

1.

(a)

System: OnePass password management service server (software).

Asset: Password of its users (data).

Vulnerability: Attackers can obtain password information.

Attack: Random guessing master password.

Defense: Two-factor authentication.

(b)

$$ALE = 10000 * 2\% * 10\% * 5 * 12 = 1200$$

Cost for two-factor authentication per year = 3000

$1200 < 3000 \Rightarrow$ It is not worthy to adopt this defense.

(c)

The reputation of the company can be damaged, leading to the decrease in the number of potential customers.

2.

(a)

integrity: the correctness of the computer is compromised.

Botnet: a master computer control others.

(b)

availability: the files are not accessible unless decrypted.

Ransomware: need to pay ransom in order to decipher the file.

(c)

confidentiality: the credit card information and passwords are stolen.

Spyware: this kit was used to access private data.

3.

(a)

Open Design:

1. The design of the system should be public.
2. Fullmetal Alchemist (Animation): Even though the homunculus had made public the secret to their powerfulness, which is a special kind of stone, people still cannot easily defeat them. That is because they do not merely rely on this secret to stay strong. This follows the principal of open design.

(b)

Economy of Mechanism:

1. The system should be implemented in a simple and understandable way.
2. Silicon Valley (TV series): The code of Pied Piper, a compression algorithm, was too messy and complicated that only the guy who wrote it can completely understand it. This violates the principle of economy of mechanism.

(c)

Least Common Mechanism:

1. There should be as few shared mechanisms that all users depend on as possible.
2. Games of Throne (TV series): The white walkers can all be killed by dragon glass as they are created based on the same mechanism.

(d)

Complete Mediation:

1. All the access to the system should be checked.
2. Ilium (Novel): In Trojan War, the horse was allowed to pass through the gate without any checking, leading to the catastrophe. This violates complete mediation.

(e)

Psychological Acceptability:

1. User interface should be designed for ease of use so that users routinely and automatically accept the protection mechanisms correctly.
2. Silicon Valley (TV series): Big Head created an App called Nip Alert which spots the nearby nipple. The UI is simple in which user only needs to press start for that, conforming to psychological acceptability.



