Assignment 1

1. **Define the term computer security.** Using the CIA triad(confidentiality, integrity, and availability) of information assets including software, firmware, and information being stored, processed, and communicated.
2. **What is the difference between passive and active security threats?** An active threat would be an attempt to change the system directly or affect its operation. A passive threat is an attempt to hide and learn from the system to make use of its information, it does not directly affect the system.
3. **Explain the difference between an attack surface and an attack tree.**
   An attack surface is a threat that can reach the system and exploit its weaknesses. An attack tree is a data structure that represents paths to potential tactics to exploit a system's weakness. An attack tree consists of a root node security flaw and OR and AND nodes branching out. Both of these are ways to plan out the security flaws in your system but an attack surface goal is to make the surface smaller so the risk is lower while the attack tree has specific branching of its data structure with the root node being one security hole and the leaf nodes with ways on how to start the attack.
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.**

Confidentiality	Integrity	Availability
An individual's PIN number and card information is an asset whose confidentiality is of high importance to the individual. This information should only be available for the individual and the bank to whom they have an account with.	The integrity of the bank would be when you deposit or withdraw money into the atm, you will trust that the atm and the bank to update your bank balance.	Network availability is most important for an ATM. The ATM would need to communicate with the bank to process transactions or else the individual cannot make a transaction.

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.**

Confidentiality	Integrity	Availability
Caller's telephone number is of moderate importance	This is of moderate importance because a user	Leaked telephone numbers will be of moderate

because if information is leaked the caller will be contacted by outside sources. This info must remain private between caller and network.	or hacker could navigate between the network by knowing the telephone number of the recipient and contacting them even if they don't know them.	importance because having the wrong numbers being called by anonymous or spam callers will cause annoyance of the recipient if their number is easily available.

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

• Economy of mechanism: the design of security measures embodied in both hardware and software should be as simple and small as possible.
• Fail-safe defaults: access decisions should be based on permission rather than exclusion.
• Complete mediation: every access must be checked against the access control mechanism.
• Open design: the design of a security mechanism should be open rather than secret.
• Separation of privilege: a practice in which multiple privilege attributes are required to achieve access to a restricted resource.
• Least privilege: every process and every user of the system should operate using the least set of privileges necessary to perform the task.
• Least common mechanism: the design should minimize the functions shared by different users, providing mutual security.
• Psychological acceptability: implies the security mechanisms should not interfere unduly with the work of users, and at the same time meet the needs of those who authorize access.
• Isolation: a principle that applies in three contexts.
• Encapsulation: can be viewed as a specific form of isolation based on object-oriented functionality.
• Modularity: refers both to the development of security functions as separate, protected modules, and to the use of a modular architecture for mechanism design and implementation.
• Layering: refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.
• Least astonishment: a program or user interface should always respond in the way that is least likely to astonish the user.

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.

Confidentiality should be necessary. This sensitive information can contain employee info and even credit card and bank details. This would be the most important requirement.

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

Every company has rules and regulations, therefore the documents must also be in order. Data integrity would be an important requirement.

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

Many companies must have daily updates and news available. Such as emails and given assignments.

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.

Confidentiality: Low because the organization deals with public information that can already be accessed.

Integrity: Moderate because anyone can change the public information in the web server.

Availability: Moderate because the web server is not as important but could cause some damage to the organisation if it's not available.

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

Confidentiality: High because the loss of extremely sensitive information can have a severe or catastrophic effect.

Integrity: Moderate because there are different personnel that can access and change the investigative information.

Availability: Moderate because the loss of the information can cause significant damage to the organisation.

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

Confidentiality: Low because it is just daily information that is not privacy related so nothing important.

Integrity: Low because since it doesn’t have privacy related information the inaccurate info such as counting cash or maintenance.

Availability: Low because since it is daily routine information, it can be accessed multiple of ways and not from just one source.

(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.

Contract Information:

Confidentiality: High because sensitive data is important and vital to the company, keeping it private is high priority.

Integrity: Moderate because an employee could alter the sensitive information causing confusion within the company however because of routine information the damage is not so severe.

Availability: Loss of availability is low

Administrative Information:

Confidentiality: Low because web server does not contain private information

Integrity: Low because its routine daily information that is not used for anything important, everyone can access this information

Availability: Low because daily data can be accessed easily in past files

Information System:

Confidentiality: High because it contains sensitive data, if theres any leaks then it will be damaging

Integrity: Moderate because it provides accurate data, wrong data could lead to confusion

Availability: Moderate because pre phase information is important but not as important as the main private data

(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.

Sensor Data:

Confidentiality: Low because there isn't private or personal information that if lossed would cause significant damage.

Integrity: High because with no supervision there can be major damage to the organisation.

Availability: High because there is a need for there to be real-time sensor data that without it there could be severe effects.

Administrative Information:

Confidentiality: Low because there is no private information at risk.

Integrity: Low because the loss would have minor influence.

Availability: Low because there is no big need for availability of administrative information.

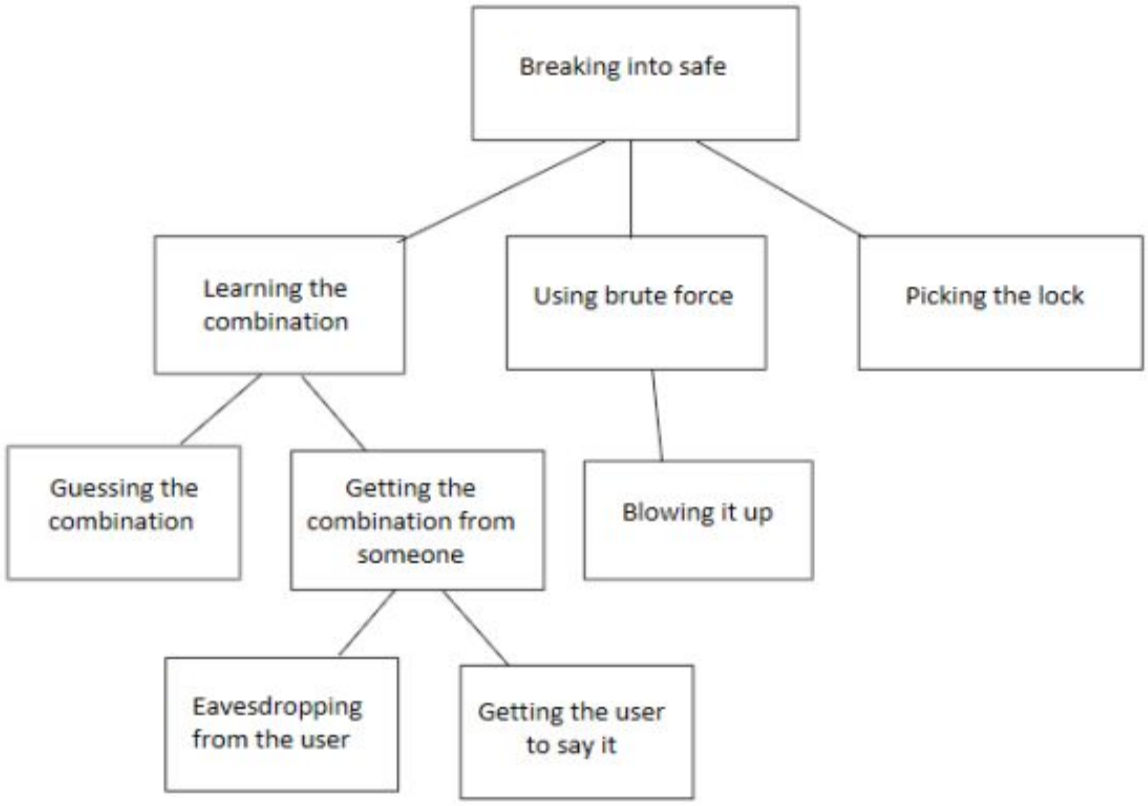
SCADA System:

Confidentiality: Low because there is no private information that if lossed would cause significant damage

Integrity: High because the system is needed f
or supervision.

Availability: High because the system is needed for the sensor data which needs to be in real-time.

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.**

The flaw in the program is that it checks if the security failed instead of checking if it passed. It also assumes that the error that IsAccessAllowed (...) produces is ERROR_ACCESS_DENIED.

(b) Rewrite the code to avoid the flaw

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

(Hint: Consider the design principle of fail-safe defaults).