Assignment 1

CPSC 525
Eddy Qiang
30058191

Part 1:

a) The assets of a webmail system should be the contents of emails. The users of the webmail system will view this as an asset because email exchanges are generally personal.

   Another asset would be the mail servers. The administrators and IT department would want to protect it.

b) The primary adversaries are cyber criminals. Their goals would be to have access to the personal, sensitive, or confidential information contained in the accounts. There would be many reasons why someone would want to steal this information. They could gain more access to other people by impersonating and pretending to be someone else.

c) One of the ways a hacker can attack the users of the webmail system is through phishing. By pretending to be legitimate, they try to lure individuals into providing sensitive data such as their passwords.

   Another threat is malware. When a system gets infected by malware it could potentially give control over to the attackers. With control they could steal information like intellectual property, or other proprietary secrets.

d) You often have to use your email to register on other systems, therefore the email is connected to other accounts. Someone could leverage this and use your email to try to access your other accounts. This can be done by resetting passwords for other accounts, or sometimes when the user uses the same passwords for multiple accounts.

e) I think the most important security concerns for webmail systems are malware. Email can be used by attackers to send malicious software like viruses, trojan horses, and spyware. You would be essentially giving the attackers complete access to your system.

   Another important security concern is how the data is stored. An attacker might not need go after the users if they can target and find vulnerabilities in the host servers.

Part 2: Security Review

Summary of the technology - Bitcoin and blockchain.

At the very basic level, Bitcoin is a digital file or ledger that contains account numbers and balances. People exchange money by changing this file. Each person maintains their own copy of the ledger. When you send Bitcoin you are simply broadcasting a message and telling everyone else how much you are sending, and to whom. Then everyone else will update their ledger. When a new account number is created, it comes a long with a private key mathematically linked to that account number. These keys are what give you access to your Bitcoin. A wallet is something that holds these keys.

The technology involved is the blockchain. The bitcoin blockchain acts as a public distributed ledger that records bitcoin transactions. It is implemented as a chain of blocks, each block containing a hash of the previous block up to the first block of the chain. Each block will also contain transaction data including the sender, receiver, and amount. Bitcoins are created by "mining" them. Miners are rewarded bitcoins when they solve a mathematical problem. Today bitcoin is used as a currency much like real money.

Assets

1. One of the most important assets of this technology is the ledger. More specifically we want to maintain the integrity of the blockchain. The goal is to make sure no one can manipulate the records. This important because it is decentralized currency with no human oversight.
2. Another asset is the identity and privacy of the users. An advantage bitcoin has is that you can complete transactions without divulging any sensitive financial information, like your name, debit, or credit card number. The goal to maintain privacy is important because it lowers the risk of fraud.

Threats

1. One possible threat to Bitcoin is technological exploitation. Since Bitcoin is relatively new, there could be bugs that open doors to exploits that are not yet discovered. An example of an adversary would be hackers that try to game the system. If hackers can manage to alter to ledger then they would be able to steal bitcoin from everyone.
2. Another possible threat is the government regulation. There are many countries that have banned Bitcoin. For example, in China it would be illegal to trade Bitcoin. The adversary would be the government, some may see the rise of cryptocurrency to be a threat to the governments currency, centralization, and banks.

Weaknesses

1. One potential weakness is attacks on the blockchain. Hypothetically if someone can gain control of more than 50% of the network's mining hashrate or computing power, the attackers would be able to reverse transactions, or block transactions from being recorded onto the ledger.
2. Another potential weakness is the risk of theft. Since Bitcoin has no physical form, it takes little effort to steal any amounts of Bitcoin. This security risk is a huge weakness because since there is not oversight like banks and law enforcement, there is little you can do to recover your losses once a thief gets their hands on your Bitcoins.

Defenses

1. One of the potential defenses against the attacks mentioned is to distribute the mining power by mining on different pools. By doing so even the largest mining pools will not be able to even get close to attaining the majority of computing power. It would not be feasible for someone to do this if they have to come up with sufficient mining power to compete with the entire world.
2. One of the potential defenses against the risk of theft is to have multiple wallets and only storing a small amount in each wallet. This will drastically decrease the risk of losing all your Bitcoin. You can also encrypt your wallets to add security. Another option is to use cold storage, or a paper wallet, which is non-digital and cannot be hacked.

Evaluation and Conclusion

The risks associated with the assets and threats is high. Cryptocurrency technology is relatively new and there could vulnerabilities that have not been discovered yet. People are incentivized to try to exploit the system because if they are successful, they will have large financial gains. While user's names are not associated with the accounts, the ledger is public and can be viewed by anyone. It may be possible to trace an account back to the owner if you do analysis combined with other information (data mining). The government has been looking into these methods because of people using cryptocurrencies to launder money and evade taxes. The risks associated with the potential weaknesses is low. As mentioned it is virtually impossible to obtain a majority of computing power to do a 51% attack on Bitcoin. Even if you could it would likely cost more than you would gain. The risk of theft is largely dependent on the user and if they are diligent in securing their assets.

I believe there is a high likelihood that the blockchain technology will evolve. Currently there is a lot of attention on the whole idea of blockchain. It has become somewhat of a buzzword. There are many people, companies, and researchers that are highly involved in researching this technology. In the bigger picture, cryptocurrencies are becoming more mainstream as more and more people are adopting its use. In countries with high inflation, their country's money could devalue and become worthless. Bitcoin can be a great alternative for commerce because it is anti-inflationary and decentralized. I predict in the next decade we will see even more advances in this technology.