Jeff Kim

Cecs 378 Sec 03

3/2/2022

Assignment 1

1. **Define the term computer security.**
   - The term computer security is defined as term to measure and control confidentiality, integrity, and availability of information system assets including hardware software, firmware, and information being processed, stored, and communicated

2. What is the difference between passive and active security threats?

- Passive security threats are done in naturally like eavesdropping whereas active threats are manually done by such as modifying a program, or data.

3. Explain the difference between an attack surface and an attack tree.

- attack surfaces are reachable vulnerabilities in a system and attack tree is data structure sets that represents potential ways to exploiting security vulnerabilities.s

4. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) 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 importance of the requirement.

- I would prioritize confidentially then integrity and lastly followed by availability. Confidential wise, they should be required to have proof of their card such as physical card or mobile tap and I personally think it would be good to require one time password via their mobile phone. Integrity wise, the amount of their bank statement while they do any action such as withdraw or deposit should be correctly shown. Availability should be least prioritized for security. Users should only be allowed to view, withdraw, and deposit their account.

5. Repeat question #4 for a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller.

I would prioritize Integrity security and availability. While the system routes calls it should prioritize users safety and moral and each user's information should be secured. Availability, they should be simply allowed to connect and call.

6. List and briefly define the fundamental security design principles.

Confidentiality: makes sure data is available or disclosed to unauthorized users and allows users to do or know what happens with their information related to the system.

Integrity: makes sure information are changed only in designated way.

Availability: makes sure service is not denied to intended users.

7. Consider a desktop publishing system used to produce documents for various organizations.

(a) Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.

- Mails

(b) Give an example of a type of publication in which data integrity is the most important requirement.

- Photoshop

(c) Give an example in which system availability is the most important requirement.

- Notepad.

8. 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.

- For loss of confidentiality: no impact because the information is already public

- Loss of integrity: moderate.information could be modified or used unlike intended.

- Loss of availability – low to moderate it is already public so the information won't be as important or its already in public for people to access it through other companies

(b) A law enforcement organization managing extremely sensitive investigative information.

- Loss of confidentiality: high impact. It could be top secret like government confidential

- Loss of integrity: High impact the Information could be used in wrong hands.

- Loss of availability: low to no impact. They want it to be kept to themselves anyways.

(c) A financial organization managing routine administrative information (not privacy-related information).

- Loss of confidentiality: low because it is not privacy related information administrative information

- Loss of integrity: low impact even if the routine administrative information is used in wrong it has no impact in organization

- Loss of availability: low impact the user won't be impacted by it

(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.

pre-solicitation info:

- Loss of confidentiality: large impact because its before the contract and they could know the information that would impact contract

- Loss of integrity: moderate impact if the data is used in wrong hand it could cause the organization financially

- Loss of availability: low. The information is rather better to have low availability

Routine administrative information

- Loss of confidentiality: low because the administrating information leaking won't impact the company

- Loss of integrity: low. Loss of integrity won't impact the organization

- Loss of availability: low. It is company's administrative information meaning not be shared with users.

System as whole

- Loss of confidentiality: moderate to high because they lost pre-solicitation info which could leak information about contracting organizaion

- Loss of integrity: moderate. System using in wrong way won't impact the organization

- Loss of availability: low loss of availability would be okay as long as the two contracting organization has availability

1

(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.

Real- time sensor data

- Loss of confidentiality: high impact. Sensor data leaking to opponent could reveal vulnerability.

- Loss of integrity: high. Information could be used for terrorism

- Loss of availability: low. Better to be kept to themselves

Routine administrative information

- Loss of confidentiality: low. Its just administrating the system. No information is leaked

- Loss of integrity: low. Administrating information loss integrity won't have much impact

- Loss of availability: low. Better to be kept to military.

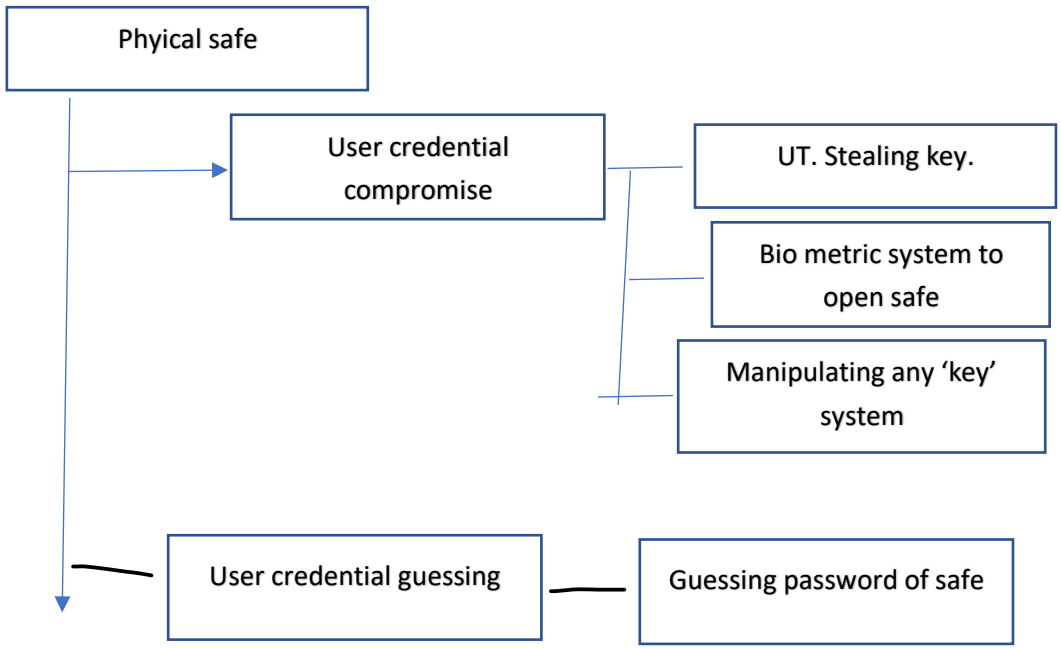
Information system

- Loss of confidentiality: losing information about electric power could reveal vunerability

- Loss of integrity: moderate because modifying real-time sensor could have big impact

- Loss of availability: Low. Information are better off with low availability

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



10. 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.

}

(a) **Explain the security flaw in this program.**

- I think the security flaw in this program is the fact that system thinks if the user's access is denied it is allowed. However, there could be a case where they are by error not denied but not allowed at the same time

(b) **Rewrite the code to avoid the flaw**

- Simply re write if (dwRet == ACCESS_ALLOWED){
  Check ok
  }
  else {
  block
  }

Deliverables. Submit the answers to the questions on Beachboard Dropbox by the indicated due date and time. Acceptable file submission formats are: .txt, .rtf, .odt, .doc, .docx, or .pdf.