Introduction and Overview of Cyber crime

- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.
- Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Most cybercrime falls under two main categories:

- Criminal activity that *targets*
- Criminal activity that *uses* computers to commit other crimes.

Cybercrime that *targets* computers often involves viruses and other types of malware.
Cybercriminals may infect computers with viruses and malware to damage devices or stop them working. They may also use malware to delete or steal data.
Cybercrime that stops users using a machine or network, or prevents a business providing a software service to its customers is called a Denial-of-Service (DoS) attack.
Cybercrime that *uses* computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images.
Sometimes cybercriminals conduct both categories of cybercrime at once. They may target computers with viruses first. Then, use them to spread malware to other machines or throughout a network.
Cybercriminals may also carry out what is known as a Distributed-Denial-of-Service (D-Dos) attack. This is similar to a DoS attack but cybercriminals use numerous compromised computers to carry it out.

Nature and Scope of Cyber crime

Nature – Cybercrime is Transnational in nature. These crimes are committed without being physically present at the crime location. These crimes are committed in the im-palpable world of computer networks.
To commit such crimes the only thing a person needs is a computer which is connected with the internet. With the advent of lightning fast internet, the time needed for committing the cybercrime is decreasing.
The cyberspace, being a boundary-less world has become a playground of the perpetrators where they commit crimes and remain conspicuously absent from the site of crime. It is an Open challenge to the law which derives its lifeblood from physical proofs and evidence.
The cybercrime has spread to such proportion that a formal categorization of this crime is no more possible. Every single day gives birth to a new kind of cybercrime making every single effort to stop it almost a futile exercise.
Identification possesses major challenge for cybercrime. One thing which is common it comes to identification part in cybercrime is Anonymous identity. It is quite an easy task to create false identity and commit crime over internet using that identity. Cybercrime being technology driven evolves continuously and ingeniously making it difficult for cyber investigators in finding solution related to cyber law crimes. Crimes committed over internet are very different in nature when compared to the physical world. In crimes relating to cyber space there is nothing sort of physical foot prints, tangible traces or objects to track cyber criminals down. Cybercrimes possess huge amount complications when it comes to investigation. There can be scenario where crimes committed over internet involve two or more different places in completely different direction of the world. This complicates the jurisdictional aspect of crimes relating to internet.

Scope – Cybercrime can be basically categorized into three parts:

- Cybercrimes against persons.
- Cybercrimes against property.
- Cybercrimes against government.

Cybercrimes against persons - Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified.

Cybercrimes against property - The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programs.

Cybercrimes against government - The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

Types of cybercrime

Here are some specific examples of the different types of cybercrime:

- **Email and internet fraud -** Email fraud (or email scam) is intentional deception for either personal gain or to damage another individual by means of email. Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them.
- **Identity fraud (where personal information is stolen and used)** - is the use by one person of another person's personal information, without authorization, to commit a crime or to deceive or defraud that other person or a third person.
- **Theft of financial or card payment data -** The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal.
- **Theft and sale of corporate data -** Data theft is the act of stealing information stored on corporate databases, devices, and servers. This form of corporate theft is a significant risk for businesses of all sizes and can originate both inside and outside an organization**.**
- **Cyber extortion (demanding money to prevent a threatened attack)** - Cyber extortion is a crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack.

  Cyber extortion attacks start with a hacker gaining access to an organization's systems and seeking points of weakness or targets of value. While ransomware attacks can be automated through malware spread by email, infected websites or ad networks, these attacks tend to spread indiscriminately, and they may result in only a small percentage of victims paying the extortionists. More targeted attacks can produce less collateral damage while providing more lucrative targets for the extortion attempt.
- **Ransomware attacks (a type of cyber extortion) -** Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever.
- **Crypto jacking (where hackers mine crypto currency using resources they do not own) -** Crypto jacking is the unauthorized use of someone else's computer to mine crypto currency. Hackersdo this by either getting the victim to click on a malicious link in an email that loads crypto mining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser.
- **Cyberespionage (where hackers access government or company data) -** Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.

Drug Trafficking

Drug traffickers generally use encrypted messaging tools to build communications with drug mules. There have been several instances of dark web site, such as the site ‘Silk Road’ was a notorious online marketplace for drugs, before it was shut down by law enforcement. It got reopened again under new management, but got shut down again later on. Another site emerged later on with the same name just to use the brand value.

A big example of drug trafficking by way of cybercrime would be cyber-attack on the port Antwerp of Belgium by 2011 - 2013. It was reported that hackers were hired by drug traffickers with the objective of breaching the IT systems which used to control the movements and location of the containers. Even in a police raid earlier, large amount of drugs, cash, along with several equipment’s for computer hacking were seized. Several persons were charged as well. It was reported by the prosecutors that a Netherlands based trafficking group had hid drugs like cocaine and other in several legitimate cargo containers. At the same time the hackers group was in function at the computer networks of Antwerp port. They could access the secure data with regard to the location and security details of the containers and by a few methods stole their marked cargo before the legitimate owner arrived. The suspicion first arose when the containers were found to be disappearing from the port without any reasonable explanation. It was found that hackers had used malicious software’s to e-mail the staffs and access data remotely. Even after the initial breach was discovered and a firewall was created to prevent any attacks, the attackers were reported to have entered the premises and installed key-loggers into the computers.

To take any measure to prevent illegal drug trafficking is not that easy, and when at the same time it happens by way of cybercrimes, it becomes more difficult, as cyberspace has no limits. Drug trade is international in nature, and law enforcement agencies are not always effective because of the wide and complex nature of cyber attackers. However, since the profit of drug trafficking and cybercrimes are equally big, mere one or two arrests here and there won’t bode any measure. International laws and partnerships across nations will have to be strong. One nation should help another in case of investigation or extradition of a criminal to the other. Overall, to neutralize drug trafficking by cybercrimes one nation’s law is never sufficient. These arethe places where United Nations or INTERPOL can come up with some measures.

Cyber Terrorism

- Cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.
- It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.
- Cyber terrorism is a controversial term. Some authors opt for a very narrow definition, relating to deployment by known terrorist organizations of disruption attacks against information systems for the primary purpose of creating alarm, panic, or physical disruption. Other authors prefer a broader definition, which includes cybercrime. Participating in a cyber-attack affects the terror threat perception, even if it isn't done with a violent approach. By some definitions, it might be difficult to distinguish which instances of online activities are cyber terrorism or cybercrime.
- Cyber terrorism can be also defined as the intentional use of computers, networks, and public internetto cause destruction and harm for personal objectives.
- Experienced cyber terrorists, who are very skilled in terms of hacking can cause massive damage to government systems, hospital records, and national security programs, which might leave a country, community or organization in turmoil and in fear of further attacks. The objectives of such terrorists may be political or ideological since this can be considered a form of terror.
- There is much concern from government and media sources about potential damage that could be

caused by cyber terrorism, and this has prompted efforts by government agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) to put an end to cyber-attacks and cyber terrorism.

- Conceptually, its use for this purpose falls into three categories:
  (i) weapon of mass destruction;
  (ii) weapon of mass distraction; and
  (iii) weapon of mass disruption

Need of Information Security

Information system means to consider available countermeasures or controls stimulated through uncovered vulnerabilities and identify an area where more work is needed. The purpose of data security management is to make sure business continuity and scale back business injury by preventing and minimizing the impact of security incidents. The basic principle of Information Security is:

- Confidentially
- Authentication
- Non-Repudiation
- Integrity

The need for Information security:

1. **Protecting the functionality of the organization:** The decision maker in organizations must set policy and operates their organization in compliance with the complex, shifting legislation, efficient and capable applications.
2. **Enabling the safe operation of applications:** The organization is under immense pressure to acquire and operates integrated, efficient and capable applications. The modern organization needs to create an environment that safeguards application using the organizations IT systems, particularly those application that serves as important elements of the infrastructure of the organization.
3. **Protecting the data that the organization collects and use:** Data in the organization can be in two forms that are either in rest or in motion, the motion of data signifies that data is currently used or processed by the system. The values of the data motivated the attackers to seal or corrupt the data. This is essential for the integrity and the values of the organization’s data. Information security ensures protection od both data in motion as well as data in rest.
4. **Safeguarding technology assets in organizations:** The organization must add intrastate services based on the size and scope of the organization. Organizational growth could lead to the need for public key infrastructure, PKI an integrated system of the software, encryption methodologies. The information security mechanism used by the large organization is complex in comparison to a small organization. The small organization generally prefers symmetric key encryption of data.

Threats to Information Systems

In Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

Software attacks mean attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the **basis of Infection** Method are following:

1. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc. and then they travel all over the Internet. Their Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms –** Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume hard disk space thus slowing down the computer.
3. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.
   Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.
   They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, and Remote Access Trojans etc.
4. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

Malware on the **basis of Actions:**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on computer's desktop or inside individual programs. They come attached with free to use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware –** It is a program or we can say a software that monitors your activities on computer and reveal collected information to interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection.
   One of the most common examples of spyware is KEY LOGGER. The basic job of Key logger is to record user keystrokes with timestamp. Thus, capturing interesting information like username, passwords, credit card details etc.
3. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e., ransom in exchange.
4. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
5. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
6. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
- **Identity theft** means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.
- **Information extortion** means theft of company's property or information to receive payment in exchange. For example, ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

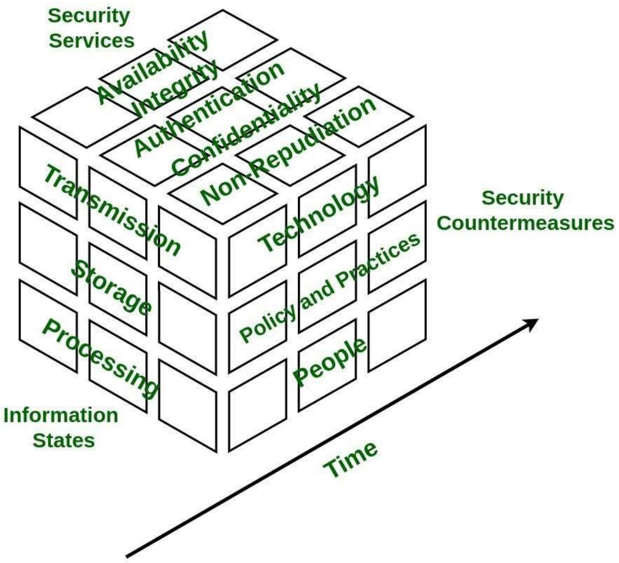
Information Assurance

Information Assurance concerns implementation of methods that focused on protecting and safeguarding critical information and relevant information systems by assuring confidentiality, integrity, availability, and non-repudiation. It is strategic approach focused which focuses more on deployment of policies rather than building infrastructures.

Information Assurance Model:

The security model is multidimensional model based on four dimensions:

1. **Information States –** Information is referred to as interpretation of data which can be found in three states stored, processed, or transmitted.
2. **Security Services –** It is fundamental pillar of the model which provides security to system and consists of five services namely availability, integrity, confidentiality, authentication, and non-repudiation.
3. **Security Countermeasures –** This dimension has functionalities to save system from immediate vulnerability by accounting for technology, policy & practice, and people.
4. **Time –** This dimension can be viewed in many ways. At any given time, data may be available offline or online, information and system might be in flux thus, introducing risk of unauthorized access. Therefore, in every phase of System Development Cycle, every aspect of Information Assurance model must be well defined and well implemented in order to minimize risk of unauthorized access.



Information States:

1. **Transmission –** It defines time wherein data is between processing steps.

Example**:** In transit over networks when user sends email to reader, including memory and storage encountered during delivery.

2. **Storage –**It defines time during which data is saved on medium such as hard drive.
   Example: Saving document on file server's disk by user.
3. **Processing –** It defines time during which data is in processing state.
   Example**:** Data is processed in random access memory (RAM) of workstation.

Security Services:

1. **Confidentiality –** It assures that information of system is not disclosed to unauthorized access and is read and interpreted only by persons authorized to do so. Protection of confidentiality prevents malicious access and accidental disclosure of information. Information that is considered to be confidential is called as **sensitive information**. To ensure confidentiality data is categorized into different categories according to damage severity and then accordingly strict measures are taken.
   Example: Protecting email content to read by only desired set of users. This can be insured by data encryption. Two-factor authentication, strong passwords, security tokens, and biometric verification are some popular norms for authentication users to access sensitive data.
2. **Integrity –** It ensures that sensitive data is accurate and trustworthy and cannot be created, changed, or deleted without proper authorization. Maintaining integrity involves modification or destruction of information by unauthorized access.
   To ensure integrity backups should be planned and implemented in order to restore any affected data in case of security breach. Besides this cryptographic checksum can also be used for verification of data.
   Example: Implementation of measures to verify that e-mail content was not modified in transit. This can be achieved by using cryptography which will ensure that intended user receives correct and accurate information.
3. **Availability –** It guarantees reliable and constant access to sensitive data only by authorized users. It involves measures to sustain access to data in spite of system failures and sources of interference.
   To ensure availability of corrupted data must be eliminated, recovery time must be sped up and physical infrastructure must be improved.
   Example: Accessing and throughput of e-mail service.
4. **Authentication –** It is security service that is designed to establish validity of transmission of message by verification of individual's identity to receive specific category of information.
   To ensure availability of various single factors and multi-factor authentication methods are used. A single factor authentication method uses single parameter to verify users' identity whereas two-factor authentication uses multiple factors to verify user's identity.
   Example: Entering username and password when we log in to website is example of authentication. Entering correct login information lets website verify our identity and ensures that only we access sensitive information.
5. **Non-Repudiation –**
   It is mechanism to ensure sender or receiver cannot deny fact that they are part of data transmission. When sender sends data to receiver, it receives delivery confirmation. When receiver receives message, it has all information attached within message regarding sender.
   Example: A common example is sending SMS from one mobile phone to another. After message is received confirmation message is displayed that receiver has received message. In return, message received by receiver contains all information about sender.

Security Countermeasures:

1. **People –** People are heart of information system. Administrators and users of information systems must follow policies and practice for designing good system. They must be informed regularly regarding information system and ready to act appropriately to safeguard system.
2. **Policy & Practice –** Every organization has some set of rules defined in form of policies that must be

followed by every individual working in organization. These policies must be practiced in order to properly handle sensitive information whenever system gets compromised.

3. **Technology –** Appropriate technology such as firewalls, routers, and intrusion detection must be used in order to defend system from vulnerabilities, threats. The technology used must facilitate quick response whenever information security gets compromised.

Cyber Security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data it's designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug-in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Security Risk analysis

Risk analysis refers to the review of risks associated with the particular action or event. The risk analysis is applied to information technology, projects, security issues and any other event where risks may be analyzed based on a quantitative and qualitative basis. Risks are part of every IT project and business organizations. The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats. The strategic risk analysis helps to minimize the future risk probability and damage.

Enterprise and organization used risk analysis:

- To anticipates and reduce the effect of harmful results occurred from adverse events.
- To plan for technology or equipment failure or loss from adverse events, both natural and human-caused.
- To evaluate whether the potential risks of a project are balanced in the decision process when evaluating to move forward with the project.
- To identify the impact of and prepare for changes in the enterprise environment.

Benefits of risk analysis

Every organization needs to understand about the risks associated with their information systems to effectively and efficiently protect their IT assets. Risk analysis can help an organization to improve their security in many ways. These are:

- Concerning financial and organizational impacts, it identifies, rate and compares the overall impact of

risks related to the organization.
- It helps to identify gaps in information security and determine the next steps to eliminate the risks of security.
- It can also enhance the communication and decision-making processes related to information security.
- It improves security policies and procedures as well as develops cost-effective methods for implementing information security policies and procedures.
- It increases employee awareness about risks and security measures during the risk analysis process and understands the financial impacts of potential security risks.

Steps in the risk analysis process

The basic steps followed by a risk analysis process are:

1. **Conduct a risk assessment survey:** Getting the input from management and department heads is critical to the risk assessment process. The risk assessment survey refers to begin documenting the specific risks or threats within each department.
2. **Identify the risks:** This step is used to evaluate an IT system or other aspects of an organization to identify the risk related to software, hardware, data, and IT employees. It identifies the possible adverse events that could occur in an organization such as human error, flooding, fire, or earthquakes.
3. **Analyze the risks:** Once the risks are evaluated and identified, the risk analysis process should analyses each risk that will occur, as well as determine the consequences linked with each risk. It also determines how they might affect the objectives of an IT project.
4. **Develop a risk management plan:** After analysis of the Risk that provides an idea about which assets are valuable and which threats will probably affect the IT assets negatively, we would develop a plan for risk management to produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.
5. **Implement the risk management plan:** The primary goal of this step is to implement the measures to remove or reduce the analyses risks. We can remove or reduce the risk from starting with the highest priority and resolve or at least mitigate each risk so that it is no longer a threat.
6. **Monitor the risks:** This step is responsible for monitoring the security risk on a regular basis for identifying, treating and managing risks that should be an essential part of any risk analysis process.

Types of Risk Analysis

The essential numbers of distinct approaches related to risk analysis are:

Qualitative Risk Analysis

- The qualitative risk analysis process is a project management technique that prioritizes risk on the project by assigning the probability and impact number. Probability is something a risk event will occur whereas impact is the significance of the consequences of a risk event.
- The objective of qualitative risk analysis is to assess and evaluate the characteristics of individually identified risk and then prioritize them based on the agreed-upon characteristics.
- The assessing individual risk evaluates the probability that each risk will occur and effect on the project objectives. The categorizing risks will help in filtering them out.
- Qualitative analysis is used to determine the risk exposure of the project by multiplying the probability and impact.

Quantitative Risk Analysis

- The objectives of performing quantitative risk analysis process provide a numerical estimate of the overall effect of risk on the project objectives.
- It is used to evaluate the likelihood of success in achieving the project objectives and to estimate contingency reserve, usually applicable for time and cost.
- Quantitative analysis is not mandatory, especially for smaller projects. Quantitative risk analysis helps in calculating estimates of overall project risk which is the main focus.

Unauthorized access to computers

Unauthorized computer access, popularly referred to as hacking, and describes a criminal action whereby someone uses a computer to knowingly gain access to data in a system without permission to access that data.

Computer Intrusion

Computer intrusions occur when someone tries to gain access to any part of your computer system. Computer intruders or hackers typically use automated computer programs when they try to compromise a computer's security. There are several ways an intruder can try to gain access to your computer. They can:

1. Access your computer to view, change, or delete information on your computer.
2. Crash or slow down your computer.
3. Access your private data by examining the files on your system.
4. Use your computer to access other computers on the Internet.

Computer Viruses and Malicious codes

Viruses –

- A virus is a computer code or program, which is capable of affecting your computer data badly by corrupting or destroying them.
- Computer virus has the tendency to make its duplicate copies at a swift pace, and also spread it across every folder and damage the data of your computer system.
- A computer virus is actually a malicious software program or "malware" that, when infecting your system, replicates itself by modifying other computer programs and inserting its own code.
- Infected computer programs may include data files, or even the "boot" sector of the hard drive.

Ways a virus can affect your computer system. The ways are mentioned below −

- By downloading files from the Internet.
- During the removable of media or drives.
- Through pen drive.
- Through e-mail attachments.
- Through unpatched software & services.
- Through unprotected or poor administrator passwords.

Impact of Virus

Let us now see the impact of virus on your computer system −

- Disrupts the normal functionality of respective computer system.
- Disrupts system network use.
- Modifies configuration setting of the system.
- Destructs data.
- Disrupts computer network resources.
- Destructs of confidential data.

Malicious Code - is the kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors, security breaches, information and data theft, and other potential damages to files and computing systems. It's a type of threat that may not be blocked by antivirus software on its own. Malware specifically refers to malicious software, but malicious code includes website scripts that can exploit vulnerabilities in order to upload malware.

It is an auto-executable application that can activate itself and take on various forms, including Java Applets, ActiveX controls, pushed content, plug-ins, scripting languages or other programming languages that are designed to enhance Web pages and email.

The code gives a cybercriminal unauthorized remote access to the attacked system — called an application back door — which then exposes sensitive company data. By unleashing it, cybercriminals can even wipe out a computer's data or install spyware.

Internet Hacking and Cracking

Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.

Computers have become mandatory to run a successful business. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Hackers are classified according to the intent of their actions. The following list classifies types of hackers according to their intent:

- **Ethical Hacker (White hat):** A security hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
- **Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
- **Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
- **Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.
- **Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
- **Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

Cracking

- Cracking is a technique used to breach computer software or an entire computer security system, and with malicious intent.
- **Cracking is when someone performs a security hack for criminal or malicious reasons,** and the person is called a “cracker.” Just like a bank robber cracks a safe by skillfully manipulating its lock, a cracker breaks into a computer system, program, or account with the aid of their technical wizardry.
- it’s always with the aim of doing something naughty when you’re there: **stealing data, impersonating someone, or even just using paid software for free**.

Some common types of cracking:

- **Password cracking -** is the act of obtaining a password from stored data. Most common password cracking methods.
  - **Brute force cracking:** The cracking algorithm outputs random strings of characters until it gets a match.
  - **Dictionary cracking:** It’s similar to brute-force cracking, but rather than using random characters, dictionary cracking limits itself to actual words.
  - **Rainbow table cracking:** A rainbow table uses pre-computed hash values to figure out theencryption used to hash a password.
- **Software cracking -** is when someone alters a piece of software to disable or entirely remove one or more of its features. Most software cracking uses at least one of the following tools or techniques:
  - **Keygen:** Short for “key generator,” a keygen is a program a cracker builds to generate valid

serial numbers for a software product.

  - **Patch:** Patches are small bits of code that modify existing programs. Developers release patches for software all the time. Crackers can make them too, and when they do, the patch's job is to alter the way the program works by removing the unwanted features.
  - **Loader:** A loader's job is to block the software's protection measures as the software starts up. Some loaders bypass copy protections, while others are popular with gamers who enjoy cheating in online multiplayer games.

- **Network cracking -** is when someone breaks through the security of a LAN, or "local area network." Cracking a wired network requires a direct connection, but cracking a wireless network is much more convenient, because the cracker just needs to be close to the wireless signal. A common example of a wireless LAN is the Wi-Fi system in your home.

Viruses and Worms

1. Worms: Worms is similar to virus but it does not modify the program. It replicate itself more and more to cause slow down the computer system. Worms can be controlled by remote. The main objective of worms to eat the system resources.

2. Virus: A virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data. When the computer program runs attached with virus it perform some action such as deleting a file from the computer system. Virus can't be controlled by remote.

Difference between Worms and Virus:

S.No.	WORMS	VIRUS
1.	A Worm is a form of malware that replicates itself and can spread to different computers via Network.	A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.
2.	The main objective of worms to eat the system resources.	The main objective of virus is to modify the information.
3.	It doesn't need a host to replicate from one computer to another.	It require host is needed for spreading.
4.	It is less harmful as compared.	It is more harmful.
5.	Worms can be detected and removed by the Antivirus and firewall.	Antivirus software are used for protection against viruses.
6.	Worms can be controlled by remote.	Virus can't be controlled by remote.
7.	Worms are executed via weaknesses in system.	Viruses are executed via executable files.
8.	Morris Worm, Storm Worm and SQL Slammer are some of the examples of worms.	Resident and Non -resident viruses are two types of Virus.
9.	It does not needs human action to replicate.	It needs human action to replicate.
10.	Its spreading speed is faster.	Its spreading speed is slower as compared.

Software Piracy

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software.

Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the proper credit and compensation for their work. When software piracy occurs, compensation is stolen from these copyright holders.

Types of Software Piracy

There are five main types of software piracy.

- **Softlifting -** is when someone purchases one version of the software and downloads it onto multiple computers, even though the software license states it should only be downloaded once. This often occurs in business or school environments and is usually done to save money. Softlifting is the most common type of software piracy.
- **Client-server overuse -** is when too many people on a network use one main copy of the program at the same time. This often happens when businesses are on a local area network and download the software for all employees to use. This becomes a type of software piracy if the license doesn't entitle you to use it multiple times.
- **Hard disk loading -** is a type of commercial software piracy in which someone buys a legal version of the software and then reproduces copies or installs it onto computer hard disks. The person then sells the product. This often happens at PC resale shops and buyers aren't always aware that the additional software they are buying is illegal.
- **Counterfeiting -** occurs when software programs are illegally duplicated and sold with the appearance of authenticity. Counterfeit software is usually sold at a discounted price in comparison to the legitimate software.
- **Online Piracy -** also known as Internet piracy is when illegal software is sold, shared or acquired by means of the Internet. This is usually done through a peer-to-peer (P2P) file-sharing system, which is usually found in the form of online auction sites and blogs.

The Dangers of Software Piracy

Software piracy may have a cheaper price point, but there are many dangers that software pirates should be aware of. Consequences of software piracy are:

- Increased chances that the software will malfunction or fail
- Forfeited access to support for the program such as training, upgrades, customer support and bug fixes
- No warranty and the software can't be updated
- Increased risk of infecting your PC with malware, viruses or adware
- Slowed down PC
- Legal repercussions due to copyright infringement

Intellectual property Rights

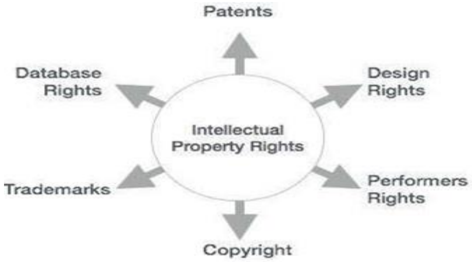
Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity. Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.

The creator/inventor gets exclusive rights against any misuse or use of work without his/her prior information. However, the rights are granted for a limited period of time to maintain equilibrium.

Types of Intellectual Property Rights

Intellectual Property Rights can be further classified into the following categories −

- Copyright
- Patent
- Patent
- Trade Secrets, etc.



Advantages of Intellectual Property Rights

Intellectual property rights are advantageous in the following ways −

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.
- Provides legal defense and offers the creators the incentive of their work.
- Helps in social and financial development.

Intellectual Property in Cyber Space

- Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical marketplace and has converted it into a virtual marketplace.
- To safeguard the business interest, it is vital to create an effective property management and protection mechanism keeping in mind the considerable amount of business and commerce taking place in the Cyber Space.
- Today it is critical for every business to develop an effective and collaborative IP management mechanism and protection strategy. The ever-looming threats in the cybernetic world can thus be monitored and confined.
- Various approaches and legislations have been designed by the law-makers to up the ante in delivering a secure configuration against such cyber-threats. However, it is the duty of the intellectual property right (IPR) owner to invalidate and reduce such *mala fide* acts of criminals by taking proactive measures.

Mail Bombs

An email bomb is an attack against an email inbox or server designed to overwhelm an inbox or inhibit the server's normal function, rendering it unresponsive, preventing email communications, degrading network performance, or causing downtime. The intensity of an email bomb can range from an inconvenience to a complete denial of service. Typically, these attacks persist for hours or until the targeted inbox or server implements a mitigation tactic to filter or block the attacking traffic. Such attacks can be carried out intentionally or unintentionally by a single actor, group of actors, or a botnet.

There are five common email bomb techniques:

1. **Mass mailing** – intentionally or unintentionally sending large quantities of random email traffic to targeted email addresses. This attack is often achieved using a botnet or malicious script, such as by the automated filling out of online forms with the target email inserted as the requesting/return address.
2. **List linking** – signing targeted email addresses up for numerous email subscriptions, which indirectly flood the email addresses with subscribed content. Many subscription services do not ask for verification, but if they do these emails can be used as the attack emails. This type of attack is difficult to prevent because the traffic originates from multiple legitimate sources.
3. **ZIP bomb** – sending very large compressed archive files to an email address, which when decompressed, consume available server resources to damage performance.
4. **Attachment** – sending multiple emails with large attachments designed to overload the storage space on a server and cause the server to stop responding.
5. **Reply-all** – responding "Reply All" to large dissemination lists instead of just to the original sender.

This inundates inboxes with a cascade of emails, which are compounded by automated replies, such as out-of-office messages. These are often accidental in nature. This can also occur when a malicious actor spoofs an email address and the automatic replies are directed toward the spoofed address.

Effects of Mail Bombs

Email bombs can create denial of service conditions that may impede election offices from conducting routine or election day activities. For example, a successful email bomb may inhibit election offices from accessing inboxes for citizen engagement, voter registration, or other services. The impact of such an attack is highly likely to compound if occurring around polling or registration dates. Additionally, cyber actors sometimes use email bomb attacks to mask other malicious activity, distract users, or prevent the regular flow of notifications associated with critical or abnormal account activity.

Exploitation

An **exploit** is a code that takes advantage of a software vulnerability or security flaw. It is written either by security researchers as a proof-of-concept threat or by malicious actors for use in their operations. When used, exploits allow an intruder to remotely access a network and gain elevated privileges, or move deeper into the network.

In some cases, an exploit can be used as part of a multi-component attack. Instead of using a malicious file, the exploit may instead drop another malware, which can include backdoor Trojans and spyware that can steal user information from the infected systems.

Common types of computer exploit

- **Known exploits -** When someone discovers software vulnerability, they'll often alert the software's developer, who can then fix the vulnerability immediately with a security patch. They may also spread the word about the vulnerability on the internet to warn others. Either way, the developer will (hopefully) be able to respond and repair the vulnerability before an exploit can take advantage of it.
- **Zero-day exploits (unknown exploits) -** Sometimes, exploits catch everyone by surprise. When a hacker discovers a vulnerability and immediately creates an exploit for it, it's called a zero-day exploit — because the exploit attack happens on the same day the vulnerability is found. At that point, the developer has known about the vulnerability for "zero days."
- **Hardware exploits -** While software exploits get most of the media attention, they're not the only types of exploits out there. Sometimes, hackers can exploit flaws in the physical hardware (and its firmware) in your device.

Stalking and Obscenity in Internet

Cyber stalking

- Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.
- Cyber stalking is often accompanied by real time or offline stalking. In many jurisdictions, such as California, both are criminal offenses. Both are motivated by a desire to control, intimidate or influence a victim. A stalker may be an online stranger or a person whom the target knows. They may be anonymous and solicit involvement of other people online who do not even know the target.
- Cyber stalking is a criminal offense under various state anti-stalking, slander and harassment laws. A conviction can result in a restraining order, probation, or criminal penalties against the assailant, including jail.

Cyber stalking can take many forms, including:

1. harassment, embarrassment and humiliation of the victim
2. emptying bank accounts or other economic control such as ruining the victim's credit score

3. harassing family, friends and employers to isolate the victim
4. scare tactics to instil fear and more

Key factors in cyber stalking:

- False accusations
- Attempts to gather information about the victim
- Monitoring their target's online activities and attempting to trace their IP address in an effort to gather more information about their victims.
- Encouraging others to harass the victim
- False victimization
- Attacks on data and equipment
- Arranging to meet
- The posting of defamatory or derogatory statements

Obscenity in Internet

Obscenity refers to a narrow category of pornography that violates contemporary community standards and has no serious literary, artistic, political or scientific value. For adults at least, most pornography — material of a sexual nature that arouses many readers and viewers — receives constitutional protection. However, two types of pornography receive no First Amendment protection: obscenity and child pornography. Sometimes, material is classified as "harmful to minors" (or obscene as to minors), even though adults can have access to the same material.

Password Cracking

- Password cracking techniques are used to recover passwords from the data that have stored in or transmitted by computer systems.
- Attackers use password-cracking techniques to gain unauthorized access to the vulnerable system.
- Most of the passwords cracking techniques are successful due to weak or easily guessable passwords.
- Password cracking may use to recover the forgot password of any user to help him/her to recover the password.

Types of Password Attacks

- **Non-Technical Attacks –** The attacker need not possess the technical knowledge to crack the password, hence known as a non-technical attack.

  These types of attacks involve the following terms:
  - **Shoulder Surfing -** is the technique that we need to do when we are in contact with that person, basically, we guess the password by seeing their hands moving or his/her shoulder movements.
  - **Social Engineering -** is one of the best concepts in the non-technical attacks. Social Engineering is to collect more and more information about the target to get or guess the password by direct contact or indirectly.
  - **Dumpster Diving -** In the dumpster diving technique we try to collect info about passwords through the dump of that person's office or from home. Sometimes it really works too good.
- **Active Online Attack -**
  - **Dictionary Attack -** is loaded into the cracking application that runs against user accounts.
  - **Brute Forcing Attack -** The program tries every combination of characters until the password is broken.
  - **Rule-Based Attack -** This attack is used when the attacker gets some information about the password.
  - **Password Guessing -** The attacker crates a list of all possible passwords from the information collected through social engineering or any other way and tries them manually on the victim's

machine to crack the passwords.

- **Trojan/Spyware/Key logger -** The attacker installs Trojan/Spyware/Key logger on the victim's machine to collect the victim's user names and passwords. Trojan/Spyware/Key logger runs in the background and sends back all user credentials to the attacker.
- **Hash Injection Attack -** allows an attacker to inject a compromised hash into a local session and use the hash to validate network resources. The attacker finds and extracts a logged on domain admin account hash. The attacker uses the extracted hash to log on to the domain controller.

- **Passive Online Attacks -**
    - Wire Sniffing - Attackers run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic. The captured data may include sensitive information such as passwords (FTP, login sessions, etc.) and emails. Sniffed credentials are used to gain unauthorized access to the target system.
    - **Man-in-the-Middle and Replay Attack -** Gain access to the communication channels: In a MITM attack, the attacker acquires access to the communication channels between victim and server to extract the information. Use Sniffer: In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant into is extracted, the tokens are placed back on the network to gain access.
    - **Default Password -** A default password is a password supplied by the manufacturer with new equipment (switches, hubs, routers) that is password protected. Attackers use default passwords in the list of words or dictionary that they use to perform password guessing attack.
- **Offline Attack -**
    - Rainbow Table Attack - is a precomputed table that contains word lists like dictionary files and brute force lists and their hash values. Capture the hash of passwords and compare them with the precomputed hash table. If a match is found then the password is cracked.

Steganography

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

Use of Steganography

There are many ways to conceal information using Steganography. The most common method is by embedding information into digital images. We all know that digital images say, a JPEG image, contains several megabytes of data in the form of pixels. This allows some room for someone to embed steganographic information within the digital file. With the use of steganographic applications, a hacker alters the least significant bits of the data file and embeds a malicious code into the image. Once the targeted user downloads and opens the image file in their computer, the malware is activated. Depending on its programming, the malware can now open a leeway for the attacker to gain control over the user's device or network. The danger of Steganography is that the difference between the original image and the steganographic image is subtle and the two cannot be distinguished by the naked eye.

3 Techniques used in Steganography

1. **Least Significant Bit -** In this Steganography method, the attacker identifies the least significant bits of information in the carrier image and substitutes it with their secret message, in this case, malicious code. When the target downloads the carrier file, they introduce the malware into their computer which allows the attacker access to this device and the hack begins. Cyber security professionals commonly use sandboxes to detect these corrupt files. However, black hat hackers have invented various methods of bypassing sandboxes like sleep patching. Sleep patched malware is not easily detected by the sandbox since it poses as benign and buys time while studying the timing artifacts of the sandbox and executes when the sandbox is vulnerable.

2. **Palette Based Technique -** This technique also uses digital images as malware carriers. Here, the attackers first encrypt the message and then hide it in a stretched palette of the cover image. Even though this technique can carry a limited amount of data, it frustrates threat hunters since the malware is encrypted and takes a lot of time to decrypt.
3. **Secure Cover Selection -** This is a very complex technique where the cyber criminals compare the blocks of the carrier image to the blocks of their specific malware. If an image with the same blocks as the malware is found, it is chosen as the candidate to carry the malware. The identical malware blocks are then carefully fitted into the carrier image. The resulting image is identical to the original and the worst part is that this image is not flagged as a threat by detection software and applications.

These are just but a few methods by which black hat hackers frustrate ethical hackers using Steganography. Steganography allows attackers to operate in stealth mode while conducting a serious attack. Most of these attacks are zero-day exploits which give threat hunters sleepless nights. Some preventive measures against Steganography include the deployment of security patches, updating software, and educating end-users.

Key loggers and spyware

Key logger –

- Key loggers are a serious threat to users and the users' data, as they track the keystrokes to intercept passwords and other sensitive information typed in through the keyboard. This gives hackers the benefit of access to PIN codes and account numbers, passwords to online shopping sites, email ids, email logins, and other confidential information, etc.
- When the hackers get access to the users' private and sensitive information, they can take advantage of the extracted data to perform online money transaction the user's account. Key loggers can sometimes be used as a spying tool to compromise business and state-owned company's data.
- The main objective of Key loggers is to interfere in the chain of events that happen when a key is pressedand when the data is displayed on the monitor as a result of a keystroke.
- A Key logger can be done by introducing a wiring or a hardware bug in the keyboard, to achieve video surveillance; terminating input and/or output; or by also implementing the use of a filter driver in the keyboard stack; and demanding data from the user's keyboard using generalized documented methods. There are two other rootkit methods used by hackers: masking in kernel mode and masking in user mode.

Types of Key loggers

Key logger tools are mostly constructed for the same purpose. But they’ve got important distinctions in terms of the methods they use and their form factor.

Here are the two forms of Key loggers

1. **Software Key loggers**
2. **Hardware Key loggers**

Software Key loggers - Software Key loggers are computer programs that install onto your device’s hard drive. Common Key logger software types may include:

- **API-based Key loggers** directly eavesdrop between the signals sent from each key press to the program you’re typing into. Application programming interfaces (APIs) allow software developers and hardware manufacturers to speak the same “language” and integrate with each other. API Key loggers quietly intercept keyboard APIs, logging each keystroke in a system file.
- **“Form grabbing”-based Key loggers** eavesdrop all text entered into website forms once you send itto the server. Data is recorded locally before it is transmitted online to the web server.
- **Kernel-based Key loggers** work their way into the system’s core for admin-level permissions. These loggers can bypass and get unrestricted access to everything entered in your system.

Hardware Key loggers - Hardware Key loggers are physical components built-in or connected to your device. Some hardware methods may be able to track keystrokes without even being connected to your device. For brevity, we'll include the Key loggers you are most likely to fend against:

- **Keyboard hardware Key loggers** can be placed in line with your keyboard's connection cable or built into the keyboard itself. This is the most direct form of interception of your typing signals.
- **Hidden camera Key loggers** may be placed in public spaces like libraries to visually track keystrokes.
- **USB disk-loaded Key loggers** can be a physical Trojan horse that delivers the keystroke logger malware once connected to your device.

Prevention from Keystroke logging

- Always read your terms of service or any contracts before accepting.
- Install internet security software on all your devices.
- Make sure your security programs are updated on the latest threats.
- Don't leave your mobile and computer devices unsupervised.
- Keep all other device software updated.
- Do not use unfamiliar USB drives or external hard drives.

Spyware

- Spyware is a broad category of malware designed to secretly observe activity on a device and send those observations to a snooper. That data can be used to track your activity online and that information can be sold to marketers.
- Spyware can also be used to steal personal information, such as account passwords and credit card numbers, which can result in identity theft and fraud.
- Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.
- Spyware is classified as a type of malware — malicious software designed to gain access to or damage your computer, often without your knowledge. Spyware gathers your personal information and relays it to advertisers, data firms, or external users.

Types of spyware

Spyware can take a number of forms. They include:

- **Adware**: It eyes your online activity and displays ads it thinks you'll be interested in based on that information. Although benign compared to some other forms of spyware, adware can have an impact on the performance of a device, as well as just being annoying.
- **Tracking cookies**: They're similar to adware, although they tend to be less intrusive.
- **Trojans**: After landing on a device, they look for sensitive information, such as bank account information, and send it to a seedy third-party who will use it to steal money, compromise accounts or make fraudulent purchases. They can also be used to gain control of a computer through the installation of a backdoor or a remote access Trojan (RAT).
- **Key loggers**: They allow a miscreant to capture every keystroke from your keyboard, including the keystrokes you use when you log into your online accounts.
- **Stalkerware**: It's typically installed on a mobile phone so the owner of the phone can be tracked by a third party. For example, during the trial of Joaquín "El Chapo" Guzmán, it was revealed the drug kingpin installed spyware on the phones of his wife, associates and female friends so he could read their text messages, listen to their conversations and follow their movements.
- **Stealware**: It's crafted to take advantage of online shopping sites awarding credits to websites that send traffic to their product pages. When a user goes to one of those sites, stealware intercepts the request and takes credit for sending the user there.
- **System monitors**: They record everything that's happening on a device—from keystrokes, emails and chat room dialogs to websites visited, programs launched, and phone calls made—and send it to a

snoop or cyber-criminal. They can also monitor a system's processes and identify any vulnerabilityon it.

Prevention from spyware

Here are four main steps to help prevent spyware.

- Don’t open emails from unknown senders.
- Don’t download files from untrustworthy sources.
- Don’t click on pop-up advertisements.
- Use reputable antivirus software.

Spyware can be harmful, but it can be removed and prevented by being cautious and using an antivirus tool. If you’ve been infected with spyware, take steps to remove it. Be proactive by changing your passwords and notifying your bank to watch for fraudulent activity.

Trojan and backdoors

- A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software.
- Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems.
- Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems.
- Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include:
  - Deleting data
  - Blocking data
  - Modifying data
  - Copying data
  - Disrupting the performance of computers or computer networks
- Unlike computer viruses and worms, Trojans are not able to self-replicate.

Trojan and its impact

- **Backdoor -** A backdoor Trojan gives malicious users remote control over the infected computer. They enable the author to do anything they wish on the infected computer – including sending, receiving, launching and deleting files, displaying data and rebooting the computer. Backdoor Trojans are often used to unite a group of victim computers to form a botnet or zombie network that can be used for criminal purposes.
- **Exploit -** are programs that contain data or code that takes advantage of vulnerability within application software that’s running on your computer.
- **Rootkit -** are designed to conceal certain objects or activities in your system. Often their main purpose is to prevent malicious programs being detected – in order to extend the period in which programs can run on an infected computer.
- **Trojan-Banker -** programs are designed to steal your account data for online banking systems, e-payment systems and credit or debit cards.
- **Trojan-Downloader -** can download and install new versions of malicious programs onto your computer – including Trojans and adware.

Protection against Trojan

Here are some dos and don’ts to help protect against Trojan malware. First, the dos:

- Computer security begins with installing and running an internet security suite. Run periodic diagnostic scans with your software. You can set it up so the program runs scans automatically during regular intervals.
- Update your operating system’s software as soon as updates are made available from the software

company. Cybercriminals tend to exploit security holes in outdated software programs. In addition to operating system updates, you should also check for updates on other software that you use on your computer.

- Protect your accounts with complex, unique passwords. Create a unique password for each account using a complex combination of letters, numbers, and symbols.
- Keep your personal information safe with firewalls.
- Back up your files regularly. If a Trojan infects your computer, this will help you to restore your data.
- Be careful with email attachments. To help stay safe, scan an email attachment first.

A lot of things you should do come with a corresponding thing not to do — like, do be careful with email attachments and don’t click on suspicious email attachments. Here are some more don’ts.

- Don’t visit unsafe websites. Some internet security software will alert you that you’re about to visit an unsafe site, such as Norton Safe Web.
- Don’t open a link in an email unless you’re confident it comes from a legitimate source. In general, avoid opening unsolicited emails from senders you don’t know.
- Don’t download or install programs if you don’t have complete trust in the publisher.
- Don’t click on pop-up windows that promise free programs that perform useful tasks.
- Don’t ever open a link in an email unless you know exactly what it is.

Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
- The information is then used to access important accounts and can result in identity theft and financial loss.
- Phishing is an example of social engineering techniques used to deceive users. Users are lured by communications purporting to be from trusted parties such as social networking websites, auction sites, banks, and mails/messages from friends or colleagues/executives, online payment systems or IT administrators.

Types of phishing

- **Spear phishing -** Phishing attempts directed at specific individuals or companies
- **Catphishing and catfishing -** is a type of online deception that involves getting to know someone closely in order to gain access to information or resources, usually in the control of the mark, or to otherwise get control over the conduct of the target.
- **Clone phishing -** is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email.
- **Voice phishing -** uses fake caller-ID data to give the appearance that calls come from a trusted organization.
- **SMS phishing -** or smishing uses cell phone text messages to deliver the *bait* to induce people to divulge their personal information.

Prevention against Phishing

- To protect against spam mails, spam filters can be used. Generally, the filters assess the origin of the message, the software used to send the message, and the appearance of the message to determine if it’s spam. Occasionally, spam filters may even block emails from legitimate sources, so it isn’t always 100% accurate.
- The browser settings should be changed to prevent fraudulent websites from opening. Browsers keep a list of fake websites and when you try to access the website, the address is blocked or an alert message

is shown. The settings of the browser should only allow reliable websites to open up.

- Many websites require users to enter login information while the user image is displayed. This type of system may be open to security attacks. One way to ensure security is to change passwords on a regular basis, and never use the same password for multiple accounts. It’s also a good idea for websites to use a CAPTCHA system for added security.
- Banks and financial organizations use monitoring systems to prevent phishing. Individuals can report phishing to industry groups where legal actions can be taken against these fraudulent websites. Organizations should provide security awareness training to employees to recognize the risks.
- Changes in browsing habits are required to prevent phishing. If verification is required, always contact the company personally before entering any details online.
- If there is a link in an email, hover over the URL first. Secure websites with a valid Secure Socket Layer (SSL) certificate begin with “https”. Eventually all sites will be required to have a valid SSL.

DOS Attack

- A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., employees, members, or account holders) of the service or resource they expected.
- Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.
- A denial-of-service (DoS) attack is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.
- DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users.
- A DoS attack is characterized by using a single computer to launch the attack.

There are two general methods of DoS attacks: flooding services or crashing services.

Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop.

Popular flood attacks include:

- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications ornetworks
- **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- **SYN flood** – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connectto.

Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system, so that it can’t be accessed or used.

Protection from DoS attack

A general rule: The earlier you can identify an attack-in-progress, the quicker you can contain the damage.

Here are some things you can do.

- **Method 1:** Get help recognizing attacks - Companies often use technology or anti-DDoS services to help defend themselves. These can help you recognize between legitimate spikes in network traffic and a DDoS attack.
- **Method 2:** Contact your Internet Service provider - If you find your company is under attack, you should notify your Internet Service Provider as soon as possible to determine if your traffic can be rerouted. Having a backup ISP is a good idea, too. Also, consider services that can disperse the massive DDoS traffic among a network of servers. That can help render an attack ineffective.
- **Method 3:** Investigate black hole routing - Internet service providers can use “black hole routing.” It directs excessive traffic into a null route, sometimes referred to as a black hole. This can help prevent the targeted website or network from crashing. The drawback is that both legitimate and illegitimate traffic is rerouted in the same way.
- **Method 4:** Configure firewalls and routers - Firewalls and routers should be configured to reject bogus traffic. Remember to keep your routers and firewalls updated with the latest security patches.
- **Method 5:** Consider front-end hardware - Application front-end hardware that’s integrated into the network before traffic reaches a server can help analyze and screen data packets. The hardware classifies the data as priority, regular, or dangerous as they enter a system. It can also help block threatening data.

DDOS Attack

- A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.
- From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

Working

- DDoS attacks are carried out with networks of Internet-connected machines.
- These networks consist of computers and other devices (such as IoT devices) which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.
- Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.
- When a victim’s server or network is targeted by the botnet, each bot sends requests to the target’s IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of- service to normal traffic.
- Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

Identification of DDOS Attack

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes — such a legitimate spike in traffic — can create similar performance issues, further investigation is usually required. Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack:

- Suspicious amounts of traffic originating from a single IP address or IP range
- A flood of traffic from users who share a single behavioral profile, such as device type, geo-

location,or web browser version

- An unexplained surge in requests to a single page or endpoint
- Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g. a spike every 10 minutes)

Types of DDOS attack

- **Application layer attacks -** Sometimes referred to as a layer 7 DDoS attack (in reference to the 7th layer of the OSI model), the goal of these attacks is to exhaust the target's resources to create a denial-of-service. The attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests. A single HTTP request is computationally cheap to execute on the client side, but it can be expensive for the target server to respond to, as the server often loads multiple files and runs database queries in order to create a web page. Layer 7 attacks are difficult to defend against, since it can be hard to differentiate malicious traffic from legitimate traffic.
- **Protocol attacks -** also known as state-exhaustion attacks, cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers. Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.
- **Volumetric attacks -** This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.
- **Fragmentation Attacks -** are another common form of a DDoS attack. The cybercriminal exploits vulnerabilities in the datagram fragmentation process, in which IP datagrams are divided into smaller packets, transferred across a network, and then reassembled. In Fragmentation attacks, fake data packets unable to be reassembled, overwhelm the server.

Protection from DDOS attack

Method 1: Take quick action
Method 2: Configure firewalls and routers
Method 3: Consider artificial intelligence
Method 4: Secure your Internet of Things devices

SQL Injection

- SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.
- The impact SQL injection can have on a business is far-reaching.
- A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.
- When calculating the potential cost of a SQLi, it's important to consider the loss of customer trust should personal information such as phone numbers, addresses, and credit card details are stolen.
- While this vector can be used to attack any SQL database, websites are the most frequent targets.

Types of SQL Injections

SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi. You can classify SQL injections types based on the methods they use to access backend data and their damage potential.

In-band SQLi - The attacker uses the same channel of communication to launch their attacks and to gather their results. In-band SQLi's simplicity and efficiency make it one of the most common types of SQLi attack. There are two sub-variations of this method:

- **Error-based SQLi**—the attacker performs actions that cause the database to produce error messages. The attacker can potentially use the data provided by these error messages to gather information about the structure of the database.
- **Union-based SQLi**—this technique takes advantage of the UNION SQL operator, which fuses multiple select statements generated by the database to get a single HTTP response. This response may contain data that can be leveraged by the attacker.

Inferential (Blind) SQLi - The attacker sends data payloads to the server and observes the response and behavior of the server to learn more about its structure. This method is called blind SQLi because the data is not transferred from the website database to the attacker, thus the attacker cannot see information about the attack in-band.

Blind SQL injections rely on the response and behavioral patterns of the server so they are typically slower to execute but may be just as harmful. Blind SQL injections can be classified as follows:

- **Boolean**—that attacker sends a SQL query to the database prompting the application to return a result. The result will vary depending on whether the query is true or false. Based on the result, the information within the HTTP response will modify or stay unchanged. The attacker can then work out if the message generated a true or false result.
- **Time-based**—attacker sends a SQL query to the database, which makes the database wait (for a period in seconds) before it can react. The attacker can see from the time the database takes to respond, whether a query is true or false. Based on the result, an HTTP response will be generated instantly or after a waiting period. The attacker can thus work out if the message they used returned true or false, without relying on data from the database.

Out-of-band SQLi - The attacker can only carry out this form of attack when certain features are enabled on the database server used by the web application. This form of attack is primarily used as an alternative to the in-band and inferential SQLi techniques.

Out-of-band SQLi is performed when the attacker can't use the same channel to launch the attack and gather information, or when a server is too slow or unstable for these actions to be performed. These techniques count on the capacity of the server to create DNS or HTTP requests to transfer data to an attacker.

SQL Injection Prevention Techniques

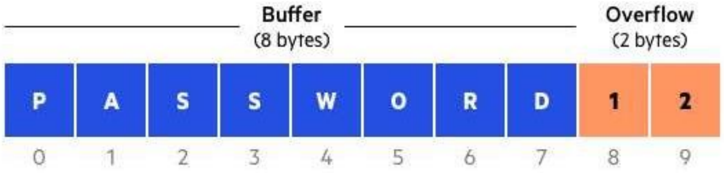
- **Input validation -** The validation process is aimed at verifying whether or not the type of input submitted by a user is allowed. Input validation makes sure it is the accepted type, length, format, and so on. Only the value which passes the validation can be processed. It helps counteract any commands inserted in the input string.
- **Parametrized queries -** are a means of pre-compiling an SQL statement so that you can then supply the parameters in order for the statement to be executed. This method makes it possible for the database to recognize the code and distinguish it from input data.
- **Stored procedures -** require the developer to group one or more SQL statements into a logical unit to create an execution plan. Subsequent executions allow statements to be automatically parameterized. Simply put, it is a type of code that can be stored for later and used many times.
- **Escaping -** Always use character-escaping functions for user-supplied input provided by each database management system (DBMS). This is done to make sure the DBMS never confuses it with the SQL statement provided by the developer.
- **Avoiding administrative privileges -** Don't connect your application to the database using an account with root access. This should be done only if absolutely needed since the attackers could gain access to the whole system.

- **Web application firewall -** A WAF operating in front of the web servers monitors the traffic which goes in and out of the web servers and identifies patterns that constitute a threat. Essentially, it is a barrier put between the web application and the Internet.

Buffer Overflow

- Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another.
- A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.
- For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.
- Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.

Buffer overflow example



Buffer Overflow Attack

- Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.
- If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

Types of Buffer Overflow Attacks

- **Stack-based buffer overflows** are more common, and leverage stack memory that only exists during the execution time of a function.
- **Heap-based attacks** are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

Protection against Buffer overflow

Developers can protect against buffer overflow vulnerabilities via security measures in their code, or by using languages that offer built-in protection.

In addition, modern operating systems have runtime protection. Three common protections are:

- **Address space randomization (ASLR)**—randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.
- **Data execution prevention**—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.
- **Structured exception handler overwrites protection (SEHOP)**—helps stop malicious code from

attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique. At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.

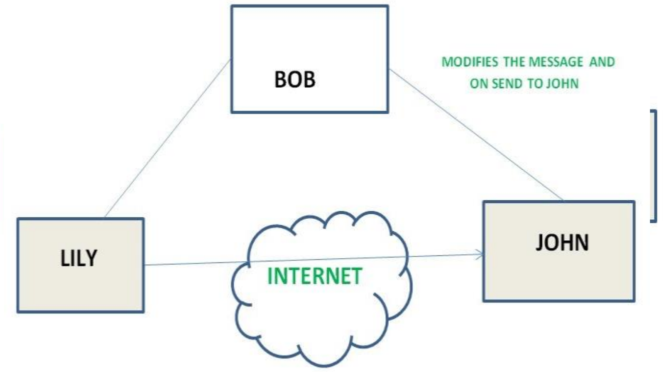
Security measures in code and operating system protection are not enough. When an organization discovers buffer overflow vulnerability, it must react quickly to patch the affected software and make sure that users of the software can access the patch.

Active and Passive attack

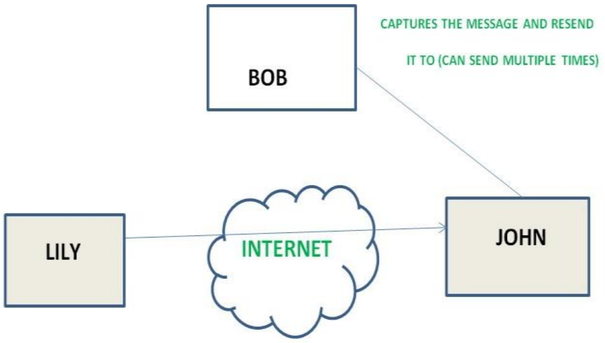
Active attacks: An Active attack attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement.

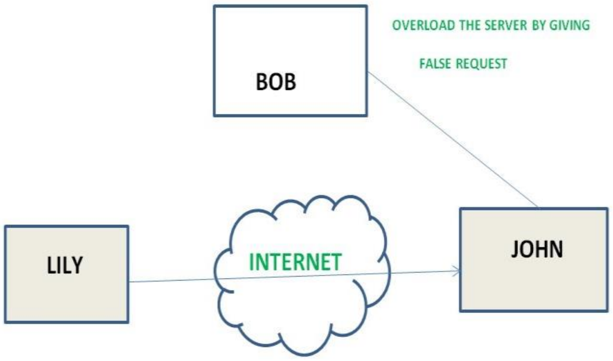
Types of active attacks are as following:

1. **Masquerade –** Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other forms of active attacks.
2. **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. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".



3. **Repudiation –** This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has sent or receive a message. For example, customers ask his Bank "To transfer an amount to someone" and later on the sender (customer) denies that he had made such a request. This is repudiation.
4. **Replay –** It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.
5. **Denial of Service –** It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network withers by disabling the network or by overloading it by messages so as to degrade performance.

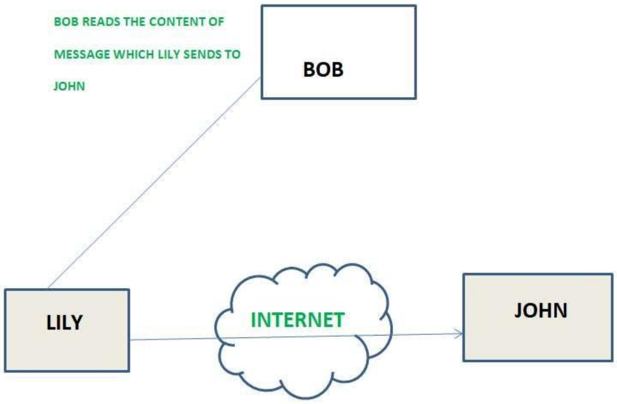

BOB
CAPTURES THE MESSAGE AND RESEND
IT TO (CAN SEND MULTIPLE TIMES)
LILY
INTERNET
JOHN

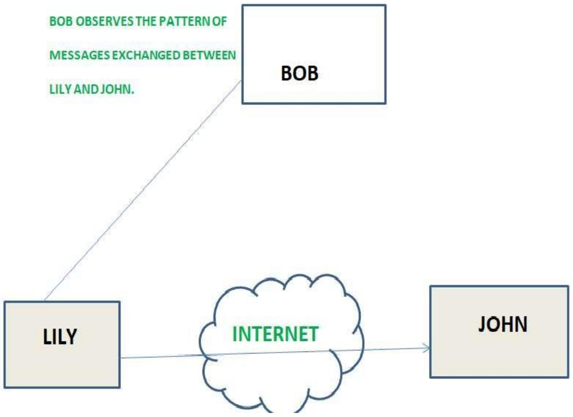


Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted.

Types of Passive attacks are as following:

1. **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 an opponent from learning the contents of these transmissions.
2. **Traffic analysis –** Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message. The opponent 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.





Cybercrime prevention methods

1. **Use Strong Passwords -** Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.
2. **Secure your computer -**
   - **Activate your firewall -** Firewalls are the first line of cyber defence; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
   - **Use anti-virus/malware software -** Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
   - **Block spyware attacks -** Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.
3. **Be Social-Media Savvy -** Make sure your social networking profiles (e.g., Facebook, Twitter, YouTube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!
4. **Secure your Mobile Devices -** Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.
5. **Install the latest operating system updates -** Keep your applications and operating system (e.g. Windows, Mac, and Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.
6. **Protect your Data -** Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.
7. **Secure your wireless network -** Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.
8. **Protect your e-identity -** Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g., when making online purchases) or that you’ve enabled privacy settings (e.g. when accessing/using social networking sites).
9. **Avoid being scammed -** Always think before you click on a link or file of unknown origin. Don’t feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.
10. **Call the right person for help -** Don’t panic! If you are a victim, if you encounter illegal Internet content (e.g., child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

Application Security (Database, Email and Internet)

- Application security is the process of making apps more secure by finding, fixing, and enhancing the security of apps. In other words, it is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.
- It describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked. It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect apps after they get deployed.
- Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities. A router that prevents anyone from viewing a computer’s IP address from the Internet is a form of hardware application security. But security measures at the application level are also typically built into the software, such as an application firewall that strictly defines what activities are allowed and prohibited. Procedures can entail things like an application security routine that

includes protocols such as regular testing.

Application security tools

- **Static testing**, which analyses code at fixed points during its development. This is useful for developers to check their code as they are writing it to ensure that security issues are being introduced during development.
- **Dynamic testing**, which analyses running code. This is more useful, as it can simulate attacks on production systems and reveal more complex attack patterns that use a combination of systems.
- **Interactive testing,** which combines elements of both static and dynamic testing.
- **Mobile testing** is designed specifically for the mobile environments and can examine how an attacker can leverage the mobile OS and the apps running on them in its entirety.

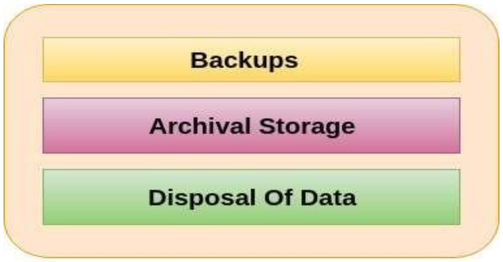
Types of application security

Different types of application security features include authentication, authorization, encryption, logging, and application security testing. Developers can also code applications to reduce security vulnerabilities.

1. **Authentication:** When software developers build procedures into an application to ensure that only authorized users gain access to it. Authentication procedures ensure that a user is who they say they are. This can be accomplished by requiring the user to provide a user name and password when logging in to an application. Multi-factor authentication requires more than one form of authentication—the factors might include something you know (a password), something you have (a mobile device), and something you are (a thumb print or facial recognition).
2. **Authorization:** After a user has been authenticated, the user may be authorized to access and use the application. The system can validate that a user has permission to access the application by comparing the user's identity with a list of authorized users. Authentication must happen before authorization so that the application matches only validated user credentials to the authorized user list.
3. **Encryption:** After a user has been authenticated and is using the application, other security measures can protect sensitive data from being seen or even used by a cybercriminal. In cloud-based applications, where traffic containing sensitive data travels between the end user and the cloud, that traffic can be encrypted to keep the data safe.
4. **Logging:** If there is a security breach in an application, logging can help identify who got access to the data and how. Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.
5. **Application security testing:** A necessary process to ensure that all of these security controls work properly.

Data Security Considerations – Backups

- Data security is the protection of programs and data in computers and communication systems against unauthorized access, modification, destruction, disclosure or transfer whether accidental or intentional by building physical arrangements and software checks.
- It refers to the right of individuals or organizations to deny or restrict the collection and use of information about unauthorized access. Data security requires system managers to reduce unauthorized access to the systems by building physical arrangements and software checks.



Data Security Consideration

Data security uses various methods to make sure that the data is correct, original, kept confidentially and is safe. It includes-

- Ensuring the integrity of data.
- Ensuring the privacy of the data.
- Prevent the loss or destruction of data.

Data security consideration involves the protection of data against unauthorized access, modification, destruction, loss, disclosure or transfer whether accidental or intentional. Some of the important data security considerations are described below:

Backups

Data backup refers to save additional copies of our data in separate physical or cloud locations from data files in storage. It is essential for us to keep secure, store, and backup our data on a regular basis.

Securing of the data will help us to prevent from-

- Accidental or malicious damage/modification to data.
- Theft of valuable information.
- Breach of confidentiality agreements and privacy laws.
- Premature release of data which can avoid intellectual properties claims.
- Release before data have been checked for authenticity and accuracy.

Keeping reliable and regular backups of our data protects against the risk of damage or loss due to power failure, hardware failure, software or media faults, viruses or hacking, or even human errors.
To use the Backup 3-2-1 Rule is very popular. This rule includes:

- Three copies of our data
- Two different formats, i.e., hard drive+tape backup or DVD (short term)+flash drive
- One off-site backup, i.e., have two physical backups and one in the cloud

Some important backup options are as follows-

1. Hard drives - personal or work computer
2. Departmental or institution server
3. External hard drives
4. Tape backups
5. Discipline-specific repositories
6. University Archives
7. Cloud storage

Some of the top considerations for implementing secure backup and recovery are-

1. Authentication of the users and backup clients to the backup server.
2. Role-based access control lists for all backup and recovery operations.
3. Data encryption options for both transmission and the storage.
4. Flexibility in choosing encryption and authentication algorithms.
5. Backup of a remote client to the centralized location behind firewalls.
6. Backup and recovery of a client running Security-Enhanced Linux (SELinux).
7. Using best practices to write secure software.

Archival Storage

- Data archiving is the process of retaining or keeping of data at a secure place for long-term storage.
- The data might be stored in safe locations so that it can be used whenever it is required.

- The archive data is still essential to the organization and may be needed for future reference.
- Also, data archives are indexed and have search capabilities so that the files and parts of files can be easily located and retrieved.
- The Data archival serve as a way of reducing primary storage consumption of data and its related costs.
- Data archival is different from data backup in the sense that data backups created copies of data and used as a data recovery mechanism to restore data in the event when it is corrupted or destroyed. On the other hand, data archives protect the older information that is not needed in day-to-day operations but may have to be accessed occasionally.

Data archives may have many different forms. It can be stored as Online, offline, or cloud storage-

- Online data storage places archive data onto disk systems where it is readily accessible.
- Offline data storage places archive data onto the tape or other removable media using data archiving software. Because tape can be removed and consumes less power than disk systems.
- Cloud storage is also another possible archive target. For example, Amazon Glacier is designed for data archiving. Cloud storage is inexpensive, but its costs can grow over time as more data is added to the cloud archive.

The following list of considerations will help us to improve the long-term usefulness of our archives:

1. Storage medium
2. Storage device
3. Revisiting old archives
4. Data usability
5. Selective archiving
6. Space considerations
7. Online vs. offline storage

Storage medium - The first thing is to what storage medium we use for archives. The archived data will be stored for long periods of time, so we must need to choose the type of media that will be lost as long as our retention policy dictates.

Storage device - This consideration takes into account about the storage device we are using for our archives which will be accessible in a few years. There is no way to predict which types of storage devices will stand the best. So, it is essential to try to pick those devices that have the best chance of being supported over the long term.

Revisiting old archives - Since we know our archive policies and the storage mechanisms we use for archiving data would change over time. So we have to review our archived data at least once a year to see that if anything needs to be migrated into a different storage medium.
For example, about ten years ago, we used Zip drives for archival then we had transferred all of my archives to CD. But in today's, we store most of our archives on DVD. Since modern DVD drives can also read CDs, so we haven't needed to move our extremely old archives off CD onto DVD.

Data usability - In this consideration, we have seen one major problem in the real world is archived data which is in an obsolete format.
For example, a few years ago, document files that had been archived in the early 1990s were created by an application known as PFS Write. The PFS Write file format was supported in the late 80s and early 90s, but today, there are not any applications that can read that files. To avoid this situation, it might be helpful to archive not only the data but also copies the installation media for the applications that created the data.

Selective archiving - In this consideration, we have to sure about what should be archived. That means we will archive only a selective part of data because not all data is equally important.

Space considerations - If our archives become huge, we must plan for the long-term retention of all our data. If we are archiving our data to removable media, capacity planning might be simple which makes sure that there is a free space in the vault to hold all of those tapes, and it makes sure that there is a room in our IT budget to continue purchasing tapes.

Online vs. offline storage - In this consideration, we have to decide whether to store our archives online (on a dedicated archive server) or offline (on removable media). Both methods of archival contain advantages and disadvantages. Storing of data online keeps the data easily accessible. But keeping data online may be vulnerable to theft, tampering, corruption, etc. Offline storage enables us to store an unlimited amount of data, but it is not readily accessible.

Disposal of Data

- Data destruction or disposal of data is the method of destroying data which is stored on tapes, hard disks and other electronic media so that it is completely unreadable, unusable and inaccessible for unauthorized purposes.
- It also ensures that the organization retains records of data for as long as they are needed.
- When it is no longer required, appropriately destroys them or disposes of that data in some other way, for example, by transfer to an archives service.

The managed process of data disposal has some essential benefits-

- It avoids the unnecessary storage costs incurred by using office or server space in maintaining records which is no longer needed by the organization.
- Finding and retrieving information is easier and quicker because there is less to search.

The disposal of data usually takes place as part of the normal records management process. There are two essential circumstances in which the destruction of data needs to be handled as an addition to this process-

- The quantity of a legacy record requires attention.
- The functions are being transferred to another authority and disposal of data records becomes part of the change process.

The following list of considerations will help us for the secure disposal of data-

1. Eliminate access
2. Destroy the data
3. Destroy the device
4. Keep the record of which systems have been decommissioned
5. Keep careful records
6. Eliminate potential clues
7. Keep systems secure until disposal

Eliminate access - In this consideration, we have to ensure that eliminating access account does not have any rights to re access the disposed of data again.

Destroy the Data - In this consideration, there is not necessary to remove data from storage media will be safe. Even these days reformatting or repartitioning a drive to "erase" the data that it stores is not good enough. Today's many tools available which can help us to delete files more securely. To encrypt the data on the drive before performing any deletion can help us to make data more difficult to recover later.

Destroy the device - In the most cases, storage media need to be physically destroyed to ensure that our sensitive data is not leaked to whoever gets the drives next. In such cases, we should not destroy them itself.

To do this, there should be experts who can make probably a lot better at safely and effectively rendering any data on our drives unrecoverable. If we can't trust this to an outsider agency that specializes in the secure destruction of storage devices, we should have a specialized team within our organization who has the same equipment and skills as outside contractors.

Keep the record of which systems have been decommissioned - In this, we have to make sure that the storage media has been fully decommissioned securely and they do not consist of something easily misplaced or overlooked. It is best if storage media that have not been fully decommissioned are kept in a specific location, while decommissioned equipment placed somewhere else so that it will help us to avoid making mistakes.

Keep careful records - In this consideration, it is necessary to keep the record of whoever is responsible for decommissioning a storage media. If more than one person is assigned for such responsibility, he should sign off after the completion of the decommissioning process. So that, if something happened wrong, we know who to talk to find out what happened and how bad the mistake is.

Eliminate potential clues - In this consideration, we have to clear the configuration settings from networking equipment. We do this because it can provide crucial clues to a security cracker to break into our network and the systems that reside on it.

Keep system secure until disposal of data - In this consideration, we should have to make clear guidelines for who should have access to the equipment in need of secure disposal. It will be better to ensure that nobody should have access authentication to it before disposal of data won't get his or her hands on it.

Security Technology – Firewall and VPNs

Firewall - A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization’s previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall’s main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Types of Firewalls

- **Packet filtering -** A small amount of data is analyzed and distributed according to the filter’s standards.
- **Proxy service -** Network security system that protects while filtering messages at the application layer.
- **Stateful inspection -** Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW) -** Deep packet inspection Firewall with application-level inspection.

Work of Firewall

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

Need of Firewall

Firewalls, especially Next Generation Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you're setting up your network with specific policies to allow or block incoming and outgoing traffic.

VPNs - A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

Working of VPN

When you connect your computer (or another device, such as a smartphone or tablet) to a VPN, the computer acts as if it's on the same local network as the VPN. All your network traffic is sent over a secure connection to the VPN. Because your computer behaves as if it's on the network, this allows you to securely access local network resources even when you're on the other side of the world. You'll also be able to use the Internet as if you were present at the VPN's location, which has some benefits if you're using pubic Wi-Fi or want to access geo-blocked websites.

When you browse the web while connected to a VPN, your computer contacts the website through the encrypted VPN connection. The VPN forwards the request for you and forwards the response from the website back through the secure connection. If you're using a USA-based VPN to access Netflix, Netflix will see your connection as coming from within the USA.

Types of VPNs

- **Remote access -** A remote access VPN securely connects a device outside the corporate office. These devices are known as endpoints and may be laptops, tablets, or smartphones. Advances in VPN technology have allowed security checks to be conducted on endpoints to make sure they meet a certain posture before connecting. Think of remote access as computer to network.
- **Site-to-site** - A site-to-site VPN connects the corporate office to branch offices over the Internet. Site-to-site VPNs are used when distance makes it impractical to have direct network connections between these offices. Dedicated equipment is used to establish and maintain a connection. Think of site-to-site access as network to network.

Uses of VPN

VPNs are a fairly simple tool, but they can be used to do a wide variety of things:

- Access a Business Network While Traveling
- Access Your Home Network While Travelling
- Hide Your Browsing Activity From Your Local Network and ISP
- Access Geo-Blocked Websites
- Bypass Internet Censorship
- Downloading Files

Intrusion Detections

Intrusion Detection System - is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying cracking the firewall.
2. **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.
3. **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
4. **Application Protocol-based Intrusion Detection System (APIDS):** Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.
5. **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. **Signature-based Method:** Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

   Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.
2. **Anomaly-based Method:** Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Access Control

Access control is a method of restricting access to sensitive data. Only those that have had their identity verified can access company data through an access control gateway.

Components of Access control –

At a high level, access control is about restricting access to a resource. Any access control system, whether physical or logical, has five main components:

1. **Authentication:** The act of proving an assertion, such as the identity of a person or computer user. It might involve validating personal identity documents, verifying the authenticity of a website with a digital certificate, or checking login credentials against stored details.
2. **Authorization:** The function of specifying access rights or privileges to resources. For example, human resources staff are normally authorized to access employee records and this policy is usually formalized as access control rules in a computer system.
3. **Access:** Once authenticated and authorized, the person or computer can access the resource.
4. **Manage:** Managing an access control system includes adding and removing authentication and authorization of users or systems. Some systems will sync with G Suite or Azure Active Directory, streamlining the management process.
5. **Audit:** Frequently used as part of access control to enforce the principle of least privilege. Over time, users can end up with access they no longer need, e.g., when they change roles. Regular audits minimize this risk.

Types of Access Control

Access control can be split into two groups designed to improve physical security or cyber security:

- **Physical access control:** limits access to campuses, building and other physical assets, e.g., a proximity card to unlock a door.
- **Logical access control:** limits access to computers, networks, files and other sensitive data, e.g., a username and password.

Access control Models

The main models of access control are:

- **Attribute-based Access Control (ABAC):** In this model, access is granted or declined by evaluating a set of rules, policies, and relationships using the attributes of users, systems and environmental conditions.
- **Discretionary Access Control (DAC):** In DAC, the owner of data determines who can access specific resources.
- **History-Based Access Control (HBAC):** Access is granted or declined by evaluating the history of activities of the inquiring party that includes behavior, the time between requests and content of requests.
- **Identity-Based Access Control (IBAC):** By using this model network administrators can more effectively manage activity and access based on individual requirements.
- **Mandatory Access Control (MAC):** A control model in which access rights are regulated by a central authority based on multiple levels of security. Security Enhanced Linux is implemented using MAC on the Linux operating system.
- **Organization-Based Access control (OrBAC):** This model allows the policy designer to define a security policy independently of the implementation.
- **Role-Based Access Control (RBAC):** RBAC allows access based on the job title. RBAC eliminates discretion on a large scale when providing access to objects. For example, there should not be permissions for human resources specialist to create network accounts.
- **Rule-Based Access Control (RAC):** RAC method is largely context based. Example of this would be only allowing students to use the labs during a certain time of day.

Hardware Protection Mechanisms

A computer contains various hardware like processor, RAM, monitor etc. So, OS must ensure that these devices remain intact (not directly accessible by the user).

Types –

1. **CPU Protection:** CPU protection is referred to as we cannot give CPU to a process forever, it should be for some limited time otherwise other processes will not get the chance to execute the process. So, for that, a timer is used to get over from this situation. which is basically give a certain amount of time a process and after the timer execution a signal will be sent to the process to leave the CPU. Hence process will not hold CPU for more time.
2. **Memory Protection:** In memory protection, we are talking about that situation when two or more processes are in memory and one process may access the other process memory. and to protecting this situation we are using two registers as:
   1. Bare register
   2. Limit register
   So basically, Base register store the starting address of program and limit register store the size of the process, so when a process wants to access the memory then it is checked that it can access or cannot access the memory.
3. **I/O Protection:** So when we ensuring the I/O protection then some cases will never have occurred in the system as:
   1. Termination I/O of other process
   2. View I/O of other process
   3. Giving priority to a particular process I/O

   If an application process wants to access any I/O device then it will be done through system call so that OS will monitor the task.
   Like In C language write () and read () is a system call to read and write on file. There are two modes in instruction execute:
   - **User mode -** The system performs a task on behalf of user application this instruction. In this mode, the user cannot directly access hardware and reference memory.
   - **Kernel mode -** Whenever a direct access to hardware is required a system call is used by the application program.

We know that when an application process wants to access any I/O device it should be done through system call so that the Operating system will monitor the task.

OS Security

- Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.
- OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions.
- Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system.
- If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So, a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc.
- OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.
- OS security may be approached in many ways, including adherence to the following:
  - Performing regular OS patch updates
  - Installing updated antivirus engines and software
  - Scrutinizing all incoming and outgoing network traffic through a firewall
  - Creating secure accounts with required privileges only (i.e., user management)

Ways to achieve OS security –
Authentication - Authentication refers to identifying each user of the system and associating the executing

programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways −

- **Username / Password** − User need to enter a registered username and password with Operating system to login into the system.
- **User card/key** − User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
- **User attribute - fingerprint/ eye retina pattern/ signature** − User need to pass his/her attribute via designated input device used by operating system to login into the system.

One Time passwords - One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password are implemented in various ways.

- **Random numbers** − Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.
- **Secret key** − User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.
- **Network password** − Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

Program Threats - Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as **Program Threats**. One of the common examples of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. E.g. Trojan horse, Trap door, Logic bomb, Virus, etc.

System Threats - System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats create such an environment that operating system resources/ user files are misused. E.g. worm, port scanning, DoS, etc.

Digital Forensics

- Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law.
- It is a science of finding evidence from digital media like a computer, mobile phone, server, or network.
- It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.
- Digital Forensics helps the forensic team to analyses, inspects, identifies, and preserves the digitalevidence residing on various types of electronic devices.

Types of Digital Forensics

The types of digital forensics are:

- **Disk Forensics:** It deals with extracting data from storage media by searching active, modified, or deleted files.
- **Network Forensics:** It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.
- **Wireless Forensics:** It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyze the data from wireless network traffic.
- **Database Forensics:** It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

- **Malware Forensics:** This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.
- **Email Forensics:** Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.
- **Memory Forensics:** It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.
- **Mobile Phone Forensics:** It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Advantages of Digital forensics

Here, are pros/benefits of Digital forensics

- To ensure the integrity of the computer system.
- To produce evidence in the court, this can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows extracting, process, and interpreting the factual evidence, so it proves the cybercriminal action's inthe court.

Disadvantages of Digital Forensics

Here, are major cause/ drawbacks of using Digital Forensic

- Digital evidence accepted into court. However, it is must be proved that there is no tampering
- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result

Example Uses of Digital Forensics

In recent time, commercial organizations have used digital forensics in following a type of cases:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

Historical Background of Digital Forensics

Here, are important landmarks from the history of Digital Forensics:

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1982 - 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.

- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
- In 2010, Simson Garfinkel identified issues facing digital investigations.

It is difficult to pinpoint when computer forensics history began. Most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field has exploded. Law enforcement and the military continue to have a large presence in the information security and computer forensic field at the local, state, and federal level. Private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such professionals or firms on an as-needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e-discovery field.

The computer forensic field continues to grow on a daily basis. More and more large forensic firms, boutique firms, and private investigators are gaining knowledge and experience in the field. Software companies continue to produce newer and more robust forensic software programs. And law enforcement and the military continue to identify and train more and more of their personnel in the response to crimes involving technology.

Forensic Software and Hardware

Evidence is an important factor in any investigations. Forensics investigations rely on this method. The evidence will prove vital for the success of investigation. Data or information should be communicated accurately in an investigation. Computer forensics depends on evidence in the form of bits and bytes for a case analysis. The bits and bytes reside on the storage medium of a digital device. Devices come in a variety of formats as PCs, Servers, Mobile Phones, Sim Cards, Memory Cards, iPods, Routers and more to come. Forensic experts always look on the data as a vital part in their analysis. In essence the data should be identified and reproduced with zero percentage of error.

Two methods are widely adopted in acquiring data from a digital device.

1. Software Methods
2. Hardware Methods

Both the methods are interdependent and a clear-cut classification is not possible. The following discusses the software forensic and the different hardware forensics techniques in use and the theory underlying it.

Software forensics is the science of analyzing software source code or binary code to determine whether intellectual property infringement or theft occurred. It is the centerpiece of lawsuits, trials, and settlements when companies are in dispute over issues involving software patents, copyrights, and trade secrets. Software forensics tools can compare code to determine correlation, a measure that can be used to guide a software forensics expert.

Hardware Forensics

- **Rule of forensics -** The golden rule of forensics states that we cannot work on the suspect device. It should be copied and any analysis should be done on the copy of the original one. The data should be copied at the earliest. There should not be any tampering of the suspect device. Hence design of any forensic tool should take into consideration these factors.

- **A Drive Lock Scenario -** An important requirement in forensics is a drive lock. This device should lock the suspect drive as to avoid any contamination of data. Software locking is possible by blocking any write operations. This requires a PC or a laptop running the software to be carried along with the investigator every time. An improper functioning of the software can cause difficulty in acquiring. Hardware methods that substitute the software techniques will be compact and easy to use. The device will be powered from the source or from the suspect machine itself. The hardware into the development should have all possible connectors available.

- **Hard Disk Scenario -** Acquiring a hard disk using software methods depend on a software running on a PC. The computation speed of the device depends on the processing capability of the processor. The acquiring of an 80 GB hard disk takes roughly 4 hours. The processing capacity of processors has increased with shrinkage in sizes. This can be taken into advantage for the design of speedy acquisition devices. A portable unit would be a better ease to the investigator. So, development of an embedded acquisition device will be an advantage in time and cost for the investigator.

- **Sim Card scenario -** GSM Mobile phones use Sim Cards as an important agent in connecting to the network. Details on the network and connections can be obtained from the Sim Card. There need to be device to read out the details in the Sim Card. This requires a combination of hardware and software. Sim Card details should be also copied and replicated further for analysis.

Advantages of hardware tools in forensics

1. Embedded development is done which saves the space and time.
2. The products will be portable.
3. Speedy acquisition of digital data’s can be done.

Need of Computer Forensic Science

Here are the essential objectives of using Computer forensics:

- It helps to recover, analyses, and preserve computer and related materials in such a manner that it helpsthe investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

Special tools and techniques

Tools – There are very many free and paid for digital forensic tools. Some of them are extensive collections of utility programs that can help with various stages of the forensic process. Examples include EnCase, CAINE (Computer Aided Investigative Environment), X-Ways Forensics, SANS Investigative Forensics Toolkit (SIFT), Computer Online Forensics Evidence Extractor (COFEE), The Coroner's Toolkit and many more.

Although forensic tools vary according to the phase of the investigation for which they are being used, good tools share some common features.

- Include an acquisition feature that allows the data to be gathered.
- Enables searching and filtering of files
- Can provide exact pathway locators to find the exact position of data.

- Full disk hashing to confirm the data hasn't changed
- Can reveal exact time and data stamps of when files were created, stored and last looked at.
- Can work with backup files and extract data

Techniques – The aims of the forensic process are to preserve the evidence; then to use the forensic tools look at the acquired data for things that may have been deleted, hidden or unusual.

Different techniques or methods for this kind of forensic work can be used at different stages of the investigative process.

- **Preserving the evidence**: Making an image (an exact copy) of the original data with the use of a **'write blocker'** - write blocker prevents any program or device making changes to the original data. Typical tools include Forensic Toolkit (FTK), Encase, SIFT, Coroner's toolkit, Sleuth Kit
- Using the *method* of **Forensic Duplication** by recovering deleted files: Getting back files which might have been to deleted to hide evidence. Typical tools FTK, Encase, SIFT, Coroner's toolkit, Sleuth Kit
- **Removing Files:** Most files on devices are harmless with known file types and names. One technique is to filter out or remove these files to leave only those worthy of investigation. The *method* used here is to **compare md5 hashes** of files to a list of known md5 hashes of known files. If they match, they can be removed. FTK or Encase are popular tools.
- **File signature verification.** Works similar to raw above. A comparison is made between the header and footer information of suspect files with those of known files. Matching files can be safely removed. Sleuth Kit, Encase or a written Perl script.
- **String searching** and looking for file fragments: Using the search command to look for keywords or known text. FTK, Encase
- **Web activity reconstruction:** Getting back web browsing history, accepted cookies and temporary internet files that where the user has been removing opportunities for deniability. Encase, FTK, Browser logs
- **Email activity reconstruction:** Using the *method* of converting email repositories to readable text FTK, Parabens Network Mail Examiner
- **Registry activity reconstruction:** Discovering any deleted programmes or recent activity by looking at Windows system and application log files. FTK, RegEdit
- **Live forensics:** Using the method of analysing volatile processes; those files that are loaded in and out of memory. Windows Forensic Toolchest, COFEE
- **Recovering hidden files:** Actively looking for hidden files or hidden data (stenography) and attempting to gain access through the **methods** of **Decryption and Cryptanalysis.** Steg Break, Steg detect, Password Cracking and Frequency analysis.

Digital Forensic life cycle

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation

Identification - It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

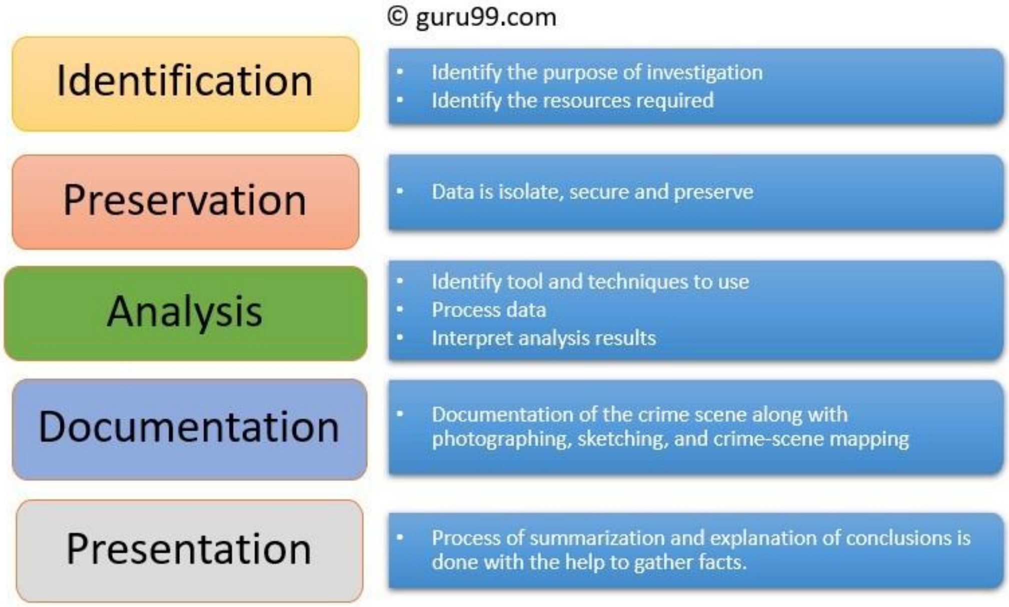
Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

Preservation - In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

Analysis - In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

Documentation - In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Presentation - In this last step, the process of summarization and explanation of conclusions is done. However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.


© guru99.com
Identification
Identify the purpose of investigation
Identify the resources required
Preservation
Data is isolate, secure and preserve
Analysis
Identify tool and techniques to use
Process data
Interpret analysis results
Documentation
Documentation of the crime scene along with photographing, sketching, and crime-scene mapping
Presentation
Process of summarization and explanation of conclusions is done with the help to gather facts.

Process of Digital Forensics

Challenges faced by Digital Forensics

Here, are major challenges faced by the Digital Forensic:

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

Digital forensic challenges are categorized into three major heads:

- Technical challenges
- Legal challenges
- Resource Challenges

TECHNICAL CHALLENGES

As technology develops crimes and criminals are also developed with it. Digital forensic experts use forensic tools for collecting shreds of evidence against criminals and criminals use such tools for hiding, altering or removing the traces of their crime, in digital forensic this process is called Anti- forensics technique which is considered as a major challenge in digital forensics world.

Anti-forensics techniques are categorized into the following types:

S. No.	Type	Description
1	Encryption	It is legitimately used for ensuring the privacy of information by keeping it hidden from an unauthorized user/person. Unfortunately, it can also be used by criminals to hide their crimes.

2	Data hiding in storage space	Criminals usually hide chunks of data inside the storage medium in invisible form by using system commands, and programs.
3	Covert Channel	A covert channel is a communication protocol which allows an attacker to bypass intrusion detection technique and hide data over the network. The attacker used it for hiding the connection between him and the compromised system.

Other Technical challenges are:

- Operating in the cloud
- Time to archive data
- Skill gap
- Steganography

Legal Challenges

The presentation of digital evidence is more difficult than its collection because there are many instances where the legal framework acquires a soft approach and does not recognize every aspect of cyber forensics, as in Jagdeo Singh V. The State and Ors, case Hon'ble High Court of Delhi held that "while dealing with the admissibility of an intercepted telephone call in a CD and CDR which was without a certificate under Sec. 65B of the Indian Evidence Act, 1872 the court observed that the secondary electronic evidence without certificate u/s. 65B of Indian Evidence Act, 1872 is not admissible and cannot be looked into by the court for any purpose whatsoever." This happens in most of the cases as the cyber police lack the necessary qualification and ability to identify a possible source of evidence and prove it. Besides, most of the time electronic evidence is challenged in the court due to its integrity. In the absence of proper guidelines and the nonexistence of proper explanation of the collection, and acquisition of electronic evidence gets dismissed in itself.

Legal Challenges		
S. no	**Type**	**Description**
1	Absence of guidelines and standards	In India, there are no proper guidelines for the collection and acquisition of digital evidence. The investigating agencies and forensic laboratories are working on the guidelines of their own. Due to this, the potential of digital evidence has been destroyed.
2	Limitation of the Indian Evidence Act, 1872	The Indian Evidence Act, 1872 have limited approach, it is not able to evolve with the time and address the E-evidence are more susceptible to tampering, alteration, transposition, etc. the Act is silent on the method of collection of e-evidence it only focuses on the presentation of electronic evidence in the court by accompanying a certificate as per subsection 4 of Sec. 65B. This means no matter what procedure is followed it must be proved with the help of a certificate.

Other Legal Challenges

- Privacy Issues
- Admissibility in Courts
- Preservation of electronic evidence
- Power for gathering digital evidence
- Analyzing a running computer

Resource Challenges

As the rate of crime increases the number of data increases and the burden to analyze such huge data is also increasing on a digital forensic expert because digital evidence is more sensitive as compared to physical evidence it can easily disappear. For making the investigation process fast and useful forensic experts use various tools to check the authenticity of the data but dealing with these tools is also a challenge in itself.

Types of Resource Challenges are:

- **Change in technology -** Due to rapid change in technology like operating systems, application software and hardware, reading of digital evidence becoming more difficult because new version software's are not supported to an older version and the software developing companies did provide any backward compatible's which also affects legally.
- **Volume and replication -** The confidentiality, availability, and integrity of electronic documents are easily get manipulated. The combination of wide-area networks and the internet form a big network that allows flowing data beyond the physical boundaries. Such easiness of communication and availability of electronic document increases the volume of data which also create difficulty in the identification of original and relevant data.

Why do we need Cyber Laws?

Cyber law is like any other legal rule or policy that should be followed in our day-to-day life to stay out of any kind of trouble. These laws are formed by keeping several issues into consideration such as our society, morals, **computer ethics**, etc. The only difference is that cyber law is applied to the internet and internet-related technologies only. Cyber law is formed to maintain discipline and justice in the cyber world. This area in the legal system is introduced because the crime related to computers and other technology was increasing rapidly. These types of crimes were not falling under the category of any existing legal category therefore a separate section was formed named Cyber Law.

Cyber law provides legal protections to people using the internet including both businesses and regular citizens. It is important for anyone using the internet to be aware of the cyber laws of their country and local area so that, they know what activity is legal online and what is not. Also, if anything happens with them online, they know how they can act regarding that matter accordingly.

Areas Encompassing in Cyber Laws

These laws cover many areas & activities occurring online and serve a variety of purposes. Some laws are formed to protect to defend people online from malicious activities, some laws explain the policies if using computers and the internet in a company. All these wide categories fall under the cyber laws. Some of the wide range areas encompassing the cyber laws are:

- **Scam/ Treachery -** Cyber laws exist to protect people from online frauds and scams, these laws prevent any financial crimes and identity theft that happen online.
- **Copyrighting Issues -** The Internet is the source of multiple types of content, but it is not right to copy the hard work of any other person. There are strict policies in cyber laws against copyright that protects the creative work of companies and individuals.
- **Online Insults and Character Degradation -** Online platforms like social media are the best platform to speak your mind freely but there is a thin line between the liberation of using the right to speak and defaming someone online. Cyber laws address issues like online insults, racism, gender targets to protect a person's reputation.
- **Online Harassment and Stalking -** Harassment is a violation of both civil and criminal laws. This crime is a major issue in cyberspace. The legal system has some strict laws to prohibit these despicable crimes.
- **Data Protection -** People using the internet risk their privacy while being online and often rely on cyber laws and policies to protect their secrets. Also, companies should maintain the confidentiality of data of their users.

Importance of Cyber Laws

- Cyber laws are important to punish criminals who commit serious crimes related to the computer such as hacking, online harassment, data theft, disrupting the online workflow of any enterprise, attacking another individual or website.

- Cyber laws decide different forms of punishment depending on the type of law you broke, who you offended, where you violated the law, and where you live.
- It is important to bring criminal behind the bars, as most cybercrimes do not enter the category of common crime and it may lead to denial of justice.
- These crimes may endanger the confidentiality and financial security of a nation therefore these problems should be addressed lawfully.

Conclusion

Implementing laws in cyberspace is an important step to create a safe and secure environment for people on cyber platforms. To protect from cybercrimes, computer forensic science should focus on **ethical hacking training** and implementing cyber security plans addressing people, process, and technology issues arise nowadays. Strict cyber laws are the need of this era where technology is growing at rapid speed because the budgets have not been increased to keep up with this rate of change in technology.

The Indian IT Act

The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.

The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from ‘section 91 – section 94’, deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

- **First Schedule –** Deals with documents to which the Act shall not apply.
- **Second Schedule –** Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000:

The offences and the punishments that falls under the IT Act, 2000 are as follows:

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows:

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from

	owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years' imprisonment or the fine of Rs.5, 00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years' imprisonment or Rs. 1, 00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years' imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine or Rs. 10,00,000 or both.

Cybercrime scenario in India

The cybercrime scenario in our country does not truly reflect the existing situation on the ground. According to the National Crime Records Bureau (NCRB), in 2016 a total of 12,187 cybercrime cases were registered all over India when compared to 11,331 cases registered in 2015. There was 20.50 per cent increase in the number of cybercrime cases in 2015 over 2014 and 6.3 per cent increase in cases in 2016 over 2015.

As far as the number of cybercrime cases is concerned, Uttar Pradesh with a figure of 2,639 registered the maximum number of cases followed by Maharashtra (2380), and Karnataka (1101). Among the Metropolitan cities, Mumbai with 980 cases stood first followed by Bengaluru 762 and Jaipur 532. Chennai city with 26 cases was ranked 16 among metros.

Social media seems to have turned antisocial at the hands of rumour mongers with more than 20 cases of lynching being reported in the last two months in our country. The advent of social media appears to have added fuel to the existing fire, by helping organizers and opposition parties' congregate multitudes swiftly, easily, cheaply and efficiently —whether it be for a cause like Jallikattu or for spreading the message of revolt against the policies of the establishment.

Quite obviously, social media played a crucial role in mobilizing and engineering some of the major agitations like the Cauvery river dispute.

If we decide to not give a damn to cyber criminals, we would be doing so at our own peril. We should not forget the kind of havoc the ill-gotten gains of cybercrime wreaked on the city of Mumbai in 2008 during the terrorist siege by Lashkar-e-Taiba (LeT). The entire operation was funded by a Filipino hacking cell workingon behalf of Jamaah Islamiyah an associate of Al-Quaeda. Millions of dollars ripped off by the cybercriminals recruited by it were channelled to their manipulators in Saudi Arabia who in turn laundered the funds to the Lashkar-e-Taiba team in Pakistan, which executed the brutal onslaught against the City of Mumbai.

The situation today is that there are several laws protect cybercrime each one having its own scope and limitations. India is no doubt imposing sanctions to deal with such crimes. However, the conviction rate is found to be insignificant. However, what is needed a specific law particularly dealing with cybercrimes. Just like what UK did in 1990, when it enacted the Computer Misuse Act 1990.

Digital Signature and the Indian IT Act

The advent of information technology revolutionized the whole world and fortunately India led a leading role and captured global attention. India passed Information technology Act 2000 (The Act) which came into force on 17-10-2000. The Act applies to the whole of India and even to persons who commit offence outside India. The Act validates "DIGITAL SIGNATURE" and provides for enabling a person to use it just like thetraditional signature. The basic purpose of digital signature is not different from our conventional signature. The purpose therefore is to authenticate the document, to identify the person and to make the contents of the document binding on person putting digital signature. Let us see what digital signature is in technical terms.

A digital signature or digital signature schemeis a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are based on public key encryption. It uses prime numbers like 2,3.5.7,9,11 and so on which can be divided only by itself or by 1 and is incapable of division by other numbers. We have unlimited prime numbers and in DS we use the multiples of prime numbers.

The functioning of DS is based on the system of public key cryptography. Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plain text, and the other unlocks or decrypts the cipher text. Neither key can perform both functions. One of these keys is published or public, while the other is kept private.

"Key encryption allows more than just privacy. It can also assure the recipient of the authenticity of a document because a private key can be used to encode a message that only a public key can decode. If I have information I want to sign before sending it to you, my computer uses my private key to encipher it. Now the message can be read only if my public key-which you and everyone else know-is used to decipher it. This message is veritably from me because no one else has the private key that could have encrypted it in this way".

Justice Yatindra Singh in his book "Cyber laws" has stated that since public key encryption is slow and time consuming the hash function is used to transform a message into a unique shorter fixed length value called the Hash result. Hash serves the purpose of an index of the original text. It is an algorithm mapping or translation of one sequence into another. The hash function is such that the same hash result is obtained every time that hash function is used on the same electronic record and two electronic records cannot produce the same hash result using the same hash function. In other words, mapping is one to one and not many to one. It is one way. One cannot reconstruct the original message from the hash result. The encryption of a hash result of the message with the private key of the sender is called a Digital signature.

Cybercrimes and Punishment

Apart from punishments in IT Act, 2000, there are certain crimes that are attracted by IPC provisions as well. The following is the enumeration of the IPC provisions along with various cybercrimes that are attracted by respective Sections and the punishment for the same.

- **Section 292 of IPC:** Although this Section was drafted to deal with the sale of obscene material, it has evolved in the current digital era to be concerned with various cybercrimes. The publication and transmission of obscene material or sexually explicit act or exploit acts containing children, etc which are in electronic form are also governed by this section. Though the crimes mentioned above seem to be alike, they are recognized as different crimes by the IT Act and IPC. The punishment imposed upon the commission of such acts is imprisonment and fine up to 2 years and Rs. 2000. If any of the aforementioned crimes are committed for the second time, the imprisonment could be up to 5 years and the fine could be imposed up to Rs. 5000.
- **Section 354C of IPC:** The cybercrime dealt with under this provision is capturing or publication of a

picture of private parts or acts of a woman without such person's consent. This section exclusively deals with the crime of 'voyeurism' which also recognizes watching such acts of a woman as a crime. If the essentials of this Section (such as gender) are not satisfied, Section 292 of IPC and Section 66E of IT Act, 2000 is broad enough to take the offenses of a similar kind into consideration. The punishment includes 1 to 3 years of imprisonment for first-time offenders and 3 to 7 years for second-time offenders.

- **Section 354D of IPC:** This section describes and punishes 'stalking' including both physical and cyber stalking. If the woman is being monitored through electronic communication, internet, or email or is being bothered by a person to interact or contact despite her disinterest, it amounts to cyber-stalking. The latter part of the Section states the punishment for this offense as imprisonment extending up to 3 years for the first time and 5 years for the second time along with a fine imposed in both the instances. In the case of Kalandi Charan Lenka v. The State of Odisha, the victim received certain obscene messages from an unknown number which are damaging her character. Moreover, emails were sent and the fake Facebook account was created by the accused which contained morphed pictures of the victim. Hence, the accused was found prima facie guilty for cyberstalking by the High Court under various provisions of IT Act and Section 354D of IPC
- **Section 379 of IPC:** If a mobile phone, the data from that mobile or the computer hardware is stolen, Section 379 comes into the picture and the punishment for such crime can go up to 3 years of imprisonment or fine or both. But the attention must be given to the fact that these provisions cannot be applied in case the special law i.e IT Act, 2000 provisions are attracted. In this regard, in the case of Gagan Harsh Sharma v. The State of Maharashtra, one of the employers found that the software and data were stolen and someone has breached the computers and gave access to sensitive information to the employees. The employer gave information to the police and they filed a case under Section 379, 408, and Section 420 of IPC and various other IT Act provisions. The question in front of the court is whether the police can file a case under IPC or not. The court decided that the case cannot be filed based on the IPC provisions as the IT Act has an overriding effect.
- **Section 411 of IPC:** These deals with a crime that follows the offenses committed and punished under Section 379. If anyone receives a stolen mobile phone, computer, or data from the same, they will be punished in accordance with Section 411 of IPC. It is not necessary that the thief must possess the material. Even if it is held by a third party knowing it to be others, this provision will be attracted. The punishment can be imposed in the form of imprisonment which can be extended up to 3 years or fine or both.
- **Section 419 and Section 420 of IPC:** These are related provisions as they deal with frauds. The crimes of password theft for the purpose of meeting fraudulent objectives or the creation of bogus websites and commission of cyber frauds are certain crimes that are extensively dealt with by these two sections of IPC. On the other hand, email phishing by assuming someone's identity demanding password is exclusively concerned with Section 419 of IPC. The punishments under these provisions are different based upon the gravity of the committed cybercrime. Section 419 carries a punishment up to 3 years of imprisonment or fine and Section 420 carries up to 7 years of imprisonment or fine.
- **Section 465 of IPC:** In the usual scenario, the punishment for forgery is dealt with in this provision. In cyberspace, the offenses like email spoofing and preparation of false documents are dealt with and punished under this Section which imbibes the imprisonment reaching up to 2 years or fine or both. In the case of Anil Kumar Srivastava v. Addl Director, MHFW, the petitioner electronically forged signature of AD and later filed a case making false allegations about the same person. The Court held that the petitioner was liable under Section 465 as well as under Section 471 of IPC as the petitioner also tried to use it as a genuine document.
- **Section 468 of IPC:** If the offenses of email spoofing or the online forgery are committed for the purpose of committing other serious offenses i.e cheating, Section 468 comes into the picture which contains the punishment of seven years of imprisonment or fine or both.
- **Section 469 of IPC:** If the forgery is committed by anyone solely for the purpose of disrupting a

particular person or knowing that such forgery harms the reputation of a person, either in the form of a physical document or through online, electronic forms, he/she can be imposed with the imprisonment up to three years as well as fine.

- **Section 500 of IPC:** This provision penalizes the defamation of any person. With respect to cybercrimes, sending any kind of defamatory content or abusive messages through email will be attracted by Section 500 of IPC. The imprisonment carried with this Section extends up to 2 years along with fine.
- **Section 504 of IPC:** If anyone threatens, insults, or tries to provoke another person with the intention of effecting peace through email or any other electronic form, it amounts to an offense under Section 504 of IPC. The punishment for this offense extends up to 2 years of imprisonment or fine or both.
- **Section 506 of IPC:** If a person tries to criminally intimidate another person either physically or through electronic means with respect to the life of a person, property destruction through fire or chastity of a woman, it will amount to an offense under Section 506 of IPC and punishment of imprisonment where the maximum period is extended up to seven years or fine or both.
- **Section 509 of IPC:** This Section deals with the offense of uttering a word, showing a gesture, and committing an act that has the potential to harm the modesty of a woman. It also includes the sounds made and the acts committed infringing the privacy of a woman. If this offense is committed either physically or through electronic modes, Section 509 gets attracted and the punishment would be imprisonment of a maximum period of one year or fine or both.