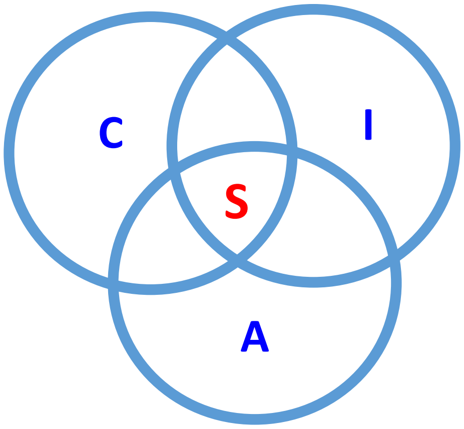
IS Assignment No. 1

Due date: 24/1/2022

1. **What is Information Security? What are the basics components of security and explain in detail?**

Information security is a set of practices designed to keep personal data secure from unauthorized access and alteration during storing or transmitting from one place to another.



Confidentiality

Confidentiality is the concealment of information or resources. Also, there is a need to keep information secret from other third parties that want to have access to it, so just the right people can access it.

Example in real life – Let's say there are two people communicating via an encrypted email they know the decryption keys of each other and they read the email by entering these keys into the email program. If someone else can read these decryption keys when they are entered into the program, then the confidentiality of that email is compromised.

Integrity

Integrity is the trustworthiness of data in the systems or resources by the point of view of preventing unauthorized and improper changes. Generally, Integrity is composed of two sub-elements – data-integrity, which it has to do with the content of the data and authentication which has to do with the origin of the data as such information has values only if it is correct.

Example in real life – Let's say you are doing an online payment of 5 USD, but your information is tampered without your knowledge in a way by sending to the seller 500 USD, this would cost you too much.

In this case cryptography plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity includes hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided in a secure way.

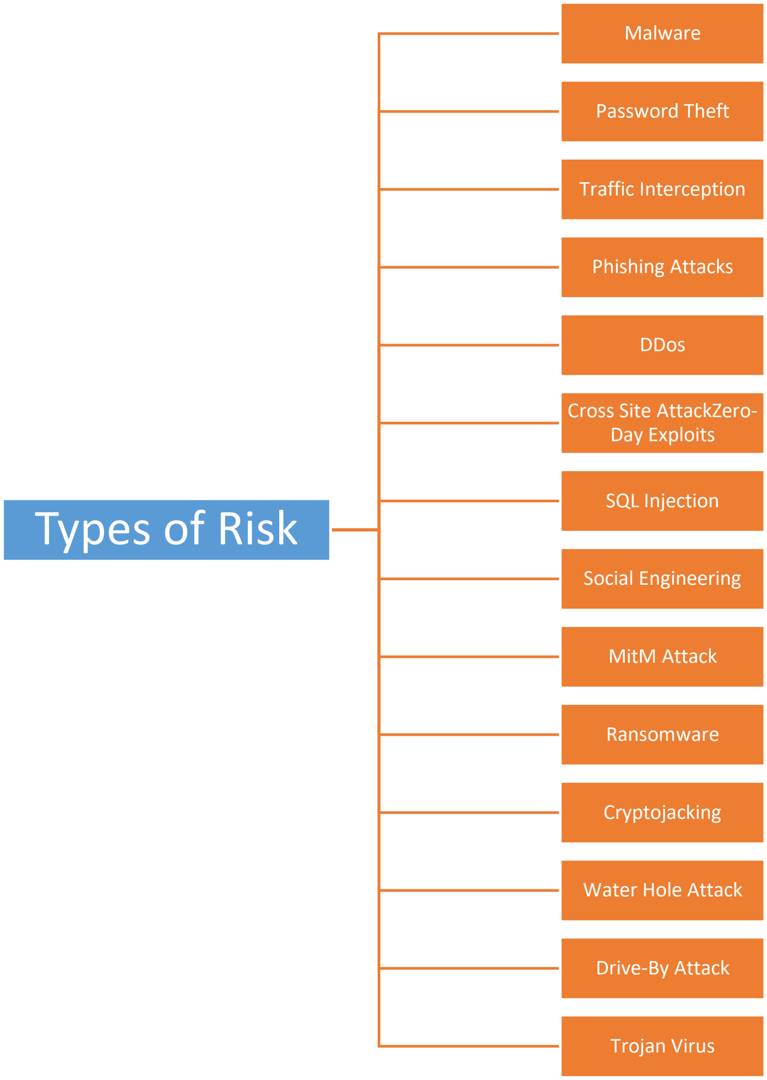
Availability

Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time. Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.

Example in real life – Let's say a hacker has compromised a webserver of a bank and put it down. You as an authenticated user want to do an e-banking transfer but it is impossible to access it, the undone transfer is a money lost for the bank.

2. What is risk and what are the types of risk?

Risk is defined as the potential for loss or damage when a threat exploits a vulnerability.



1 – Malware

We'll start with the most prolific and common form of security threat: malware. It's been around since the internet's inception and continues to remain a consistent problem. Malware is when an unwanted piece of programming or software installs itself on a target system, causing unusual behavior. This ranges from denying access to programs, deleting files, stealing information, and spreading itself to other systems.

2 – Password Theft

"I've been hacked!" A common conclusion when you log in to an account, only to find your password changed and details lost. The reality is an unwanted third party managed to steal or guess your password and has since run amok with the information. It's far worse for an enterprise, which may lose sensitive data.

3 – Traffic Interception

Also known as "eavesdropping," traffic interception occurs when a third-party "listens" to info sent between a user and host. The kind of information stolen varies based on traffic but is often used to take logins or valuable data.

4 – Phishing Attacks

Phishing scams are an older attack method and rely on social engineering to achieve its goal. Typically, an end user receives a message or email which requests sensitive data, such as a password. Sometimes, the phishing message appears official, using legitimate appearing addresses and media. This compels an individual to click on links and accidentally give away sensitive information.

5 – DDoS

Distributed Denial of Service is an attack method in which malicious parties target servers an overload them with user traffic. When a server cannot handle incoming requests, the website it hosts shuts down or slows to unusable performance.

6 – Cross Site Attack

Referred to as an XSS attack. In this instance, a third-party will target a vulnerable website, typically one lacking encryption. Once targeted the dangerous code loads onto the site. When a regular user access said website, that payload is delivered either to their system or browser, causing unwanted behaviour. The goal is to either disrupt standard services or steal user information.

7 – Zero-Day Exploits

Occurring after the discovery of a "zero-day vulnerability," an exploit is a targeted attack against a system, network, or software. This attack takes advantage of an overlooked security problem, looking to cause unusual behavior, damage data, and steal information.

8 – SQL Injection

An SQL attack is essentially data manipulation, implemented to access information which isn't meant to be available. Essentially, malicious third parties manipulate SQL "queries" (the typical string of code request sent to a service or server) to retrieve sensitive info.

9 – Social Engineering

Like phishing, social engineering is the umbrella method for attempting to deceive users into giving away sensitive details. This can occur on any platform, and malicious parties will often go to great lengths to accomplish their goals, such as utilizing social-media info.

10 – MitM Attack

A Man-in-the-Middle attack occurs when a third-party hijack a session between client and host. The hacker generally cloaks itself with a spoofed IP address, disconnects the client, and requests information from the client. For example, attempting to log-in to a bank session would allow a MITM attack to hijack user info related to their bank account.

11 – Ransomware

A nasty variant of malware, ransomware installs itself on a user system or network. Once installed, it prevents access to functionalities (in part or whole) until a "ransom" is paid to third parties.

12 – Cryptojacking

Cryptojacking is an attempt to install malware which forces the infected system to perform "crypto-mining," a popular form of gaining crypto-currency. This, like other viruses, can infect unprotected systems. It is deployed because the act of crypto mining is hardware intensive.

13 – Water Hole Attack

Generally used to target organizations, water hole attacks occur when a group infects websites a particular organization frequently uses. The goal – much like a cross-site attack – is to load a malicious payload from the infected sites.

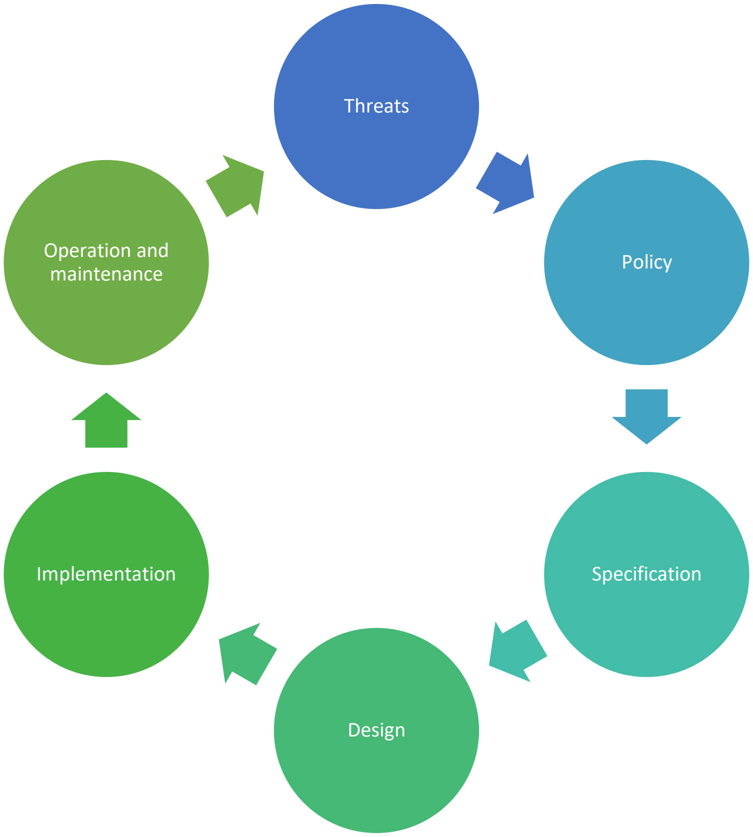
14 – Drive-By Attack

In a drive-by-attack, malicious code is delivered onto a system or device. The distinction, however, is that no action is needed on the user end, where typically they need to click a link or download an executable.

15 – Trojan Virus

Trojan malware attempts to deliver its payload by disguising itself as legitimate software. One technique used was an "alert" a user's system was compromised by malware, recommending a scan, whereby the scan delivered the malware.

3. **Explain the Phases of Security Life Cycle with diagram.**



The operation and maintenance stage are critical to the life cycle.

EXAMPLE:

- A major corporation decided to improve its security. It hired consultants, determined the **threats**, and created a policy.
- From the **policy**, the consultants derived several specifications that the security mechanisms had to meet.
- They then developed a design that would meet the **specifications**.
- During the **implementation** phase, the company discovered that employees could connect modems to the telephones without being detected.
- The **design** required all incoming connections to go through a firewall. The design had to be modified to divide systems into two classes: systems connected to "the outside," which were put outside the firewall; and all other systems, which were put behind the firewall. The design needed other modifications as well.
- When the system was deployed, the **operation and maintenance** phase revealed several unexpected threats.

4. What is authentication? Explain the Authentication methods in details.

Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. In doing this, authentication assures secure systems, secure processes, and enterprise information security.

1. Password-based authentication

Passwords are the most common methods of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.

However, passwords are prone to phishing attacks and bad hygiene that weakens effectiveness. An average person has about 25 different online accounts, but only 54% of users use different passwords across their accounts.

The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. Most people use simple passwords instead of creating reliable passwords because they are easier to remember.

The bottom line is that passwords have a lot of weaknesses and are not sufficient in protecting online information. Hackers can easily guess user credentials by running through all possible combinations until they find a match.

2. Multi-factor authentication

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user's smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.

MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security. MFA may be a good defense against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code.

3. Certificate-based authentication

Certificate-based authentication technologies identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver's license or a passport.

The certificate contains the digital identity of a user including a public key, and the digital signature of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.

Users provide their digital certificates when they sign in to a server. The server verifies the credibility of the digital signature and the certificate authority. The server then uses cryptography to confirm that the user has a correct private key associated with the certificate.

4. Biometric authentication

Biometrics authentication is a security process that relies on the unique biological characteristics of an individual. Here are key advantages of using biometric authentication technologies:

- Biological characteristics can be easily compared to authorized features saved in a database.
- Biometric authentication can control physical access when installed on gates and doors.
- You can add biometrics into your multi-factor authentication process.

Biometric authentication technologies are used by consumers, governments and private corporations including airports, military bases, and national borders. The technology is increasingly adopted due to the ability to achieve a high level of security without creating friction for the user. Common biometric authentication methods include:

- **Facial recognition**—matches the different face characteristics of an individual trying to gain access to an approved face stored in a database. Face recognition can be inconsistent when comparing faces at different angles or comparing people who look similar, like close relatives. Facial liveness like ID R&D's passive facial liveness prevents spoofing.
- **Fingerprint scanners**—match the unique patterns on an individual's fingerprints. Some new versions of fingerprint scanners can even assess the vascular patterns in people's fingers. Fingerprint scanners are currently the most popular biometric technology for everyday consumers, despite their frequent inaccuracies. This popularity can be attributed to iPhones.
- **Speaker Recognition** —also known as voice biometrics, examines a speaker's speech patterns for the formation of specific shapes and sound qualities. A voice-protected device usually relies on standardized words to identify users, just like a password.
- **Eye scanners**—include technologies like iris recognition and retina scanners. Iris scanners project a bright light towards the eye and search for unique patterns in the colored ring around the pupil of the eye. The patterns are then compared to approved information stored in a database. Eye-based authentication may suffer inaccuracies if a person wears glasses or contact lenses.

5. Token-based authentication

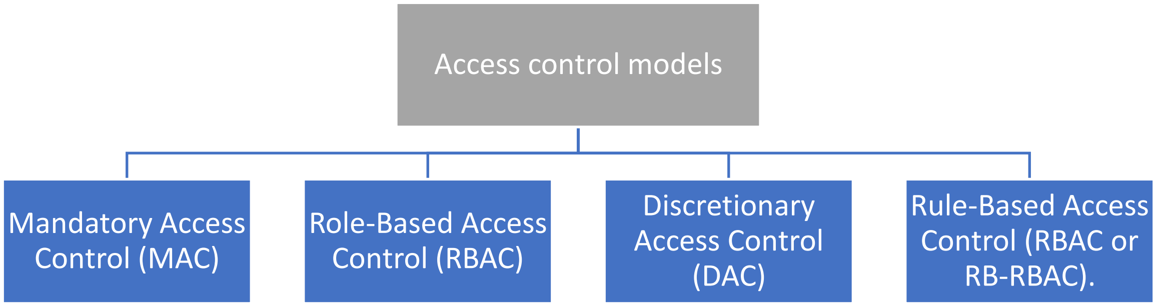
Token-based authentication technologies enable users to enter their credentials once and receive a unique encrypted string of random characters in exchange. You can then use the token to access protected systems instead of entering your credentials all over again. The digital token proves that you already have access permission. Use cases of token-based authentication include RESTful APIs that are used by multiple frameworks and clients.

5. What is Access Control Models? Explain DAC, MAC and RBAC.

Access control is identifying a person doing a specific job, authenticating them by looking at their identification, then giving that person only the key to the door or computer that they need access to and nothing more. In the world of information security, one would look at this as granting an individual permission to get onto a network via a username and password, allowing them access to files, computers, or other hardware or software the person requires and ensuring they have the right level of permission (i.e., read only) to do their job. So, how does one grant the right level of permission to an individual so that they can perform their duties? This is where access control models come into the picture.

Access control models have four flavors:

- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)
- Discretionary Access Control (DAC)
- Rule-Based Access Control (RBAC or RB-RBAC).


Access control models
Mandatory Access Control (MAC)
Role-Based Access Control (RBAC)
Discretionary Access Control (DAC)
Rule-Based Access Control (RBAC or RB-RBAC).

Discretionary Access Control

Instead of all data and access being controlled by the operating system, this paradigm allows users to control access to their data. So, the user can define what users and categories of users will get what type of an access to his or her data using an access control list (ACL). Each ACL includes a list of users and groups and a level of access they might have, for example, read-only, read and write, or full access. Often system administrators set up a range of access control privileges that users might grant via their ACL.

The key thing here is that users can only define access to resources they own, but not change the access type for files owned by someone else. An example of DAC in the real world is a social network where people can change the visibility of their content.

Mandatory Access Control

The mandatory access control (MAC) model was designed by the government and initially used for its purposes. It is a very strict access control model. In MAC, access to all data in the system is pre-defined by an administrator and controlled by the operating system.

MAC implements two concepts, the first one is the classification of the data (such as the degree of its importance or secrecy) and, second, the user category (department, project-related etc). As a result, it is possible to create rules describing which objects should be available to users included in a certain group.

Each user account also has these properties. When a user wants to access a certain file or folder, the OS checks what properties the object has and compares them to what is listed in the user profile. If this user belongs to a group that is allowed to access this type of data, the access will be granted. If not, declined.

Role-Based Access Control

The role-based access control (RBAC) is a tool used by companies to grant access based on a user’s job function. In this model, permissions are assigned to roles within the organization. Thus accountants will gain access to financial information, sales reps to CRM with customer data, software engineers to code repositories or documentation, etc.