CSCI 3403 **Erika Bailon**
Homework 1 **Fall 2018, CU-Boulder**

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

   Passive security threat is when the person attacking has no intention of being discovered, no intention of altering your system or cause some damage. The only purpose is to obtain information/data. I can think that (as the book and some movies show) the passive person attacking is obtaining information to know when the delivery of drugs will be made, when is the president going to show up at some place, how are they passing fake merchandise to other country, etc. It is difficult to detect since there is no damage or change to the system.
   In the contrary, **Active** is when the purpose is to alter/damage the system or the data in it. Is basically all the opposite to passive, you can detect it because you will see some corruption. There are 4 different attacks when it comes to active threats: replay, masquerade, modification of message, denial of service. All this affect the performance and the security of a system or data.

2. **Problem 1.1**. Consider an automated teller machine (ATM) to 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.

   Confidentiality
   An example of confidentiality during this transaction would be when the ATM ”receives” the PIN number, it needs to keep that data confidential. The user expects this information to be private and not shared with just anyone. The degree of importance I think is moderate. The ATM not having a proper way of keeping your PIN private/confidential is definitely dangerous because people can withdraw money from your account by cloning your card or stealing your card. However, I cannot think is a high degree of importance because ATMs have a limit of withdrawal. The person who has access to your PIN cannot empty your account in one day. You can notice the withdraw you did not make and report it.

   Integrity
   Imagine you want to buy a new puppy and it cost $1,200. You go and check your account online and the balance is $3000. You are so excited about the puppy that you

don't question your balance and you pay with the card that actually had a balance of $300! You overdraft your account and now you have to find out the way to pay the fee and the money you overspent. I would say the level of importance is low for the person because the puppy can be returned to get your money back. Also, you can blame the bank or application and waive the overdraft fee. However, I would say is high importance for the back since this user can decide to close the account with this bank and go to another bank with integrity. This will affect the economy of the bank, and even more if this keeps happening and a lot of users close their accounts.

Availability
I think that an example would be something that happened to me. I was in Mexico and I needed to eat because I was starving so I stopped at a food place and when I wanted to pay I noticed they only accept cash!! There was an ATM close and I was able to pay and leave happy. I can say is high importance because if the ATM would have NOT worked at that moment because it was denying me access, I have no idea what could I have done to be able to pay the bill. Not only that could be an example, but there are many situations where you have to pay cash and being able to use an ATM and withdraw money from your account is something that should never be a problem caused by the system not being available. What if you're in the border and the cartel is asking you for $500 or you die?

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 the information is public already, so is just like a third party or a preferred website to release information that is already released by someone else. There is no private or confidential information so is low.

   Integrity - HIGH - If public information is modify, it could affect someone getting a job because the manager would research that person information and can say he/she has felonies. It can affect someone who has a private plane is planning a trip based on the weather, if the weather is changed maliciously and erased the possibility of a storm, the person in the plane will crash. The time of operations or location of a hospital, if someone is in a need of a hospital urgently and the address or hours of operation are wrong, this person can die if it's a extreme emergency or can make worst the illness and stress for the person driving to the given address and find out the address was corrupted.

Availability - MODERATE - The information you need the request might be really necessary at the moment you need it but if the system is not giving you access, since is public information, you can look it up somewhere else. It would be more work since you would have to do extra research to obtain the information, but it can be still reachable.

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

Confidentiality - HIGH - First, is law enforcement, most information is confidential, second, is a sensitive investigation, therefore, confidentiality is one of the most important things because information about how the event happened, or who were the responsible people, cannot be disclose to public or we would see that many people tried doing the same (if the robbery or murder for example were successful), or we would see in the news that the community took justice in their own hands and killed the people responsible or did something against them. Also if there were witnesses and the information is not confidential, those witnesses will "disappear" (killed or kidnapped by the family or by the responsible of the event).

Integrity - HIGH - Again, is a sensitive investigation, therefore all the information needs to be accurate and not corrupted in order for the investigation to be successful and find justice if its the case. Things like names of witnesses, weapons used, details of the case, suspects, cannot be changed maliciously or the wrong people could end up paying for something they did not do, and the people responsible can end up in the streets.

Availability - HIGH - If an investigation is going on and some detectives are in the scene of crime or interrogating a suspect and they have no access back to their unit, it can be deadly for them because they won't be able to request backup if something is happening, or if they needs names, and order, a warrant, and they don't have access to this, they can lose the responsible or important and critical information for the case.

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

Confidentiality - LOW - There is no privacy in the information so if the information is released or accessed by someone else, it is not critical. More bridges of security can be created if needed but since is not confidential, the information obtained cannot cause a critical issue.

Integrity - MODERATE - The information can be modify and lets say is the address of employees and therefore everyone gets their taxes forms to another address. It would be annoying because you will have all the employees calling to ask about their forms and the organization will have to re send all the forms, but is not critical, just waste of time.

Availability - MODERATE - People might need access of someone's information to process a loan, a raise, a promotion, and if is not available, it will delay the process. However, is not critical. A report can be issued and eventually the access will be fixed so the information can be obtain.

(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: ; Admin: ; System:
Contract info - moderate, since it contains sensitive information, this can mean that bank accounts, addresses, are disclosed in this, people having access to it might result in hack of bank accounts or criminal acts to the people in the contract like kidnaps since they have their addresses or blackmailing.
Admin - low, because there cannot be much information that is confidential that would cause a critical harm on the acquisition of the organization.
System - moderate, again, people could have access to routing numbers of bank accounts or other important information that can be sensitive.

Integrity - Contract info: ; Admin: ; System:
Contract info - high, if the data is modify one company can have big losses in

their financial, like if the contract was modify to be in a higher price than the agreed amount. Or the company who was having the deal with another company, can be change to sign it with a total different company and this will be critical for one of the companies. Also if the bank account number if modify, the money will go to someone else.
Admin - high because if the information is modify, the deal or contract will not take place. Like if correspondence is sent to the wrong address/email and the company sending it gives a deadline, the deal will be off the table for the other company because they never received the document.
System - high because again information such as bank account number, addresses, can be modify and this will cause for the contract to not be valid or for the wrong people to receive the money of the contract.

Availability - Contract info: ; Admin: ; System:
Contract info- moderate because the information of the contract needs to be available for the people reviewing it so they can take decisions and make requests in the contract, however, is not critical since the only problem of not having access to it will be time to fix the access.
Admin - low because admin information not being accessible will only delay the process but is not critical.
System - moderate because not having access to the system will cause a big delay since I am sure this organization will have more than one company trying to make deals with them at the same time. This can cause some companies to stop wanting to work with them. In addition, the delay in a contract can cause a delay in some critical things such as season of construction.

(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: ; Admin: ; System:
Sensor Data - high because we are dealing with military information, people having access to this can do severe terrorist attacks. They will know the necessary information to create a stronger plan since they know exactly how everything works in the opposite force.

Admin - high because this can cause terrorist to have access to the families of the militaries and can send threats. They could also obtain sensitive information from the government and use it to their advantage.
System - high because they can have the information necessary to plan a bigger attack and a better plan on how to affect their stradegy.

Integrity - Sensor data: ; Admin: ; System:
Sensor Data - high because they can modify the information for the plant to have another electric power and this can cause an explosion or can cause damages to all the towers and till will block communication.
Admin - high because this can cause for the military to do the wrong moves and give the wrong power to the towers and they will have severe consequences, making them weak and giving the opposites an opportunity to attack.
System - high because again they can cause damage without them even having to go to the location since providing the wrong power to the towers will be critical.

Availability - Sensor data: ; Admin: ; System:
Sensor Data - high because the information about the strategies and the information about the power provided to the towers needs to be accessible all the time. Otherwise there can be windows where they won't have control or knowledge of how to do things and can be attack.
Admin - high because admin information can contain the right amount of power that needs to be provided or who to reach out to in case of a problem and if is not available there will be critical consequences (the ones I mentioned before).
System - high because is they cannot modify lets say the power of a tower that needed to be lower or higher at a certain time, this can cause explosions or some other critical leaks of information, that will result in a point of weakness and they can receive an attack.

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.
I think that the flaw in this program is that the if statement is only checking if dwRet grants the access or not but it does not kick the user out of the program to try again and input the right information. As I can think of, the program can still granting access even if the dwRet generates the message that the access will be denied.

(b) Rewrite the code to avoid the flaw

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
    // Security check failed.
    // Inform user that information provided does not grant access
    //Send user back to input the information
    //Allow the user to input information two more times
    //if after the two more times
    information is still incorrect, block user and ask them to
    call support
} else {
    // Security check OK.
}
```