COMP3632 Assignment 1

SU, Heng
20310671
hsuab@connect.ust.hk

September 15, 2017

Problem 1

(a)

System	The OnePass password management service (software) and servers (hardware).
Asset	The passwords, protected data, and goodwill and trust of the OnePass users.
Vulnerability	Thereotical limitation of using only a master password, which can be guessed/brute-forced.
Attack	Using software to guess/brute-force the master password of a user.
Defense	Enabling two-factor authentication.

(b)

$$\text{Asset value} = 5 \times 10,000 \times 12 = \$600,000$$

$$\text{Exposure factor} = 0.1$$

$$\text{Single Loss Expectancy (SLE)} = \text{Asset value} \times \text{Exposure factor} = \$60,000$$

$$\text{Annual rate of occurrence} = 0.02$$

$$\text{Annual Loss Expectancy (ALE)} = \text{SLE} \times \text{Annual rate of occurence} = \$1,200$$

Assuming the worst case where hacks occurs at the start of the year (so OnePass misses out on 12 full months of payment from customers), it costs $\$1,200$ per year to accept the hack, whereas it costs $\$3,000$ to implement two-factor authentication, so it's not worth enabling two-factor authentication.

(c)

News of the hack could deter potential future customers from trusting OnePass and instead lead them to choose a competitor, which would result in lost revenue.

Problem 2

(a)

(i) Availability is being violated because mining bitcoins is CPU intensive. If the computer is laggy as a result of the mining, then the user has access to fewer CPU cycles to perform tasks he actually wants. **(ii)** By method of spreading, the Sundown malware is a trojan, since it tricks users into installing it onto their computer by hiding on an innocuous looking website. It then has a hidden, secondary, malicious effect (mining bitcoins in the background). By effect on system, it is a botnet, since it is commanding thousands of different computers owned by different people to perform a malicious task on behalf of the attacker.

(b)

(i) Availability is being violated because the user's files have been encrypted and are inaccessible to the user, sometimes even after paying the ransom. **(ii)** By method of spreading, the WannaCry malware is a worm, since it replicates across a network without user intervention. By effect on system, it is ransomware, because it holds data hostage in exchange for money.

(c)

(i) Integrity is being violated because the trustworthiness of the data being sent from the legitimate website to the user has been compromised; malicious code has been inserted to steal user data. The integrity of the hacked computers have also been violated, because they are running code that the users did not authorize. **(ii)** By method of spreading, the Angler exploit is a trojan, since it tricks users into installing it (by inserting itself into a legitimate website that users trust). By effect on system, it is spyware, since it is designed to spy on a user and collect private information.

Problem 3

(a) Open Design

(i) This principle states that by making a system open to the public for scrutiny, more people can check it and discover any potential bugs/mistakes. According to this principle, such a system with an open design is more secure than a system with a closed design—where the security of the system relies on the fact that nobody knows how it works (security through obscurity). If someone were to reverse engineer it, then the protection is lost. Instead, the protection should lie in the secrecy of keys/passwords, which is much easier to protect.
(ii) In season 5 episode 13 of the tv show *Community*, Abed discovers a hidden trapdoor leading to a basement lab which holds millions of dollars in cash. This is an example of security through obscurity (violating open design). Since the trapdoor was hidden, the school administrator thought that this would keep the money safe. However, when someone "reverse engineered" the design (found the trapdoor), the money was no longer protected. The "open design" solution would have been to make the basement floor open to public, and put the money in a well-known yet publicly trusted and scrutinized location (i.e. a bank).

(b) Economy of Mechanism

(i) This principle states that by keeping a design simple (i.e. KISS principle), it's easier to design, implement, analyze, test, and verify the correctness/safety of a system.
(ii) In the Wallace and Gromit series *Cracking Contraptions*, Wallace designs a convoluted robot (violating economy of mechanism) which tries to automate his breakfast cooking process. However, because the machine is too complex and unstable to function reliably, it explodes and blinds Wallace with half cooked eggs.

(c) Least Common Mechanism

(i) This principle states that the amount of shared resources different parties rely on should be minimized, similar to preventing a single point of failure. If one party corrupts the resource, then everyone else would be unable to access the resource properly too. From a security standpoint, shared channels may also potentially leak undesired information.
(ii) In *Edge of Tomorrow*, Major William Cage fights alongside the United Defense Force against an alien species (Mimics) able to manipulate time. After realizing that the Mimics are controlled by a singular being known as the "Omega" (violating least common mechanism), Cage sets out to find and destroy it, thus crippling the rest of the Mimic fighters.

(d) Complete Mediation

(i) This principle states that every access attempt along the way should be checked for proper authorization. This prevents user attempts at circumventing imposed restrictions, and accounts for situations where the user's permissions have changed, and the old permissions are no longer valid.
(ii) In *Dr. Strangelove, or How I Learned to Stop Worrying and Love the Bomb*, the insane General Jack D. Ripper orders a pre-emptive nuclear strike on the Soviets. The president is shocked at the fact that the military system in fact allowed the general to launch a nuke without the president's approval. This demonstrates how the principle of complete mediation was violated, since the general had been given "complete authority" under an emergency situation, and this included the ability to launch a nuke under his authority. The entire world ended in nuclear war as a result. To prevent this outcome, every action by the general should have required approval by the president.

(e) Psychological Acceptibility

(i) This principle states that security mechanisms should be intuitive and friendly for the user. As well, the security mechanisms should not hinder usage of the service, or else the users may potentially disable the security mechanisms.

(ii) In *The Matrix*, humanity has become enslaved by sentient machines who harvest humans as a resource. What remains of humanity only exists in a simulated world hosted by the machines. However, the main protagonist Neo starts to realize something is wrong with his world, and seeks to find out his true existence. He is "unplugged" into the real world by a group of other people who have also "escaped" the Matrix. In the second installment of the Matrix trilogy, the Architect (designer of the Matrix) reveals that he is on the sixth version of the matrix, where previous generations had failed because a small percentage of humans (including Neo) psychologically rejected the world the machines had tried to contain them in. This demonstrates that the world the machines had constructed were not psychologically acceptable for the humans, so they rejected the system, ultimately causing the entire Matrix design to fail multiple times.