Assignment 1.   COMP 3632   MENG Zihan

Written Assignment   20412027

1. (a). System : OnePass password management service.

        Asset : Passwords of its users

        Vulnerability = Passwords of its users to be obtained by attackers.

                                                    attack
        Attack: Attackers using password guessing ∨ to obtain master password.

        Defense= two-factor authentication.

   (b)   ALE = Asset Value * Exposure Factor * annualized rate of occurrence

                = 10000× 2% × 10% × 5 × 12 = 1200

           Since   1200 < 3000,

           it is not   worth enabling two-factor authentication.

   (c)   The reputation of the company might be damaged, which
         may lead to declining of future customers, and a decrease in incomes.

   (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 attacker to succeed by using password-guessing technique is increased.

2. (a) ① Principle= integrity. Because the behavior of the infected system is changed.
        Malware= Botnet. There will be a master computer controlling infected
                  computers on the net, for instance, control them to do bitcoin
                  mining
        ② Principle= availability. Because the system has suffered severe disruption due to
                                                                          infection.
        Malware= Ransomware. In order 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.

2. (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 type 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 attack implant 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 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