CECS 378 Assignment 1 - Intro to Computer Security

20 points

Assignment Description. Answer the following questions from the Chapter 1 reading from your textbook. Be through and complete with your answers. You *may* work on these questions with a partner (no more than two working together), but **both** students must submit the document individually on Beachboard Dropbox along with both students' names on each submission.

1. Define the term *computer security.*
2. What is the difference between passive and active security threats?
3. Explain the difference between an attack surface and an attack tree.
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.
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.
6. List and briefly define the fundamental security design principles.
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.
   (b) Give an example of a type of publication in which data integrity is the most important requirement.
   (c) Give an example in which system availability is the most important requirement.
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.
   (b) A law enforcement organization managing extremely sensitive investigative information.
   (c) A financial organization managing routine administrative information (not privacy-related 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.

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.

(b) Rewrite the code to avoid the flaw
(Hint: Consider the design principle of fail-safe defaults).

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.