Introduction to Computer Security Module – G6077

Concepts: Confidentiality, Integrity and Availability

Learning objectives:

1) Describe the key security requirements – Confidentiality, Integrity and Availability
2) Discuss types of security threats
3) Explain the fundamental security design principles
4) Discuss attack surfaces and trees

Task 1

Apart from the card and USN, if the student needs to enter a pass key to access the information, then the system must keep the pass key confidential, both in the host system and during transmission for a transaction. It must protect the integrity of student records. Availability of the host system is important for maintaining the reputation of the Institution. The availability of SIS machines is of less concern.

Task 2

The system has high requirements for integrity on individual data packet, as lasting damage can incur by occasionally losing a data packet. The integrity of routing algorithm and routing tables is also critical. Without these, the routing function would be defeated. A network routing system must also preserve the confidentiality of individual data packets, preventing one from accessing the contents of another.

Task 3

a. The system will have to assure confidentiality if it is being used to publish corporate proprietary material.

b. The system will have to assure integrity if it is being used to laws or regulations.

c. The system will have to assure availability if it is being used to publish a daily paper.

Task 4

a.

An organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability.

b.

A law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate.

c.

A financial organization managing routine administrative information (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

d.

The management within the contracting organization determines that:

(i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and

(ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

e.

The management at the power plant determines that:

(i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and

(ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability.

Task 5

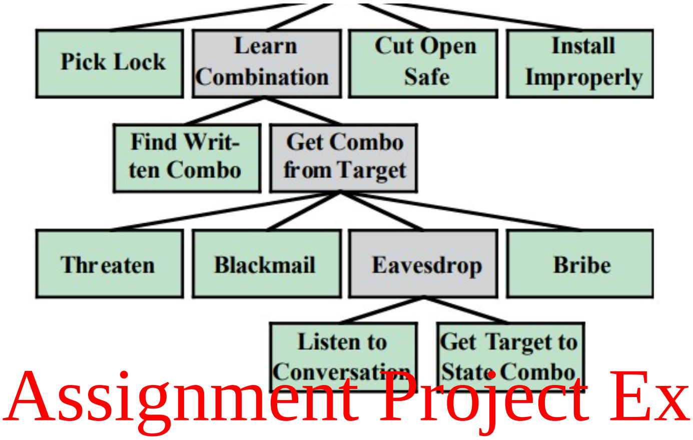
a. At first glance, this code looks fine, but what happens if IsAccessAllowed fails? For example, what happens if the system runs out of memory, or object handles, when this function is called? The user can execute the privileged task because the function might return an error such as ERROR NOT ENOUGH MEMORY.

b.

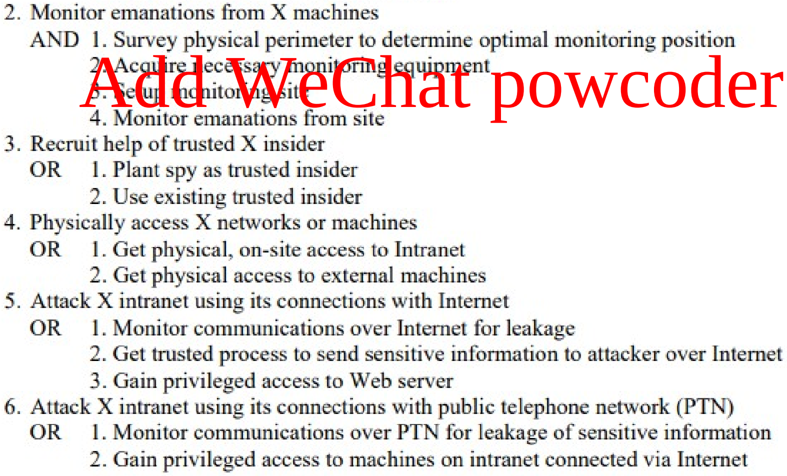
```
DWORD dwRet = IsAccessAllowed(...);
 if (dwRet == NO_ERROR)
   {
        // Secure check OK.
       // Perform task.
    }
else
  {
        // Security check failed.
        // Inform user that access is denied.
   }
```

In this case, if the call to IsAccessAllowed fails for any reason, the user is denied access to the privileged operation.

Task 6



Task 7



2. Monitor emanations from X machines
   AND 1. Survey physical perimeter to determine optimal monitoring position
   2. Acquire necessary monitoring equipment
   3. Setup monitoring site
   4. Monitor emanations from site
3. Recruit help of trusted X insider
   OR 1. Plant spy as trusted insider
   2. Use existing trusted insider
4. Physically access X networks or machines
   OR 1. Get physical, on-site access to Intranet
   2. Get physical access to external machines
5. Attack X intranet using its connections with Internet
   OR 1. Monitor communications over Internet for leakage
   2. Get trusted process to send sensitive information to attacker over Internet
   3. Gain privileged access to Web server
6. Attack X intranet using its connections with public telephone network (PTN)
   OR 1. Monitor communications over PTN for leakage of sensitive information
   2. Gain privileged access to machines on intranet connected via Internet

Challenge Task 8

List key points to answer questions after reading the anatomy of one of the most famous security incidents.

https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Question	Answers (Key points)
We studied different types of general categories of attack in the lecture. What type of attack was it?	
What assets of Target were compromised?	
Keep in view the CIA triad, describe how each of the principle were compromised.	
What mechanism was used to compromise HVAC contractor's credential? Please propose at least two security mechanisms to guard against the mechanism used to compromise the security credential.	Email spam filter; phishing education
Stolen credentials were not enough to access company's POS devices. What did the hackers do to acquire elevated rights that allow them access to company's network and to deploy malware.	SQL injection attack; buffer overflow attack; XSS attack; 0- day attack; weak or default password
For privilege escalation, the hackers need to do vulnerability scanning on the Target network. Please propose as many ways as you know to do vulnerability scanning?	Nmap; Nessus; penetration test
Target admitted that they ignored many alerts from their network security devices because of alert overload. If you are the Target CTO, what would you do to alleviate the problem of alert overload?	Upgrade security soft-ware; better training
