CECS 378 Assignment 1 - Intro to Computer Security

1. Define the term computer security.
   1. Computer security is defined as a measure and control that ensures 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?
   1. The difference between passive security threats is that an active threat attempts to alter system resources or affect their operation while passive threats attempts to learn or make use of information from the system that does not affect system resources.
3. Explain the difference between an attack surface and an attack tree.
   1. An attack surface consists of the reachable and exploitable vulnerabilities in a system which are categorized as network, software, and human attacks. An analysis of these attacks is a useful technique to assess the scale and severity of threats to a system. Attack trees are a branching, hierarchical data structure that represent a set of potential techniques for exploiting security vulnerabilities. The exploited node in the tree is called the root node of the attack tree. The reason for these types of attacks are to exploit the information available on attack patterns. The fact that these trees are structured makes it easy to find key vulnerabilities at each node in the tree when using these attack trees.
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.
   1. Examples of confidentiality include a pass key or a PIN which is going to be during the transaction and the bank system. Integrity can include the protection of the records of the transaction and the person doing making the transaction. Availability would be having the most amount of ATM’s possible for all its clients. For a bank, availability, integrity, then confidentiality is the degree of importance that they give to their ATM’s.
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.
   1. The telephone system must be in high integrity so that no packets of telephone transmission are lost. The network switches must also protect the confidentiality of the calls making sure that each switch is routing each call to where it needs to lead. The availability of switches is also very important so that more calls can be made.
6. List and briefly define the fundamental security design principles.
   1. Authentication: assuring that the entity that is communicating is the one that it claims to be
   2. Access control: preventing the unauthorized use of a resource
   3. Data confidentiality: protecting data from unauthorized disclosure
   4. Data integrity: assuring that data received are exactly as sent by the entity who sent it
   5. Nonrepudiation: protection against denial by one of the entities involved in a communication
   6. Availability service: property of a system being accessible and usable upon demand by an authorized system entity
7. Consider a desktop publishing system used to produce documents for various organizations.
   1. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
      1. Corporate papers that are exclusive only to the company
   2. Give an example of a type of publication in which data integrity is the most important requirement.
      1. Laws governing the usage of the service provided by the company
   3. Give an example in which system availability is the most important requirement.
      1. Publishing something everything like a blog or an online newspaper
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.
   1. An organization managing public information on its Web server.
      1. Low confidentiality and moderate loss of availability
   2. A law enforcement organization managing extremely sensitive investigative information.
      1. High impact from loss of confidentiality as their information is very private, loss of integrity is moderate, and loss of availability is moderate
   3. A financial organization managing routine administrative information (not privacy-related information).
      1. Given the bank system earlier, loss of confidentiality is low, loss of integrity moderate, and loss of availability is high
   4. 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.
      1. For the phase contact information, the loss of confidentiality is moderate, the loss of integrity is low, and loss of availability is high. For the routine administrative information the impact from a loss of confidentiality is low, loss of integrity is moderate and loss of availability is high.
   5. 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.
      1. For the real-time sensor data, loss of confidentiality is low, loss of integrity is high and loss of availability is high. For the administrative information, the loss of confidentiality is low, loss of integrity is moderate, and loss of availability is moderate.
9. Develop an attack tree for gaining access to the contents of a physical safe.
   * + 1. Open safe
   1. / | \ \
   2. Lock picking Combo access Cut Build it wrong
      1. / \
   3. Find combo on sticky Force it out of person
      * + 1. / | \
        1. Threat Eavesdrop Bribe
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.

}

* 1. Explain the security flaw in this program.
     1. IsAccessAllowed is a function in the program, if it fails then it can go to the else statement, and the user can access non-privileged information
  2. Rewrite the code to avoid the flaw (Hint: Consider the design principle of fail-safe defaults).
     1. DWORD dwRet = IsAccessAllowed(…);
     2. If (dwRet == NULL\_ERROR) {
        1. // Secure check good
        2. // Execute task
     3. } Else {
        1. // Security check failed
        2. // Access denied
     4. }