Unit II

What is Security?

Security-“The quality or state of being secure--to be free from danger”

Types of Security

1. **Physical Security –** to protect physical items,objects or areas of organization from unauthorized access and misuse.
2. **Personal Security –** involves protection of individuals or group of individuals who are authorized to access the organization and its operations
3. **Operations security –** focuses on the protection of the details of particular operations or series of activities.
4. **Communications security –** encompasses the protection of the organization's communications media ,technology and content.
5. **Network security –** is the protection of networking components, connections, and contents

Information security

Information security is the protection of information and its critical elements, including the systems and hardware that use ,store, and transmit the information

Need for Security

The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents. The Audit Commission Update report (1998) shows that fraud or cases of IT abuse often occur due to the absence of basic controls, with one half of all detected frauds found by accident. An Information Security Management System

(ISMS) enables information to be shared, whilst ensuring the protection of information and computing assets.

At the most practical level, securing the information on your computer means:

- Ensuring that your information remains confidential and only those who *should* access that information, *can*.
- Knowing that no one has been able to change your information, so you can depend on its accuracy (information integrity).
- Making sure that your information is available when you need it (by making back-up copies and, if appropriate, storing the back-up copies off-site).

Business Needs

Information security performs four important functions for an organization:

a. Protects the organization’s ability to function

b. Enables the safe operation of applications implemented on the organization’s IT systems.

c. Protects the data the organization collects and uses.

d. Safeguards the technology assets in use at the organization.

Protecting the functionality of an organization

Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

Enabling the safe operation of applications

Organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications

The modern organization needs to create an environment that safeguards applications using the organization’s IT systems, particularly those applications that serve as important elements of the infrastructure of the organization.

Protecting data that organizations collect & use

- Protecting data in motion
- Protecting data at rest
- Both are critical aspects of information security.
- The value of data motivates attackers to seal, sabotage, or corrupt it.

It is essential for the protection of integrity and value of the organization’s data

Safeguarding Technology assets in organizations

Must add secure infrastructure services based on the size and scope of the enterprise.

Organizational growth could lead to the need for **public key infrastructure,** PKI, an integrated system of software, encryption methodologies.

What are the threats to information security?

➢A threat is an object, person, or other entity that represents a constant danger to an asset

➢ Management must be informed of the various kinds of threats facing the organization

➢ By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

Cybersecurity Threat

A cybersecurity threat is a malicious and deliberate attack by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.

Types of Cybersecurity Threats

While the types of cyber threats continue to grow, there are some of the most common and prevalent cyberthreats that present-day organizations need to know about. The top 10 cyber security threats are as follows:

1) Malware

Malware attacks are the most common cyber security threats. Malware is defined as malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email. Once inside the system, malware can block access to critical components of the network, damage the system, and gather confidential information, among others.

2) Phishing

Cybercriminals send malicious emails that seem to come from legitimate resources. The user is then tricked into clicking the malicious link in the email, leading to malware installation or disclosure of sensitive information like credit card details and login credentials.

3) SQL Injection

A Structured Query Language (SQL) injection attack occurs when cybercriminals attempt to access the database by uploading malicious SQL scripts. Once successful, the malicious actor can view, change, or delete data stored in the SQL database.

4) Ransomware

Ransomware is a type of malware that restricts or limits users of a targeted organization from accessing their IT systems until the ransom is paid. However, there is no guarantee of regaining system access even after the ransom is paid.

5) DNS Attack

A DNS attack is a cyberattack in which cybercriminals exploit vulnerabilities in the Domain Name System (DNS). The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and remove data from compromised systems (DNS Tunneling).

Cybersecurity Best Practices to Protect from Cyber Threats

1) Create an Insider Threat Program

Creating an insider threat program is imperative for organizations to prevent employees from misusing their access privileges to steal or destroy corporate data. The IT security team should not delay and gain the approval of top management to deploy policies across departments.

2) Train employees

Employees are the first line of defense against cyber threats for every organization. Thus, organizations must conduct comprehensive cybersecurity awareness programs to train employees in recognizing and responding to cyber threats. This dramatically improves an organization's security posture and cyber resilience.

3) Maintain Compliance

Irrespective of the level of cybersecurity an organization implements, it must always maintain compliance with data regulations that apply to its industry and geographical location. The organization must stay informed about the evolving compliance regulations to leverage its benefits.

4) Build a Cyber Incident Response Plan

In the present digital era, no organization is exempt from cyberattacks. Thus, organizations of all sizes must build an effective Cyber Security Incident Response Plan (CSIRP) to navigate cyber adversaries. It enables businesses to prepare for the inevitable, respond to emerging threats, and recover quickly from an attack.

5) Regularly Update Systems and Software

As cyber threats are evolving rapidly, your optimized security network can become outdated within no time, putting your organization at the risk of cyberattack. Therefore, regularly update the security network and the associated systems and software.

6) Backup Data

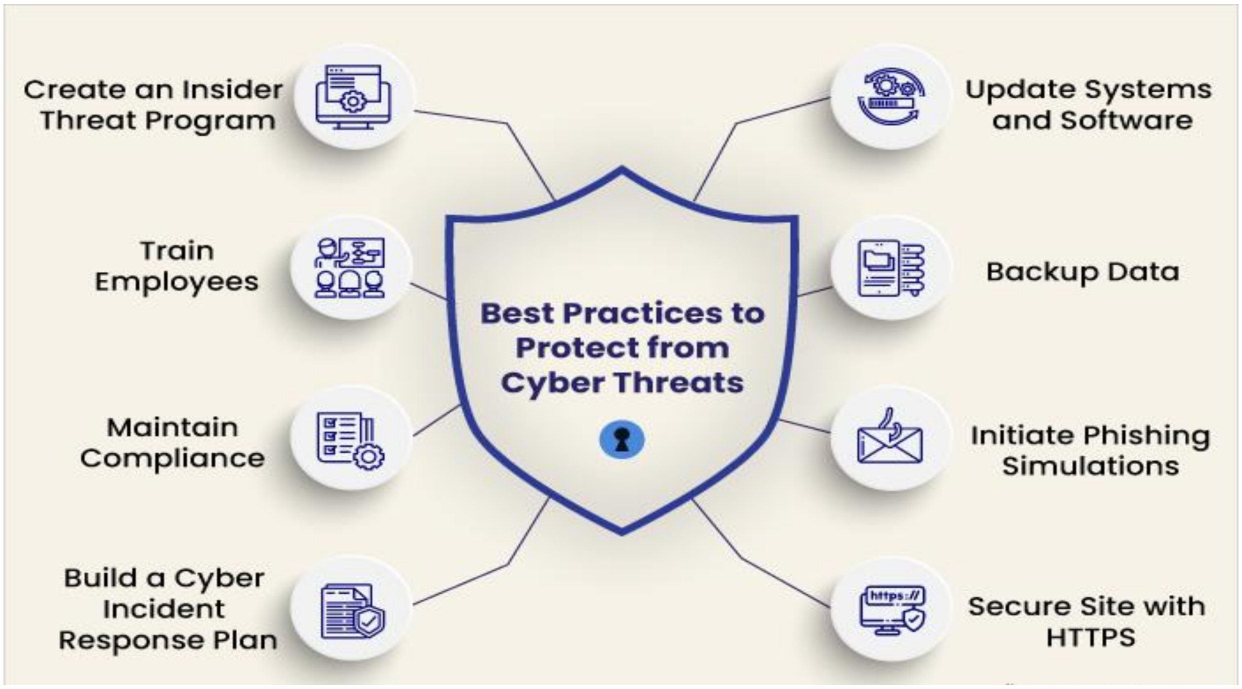
Backing up data regularly helps reduce the risk of data breaches. Back up your website, applications, databases, emails, attachments, files, calendars, and more on an ongoing and consistent basis.

7) Initiate Phishing Simulations

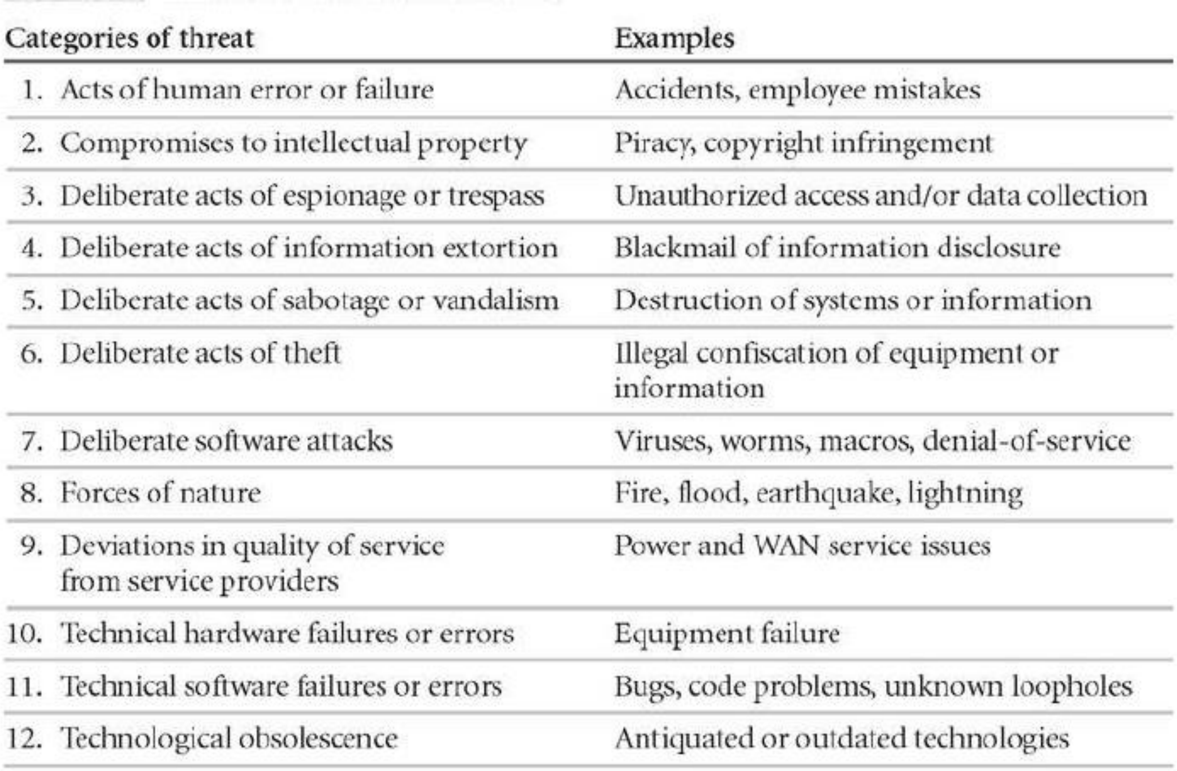
Organizations must conduct phishing simulations to educate employees on how to avoid clicking malicious links or downloading attachments. It helps employees understand the far-reaching effects of a phishing attack on an organization.

8) Secure Site with HTTPS

Organizations must encrypt and secure their website with an SSL (Secure Sockets Layer) certificate. HTTPS protects the integrity and confidentiality of data between the user and the website.


Best Practices to Protect from Cyber Threats
Create an Insider Threat Program
Update Systems and Software
Train Employees
Backup Data
Maintain Compliance
Initiate Phishing Simulations
Build a Cyber Incident Response Plan
Secure Site with HTTPS
https://

What are the different categories of threat? Give Examples.



Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Attack

An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

Types of Security Attacks

Security attacks can be of the following two types:

- Active attacks
- Passive attacks

1. Active Attacks

Active attacks are a type of cybersecurity attack in which an attacker attempts to alter, destroy, or disrupt the normal operation of a system or network. Active attacks involve the attacker taking direct action against the target system or network, and can be more dangerous than passive attacks, which involve simply monitoring or overhearing on a system or network.

Types of active attacks are as follows:

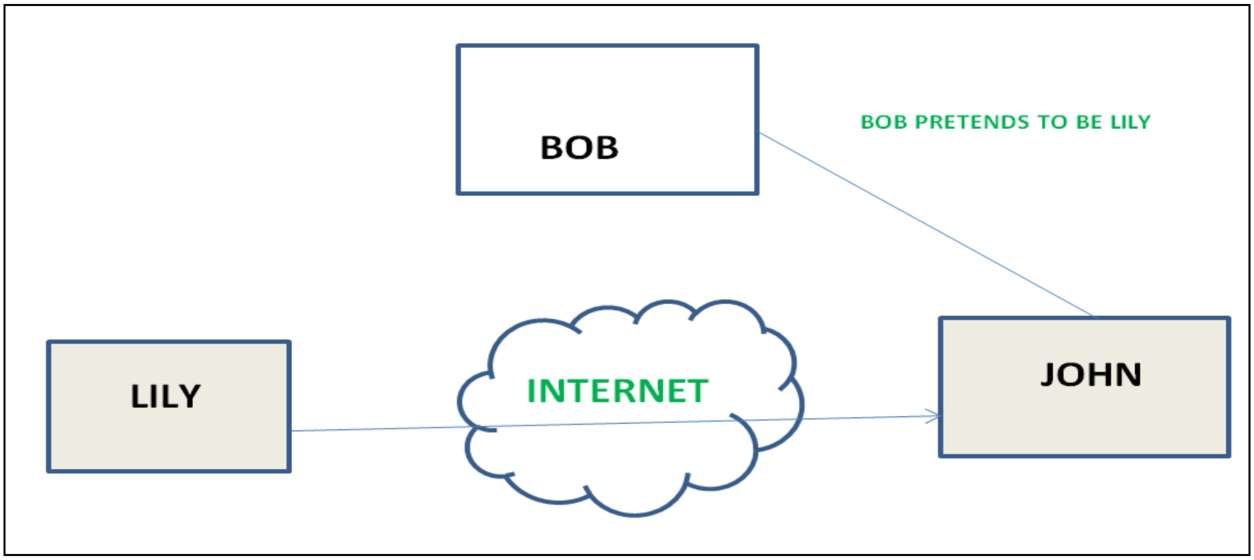
- Masquerade
- Modification of messages
- Repudiation
- Replay
- Denial of Service

Masquerade

Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data. This can involve impersonating a legitimate user or system to trick other users or systems into providing sensitive information or granting access to restricted areas.

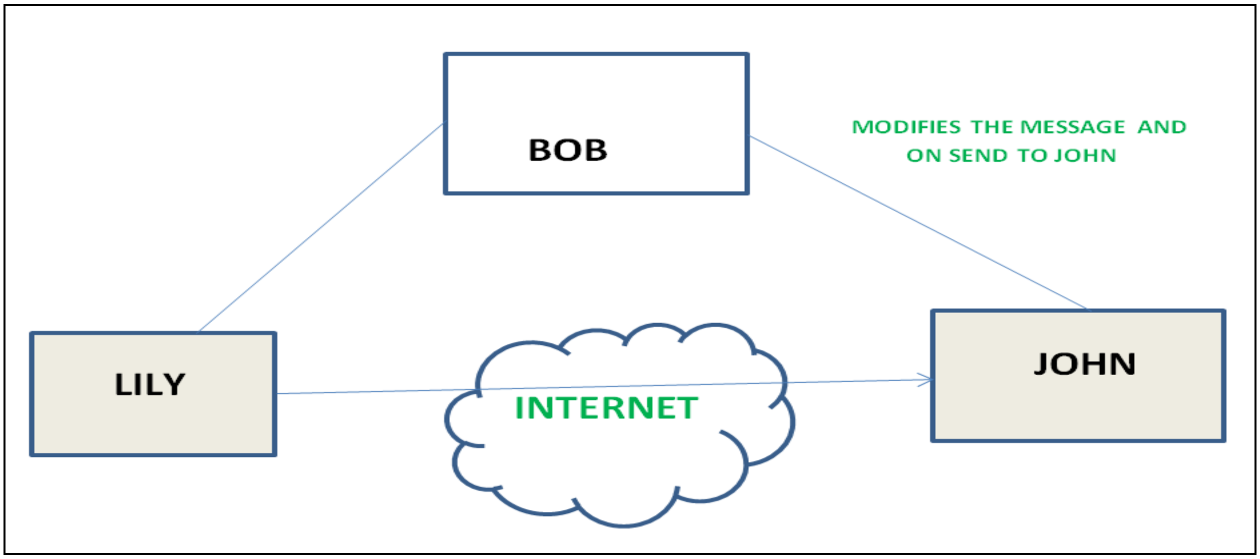
There are several types of masquerade attacks, including:

- **Username and password masquerade:** In a username and password masquerade attack, an attacker uses stolen or forged credentials to log into a system or application as a legitimate user.
- **IP address masquerade:** In an IP address masquerade attack, an attacker spoofs or forges their IP address to make it appear as though they are accessing a system or application from a trusted source.
- **Website masquerade:** In a website masquerade attack, an attacker creates a fake website that appears to be legitimate in order to trick users into providing sensitive information or downloading malware.
- **Email masquerade:** In an email masquerade attack, an attacker sends an email that appears to be from a trusted source, such as a bank or government agency, in order to trick the recipient into providing sensitive information or downloading malware.



Modification of Messages

It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".



Repudiation

Repudiation attacks are a type of cybersecurity attack in which an attacker attempts to deny or repudiate actions that they have taken, such as making a transaction or sending a message. These attacks can be a serious problem because they can make it difficult to track down the source of the attack or determine who is responsible for a particular action.

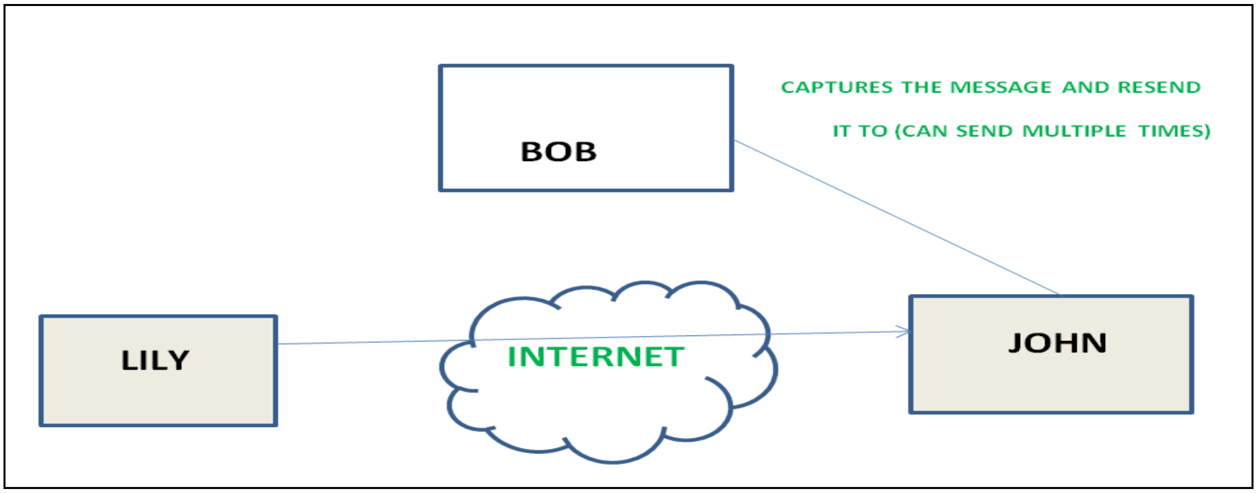
There are several types of repudiation attacks, including:

- **Message repudiation attacks**: In a message repudiation attack, an attacker sends a message and then later denies having sent it. This can be done by using spoofed or falsified headers or by exploiting vulnerabilities in the messaging system.

- **Transaction repudiation attacks:** In a transaction repudiation attack, an attacker makes a transaction, such as a financial transaction, and then later denies having made it. This can be done by exploiting vulnerabilities in the transaction processing system or by using stolen or falsified credentials.
- **Data repudiation attacks:** In a data repudiation attack, an attacker modifies or deletes data and then later denies having done so. This can be done by exploiting vulnerabilities in the data storage system or by using stolen or falsified credentials.

Replay

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.


BOB
CAPTURES THE MESSAGE AND RESEND
IT TO (CAN SEND MULTIPLE TIMES)
LILY
INTERNET
JOHN

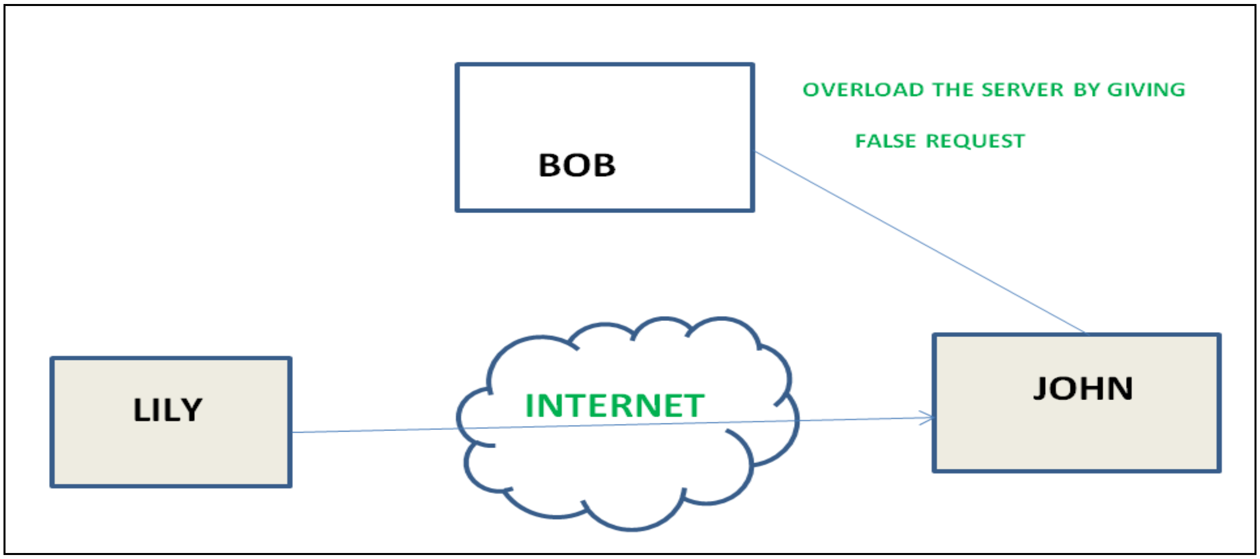
Denial of Service

Denial of Service (DoS) is a type of cybersecurity attack that is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests. In a DoS attack, an attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it.

There are several types of DoS attacks, including:

Flood attacks: In a flood attack, an attacker sends a large number of packets or requests to a target system or network in order to overwhelm its resources.

Amplification attacks: In an amplification attack, an attacker uses a third-party system or network to amplify their attack traffic and direct it towards the target system or network, making the attack more effective.



2. Passive Attacks

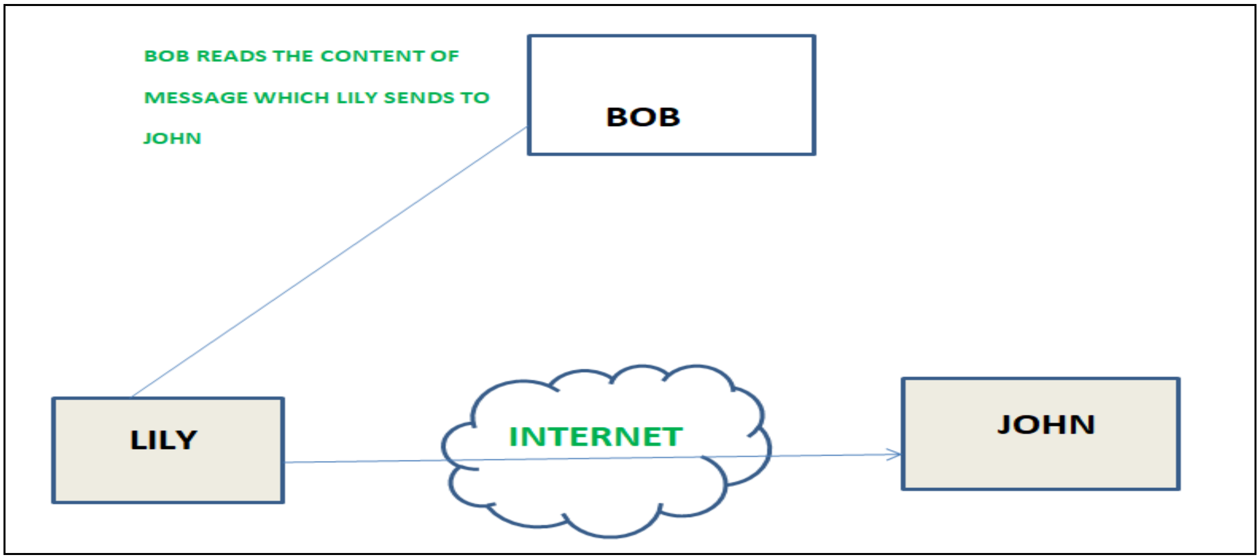
A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the competitor is to obtain information that is being transmitted. Passive attacks involve an attacker passively monitoring or collecting data without altering or destroying it. Examples of passive attacks include eavesdropping, where an attacker listens in on network traffic to collect sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information.

Types of Passive attacks are as follows:

- The release of message content
- Traffic analysis

- **The release of message content**

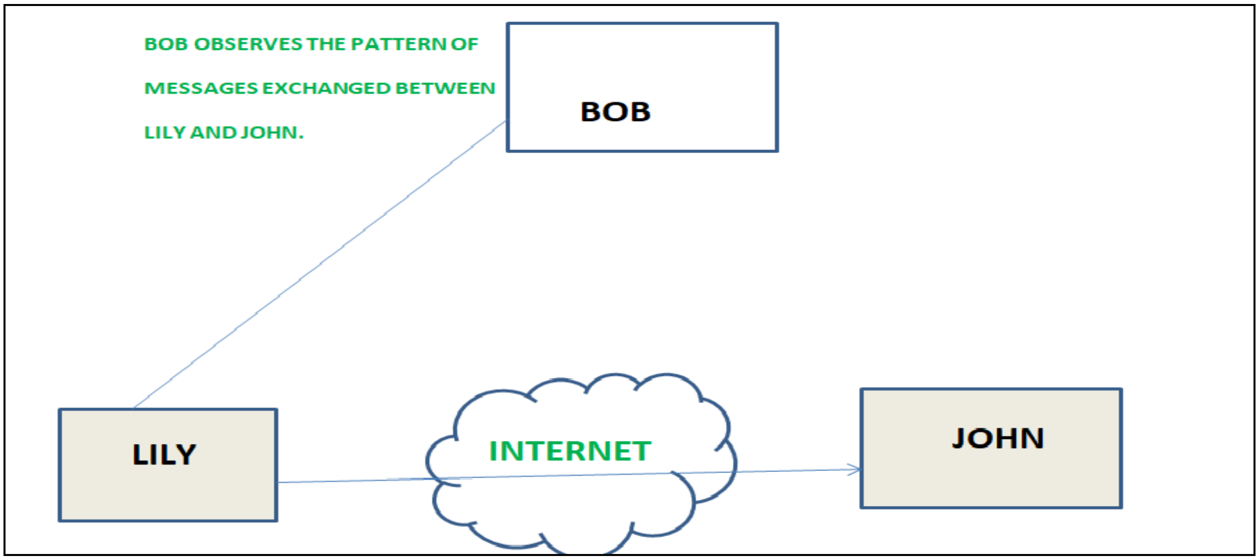
  Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent competitor from learning the contents of these transmissions.



- **Traffic analysis**

Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message.

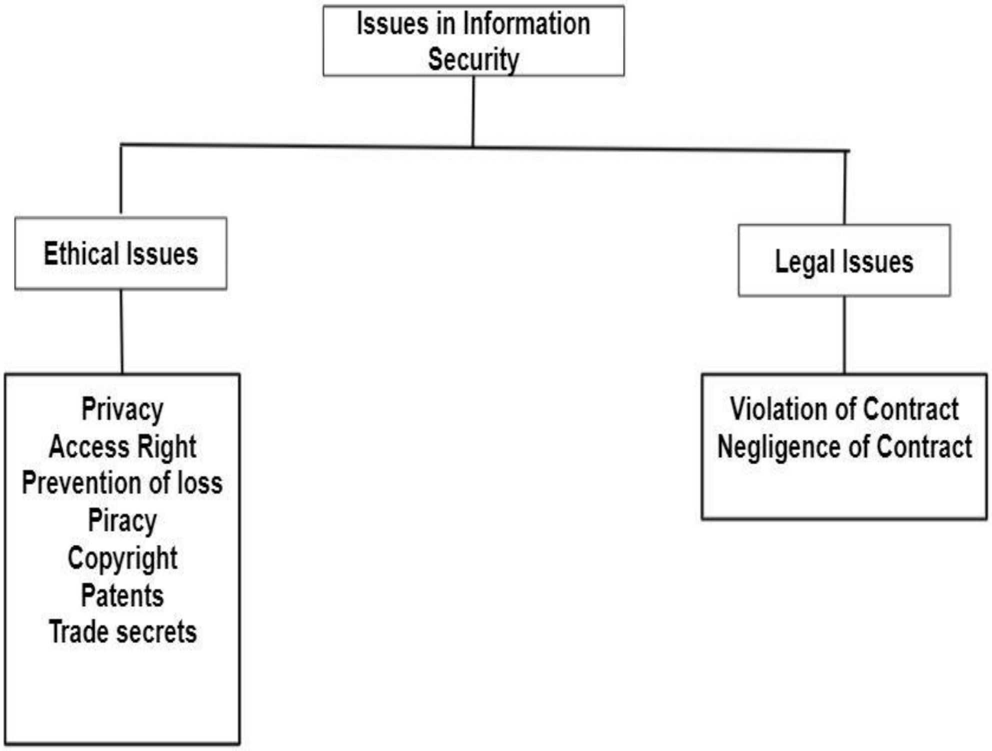
The opponent (competitor) could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place. The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.


BOB OBSERVES THE PATTERN OF MESSAGES EXCHANGED BETWEEN LILY AND JOHN.
BOB
LILY
INTERNET
JOHN

What are the ethical and legal issues in information security?

In computer science, ethics are regarded as how professionals make decisions. There are rules and practices that determine what is right or wrong. Ethical issues occur when a decision or activity creates a dispute with society's moral policies. They could be generated due to an individual or an entire organization.

Legal factors are the laws that the Government has passed. The Government has issued several acts/ laws specifically for the computer industry. All professionals in this industry need to obey these rules. Legal issues occur when a company or an individual violates the laws given by the Government.



Ethical issues in information security

Ethics plays a vital role in technology for several reasons. Firstly, ethical behavior fosters trust and confidence among users, crucial for successful technological advancements and user adoption.

Secondly, ethical considerations protect individuals' privacy and ensure responsible handling of personal data. Fairness and equity are also essential, as technology should benefit everyone regardless of their background.

Some of the common ethical issues in the cyber world are as follows:

- **Privacy**

Nowadays, computer users can access different information from various servers located all over the world. Though the users have their private computer, tools, and operating system, their network is distributed at a large scale when they try to access information. As a result, their information is likely to be disclosed to various organizations, and their privacy is not maintained.

Furthermore, hackers often intrude into the computer system of people and access the user's information without authorization. Some organizations also sell the information and data of their users. This also raises the question of user information privacy.

That is why companies need to develop ethical policies that can keep the information of their users safe from hackers.

Example: A social media platform that collects and sells users' data without explicit consent violates ethical privacy and data protection standards. Users' information should be safeguarded and used responsibly (GDPR standards), with transparent privacy policies and options for users to control their data.

- **Access right**

Lots of industries use computer software and technology to provide services to their customers. This software should be capable of preventing unauthorized access to the system.

Especially in payment or banking software, the developers need to create software that guarantees authorized access and stops malware, viruses, or unauthorized access to the system.

Example: A government or a nonprofit organization is implementing a program to provide free internet access and computer literacy programs to underprivileged communities, which ensures equal opportunities for education, employment, and access to essential services. This initiative promotes ethical principles of inclusivity and fair access to technology.

- **Prevention of loss**

According to this ethical principle, information technology should not be used in a manner that would cause harm or loss of property, information, ownership, or destruction of the property. The employees, users, and other public should use all the equipment with care to prevent any severe loss.

- **Patents**

Ethical issues that are regarded to patents are tough to deal with. Patents preserve the unique and secret part of an idea. To acquire a patent, companies need to provide proper disclosure of the software. The patent holder also has to reveal the entire program details to a proficient programmer. If any issues in the patent are found, the company will be answerable to the public or Government.

- **Copyright**

Copyright issues need to be taken extremely seriously by information security professionals. Copyright laws are created to protect computer software before and after a security breach such as the mishandling of data, misusing information, documentation, computer programs, or any other material. Most countries have different laws to handle copyright issues occurring in the cyber world.

- **Trade secrets**

Another common ethical issue in the computer world is trade secrets. Trade secrets keep the value and importance of the ideas, business, or software secure. According to this ethic, the confidential data of an organization should not be leaked to outsiders. If this law is broken, it may cause much harm to the company. Therefore, the company's staff and all individuals need to obey this law.

- **Piracy**

Piracy means the creation and usage of illegal copies of the software. This issue commonly occurs in today's world. Software owners have the right to choose how to distribute the software and whether users can create copies of the software. If a developer does not allow duplication of the software, it is considered piracy whenever the software is duplicated. The individual who duplicates the software is also held guilty for that.

The software industry is facing a high number of piracy issues nowadays. Courts are also working to prepare strict laws to prevent piracy.

Legal issues in information security

Similar to ethical issues, information technology organizations are also bound to follow laws issued by the Government. If a company fails to provide satisfactory service to the client or cheats the client, the organization is held guilty in court. The most common legal issues that occur in the information security industry are as mentioned below.

- **Violation of contract**

When a client or organization decides to work with each other, the details are finalized by creating a contract. The contract contains the work duration, the purpose of the work, and other details related to the project. Before getting the client on board, it is necessary to discuss the contract and get all the details approved by the client.

Later, if the client or the organization violates the contract, they may face legal issues. Either party can file an issue in court and get the conflict solved according to the computer acts defined by the Government.

- **Negligence of contract**

If a company fails to fulfill the client's requirements (as mentioned in the contract), it is considered negligence of the contract. In such cases, the company will also be considered guilty and will have to prove itself in court.

Information technology needs to ensure they deliver the correct services to the client within the mentioned time duration to avoid such legal issues.

Professional issues:- Professional issues that occur in the information security industry are as mentioned below:

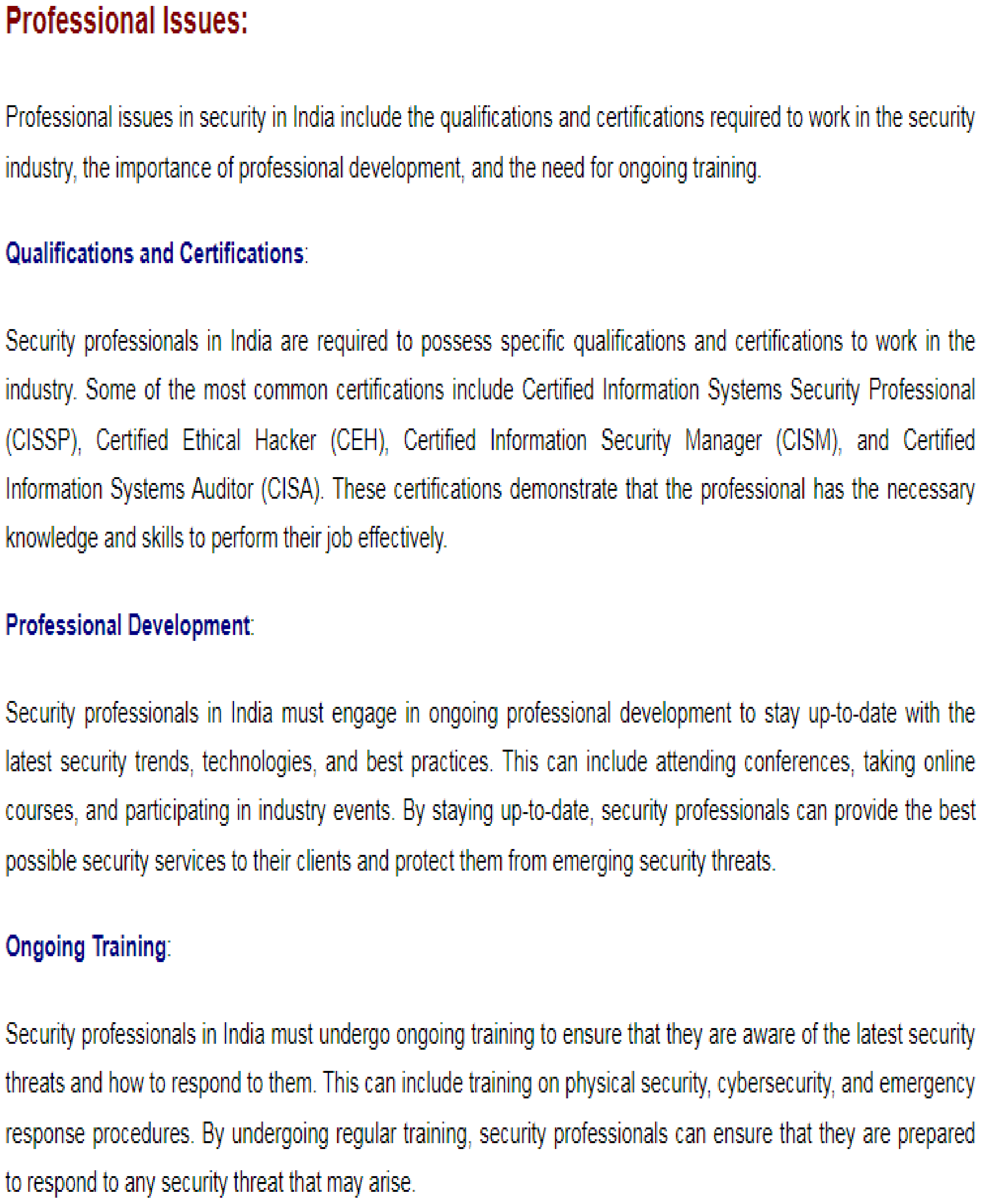
Vulnerability Disclosure - Vulnerability disclosure is the "act of initially providing vulnerability information to a party that was not believed to be previously aware."

Spam - Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

Scams - A scam is a way of tricking people into handing over money or personal details.

Hacking - Hacking is the act of gaining unauthorized access to data in a system or computer.

Conflict of Interest - A conflict of interest (COI) is a situation in which a person or organization is involved in multiple interests, financial or otherwise, and serving one interest could involve working against another.



Professional Issues:

Professional issues in security in India include the qualifications and certifications required to work in the security industry, the importance of professional development, and the need for ongoing training.

Qualifications and Certifications:

Security professionals in India are required to possess specific qualifications and certifications to work in the industry. Some of the most common certifications include Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), and Certified Information Systems Auditor (CISA). These certifications demonstrate that the professional has the necessary knowledge and skills to perform their job effectively.

Professional Development:

Security professionals in India must engage in ongoing professional development to stay up-to-date with the latest security trends, technologies, and best practices. This can include attending conferences, taking online courses, and participating in industry events. By staying up-to-date, security professionals can provide the best possible security services to their clients and protect them from emerging security threats.

Ongoing Training:

Security professionals in India must undergo ongoing training to ensure that they are aware of the latest security threats and how to respond to them. This can include training on physical security, cybersecurity, and emergency response procedures. By undergoing regular training, security professionals can ensure that they are prepared to respond to any security threat that may arise.

Computer security

Computer security refers to protecting and securing computers and their related data, networks, software, hardware from unauthorized access, misuse, theft, information loss, and other security issues. The Internet has made our lives easier and has provided us with lots of advantages but it has also put our system's security at risk of being infected by a virus, of being hacked, information theft, damage to the system, and much more.

Technology is growing day by day and the entire world is in its grasp. We cannot imagine even a day without electronic devices around us. With the use of this growing technology, invaders, hackers and thieves are trying to harm our computer's security for monetary gains, recognition purposes, ransom demands, bullying others, invading into other businesses, organizations, etc. In order to protect our system from all these risks, computer security is important.

Types of Computer Security

Computer security can be classified into four types:

1. Cyber Security: Cyber security means securing our computers, electronic devices, networks , programs, systems from cyber attacks. Cyber attacks are those attacks that happen when our system is connected to the Internet.

2. Information Security: Information security means protecting our system's information from theft, illegal use and piracy from unauthorized use. Information security has mainly three objectives: confidentiality, integrity, and availability of information.

3. Application Security: Application security means securing our applications and data so that they don't get hacked and also the databases of the applications remain safe and private to the owner itself so that user's data remains confidential.

4. Network Security: Network security means securing a network and protecting the user's information about who is connected through that network. Over the network hackers steal, the packets of data through sniffing and spoofing attacks, man in the middle attack, war driving, etc, and misuse the data for their benefits.

Steps to Ensure Computer Security

In order to protect our system from attacks, users should take certain steps to ensure system security:

1. Always keep your Operating System up to date. Keeping it up to date reduces the risk of their getting attacked by malware, viruses, etc.

2. Always use a secure network connection. One should always connect to a secure network. Public wi-fi's and unsecured networks should be avoided as they are at risk of being attacked by the attacker.

3. Always install an Antivirus and keep it up to date. An antivirus is software that scans your PC against viruses and isolates the infected file from other system files so that they don't get affected. Also, we should try to go for paid anti-viruses as they are more secure.

4. Enable firewall. A firewall is a system designed to prevent unauthorized access to/from a computer or even to a private network of computers. A firewall can be either in hardware, software or a combination of both.

5. Use strong passwords. Always make strong passwords and different passwords for all social media accounts so that they cannot be key logged or detected easily using dictionary attacks. A strong password is one that has 16 characters which are a combination of upper case and lower case alphabets, numbers and special characters. Also, keep changing your passwords regularly.

6. Don’t trust someone easily. You never know someone’s intention, so don’t trust someone easily and end up giving your personal information to them. You don’t know how they are going to use your information.

7. Keep your personal information hidden. Don’t post all your personal information on social media. You never know who is spying on you. As in the real world, we try to avoid talking to strangers and sharing anything with them. Similarly, social media also have people whom you don’t know and if you share all your information on it you may end up troubling yourself.

8. Don’t download attachments that come along with e-mails unless and until you know that e-mail is from a genuine source. Mostly, these attachments contain malware which, upon execution infect or harms your system.

9. Don’t purchase things online from anywhere. Make sure whenever you are shopping online you are doing so from a well-known website. There are multiple fraud websites that may steal your card information as soon as you checkout and you may get bankrupt by them.

10. Learn about computer security and ethics. You should be well aware of the safe computing and ethics of the computing world. Gaining appropriate knowledge is always helpful in reducing cyber-crime.

11. If you are attacked, immediately inform the cyber cell so that they may take appropriate action and also protect others from getting attacked by the same person. Don’t hesitate to complain just because you think people may make your fun.

12. Don’t use pirated content. Often, people try to download pirated movies, videos or web series in order to get them for free. These pirated content are at major risk of being infected with viruses, worms, or malware, and when you download them you end up compromising your system security.

Access Control Matrix

An access control matrix is a table that contains both subjects and objects. Subjects usually refer to people who may need to access objects. Objects are typically files, data, or resources that subjects may need to access. They can also be a system process or a piece of hardware. The information contained in the matrix designates permissions and access levels between subjects and objects. Organizations build access control matrices to ensure authorized access and prevent intentional or unintentional unauthorized access to sensitive data.

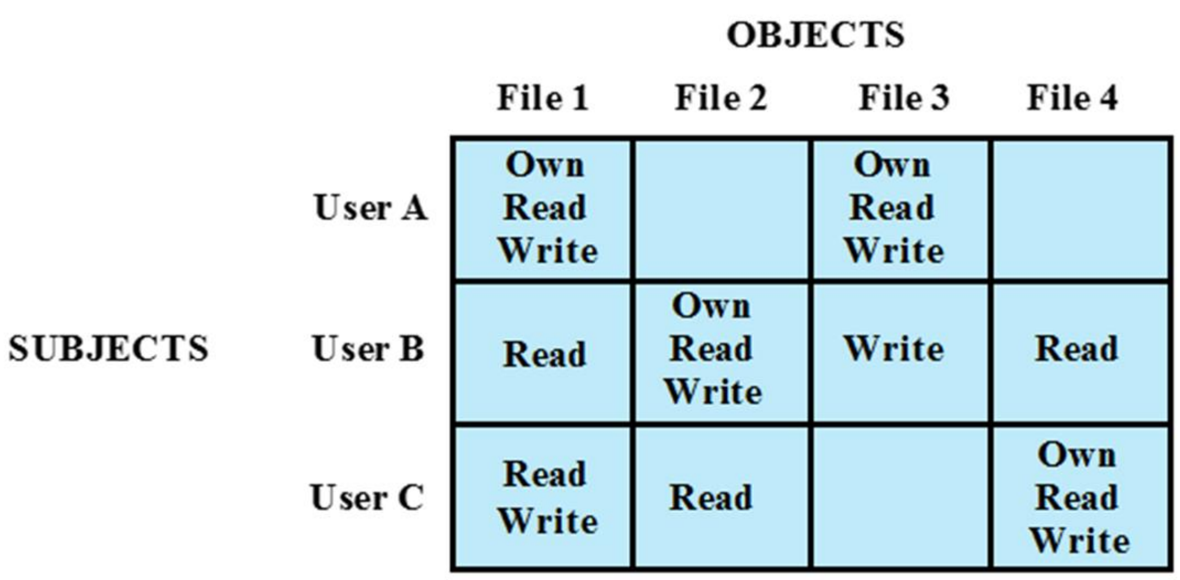
The purpose for granting any access corresponds to the three pillars of cyber security: availability, integrity, and confidentiality. Availability measures are those that ensure that users can access a system. Issues such as hardware and software failures, network disconnections, and hacking can influence availability. Integrity refers to measures that ensure that information on a system is not altered intentionally or unintentionally. Confidentiality refers to the measures that are put in place to ensure that information is not misused and that those who are unauthorized do not access information. System administrators usually assign right in an access control matrix, avoiding the possibility that others may tamper with it. The access rights that are assigned to individual subjects are called capabilities and those assigned to objects are called Access Control Lists (ACL).

How an Access Control Matrix Works

In a user permissions matrix, permissions are designated using these five commonly used attributes.

- Read (R) – Read access permits the subject to open and read the file, but not to edit it in any way.

- Write (W) – Write access allows the subject to not only read the file but to add or write new content in the file.
- Delete (D) – Subjects with delete or edit permissions can delete files or content.
- Execute (E) – Execute permission allows a user to execute particular programs.
- Dash (-) – A dash in an access control matrix indicates that the subject is prohibited from accessing the object.



		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

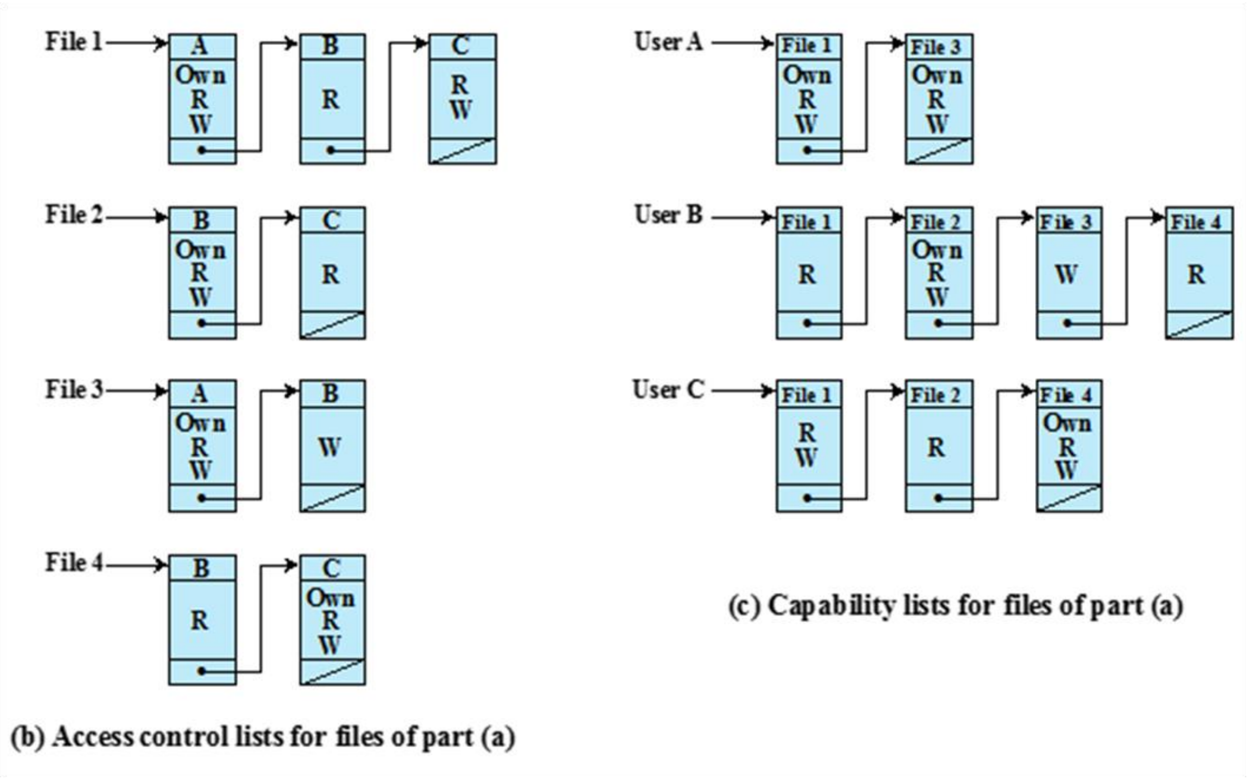
(a) Access matrix

Access Control List (ACL)

ACL is a table that notifies the computer system of a user’s access rights to a given system file or file directory. Every object is assigned a security attribute to establish its access control list. The ACL has a specific entry for every system user with the related access privileges. These privileges touch on the ability to write and read a file or files, and if it is a program of an executable file, it defines the user access to those rights.

User Capability List

A capability list is a key, token, or ticket that grants the processor approval to access an object within the computer system. The user is evaluated against a capability list before gaining access to a specific object.



(b) Access control lists for files of part (a)

(c) Capability lists for files of part (a)

Security Policy

An security policy is a set of rules, guidelines, and procedures that outline how an organization should manage, protect, and distribute its information assets. The policy aims to reduce the risk of data breaches, unauthorized access, and other security threats by providing a structured approach to information security management.

A security policy is a document that states in writing how a company plans to protect its physical and information technology (IT) assets. Security policies are living documents that are continuously updated and changing as technologies, vulnerabilities and security requirements change.

Why Does Your Organization Need an Information Security Policy?

Security policies play a critical role in an organization's overall security posture. They serve as a foundation for establishing a secure environment and reduce potential risks. The value of security policies can be outlined as follows:

- Risk management: Security policies provide a systematic approach to identifying, assessing, and managing risks associated with information assets. By addressing vulnerabilities and implementing appropriate controls, organizations can minimize the potential damage caused by security incidents.
- Security culture and awareness: Security policies promote a culture of security awareness within an organization. By providing training and resources, organizations can educate employees on security best practices and encourage them to play an active role in protecting information assets.
- Trust and reputation: By implementing and maintaining a robust (durable) security policy, organizations can demonstrate their commitment to protecting customer, employee, and partner data. This fosters trust and confidence, which is crucial for maintaining a positive reputation and building strong business relationships.

- Competitive advantage: As data breaches and cyberattacks become more common, organizations with effective security policies can differentiate themselves from competitors. Demonstrating strong security practices can provide a competitive advantage, particularly when dealing with clients or partners who prioritize data protection.
- Cost savings: By proactively addressing security risks, organizations can reduce the financial impact of security incidents, including costs associated with data breaches, system downtime, and regulatory fines.
- Continuous improvement: Security policies include processes for regular monitoring, auditing, and reviewing security practices. This allows organizations to identify areas for improvement, adapt to evolving threats, and ensure that their security measures remain effective over time.

Integrity Policy

Integrity is the protection of system data from intentional or accidental unauthorized changes. The challenges of the security program are to ensure that data is maintained in the state that is expected by the users. Although the security program cannot improve the accuracy of the data that is put into the system by users. It can help ensure that any changes are intended and correctly applied. A critical requirement is to ensure the integrity of data to prevent fraud and errors. It is compulsory, therefore, no user is able to modify data in a way that might corrupt or lose assets or financial records or render decision making information unreliable. Examples of government systems in which integrity is crucial include air traffic control system, military fire control systems, social security and welfare systems. Examples of commercial systems that require a high level of integrity include medical prescription system, credit reporting systems, production control systems and payroll systems.

Protecting against Threats to Integrity: Like confidentiality, integrity can also be arbitrated by hackers, masqueraders, unprotected downloaded files, unauthorized user activities, and unauthorized programs like Trojan Horse and viruses, because each of these threads can lead to unauthorized changes to data or programs. For example, unauthorized users can corrupt or change data and programs intentionally or accidentally if their activities on the system are not properly controlled. Generally, three basic principles are used to establish integrity controls:

1. **Need-to-know access:** Users should be granted access only into those files and programs that they need in order to perform their assigned jobs functions.
2. **Separation of duties:** To ensure that no single employee has control of a transaction from beginning to end, two or more people should be responsible for performing it.
3. **Rotation of duties:** Job assignment should be changed periodically so that it becomes more difficult for the users to collaborate to exercise complete control of a transaction and subvert it for fraudulent purposes.