COMP 3632- Principles of Cybersecurity

Ali Symeri
20591029

1.

a)

System: The system is the actual service itself, password management service.
Asset: The assets are the OnePass servers (Machines), the password management service (program), the stored passwords in their servers (Data) and the trust of the users (Values).
Vulnerability: The vulnerability is the fact that there is a master password that can be guessed.
Attack: The attack is that an attacker can do a brute-force attack and try all possible passwords.
Defense: The defensive solution could be to buy and enable the two-factor authentication.

b)

Service cost per user = $5 per month
Estimated hacked rate for 10,000 users = 2% per year
Two-factor authentication (2FA) cost = $3,000 per year

Exposure factor (user notices hack) = 10%
Asset Value = ($5 per month * 12 months) * 10,000 users = $600,000 per year
Single loss expectancy (SLE) = Asset Value * Exposure Factor => $600,000 per year * 0.1 = $60,000 per year
Annual loss expectancy (ALE) = SLE * annualized rate of occurrence => $60,000 * 0.02 = $1,200 per year

This mean that they lose $1,200 per year with the estimated hacked rate of 2% for 10,000 users per year. Now, the 2FA costs $3,000 per year which is higher than the lost amount of $1,200 per year, which means that it is not worth using 2FA.

c)

Providing such a service is not monopolized, so there will be other similar services out there. This means that OnePass needs to generate loyalty and trust, to keep their users and if they get hacked, they will lose users trust and probably not attract new users to their service.

d)

It is always a good idea to force the users to use a more complex password as it makes it harder to brute-force. However, it is still prone to brute-forcing. Based on the design of Separation of Privileges, it would be better to simply use the 2FA to

authenticate users, as the user gets bound to password and a physical object, the phone, to authenticate and not only password.

2.

a)

The principle of Integrity is violated in this case. This is because the user simply visits a website where some content is expected but in fact it will inject your computer and do something else, mine bitcoins. So, it is not doing what you thought it would do. The malware can be of the type Trojan because it is packaged in a harmless looking website and the user is tricked into entering it and gets infected.

b)

The principle of Availability is violated in this case. This is because the service and computer files are not accessible without paying the hackers, so the data cannot be reached. The malware can be of the types Worm and Ransomware because it required no user interaction for spreading to the computer, probably to network facing connections and it demands payment upon decryption.

c)

The principle of Confidentiality is violated in this case. This is because your secret and private passwords and credit card information is being stolen. The malware can be a combination of the type Spyware and Trojan since it is spying on you and stealing information and also being a Trojan by tricking the user to trust the legitimate website and get infected.

3.

a)

This is false, because the encryption and decryption algorithm are generally public and not hidden from the public, so, they instead rely on people trying to find flaws with these algorithms to ensure that they are secure enough for usage. What is hidden are the secret keys.

b)

This is true, because TOCTTOU will try to modify some file in between an action, for example after the user has been authenticated for an action it will intervene after the authentication and before the action and modify the file or similarly. So, the system has not followed complete mediation like locking the files or something similar.

c)

This is false, because Heartbleed was found in OpenSSL which is open source and available for everyone to look at. So, it followed the open design but was flawed.

d)

I think this is false, because with XSS, the attacker writes and executes code on the web site and so it's not web server related.

e)

This is true, because a Virus self-replicates and infects files and uses the spreading mechanism and payload while a Trojan is meant for tricking users and is packaged with software, and I believe they are not self-replicating or infecting files. The same piece of malware will be one of the two.

f)

I think this is false, because the blaster worm caused buffer overflow in the RPC so that it would stop to function, and since RPC is a critical service, the system would just reboot all the time.