Introduction to Computer Security Module – G6077

Concepts: Confidentiality, Integrity and Availability, Security attacks

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

Consider a student information system (SIS) in which students provide a university student number (SID) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of the importance of the requirement.

Task 2

Repeat Problem task 1 for a network routing system that routes data packets through a network based on the IP address provided by the sender.

Task 3

Consider a desktop publishing system used to produce documents for various organizations. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement. Give an example of a type of publication in which data integrity is the most important requirement. Give an example in which system availability is the most important requirement.

Task 4

For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

a. An organization managing public information on its Web server.
b. A law enforcement organization managing extremely sensitive investigative information.
c. A financial organization managing routine administrative information (not privacyrelated information).
d. An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

Task 5

Consider the following general code for allowing access to a resource:

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

Explain the security flaw in this program.

Rewrite the code to avoid the flaw.

Hint: Consider the design principle of fail-safe defaults.

Task 6

Develop an attack tree for gaining access to the contents of a physical safe.

Task 7

Consider a company whose operations are housed in two buildings on the same property: one building is headquarters, the other building contains network and computer services. The property is physically protected by a fence around the perimeter. The only entrance to the property is through a guarded front gate. The local networks are split between the Headquarters' LAN and the Network Services' LAN. Internet users connect to the Web server through a firewall. Dial-up users get access to a particular server on the Network Services' LAN. Develop an attack tree in which the root node represents disclosure of proprietary secrets. Include physical, social engineering, and technical attacks. The tree may contain both AND and OR nodes. Develop a tree that has at least 15 leaf nodes.

Task 8

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

https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

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.	
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.	
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?	
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?	