use it maliciously
- make sure that users are not using apps during tasks that require their full attention like driving.

There are definitely serious risks when it comes to smart glasses. The privacy issues cannot be ignored and having a small lit up LED is not the right solution to such a problem. Being able to record in such a discrete matter will definitely lead to huge problems in the future while laws surrounding in this area are outdated. The user's health is also a huge risk and can really damage a person life in multiple ways.

In conclusion smart glasses come with huge risks for the user and the general public. Now the companies themselves can shield themselves behind a terms and conditions agreement and pass all the blame to the user. The technology is only in its infancy, the future of smart is quite large. Imagine having thermal vision touch, look at a person and know everything about them even their credit score, or a zoom so powerful you could see the content on a person's phone sitting across the room. Smart glasses are a technology that has the same potential as the smart phone to impact our society. Its one step closer in our journey to become cyborgs.

References

[1] https://internetofthingsagenda.techtarget.com/definition/Google-Glass

[2] https://sphere3d.com/glassware-2-0-technology/

[3] https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/as-smart-glasses-come-back-into-focus-privacy-risks-fog-the-lens-63696709

[4] https://techcrunch.com/2021/09/20/facebook-warned-over-very-small-indicator-led-on-smart-glasses-as-eu-dpas-flag-privacy-concerns/