Name: Chen Hao Cheng

Course: CSCI-3403 Cyber Security

Review Question

1.2) What is the difference between passive and active security threads?

Passive Attack	Active Attack
Attempts to learn or make use of information from the system but does not affect system resources	Attempts to alter system resources or affect their operation
They are in the nature of eavesdropping on, or monitoring of, transmissions.	Involve some modification of the data stream or the creation of a false stream.
The goal of the attacker is to obtain information that is being transmitted.	Four categories: 1. Replay 2. Masquerade 3. Modification of messages 4. Denial of service
Two types: 1. Release of message contents 2. Traffic analysis	
Difficult to detect, measures are available to prevent their success	Difficult to prevent active attacks absolutely because to do so would require physical protection of all communication facilities and paths at all times.

Problems:

1.1) Consider an automated teller machine (ATM) to which users provide a personal identification number (PIN) and a card for account. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement

Confidentiality: The user accesses their account with PIN and their card and he or she will expect their information of PIN is confidential as well as any transaction between bank server and the host system.

Degree of importance: Because unsecure PIN during transaction may lead to compromise of account so it might result in major financial loss. Thus, PIN has to be encrypted.

Integrity: The user will expect the transaction record correctly and PIN information without being changed accidentally or some malicious software would modify it.

Degree of importance: Taking into account if a user withdraws $1000, the balance is $3000 left, but the system has a wrong record that only $2000 left. Then the user would have unexpected loss. The other situation is after the user withdraws, their PIN has been changed, then the user might not be able to login in some emergency situation. Thus, all transaction should operate and affect user's account correctly and directly (Real time). All transactions should be encrypted.

Availability: All ATM machines need to be available to use all the time.

Degree of importance: ATM can increase the potential growth for bank. Therefore, it needs to available at all times.

1.4)

a) **Confidentiality:** No loss of confidentiality because the organization manages public information on Web server. Since it's public information, so not applicable.

   Integrity: Information could be changed by unauthorized manner even if it might not be a serious issue Or life-threatening injuries. Thus, it's moderate.

   Availability: It might cause to bother some people's public of access, or use of information even though it doesn't have high impact. Thus, it's the impact level for the loss of moderate.

b) **Confidentiality:** The law enforcement organization manages extremely sensitive investigative information, and because it is extremely sensitive so the loss of confidentiality is high.

   Integrity: The sensitive investigative information might be changed by unauthorized manner, so some serious criminal might not be justified. This could be the loss of moderate or high.

   Availability: It doesn't have high impact but it might bother some access or use of information. Thus, The loss of available is moderate.

c) **Confidentiality:** The organization manages routine administrative information and it's not privacy related. Thus, the potential of impact level for the loss of confidentiality is low.

   Integrity: Because it's not a privacy related information, so even if it's been modified, it's not a problem. The impact of level for the loss of integrity is low.

   Availability: It will not cause the problem for administrative information so the impact level for the loss of availability is low.

d) <u>Sensitive contract information:</u>

Confidentiality: The contracting organization manages sensitive, pre-solicitation phase contract information but it does not cause death issues. The impact of level for the loss of confidentiality is moderate.

Integrity: This would cause damages of sensitive information and data, and also untheorized manner. Hence, the impact level for the loss of integrity is moderate.

Availability: This would not affect availability for contracting organization so it will not be an issue. Hence, the impact level for the

Loss of availability is low.

Routine administrative information:

Confidentiality: The contracting organization only manages the routine administrative information and it doesn't have privacy related information. Thus, the impact level for the loss of confidentiality is low.

Integrity: The potential impact level for the loss of integrity is low because the loss of exact administrative data won't cause a problem.

Availability: It might damage minor of organization's assets, minor financial loss, or harm individuals but it won't cause a big problem. Therefore, the potential impact level for the loss of availability is low.

e) **Real-time sensor data:**

Confidentiality:

The organization manages real-time sensor data, but it doesn't have private related information so the impact level for the loss of confidentiality is low.

Integrity: The real-time sensor data should be provided essentially so the impact level for the loss of integrity is high.

Availability: Because it is real-time data so providing real-time information is essential, then the impact level for the loss of availability is high.

Routine administrative information:

Confidentiality:

The organization manages the routing administrative information, but it doesn't have private related information so the impact level for the loss of confidentiality is low.

Integrity:

It would not be a problem if it loss of exact administrative data so the impact level for the loss of integrity is low.

Availability:

It would not be a problem if it loss of administrative data so the impact level for the loss of available is low.

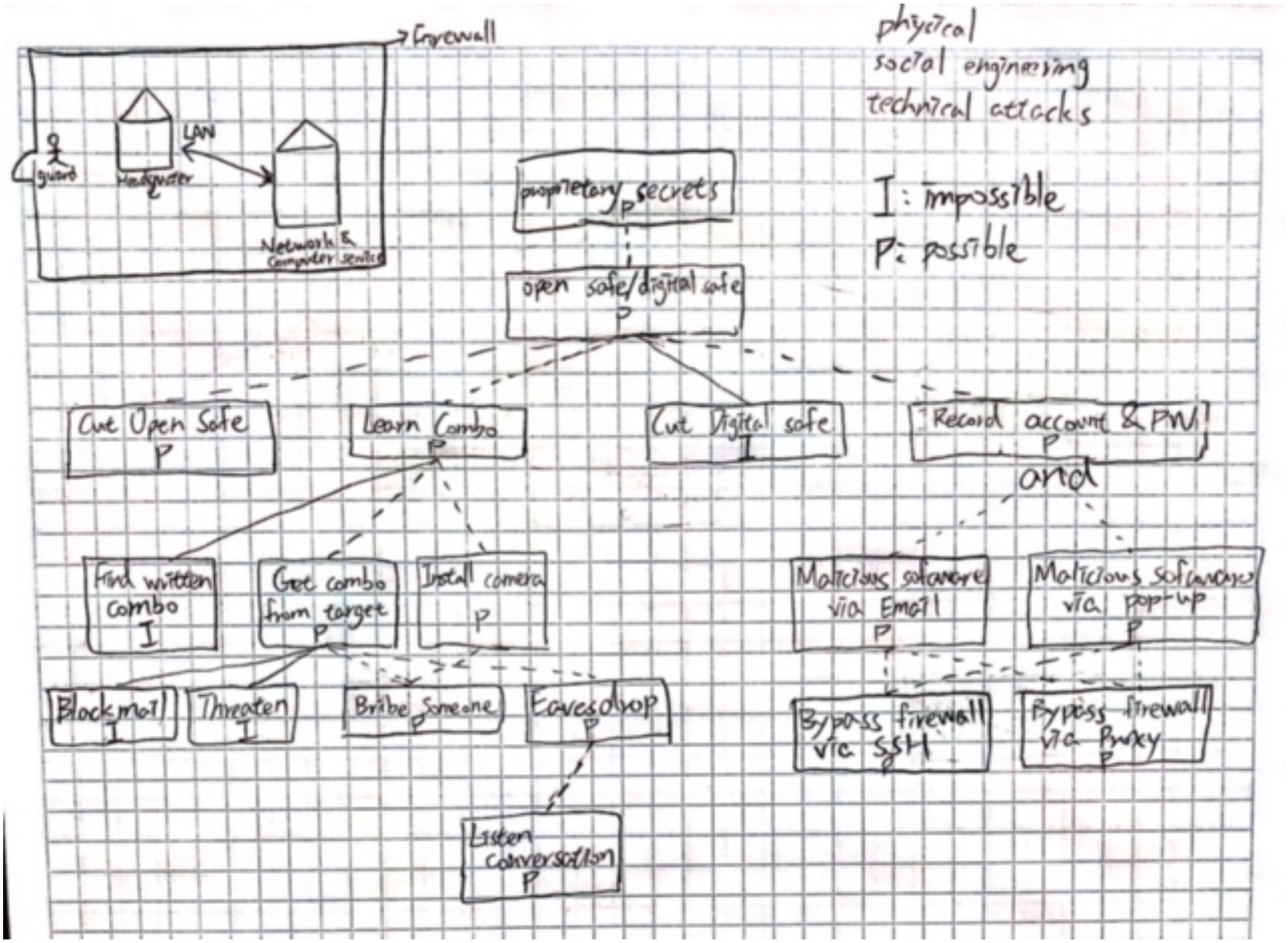
1.5)

a. This general code violets the Fail-safe default principle. It has to give permission to access the decision. The program it firstly executed the access denied condition that need to eliminated and give permission to access the resource. We can see it executes the function IsAccessAllowed() and returns a value and stored in the object dwRet of type DWORD, and then the dwRet compares with ERROR_ACCESS_DENIED in the if-statement so it checks first denied condition. In the case of access to resource of system, it has to check ACCESS condition first, and then ACCESS DENIED condition.

b.

```
DWORD dwRet = IsAccessAllowed(…)
If (dwRet == ACCESS_IS_OK){
// Security check pass
// Inform user that access is fine
} else {
// Security check fails
// Inform user that access is denied
}
```

1.7)


Firewall
LAN
guard
Headquarter
Network & Computer service
physical
social engineering
technical attacks
I: impossible
P: possible
proprietary secrets
P
open safe/digital safe
P
Cut Open Safe
P
Learn Combo
P
Cut Digital safe
I
Record account & PW
P
and
Find written combo
I
Get combo from target
P
Install camera
P
Malicious software via Email
P
Malicious software via pop-up
P
Blackmail
I
Threaten
I
Bribe Someone
P
Eavesdrop
P
Bypass firewall via SSH
P
Bypass firewall via Proxy
P
Listen conversation
P