1. **Review Question 1.2**. What is the difference between passive and active security threats?

   The difference between passive and active securty threats is that passive is an attempt to learn information from a system without altering it. Active security threats on the otherhand attempt to alter or affect the systems operation.

2. **Problem 1.1**. Consider an automated teller machine (ATM) to which users provide a personal identificaiton 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.

   The user's PIN must remain confidential. This is crucial from a user's perspective. Otherwise anyone with my card may access my accounts. The integrity of the users account information is also vital to the user and bank. If those records are incorrect, then the user is misinformed on how much money their account has and the bank will have a harder time keeping track of where the money is. Lastly, the availability is important for banks to market themselves from a business perspective. Other than that, availability is not crucial from a security standpoint.

3. **Problem 1.4**. 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
   Confidentiality - Low Because this organization is handling public info that is already avaible to the public.
   Availability - High Especially if their business model depends on the availability of this information being live
   Integrity - Moderate It's important that this information is correct but with it being public info, it will be easier for the public to find the truth elsewhere.

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

Confidentiality - Moderate the unauthorized disclosure of this information is bad and in the wrong hands like the bad guys, they are given an advantage to get out of their predicament.
Availability - Low the loss of availability is good because there shouldn't be a ton of people who have access to this information.
Integrity - High This information could led to imprisonment and if it is wrong, then an innocent person could be sentenced.

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

Confidentiality - Low Since this information is not private, it is okay for it to be disclosed.
Availability - High Users of this financial organization need to be able to access this administrative information.
Integrity - Moderate False administrative information at this level could lead to confusion but can easily be corrected without much damage.

(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.

Confidentiality - Contract info: High, Admin: Low, System: Moderate The sensitive contract information must remain undiscolosed. If known publicly, the acquisition could turn south. The Admin information is publicily known so does not matter to be confidential. For the system, it remains moderate due to the nature of the contract info.
Availability - Contract info: Low, Admin: High, System: Moderate The sensitive information does not need to have high availability. The administrative does from a user's perspective. Overall, it is imporant to the overall system.
Integrity - Contract info: High, Admin: Moderate, System: Moderate Integrity must be high for the contract info because the sale itself depends on this information and both parties need to be clear on the acquisition contract deal. The administrative information should have moderate integrity but this information is public and can be corrected easily. The system should have moderate level

integrity

(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 systems as a whole

Confidentiality - Sensor data: High, Admin: Low, System: Moderate Confidentiality of the sensor data is crucial since leaked information could lead to a possiblilty where attackers have an advantage. The administrative information is not nearly as important. But for the system together, it is fairly important that Confidentiality is maintained.
Availability - Sensor data: Low, Admin: Moderate, System: Moderate Low availability is good for the confidential information but might need higher availability for administrative work. The system itself should have moderate amount of availability and not be availabile to everyone.
Integrity - Sensor data: High, Admin: Moderate, System: High The integrity of the sensor is extremely imporant because mislead information could led to triggered alarms for the military installation. Admin integriy is also important but could be corrected easily. The system overall should have high integrity.

4. **Problem 1.5**. 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.
}
```

(a) Explain the security flaw in this program.

The problem with the code implementation above is the if condition is specifically checking for an error and assumes any other response is ok. We should rather check for a specific success response. If and only if that response is returned shoud we assume the security check was ok. Any other response should be considered an failed security check.

(b) Rewrite the code to avoid the flaw

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