CPSC 525 – Assignment 1

Alex Stevenson – 30073617

1. Assets, Vulnerabilities, Threats, & Controls

a) Choose a specific social network

Social Network: Facebook

Facebook is the most user-centric social network. Users set up a profile of personally identifying information and can add various types of posts to their user wall for anybody to view or interact with via reactions and comments. Users create a network of friends to interact with, where friends automatically get updates on each other's profiles and can message each other directly through the secondary *Facebook Messenger* app.

Facebook offers various additional functionalities such as User Groups and Public Business Profiles. User Groups are created by group administrators that link member profiles together where member profiles can post and interact with the group, receiving notifications whenever the group is updated. Public Business Profiles are special accounts created for businesses that include extra information such as a business phone number and special events that the business can create. Business posts can be advertised to users based on user interaction history.

Facebook also contains a marketplace for individual users to add listings and perform transactions between people. These transactions and interactions with listings are tracked by Facebook to better personalize advertisements towards users based on their financial activity.

b) What are the most notable assets?

The primary asset of Facebook is the immense amounts of information that it collects on everything and everybody. This has resulted in numerous lawsuits and scandals but Facebook continues to collect exceptional amounts of data, primarily for selling to advertising firms and other companies for financial gain.

User Assets: Personal user information, authentication information, geographic location, finances and marketplace habits, posting ability (malicious actors posting detrimental information), messenger chat history, interaction history with other posts and the marketplace
Business Assets: Authentication information, employees, marketplace listings
Group Assets: Administrator information, user list

c) **How do you think someone might attack the social network or its users?**
The main threat is social engineering performed on users to gain access to their information that is linked to their profiles. This can gain their authentication information to access their account, to then access their personal information. Social engineering can also be performed on the marketplace, to simply scam other users through real-life transactions. Once a user's authentication information is stolen one can also post publically on their user account, either posting malicious information about the user to cause social harm or spreading false information through otherwise trusted profiles.

d) **Who are the primary adversaries that might target various threats?**
Amateur hackers targeting users can cause social harm to the user as detailed above.
Government agencies or hacker groups can target prominent profiles to post propaganda to further a political cause.
Marketing firms may target groups, businesses, or Facebook itself to acquire mass amounts of personal user information for advertising or other business related purposes.
Other groups may do the same to gain personal information to sell for financial gain.

e) **What are some reasonable controls to help mitigate the threats you identified?**
Prevent Facebook from collecting such an insane amount of data on individual users. If they were more limited in their personal data collection then they would be less useful to potential adversaries that are trying to do societal harm.
Implement Two-Factor Authentication for Facebook accounts across several devices to minimize the risk of social engineering to easily gain authentication info.

f) **How do you think someone might use the social network to implement attacks or defenses affecting other networked systems?**
Gaining personal authentication information on a user could allow you to use that same authentication info to try to access their accounts on different systems.
You could use a user's public posts to try to gain insight on security questions across other systems (such as the name of their first pet or their mother's maiden name)
With access to enough personal imagery of the user, AI generated deepfakes could be created of that user to destroy their reputation or further political goals.

g) **What are the most important security concerns for your chosen social network?**
As Facebook is centered on individual users, the primary security concerns are certainly the individual users and the ridiculous amount of data that Facebook collects on them. Being able to access the data on different users can be used in various ways to harm those individuals and society as a whole. The easiest way to access systems that you shouldn't be able to is through the massive amounts of people that are present on facebook.

3. Security Review – Rideshare Services

Summary:

A ridesharing service is a company that matches customers with drivers through a website or mobile app. These services organize one-way transportation transactions between customers and drivers. Customers request routes between two points and drivers can choose to accept that job, delivering the customer to where they need to be and receiving payment for the trip. Drivers for ridesharing companies make accounts with them and are considered an independent contractor for the company.

Ridesharing companies take a cut of the payment for each transaction between customer and driver. Many of these companies will influence the prices of trips through a *surge pricing* algorithm, where the price for a trip is drastically increased during busy times of certain locations. This serves to balance the rideshare marketplace by encouraging more drivers to work during that period of inflated prices and discouraging customers from overwhelming the system. Popular ridesharing companies include Uber, Lyft, and Sidecar.

Assets:

- *Payment Information* (both customers and drivers of the system): In order to pay for a ride share service as a customer, you must input your payment information. Likewise, drivers must provide their banking information so that they can receive payment for taking jobs. A security goal for payment information is to obviously keep this information totally secure, such that nobody can access these details directly.
- *Job Routes*: The route should be consistent, such that the driver takes the customer to the location that they specify. A security goal for this will be to prevent routes from being altered by a third party.
- *Personal Information:* Identifying information of both drivers and customers are required by the rideshare service in order to match customers and drivers. A security goal is to keep this information private and inaccessible for anybody outside of the individuals involved with a transaction.

Threats:

- *Phishing Payment Information*: An adversary can attempt to compromise payment information by sending phishing links to potential customers and drivers of the rideshare system. By making an identical website to the rideshare website, an adversary could trick unsuspecting users of the rideshare service into providing their payment information directly. Adversaries include malicious individuals who want to scam money out of other people.
- *Middleman Attack on Job Routes:* As the route for any given job needs to be transmitted through the internet from a customer to a driver, it would be possible to intercept this job route and replace it with a new one. Adversaries that would want to do this are most likely random people who are confusing people and ruining routes for fun.

Weaknesses:

- There is inherent weakness with sending data over the internet. This data can be intercepted or modified by adversaries that can access it. As ride-share services are inherently tied to the internet they will also have this weakness.
- There is another weakness around storing personally identifying information regarding customers and drivers in a single place. There is quite a bit of information that is stored that can be used maliciously against an individual, such as current and expected location, and make and model of vehicle.

Defenses:

- Internet transmissions should be using standard cryptographic protocols between customer and driver to prevent third party access.
- Personally identifying information should be encrypted. When a new transaction begins there should be some sort of temporary access to specific pieces of data for the other person in the transaction. An example of this is revealing the make, model, and colour of the driver car to the customer when the transaction begins, without revealing other information of the driver such as their social insurance number.

Evaluation:

The above combination of assets, threats, and weaknesses has the potential to pose significant risk to users of rideshare services. However given the widespread adoption and use of these services as a one-way transportation transaction and government attention makes it unlikely for individuals to be put at risk by using them. Rideshare companies are financially incentivized to ensure the security of their assets and there are many protocols and standardized processes to assist them in this.

Conclusion:

As someone who has never actually used a rideshare service, I believe that the major rideshare companies can be trusted with your personal and financial information about as much as any other major service provider. The issues that arise with using these rideshare services are not related to computer security, and are instead related to ethical and economic implications. The technology and algorithms used will continue to be developed as these services grow in popularity, however predatory pricing practices and exploitation of those that register to be drivers can be concerns for governments and lower income individuals.