

# COMP3632 Assignment1

MENG Zihan 20412027

## Written Assignment

1.

(a) **System:** OnePass password management service

**Asset:** Passwords of users

**Vulnerability:** Passwords of users to be attacked and obtained by attackers

**Attack:** Attackers using password guessing attack to obtain master passwords

**Defense:** two-factor authentication

(b)  $ALE = \text{Asset Value} * \text{Exposure Factor} * \text{Annualized Rate of Occurrence}$

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

$$= 1200 < 3000$$

Hence, it is not worth enabling two-factor authentication

(c) The company might lose their reputation, leading to declining of future potential customers and a decrease in income.

(d) I think this is a good idea.

By setting up this requirement, the mechanism of protection is simple enough. This fulfills “economy of mechanism” and “psychological acceptability” principles.

By increasing the complexity of the master password, the difficulty of attackers to succeed by using password-guessing technique is decreased.

2.

- (a) **Principle:** Integrity. Because the behavior of the infected system is changed.

**Malware:** Botnet. There is a master computer controlling infected computers on the net, for instance, control them to do bitcoin mining.

- (b) **Principle:** Availability. Because the system has suffered severe disruption due to infection.

**Malware:** Ransomware. To get the files decrypted, infected systems need to pay ransom to attackers.

- (c) **Principle:** Confidentiality. Since important information such as credit card information and passwords are exposed to attackers.

**Malware:** Spyware. The malware gains important information without user's knowledge.

3.

- (a) **False.** Security through obscurity means the design or implementation of the system is hidden. Cryptographic protocols are generally following open design principle. Also, using private key doesn't mean the algorithm is using security of obscurity.

- (b) **True.** Complete mediation means all accesses should be checked.

"TOCTTOU" happens between "time of check" and "time of use". During the period, attackers may do some changes, but the accesses are not checked.

- (c) **False.** Heartbleed is a vulnerability that was found in a open source software. The vulnerability of Heartbleed is classified as a buffer overread vulnerability.
- (d) **False.** There are two types of XSS vulnerabilities: persistent XSS vulnerability and reflected XSS vulnerability. Both types of vulnerabilities occur when users can write code onto a web page. The former type happens when user changes the content of a page persistently; the latter happens when attacker implants malicious link that changes content of a page to execute code.
- (e) **True.** A virus is a piece of malicious program that self-replicates. A trojan horse is a destructive program that looks like a genuine application. Trojan horses do not replicate themselves but can be destructive.
- (f) **False.** The Blaster worm caused Windows system shutdowns because of the unexpected shutdown of Remote Procedure Call (RPC) service.