INTRODUCTION TO CYBER SECURITY, CYBER SECURITY VULNERABILITIES AND CYBER SECURITY SAFEGUARDS:

Introduction to Cyber Security: Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.

Cyber Security Vulnerabilities: Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness.

Cyber Security Safeguards: Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

Q) What is Cyber & CYBER SPACE ?

A) The term, **'Cyber'** is used in relation to the culture of computers, information technology, and virtual reality.

The connection between internet ecosystems forms **cyberspace**.

The threat to cyberspace leads to an issue and gives rise to the need for cybersecurity

The cyber attacks lead to the exposure of:

1. Sensitive information
2. Personal information and
3. Business information

Q) What is Cyber security?

A) Cyber Security is the practice of Protecting computers, mobile devices, Servers, electronic Systems, networks, and data from malicious attacks. It's also known as **Information Security** (INFOSEC) or **Information Assurance** (IA), System Security.

Cyber Security is important because the government, Corporate, medical organizations collect, military, financial, process, and store the unprecedented amount of data on a computer and other property, personal information, or exposure could have negative consequences.

Cyber Security proper began in 1972 with a research project on ARPANET (The Advanced Research Projects Agency Network), a precursor to the internet. ARPANET developed protocols for remote computer networking.

Example – If we shop from any online shopping website and shared information like email id, address, and credit card details as well as saved on that website to enable a faster and hassle-free shopping experience then the required information is stored in server one day we receive an email which state that the eligibility for a special discount voucher from XXXXX (hacker use famous website Name like Flipkart, Amazon etc.) website in order to receive the coupon code, and we will be asked to fill the details then we will use saved card account credentials. Then our data will be shared because we think it was just an account for the verification step then they can wipe a substantial amount of money from our account.

That is why Cyber Security provides Service as a Security Gate-Way to make information more Secure, in today's time hackers are advance we can't surely say the data store in my Devices is safe or not by outside threats. With Cybercrime increasing at a rapid pace, it's crucial to have Cyber Security in place of personal life and our Business.

Cyber Security – Evolution

With the introduction of cyberattacks, cybersecurity initiatives have evolved. They are mentioned in the table below:

Evolution of Cyber Security	
Issues	**Cyber Security Initiatives**
Virus (1990s)	• Anti-Virus • Firewalls
Worms (2000)	Intrusion Detection and Prevention
Botnets (2000s – Present)	DLP, Application-aware Firewalls, SIM
APT Insiders (Present)	Network Flow Analysis

CIA Triad

The security of any organization starts with three principles: Confidentiality, Integrity, Availability. we will learn about the CIA Triad, which has served as the industry standard for computer security since the time of first mainframes.

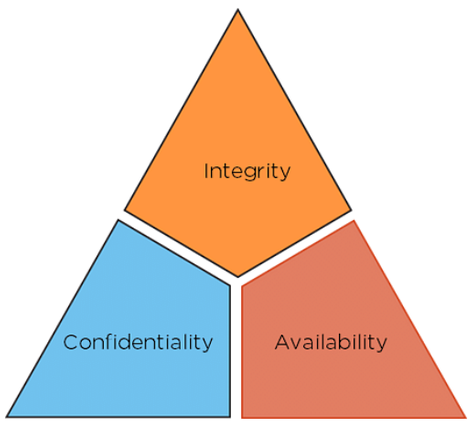


Fig: CIA triad

- Confidentiality: The principles of confidentiality assert that only authorized parties can access sensitive information and functions. Example: military secrets.
- Integrity: The principles of integrity assert that only authorized people and means can alter, add, or remove sensitive information and functions. Example: a user entering incorrect data into the database.
- Availability: The principles of availability assert that systems, functions, and data must be available on-demand according to agreed-upon parameters based on levels of service.

Types of Cybersecurity :

1. Application Security –

1. Most of the App that we use in our Cell-phone are Secured and work under the rules and regulations of the Google Play Store.

2. There are 1.85 million different apps are available for users to download. Now when we have different choices then this does not mean that all apps are safe.
3. Many of the apps pretend to be safe but after taking all information from ours, the app users to share information in money to the 3rd-party as well app stop working suddenly this comes under Cyber attack.
4. The app must be installed from a trust-worthy platform, not from Google Chrome.

2. Network Security –

1. Guard your internal network against outside threats with increased network security.
2. Some times we used to utilize free Wi-Fi on public area such as cafe, Malls, etc., by this activity 3rd Party start tracking your Phone over the internet that time if you are using any payment gateway then our bank account can be Empty.
3. So, avoid using Free Network because free network Doesn't support Securities.

3. Cloud Security –

1. Cloud base data storage has become a popular option over the last Decade due to it enhance privacy as well saving data on cloud make it excess able from any device but need correct authentication.
2. Some Famous platforms are Google Drive, Microsoft Cloud, Dropbox, etc.
3. These platforms are free to some extent, if we want to save more data than we have to pay.
4. ASW is also a new Technique that helps to run your business over the internet provides security to your data

4. Mobile Security –

1. Mobile is the very common gadgets we use daily, everything we excess is by mobile phone online class then the mobile phone, Call to the client then the mobile phone, sending money need a mobile phone and many more.
2. The mobile phones made our life so easy only by single touch we can be excess news from another country. Then this mobile phone must come under all security patches.
3. We must lock all the payment applications by phone in-built app as well never share your phone password except your family.

Q) What is Internet Governance? Explain Challenges and Constraints of Internet Governance.

A) Internet governance refers to the rules, policies, standards and practices that coordinate and shape global cyberspace.

Internet governance is 'the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet'.

> Internet governance is 'the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures, and programs that shape the evolution and use of the Interne(.

Challenges of Internet Governance

Some of the various challenges of internet governance are as follows,

1. The pace and changing nature of the internet.
2. The internet as part of digitalization.
3. The concentration of digital power.
4. The shifts in digital geopolitics i.e., environment.
5. The co-ordination and shaping of digital future.
6. The future of regulations.
7. The participation in taking the managerial decisions.

Constraints of Internet Governance

The Constraints of Internet Governance are as follows :

Privacy: End user privacy must also be ensured. Whenever an end user participates in a transaction with a government agency, he/ she discloses personal details which may include sensitive data. Thus, security for such data should be provided in order to maintain the end-user privacy. This security can be provided by making use of secure transmission channels, firewalls, preventing unauthorized access etc.

Authentication: Authentication is another issue that must be considered while providing the government services. In other words, the government agency must ensure that the services are provided only to the legitimate users. This can be done by using digital signatures. However, it incurs an additional cost and overhead.

High Setup Costs and Technical Difficulties: Government agencies must consider the financial status of the end user because, internet access and PC is rare in certain locations. Therefore, a framework for delivery of e-services to the poor and uneducated people must also be designed.

Q) What is Cyber threat?

A) A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

Cyber threats include

- Computer viruses,
- Data breaches,
- Denial of Service (DoS) attacks, and
- other attack vectors.

Cyber threats also refer to the possibility of a successful cyber attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data.

Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.

Types of Cyber Threats:

- Cyber warfare
- Cyber Crime
- Cyber terrorism
- Cyber Espionage

Cyber Warfare

Cyber Warfare is typically defined as a set of actions by a nation or organization to attack countries or institutions' computer network systems with the intention of disrupting, damaging, or destroying infrastructure by computer viruses or denial-of-service attacks.

This means cyber warfare may take several different shapes:

1. Attacks on financial infrastructure
2. Attacks on public infrastructure like dams or electrical systems
3. Attacks on safety infrastructure like traffic signals or early warning systems
4. Attacks against military resources or organizations

Types of Cyber Warfare

Espionage

Espionage refers to spying on another country to steal secrets. In cyber warfare, this may involve using a botnet(Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the word’s “robot”

and "network.")or spear-fishing attack to gain a foothold in a computer before extracting sensitive information.

Sabotage
With sensitive information identified, organizations then need to determine the potential threats presented to this data. This includes third parties that may want to steal the data, competitors that could gain an advantage by stealing information, and insider threats or malicious insiders like disgruntled workers or negligent employees

Denial-of-Service Attack
A denial-of-service (DoS) attack involves flooding a website with fake requests, forcing the site to process those requests, thereby making it unavailable for legitimate users. This kind of attack could be used to cripple a critical website used by citizens, military personnel, safety personnel, scientists, or others to disrupt critical operations or systems.

Electrical Power Grid
Hacking the electrical power grid could give an attacker the ability to disable critical systems, crippling infrastructure and causing the deaths of thousands. Further, an attack on the electrical power grid could disrupt communications, making it impossible to use services like text messaging or telecommunication.

Propaganda
Propaganda attacks involve trying to control the minds or hearts of the people living in or fighting for the targeted country. Propaganda can be used to expose embarrassing truths or to spread lies that cause people to lose faith in their country—or even sympathize with the enemy.

Economic Disruption
Most modern economic systems depend on computers to function. Attacking the computer networks of economic facilities like stock markets, payment systems, or banks can give hackers access to funds or prevent their targets from getting the money they need to live or engage in cyber or other warfare.

Surprise Cyberattack
These refer to the kinds of cyberattacks that would have an effect similar to Pearl Harbor or 9/11—massive strikes that catch the enemy off guard, weakening their defenses. They could be used to weaken the opponent in preparation for a physical attack as a form of hybrid warfare.

Cyber Crime

The term **cyber Crime** is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are standalone or a part of a network are used as a tool or/and target of criminal acitivity. It is often commited by the people of destructive and criminal mindset either for revenge, greed oradventure.
There are three major categories of cyber crimes:

1. Crimes Against People
These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft, and online libel or slander.

2. Crimes Against Property
Some online crimes occur against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and IPR violations.

3. Crimes Against Government
When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software

Reasons for Commission of Cyber Crimes

There are many reasons which act as a catalyst in the growth of cyber crime. Some of the prominent reasons are:

a. *Money:* People are motivated towards committing cyber crime is to make quick and easy money.

b. *Revenge:* Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
c. *Fun:* The amateur do cyber crime for fun. They just want to test the latest tool they have encountered.
d. *Recognition:* It is considered to be pride if someone hack the highly secured networks like defense sites or networks.
e. *Anonymity*- Many time the anonymity that a cyber space provide motivates the person to commit cyber crime as it is much easy to commit a cyber crime over the cyber space and remain anonymous as compared to real world.
It is much easier to get away with criminal activity in a cyber world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.

Cyber Terrorism

A) Cyber terrorism means using cyberspace to hurt the general public and damage the integrity and sovereignty of any country.

Cyber terrorism is generally carried out in the following ways:

1. Hacking government-owned systems of the target country and getting confidential information.
2. Destructing and destroying government databases and backups by incorporating viruses or malware into the systems.
3. Disrupting government networks of the target nation.
4. Distracting the government authorities and preventing them from focusing on matters of priority.

Cyberterrorism can be broadly categorized under three major categories:

- Simple: This consists of basic attacks including the hacking of an individual system.
- Advanced: These are more sophisticated attacks and can involve hacking multiple systems and/or networks.
- Complex: These are coordinated attacks that can have a large-scale impact and make use of sophisticated tools.

The punishment for cyber terrorism as provided under Section 66F of the IT Act is imprisonment of up to 3 years and/or up to Rs 2 lakh fine.

Cyber Espionage

Espionage is “the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company.” Similarly, cyber espionage refers to the unauthorized accessing of sensitive data or intellectual property for economic, or political reasons. It is also called ‘cyber spying’.

At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically socially motivated.

In most cases of cyber espionage, spies in the form of hackers are deliberately recruited to launch cyber attacks on the government systems of enemy nations to stealthily collect confidential information. The cross-border exposure of sensitive data related to any country can continue as long as it stays undetected. The information gathered through cyber espionage is then used by the gathering country to either combat or launch military or political attacks on the enemy country.

Generally, the following data are gathered through cyber espionage:

- Military data
- Academic research-related data
- Intellectual property
- Politically strategic data, etc.

Q) what is Cyber Security policy? Explain Need for a Comprehensive Cyber Security Policy.

A) Cyber security policies are a set of rules of how companies should practice responsible security. It begins with general security expectations, roles, and responsibilities inside the company. There are a set of templates that platforms offer to make a well efficient cyber policy.
The larger organizations have more clauses as they have more stakeholders inside and outside. While the smaller ones follow basic precautions to ensure safety at the operational level.

They are mainly –
1. Rules for using email encryption
2. Steps for accessing work applications remotely
3. Guidelines for creating and safeguarding passwords
4. Rules on the use of social media

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

Need of Security policies-

1) It increases efficiency.
The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2) It upholds discipline and accountability
When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3) It can make or break a business deal
It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

4) It helps to educate employees on security literacy
A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data. It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

Types of security policies

Security policy types can be divided into three types based on the scope and purpose of the policy:

- **Organizational**. These policies are a master blueprint of the entire organization's security program.
- **System-specific.** A system-specific policy covers security procedures for an information system or network.
- **Issue-specific.** These policies target certain aspects of the larger organizational policy.
  Examples of issue-related security policies include the following:
  - Acceptable use policies define the rules and regulations for employee use of company assets.
  - Access control policies say which employees can access which resources.
  - Change management policies provide procedures for changing IT assets so that adverse effects are minimized.
  - Disaster recovery policies ensure business continuity after a service disruption. These policies typically are enacted after the damage from an incident has occurred.
  - Incident response policies define procedures for responding to a security breach or incident as it is happen

Q) Explain need of Nodal Authority.

A) The Indian **Computer Emergency Response Team** (CERT-IN or ICERT) is the national nodal authority to deal with cyber security threats like- hacking and phishing. It strengthens security related defence of the Indian Internet domain. It responds to computer security issues as and when they occur.

CERT-In is operational since January 2004. It is a functional organization of the Ministry of Electronics and Information Technology, Government of India, to secure Indian cyberspace.

CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and distribution of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures to deal with cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

Q) What are Cyber Security Vulnerabilities?

A) Any **flaw** in an organization’s internal controls, system procedures, or information systems is a vulnerability in cyber security. Cybercriminals and Hackers may target these vulnerabilities and exploit them through the points of vulnerability.

These hackers can enter the networks without authorization and seriously harm data privacy. As a result, it is crucial to constantly check for cybersecurity vulnerabilities because flaws in a network could lead to a complete compromise of an organization’s systems.

Examples of Cyber Security Vulnerabilities

Here are a few examples of cybersecurity vulnerabilities

- Missing data encryption
- Lack of security cameras
- Unlocked doors at businesses

- Unrestricted upload of dangerous files
- Code downloads without integrity checks
- Using broken algorithms
- URL Redirection to untrustworthy websites
- Weak and unchanged passwords
- Website without SSL

Q) List out some Cyber Security Vulnerabilities. Explain each in detail.

A) Cyber Security Vulnerabilities are listed below:

1) Vulnerabilities in Software

2) System Administration

3) Complex Network Architectures

4) Open Access to Organizational Data

5) Weak Authentication

6) Unprotected Broadband Communications

7) Poor Cyber Security Awareness

1) Vulnerabilities in Software:

A security flaw, glitch, or weakness found in software code that could be exploited by an attacker (threat source). Software vulnerabilities are flaws in your code that are often caused by a weakness present in the software. These vulnerabilities may also be due to errors in user management processes.

Common Software Vulnerabilities

1. **Missing data encryption**

When data is not effectively encrypted before storage, the vulnerability to cyber invasion is high.

Solution: Consider getting an encryption solution that meets your needs specifically to avoid human mistakes. You could also consider working with trusted software development teams to educate your personnel.

2. **OS command injection**

The shell or OS command injection occurs when your software's operating system is attacked when you're running an application. It is a method used to prey on an organization so that the hacker gets deeper access. Again, incomplete or incorrect input data validation is a major culprit.

Solution: Don't allow OS commands from application-layer code. Register strong validation protocols in your organization.

3. **Missing authorization**

Missing authorization is due to insufficient authentication or limitations in the authorization. Additionally, this vulnerability is an easy way for attackers to enter.

Solution: Tighten and fully implement authorization protocols. Consider opting for identity management, multi-factor management, and privileged management tools, amongst others.

4. **Cross-site scripting and forgery (CSRF/XSS/XSRF)**

When this occurs, the attacker tricks the web browser into executing unwanted commands. Hence impacting the software and possibly your business adversely.

Solution: You can adopt a randomly generated token for general use. However, use double submission of cookies and matching random tokens before access is allowed.

5. **URL redirection**

URL redirection is one of the most annoying kinds of glitches. It leads you directly to the predator as your browser takes you to an external site.

Solution: Use a web browser or application firewall. Also, adopt automated scanning to keep your software up-to-date.

6. **Path traversal**

Directory traversal is common. It allows the hacker to access files on the server and read them, especially when running. These files could include code and data, credentials for back-end systems, and OS files. Solution:

- Avoid the passage of user-supplied input into your filesystem APIs.
- In addition to this, add multiple layers of defense or firewalls.
- Consider opting for additional protective steps from trusted providers.

General Ways To Prevent Software Vulnerabilities

Review Software Design : Once the initial software development process is complete, the team presents a fresh, qualified set of eyes to review it. The software must pass all security requirements and address the identified risk information.

Verify Third-Party Software : When third-party components are unavoidable, we use only those with code signing certificates to ensure authenticity and trustworthiness.

Regularly Identify and Confirm Vulnerabilities : Limit an attacker's window of opportunity by proactively looking out for vulnerabilities in your system. The service includes regular reviews, analysis, and software testing to see if any new risks will arise.

Prioritize Fixes Based on Risks: Companies need to address the mitigation of vulnerabilities promptly. This development service provider scrutinizes each weakness and determines the complexity in resolving it, as well as its impact on your network.

2) System Administration:

A system administrator (sysadmin) is an information technology professional who supports a multiuser computing environment and ensures continuous, optimal performance of IT services and support systems.

Sysadmins are responsible for ensuring the uptime of their companies' computers, servers and internet -- basically "keeping the lights on" to limit work disruptions.

This includes system maintenance and configuration, such as installing and troubleshooting hardware and software and assessing new technologies for their companies.

The System Administrator role and responsibilities :

1. User administration (setup and maintaining account)
2. Maintaining system
3. Verify that peripherals are working properly
4. Quickly arrange repair for hardware in occasion of hardware failure
5. Monitor system performance
6. Create file systems
7. Install software using tools such as apt command/apt-get command, dnf command/yum command, zypper command, apk command and others.
8. Patching firmware and software
9. Create a backup and recover policy (disaster recovery [DR])
10. Monitor network communication
11. Update system as soon as new version of OS and application software comes out
12. Implement the policies for the use of the computer system and network

13. Setup security policies for users. A sysadmin must have a strong grasp of computer security (e.g. firewalls and intrusion detection systems. You must know how to use tools such as wireshark and nmap command)
14. Documentation in form of internal wiki. You must know how to read manual pages using the man command or help command.
15. Password and identity management
16. Network administration
17. Database administration
18. How to view and troubleshoot with Unix and Linux log files
19. Setting up cron jobs on your Unix and Linux system using the crontab command

3) Complex Network Architectures:

Generally, the data which is in the form of a stream or a block can be transmitted over network between the two communicating parties. The entity which is responsible for transmitting the data is called a sender and the entity which receives the data (from the sender) is called a receiver. Both the parties must have certain level of coordination between them in order to exchange the data. If the sender and receiver are linked through connection-oriented means then they must use a connection-oriented protocol like TCP/IP for transmitting the data. During the process of data transmission, some unauthorized interruption from intruders occur which can be avoided by providing security to the transmitting data.

The model for the network security is shown below,

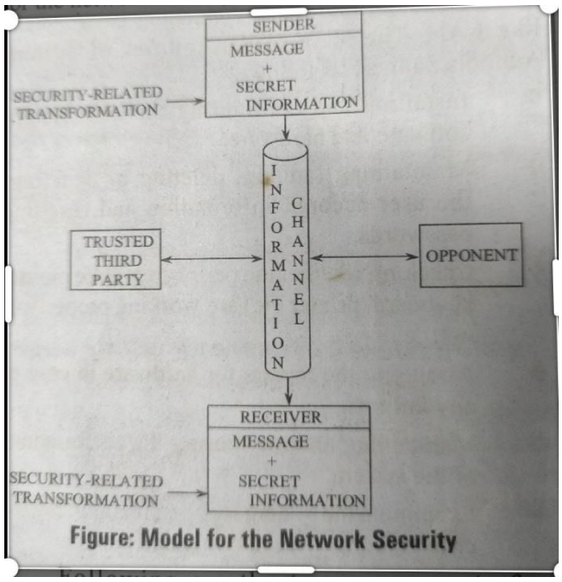


Figure: Model for the Network Security

Following are the two components for providing security,

- Some security-related information must be sent along with the actual information i.e ., a message. Example of the additional information is an encrypted text which encodes the original message in such a way that it becomes unreadable for the opponent.
- Some secret information is shared among only sender and receiver where the opponent is unaware of it. An example of such an information is the encryption key along with the transformation for scrambling the prior to its transmission and unscrambling it upon reception.

In order to achieve secure transmission, a trusted third party is needed for distributing the secret Information and to resolve the conflicts that arises between the sender and the receiver.

The network security model shown above describes the four tasks in designing a specific security service,

1. Designing an Algorithm: An algorithm must be designed for doing all the security related transformations in such a way that an opponent is unable to fail its intent.

2. Generating Secret Information: Some secret information to be used along with the algorithm must be generated.

3. Developing Various Distribution Methods: Various methods for distributing and sharing of secret information must be developed or evolved.

4.Specifying a Protocol: A protocol which employs the security algorithm for achieving security service must be used by both the and the receiver.

4) Weak Authentication

Weak authentication can be defined as a process that involves the authentical either through a password or through a simple question that should be answered by the user. It may provide inefficient and incomplete results. The two different classes of weak authentication schemes are as follows,

1. Password-based Authentication
2. PIN-based Authentication.

1. Password-based Authentication

Password-based authentication is the most common and widely used method for, E- commerce transaction. In this method, the user is provided a user name and log in pass word .Only the genuine end user knew the correct combination of log in name and password. Before accessing the payment gateway, the system asks for user name and password. If it is correctly entered, it is authenticated that the user is the genuine party and not cyber criminal. The intelligent people may guess the password easily and can use them further to theft the confidential information of user.

2. PIN-based Authentication

Pin-bases authentication can be used in banking transactions such as a 4-digit password for ATM card. This Pin can be identified or cracked by the attackers easily.

5)Open Access to Organizational Data

In digital world, connecting a digital device to internet enables the possibility of an attacker to attack or theft the sensitive information of an organization. The cyber crimes have been rapidly increasing in this generation. Mostly, some organizations enable their data to be accessed by the users.

Due to the open access of data in an organization feature, the cyber terrorism gains popularity. It is conducted against organizations and governments. In doing so, the attacker makes use of various computer tools and Internet facilities to get secret access to private information of the citizen. Apart from this, it also destroys the programs, files, plant programs to acquire the access of complete network.

Procedure for Open Access to Organisational Data

At first the attacker determines the weak points or vulnerabilities in the target. They do this by using various methods or tools and the target is usually an individual or an organization. In principle, the attacker makes use of two attacks namely active attack and Passive attack. The former one make changes to the system making the bad impact on the availability; integrity and authenticity of the data. On the other hand, his passive attack is used to obtain information regarding the target. Thus, affecting the confidentiality of the network. Moreover, there also exist other attacks which can be categorised inside or outside.

1. Inside Attack: If the attack is initiated by a person working within the organization is called inside attack.
2. Outside Attack: If the attack is initiated by any outside source and lies outside of the security perimeter of the organization is called outside attack.

6) Unprotected Broadband Communications

Broadband is the transmission of wide bandwidth data over a high-speed internet connection. Broadband communication networks are regarded as aggregated networks (providing voice, video, and data) over the wired network including Ethernet and fibre These technologies include, but are not limited to, mobile and fixed broadband, backhaul satellite networks, Wi-Fi (unlicensed) technologies and cellular (licensed) networks.

An unsecure broadband communication is one you can access broadband without a password. Public networks offered in places like cafes are often open. Although these provide free wireless Internet access, using public Internet comes with dangers.

When you connect to a public network, remember that several other users are also connected at the same time. So, if a hacker can access the public Wi-Fi router, there is a risk that he may be able to steal your personal and confidential information.

Risk of Eavesdropping

There is a risk of eavesdropping by hackers when you use networks. They may use "man in the middle" style to gain access to your data. The hacker may be able to eavesdrop on your information as it passes your phone or computer to any website you may use.

Here are some other risks of using unprotected public networks:

- As these networks do not require any authentication, the hackers receive unfettered access to unprotected gadgets within the same network .
- The hackers may position between you and the hotspot, which leaves you vulnerable to attacks.
- If a hacker gets access to your personal information, he may misuse the same at any point in time.
- Unsecured Wi-Fi networks are also used by cyber criminals to distribute infected software like viruses and malware.
- Intruders may not damage the public network but may use it for illegal purposes that may have severe repercussions.

Security in Unprotected Broadband Communication :

Hackers target users who do not have the right knowledge to remain protected. Here are a few tips that ensure security while connecting to a unprotected broadband Communication.

1. Use a Virtual Private Network (VPN)
2. Choose Secure Sockets Layer(SSL) connections
3. Switch off Sharing
4. check the terms and conditions
5. Security Protocols
6. Use a Security tool

7) Poor Cyber Security Awareness

One of the most common reasons why cyber-attacks cause so much damage is because Of the lack of proper understanding. A lot of people believe themselves to be immune from threats and don't really put thought into how dangerous attacks can become. Even something as simple as a web browser can lead to all kinds of problems in work and personal lifestyles. Educate Yourself and learn what you can about the different ways hackers can steal, corrupt or even destroy your information. Understanding the risks can help you make better decisions to keep yourself protected from more than just email scams.

The following are to get awareness to avoid breeches to personal information:

1. Outdated Software: Updates to software are more than just fixing operational bugs. In many instances, these updates include fixes to vulnerabilities.
2. Lack of Proper Protection: Investing in security and anti-malware software is an investment into keeping yourself and your family safe from cyber thugs.
3. Carelessness through Email: Messages that may look legitimate are often points for the criminal element to steal information. This is called, "phishing". In many cases, these messages are almost impossible to discern from the real thing.
4. Unprotected Home Networks: Approximately 25% of wireless networks are vulnerable to all kinds of attacks. However, many of these invasions come from people simply not using the security features that are available on the device.

Q) Define Security Safeguards. List out some Important Safe Guards of Cyber Security.

The protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system.

Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Some of the important safeguards listed below:

- Access control
- Audit
- Authentication
- Biometrics
- Cryptography
- Deception
- Denial of Service Filters
- Ethical Hacking
- Firewalls
- Intrusion Detection Systems
- Response
- Scanning
- Security policy
- Threat Management

1) Access control

Access control: Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources.

Access control is a mechanism that defines and controls access rights for individuals who can use specific resources in the OS. In other words, you can say that access control is a security feature through which the system permits or revokes the right to access any data and resource in a system. The permission to access a resource is called authorization.

Access control systems include:

File permissions: Refer to the access control in which the user can create, read, edit, or delete on a file server

Program permissions: Refer to the access control in which the user can execute a program on an application server

Data rights permissions: Refer to the access control in which the user can retrieve or update information in a database

4 Types of Access Control

- **Discretionary access control (DAC)**
  With DAC models, the data owner decides on access. DAC is a means of assigning access rights based on rules that users specify.

- **Mandatory access control (MAC)**
  MAC was developed using a nondiscretionary model, in which people are granted access based on an information clearance. MAC is a policy in which access rights are assigned based on regulations from a central authority.

- **Role Based Access Control (RBAC)**
  RBAC grants access based on a user's role and implements key security principles, such as "least privilege" and "separation of privilege." Thus, someone attempting to access information can only access data that's deemed necessary for their role.

- **Attribute Based Access Control (ABAC)**
  In ABAC, each resource and user are assigned a series of attributes, Wagner explains. "In this dynamic method, a comparative assessment of the user's attributes, including time of day, position and location, are used to make a decision on access to a resource."

Audit: Cyber security audits are a vital component of an organisation's defences against data breaches and privacy violations.
A cyber security audit is a comprehensive review of an organisation's IT infrastructure. Audits ensure that appropriate policies and procedures have been implemented and are working effectively.
The audit should be performed by a qualified third party.
The main reason to conduct a cyber security audit are

- **Data security**: network access controls, data encryption and the way sensitive information moves through the organisation;
- **Operational security**: information security policies, procedures and controls;
- **Network security**: network controls, antivirus configurations and network monitoring;
- **System security**: patching, privileged account management and access controls; and
- **Physical security**: the organisation's premises, and physical devices that are used to store sensitive information.

Authentication: Authentication is the process of verifying a user or device before allowing access to a system or resources.
Authentication is part of a three-step process for gaining access to digital resources:

1. Identification—Who are you?
2. Authentication—Prove it.
3. Authorization—Do you have permission?

Types of Authentication
Single-Factor Authentication
Single-factor authentication (SFA) or one-factor authentication involves matching one credential to gain access to a system (i.e., a username and a password). Although this is the most common and well-known form of authentication, it is considered low-security and the Cybersecurity and Infrastructure Security Agency (CISA) recently added it to its list of **Bad Practices**.

Two-Factor Authentication
Two-factor authentication (2FA) adds a second layer of protection to your access points. Instead of just one authentication factor, 2FA requires two factors of authentication out of the three categories:

- Something you know (i.e., username and password)

- Something you have (e.g., a security token or smart card)
- Something you are (e.g., TouchID or other biometric credentials)

2FA is more secure because even if a user's password is stolen, the hacker will have to provide a second form of authentication to gain access—which is much less likely to happen.

Three-Factor Authentication
Three-factor authentication (3FA) requires identity-confirming credentials from three separate authentication factors (i.e., one from something you know, one from something you have, and one from something you are). Like 2FA, three-factor authentication is a more secure authentication process and adds a third layer of access protection to your accounts.

Multi-Factor Authentication
Multi-factor authentication (MFA) refers to any process that requires two or more factors of authentication. Two-factor and three-factor authentication are both considered multi-factor authentication.

Single Sign-On Authentication
Single sign-on (SSO) authentication allows users to log in and access multiple accounts and applications using just one set of credentials. We see this most commonly in practice with companies like Facebook or Google, which allow users to create and sign in to other applications using their Google or Facebook credentials. Basically, applications outsource the authentication process to a trusted third party (such as Google), which has already confirmed the user's identity.

One-Time Password
A one-time password (OTP) or one-time PIN (sometimes called a dynamic password) is an auto-generated password that is valid for one login session or transaction. OTP is often used for MFA. For instance, a user will start to log in with their username and password, which then triggers the application to send an OTP to their registered phone or email. The user can then input that code to complete the authentication and sign in to their account.

Biometrics : Biometrics is the statistical analysis and measurement of people's unique behavioral and physical characteristics. Biometric authentication relies on biometrics like fingerprints, retinal scans, and facial scans to confirm a user's identity.

Passwordless Authentication
Passwordless authentication, as the name suggests, doesn't require a password or other knowledge-based authentication factor. Typically, the user will enter their ID and will then be prompted to authenticate through a registered device or token. Passwordless authentication is often used in conjunction with SSO and MFA to improve the user experience, reduce IT administration and complexity, and strengthen security.

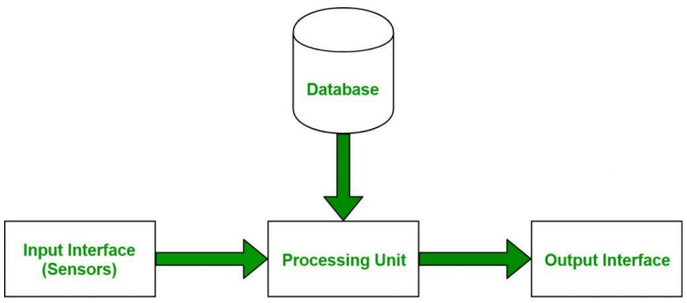
Certificate-Based Authentication
Certificate-based authentication (CBA) uses a digital certificate to identify and authenticate a user, device, or machine. A digital certificate, also known as a public-key certificate, is an electronic document that stores the public key data, including information about the key, its owner, and the digital signature verifying the identity. CBA is often used as part of a two-factor or multi-factor authentication process.

Q) Write about Biometrics in detail.

A) Biometrics is the statistical analysis and measurement of people's unique behavioral and physical characteristics.

Biometric authentication relies on biometrics like fingerprints, retinal scans, and facial scans to confirm a user's identity.

To do this, the system must first capture and store the biometric data. And then when the user goes to log in, they present their biometric credentials and the system compares them to the biometric data in their database. If they match, they're in.



Biometric System

The following are components of biometric devices:

- A scanning device or reader or input interface to capture the biometric factor to be authenticated.
- A database for storing and securely comparing biometric data.
- And software that converts scanned biometric data into a digital format and compares observed and recorded data match points.
- A output interface or display device for displaying result

Authentication can be in one of the following forms

- Identification: Matching an individuals features against all records to check whether his/her record is present in the database.
- Verification: To check whether the person is who he/she is claiming to be. In this case the features of the person is matched only with the features of the person they claims to be.

characteristics are the two main types of biometrics used for security

1) Behavioural and
2) physical.

Physical biometrics analyze your hand shape, eye structures, facial features, and other physical characteristics. Physical biometrics include the following:

- DNA Matching
- Finger or Palm Veins Recognition
- Hand Geometry
- Iris Recognition
- Retina Scanning
- Skull Shape
- Fingerprints
- Facial Geometry

Behavioural biometrics evaluates individuals' unique ways of acting or any pattern of behavior linked to a certain person.
Behavioral biometrics include the following:

- Walking Gait
- Keystroke Dynamics
- Finger and Mouse Movements
- Signature
- Typing Patterns
- Speaker Recognition
- Walking Gait Recognition

Cryptography: Refer Unit IV

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden.

FEATURES OF CRYPTOGRAPHY:

1.Confidentiality

2. Data Integrity

3.Authentication

4.Non - repudiation

5.Availability

Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system –

1.Symmetric Key cryptography: Symmetric Key Cryptography, or Symmetric Encryption, uses a secret key for both encryption and decryption

2.Asymmetric Key cryptography: Asymmetric cryptography, better known as public-key cryptography, encrypts and decrypts a message using a pair of similar keys. In asymmetric key cryptography, the private key is kept by one public key and one private key — to prevent unauthorized entry or usage.

Deception :

Building security defenses that detect threats early with little performance impact on the network and few false positives is possible with the help of deception technology, which is a straightforward but effective technique.

The technology works by deploying decoys in your network alongside real assets, such as domains, databases, applications, servers, cookies, files, credentials, and sessions. Decoys are realistic-looking but fake assets.

There is no way to tell the difference between the false and the real for an attacker who has broken into the network. As soon as they come in contact with a decoy, a silent alarm goes off and the systems begin to gather data on the attacker's actions and motivation.
Some of theTools for deception technologies :

1. Attivo 2. Illusive 3. Acalvio 4. Cyber Trap

Denial of Service Filters:

Denial of service (DoS) is a type of cyber-attack designed to disable, shut down or disrupt a network, website or service.

Typically, a malware is used to interrupt or inhibit the normal flow of data into and out of a system to render the target useless or inaccessible for a certain period.

An example of a DoS attack: when a website is accessed massively and repeatedly from different locations, preventing legitimate visitors from accessing the website.

For example, if a bank website can handle 10 people a second clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no legitimate users can login.

When a DoS attack is launched from different locations in a coordinated fashion, it is often referred to as a distributed denial of service attack (DDoS).

Denial of Service (DOS) is a cyber-attack on an individual computer or website with the intention of denying service to intended users. Its purpose is to disrupt an

organization's network operations by denying users access. DOS is usually accomplished by flooding the target machine or computer with excessive requests in order to overload systems and prevent some or all legitimate requests from being met. For example, if a banking website can handle 10 people per second clicking the "Login" button, an attacker only needs to send 10 fake requests per second to keep legitimate users from logging in.

1.16.1 FILTERING TECHNIQUES

There is no complete solution to detect DOS attacks. Each technique has its benefits and limitations. Here is a list of some of these techniques:

(l) **Intrusion prevention:** The best way to prevent DOS attack from happening is complete prevention, such as using filters that are synchronized and coordinated globally such that data packets that are detected to be originating from attackers can be stopped before they cause real damage. This can be achieved using two filtering techniques:

A) Ingress filtering: It's a defensive approach, where a router is designed to block inbound traffic if its source address is suspicious. Incoming packets from IP addresses that do not match the domain prefix are blocked. This reduces a attack that can be caused by IP spoofing. This protects the system from resource exhaustion.

B) Egress filtering: This is a defence mechanism where outbound traffic is only assigned to IP addresses that are known to be legitimate such that it protects other domains from being hit by huge traffic from the IP addresses of the company if the company devices become botnets.

2)Distributed packet filtering: This is a defence mechanism, whereby spoofed addresses can be filtered to prevent an attack on targets and it helps in get ång a traceback of IP addresses. It is route based.

3)History based IP filtering: Using this mechanism, a database of IP addresses is prebuilt based on the connection history of a router. This mechanism is fairly effective and robust, and can be applied to a variety of packet types. This helps block incoming traffic requests from source addresses unknown to the database.

4)Secure overly services: This is a defence mechanism where only traffic that is coming from few selected network nodes is accepted to be genuine and is allowed to reach the servers while any other traffic is rejected. This mechanism is ideal for protecting a particular server and it may not be ideal for protecting public servers.

Q) Write about Ethical Hacking in detail.

A) Hacking is the process of finding vulnerabilities in a system and using these found vulnerabilities to gain unauthorized access into the system to perform malicious activities ranging from deleting system files to stealing sensitive information. Hacking is illegal and can lead to extreme consequences if you are caught in the act. People have been sentenced to years of imprisonment because of hacking.

hacking can be legal if done with permission. Computer experts are often hired by companies to hack into their system to find vulnerabilities and weak endpoints so that they can be fixed. This is done as a precautionary measure against legitimate hackers who have malicious intent. Such people, who hack into a system with permission, without any malicious intent, are known as e*thical hackers* and the process is known as e*thical hacking*.

Types of Hacking

We can define hacking into different categories, based on what is being hacked. These are as follows:

1. Network Hacking
2. Website Hacking

3. Computer Hacking
4. Password Hacking
5. Email Hacking

1. **Network Hacking:** Network hacking means gathering information about a network with the intent to harm the network system and hamper its operations using the various tools like Telnet, NS lookup, Ping, Tracert, etc.
2. **Website hacking:** Website hacking means taking unauthorized access over a web server, database and make a change in the information.
3. **Computer hacking:** Computer hacking means unauthorized access to the Computer and steals the information from PC like Computer ID and password by applying hacking methods.
4. **Password hacking:** Password hacking is the process of recovering secret passwords from data that has been already stored in the computer system.
5. **Email hacking:** Email hacking means unauthorized access on an Email account and using it without the owner's permission.

Types of Hackers
Hackers can be classified into three different categories:

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker

Black Hat Hacker

Black-hat Hackers are also known as an **Unethical Hacker or a Security Cracker**. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

White Hat Hacker

White hat Hackers are also known as **Ethical Hackers or a Penetration Tester**. White hat hackers are the good guys of the hacker world.

These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray Hat Hacker

Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.

In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.

Ethical hacking: Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating the strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Importance of Ethical Hacking

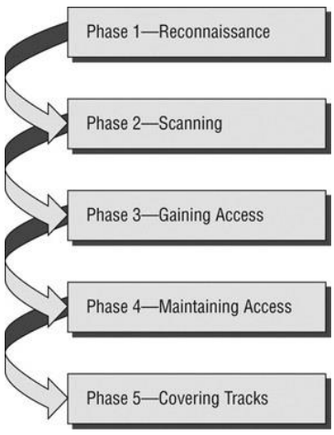
- Testing password strength
- Ensuring security settings and privilege levels in the domain account and database administration by testing out exploits
- Penetration testing after every software update/upgrade or after adding a new security patch
- Ensuring that data communication channels cannot be intercepted
- Testing validity of authentication protocols
- Ensuring security features in applications, which protect organizational and user databases
- Defense against denial-of-service attacks
- Network security and testing of anti-intrusion features

Phases of Ethical Hacking

There are multiple phases involved in any elaborate hacking process.

Reconnaissance: Before executing any hack, you need to gather some preliminary information about the target system. This information could be about the people or organizations associated with the target, details about the host system, or the target network. The primary intention of this step is to engineer a hack based on the exact technology and security measures implemented by the target system.

Scanning: Most of the time, hacking is done through network access. Most of our devices, whether in an organization or at home, are connected to a network. The common form of this network is Wi-Fi or WLAN. In offices, ethernet connections are also laid down to ensure maximum efficiency. As a hacker, you can take advantage of this factor and focus on gaining unauthorized access to the network of the target host. In this process, the network topology and vulnerable ports are revealed.



Gaining Access: The two aforementioned steps complete the information gathering phase. Now, based on that information, you need to start your hack. This step involves breaking into the target system by cracking the password or bypassing the security measures.

Maintaining access: After gaining access, you need to ensure that once you are done with your first session, you are able to retain access to the target system. This is done through a backdoor. A backdoor is an exploit or a hack that is left in the target system for future access. If you don't leave a backdoor, the target system may implement a newer security patch or reset its security measures, and you may have to execute or craft the hack once again.

Clearing tracks: After finishing up with the attack or hack, it is important to remove the traces of your incursion. This step involves removing any backdoors, executables, or logs that may lead to the attack being traced back to you or found out in the first place.

Ethical Hacking experts follow four key protocol concepts:

1. **Stay legal**. Obtain proper approval before accessing and performing a security assessment.
2. **Define the scope**. Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.
3. **Report vulnerabilities**. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.
4. **Respect data sensitivity**. Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

The following are some of the advantages of ethical hacking.

- This plays a key role in the battle against cyber terrorism and national security breaches.
- It helps in preventing possible hacker attacks.
- This supports the development of a system that is resistant to hacker intrusion.
- Banking and financial institutions will be much safer due to proper ethical hacking measures.
- It supports detecting and closing security flaws in a computer system or network.

Limitations of ethical hacking:

- **Limited scope**. Ethical hackers cannot progress beyond a defined scope to make an attack successful. However, it's not unreasonable to discuss out of scope attack potential with the organization.
- **Resource constraints**. Malicious hackers don't have time constraints that ethical hackers often face. Computing power and budget are additional constraints of ethical hackers.

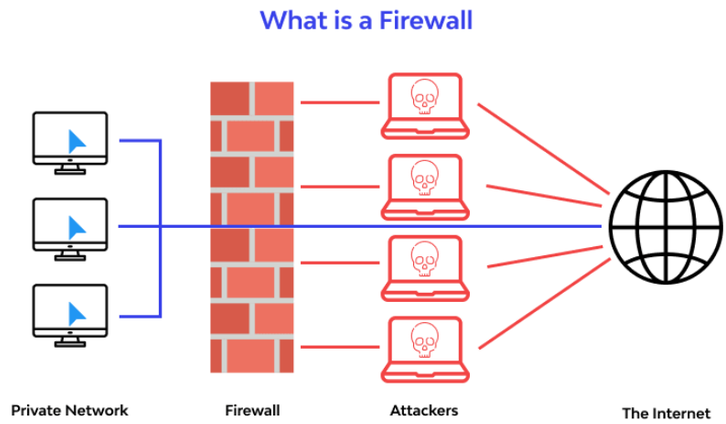
- **Restricted methods**. Some organizations ask experts to avoid test cases that lead the servers to crash (e.g., Denial of Service (DoS) attacks).

The most common vulnerabilities discovered by ethical hackers include:

- Injection attacks
- Broken authentication
- Security misconfigurations
- Use of components with known vulnerabilities
- Sensitive data exposure

Firewall: refer unit-IV

These are the devices that are used to prevent private networks from unauthorized access. A Firewall is a security solution for the computers or devices that are connected to a network, they can be either in form of hardware as well as in form of software. It monitors and controls the incoming and outgoing traffic (the amount of data moving across a computer network at any given time).



The major purpose of the network firewall is to protect an inner network by separating it from the outer network. Inner Network can be simply called a network created inside an organization and a network that is not in the range of inner network can be considered as Outer Network.

Intrusion Detection System : Refer Unit - III

Response or Incident Response

Incident Respose(IR) is a set of information security policies and procedures that you can use to identify, contain, and eliminate cyber attacks. The goal of incident response is to enable an organization to quickly detect and halt attacks, minimizing damage and preventing future attacks of the same type.

Phases of the Incident Response Lifecycle

There are six steps to incident response. These six steps occur in a cycle each time an incident occurs, The steps are:

- Preparation of systems and procedures
- Identification of incidents
- Containment of attackers and incident activity
- Eradication of attackers and re-entry options
- Recovery from incidents, including restoration of systems

Scanning

Scanning is the second step in ethical hacking. It helps the attacker get detailed information about the target. Scanning could be basically of three types:

1. **Port Scanning** – Detecting open ports and running services on the target host
2. **Network Scanning** – Discovering IP addresses, operating systems, topology, etc.
3. **Vulnerability Scanning** – Scanning to gather information about known vulnerabilities in a target

Security policy :

A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Security policies are important because they protect both physical and digital assets of an organization.

Physical security policies protect all physical assets in an organization, including buildings, vehicles, inventory and machines. These assets include IT equipment, such as servers, computers and hard drives. Protecting IT physical assets is particularly important because the physical devices contain company data. If a physical IT asset is compromised, the information it contains and handles is at risk. In this way, information security policies are dependent on physical security policies to keep company data safe.

Data security policies protect intellectual property from costly events, like- data breaches and data leaks.

Threat Management

Threat management is a process used by cyber security professionals to prevent cyberattacks, detect cyber threats and respond to security incidents.

How Threat Management Works

Many modern threat management systems use the cyber security framework established by the National Institute of Standards and Technology (NIST). NIST provides comprehensive guidance to improve information security and cyber security risk management for private sector organizations. One of their guides, the NIST Cyber security Framework (NIST CF), consists of standards and best practices. Five primary functions make up its core structure.

They are to identify, protect, detect, respond and recover.

1. **Identify:** Cybersecurity teams need a thorough understanding of the organization's most important assets and resources. The identify function includes categories, such as asset management, business environment, governance, risk assessment, risk management strategy and supply chain risk management.
2. **Protect:** The protect function covers much of the technical and physical security controls for developing and implementing appropriate safeguards and protecting critical infrastructure. These categories are identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance and protective technology.

3. **Detect:** The Detect function implements measures that alert an organization to cyber-attack. Detect categories include anomalies and events, continuous security monitoring and early detection processes.

4. **Respond:** The respond function ensures an appropriate response to cyberattacks and other cybersecurity events. Categories include response planning, communications, analysis, mitigation and improvements.
5. **Recover:** Recovery activities implement plans for cyber resilience and ensure business continuity in the event of a cyberattack, security breach or another cybersecurity event. The recovery functions are recovery planning improvements and communications.

Challenges of Cyber Threat Management

Some of the various challenges faced by cyber threat management are as follows,

Lack of Visibility: The organizations must ensure that they don't have any blind spots in their security processed.

Lack of Insight and Reporting: A threat management system in an organization must have KPIs(Key Performance Indicators) in order to detect and respond to the cyber security incidents.

Lack of Skilled Employees or Staff: Most of the organizations reports that more than half of the employees in their organization are not skilled.

Keywords

- Adware – Adware refers to any piece of software or application that displays advertisements on your computer.
- Advanced Persistent Threat (APT) – An advanced persistent threat is an attack in which an unauthorised user gains access to a system or network without being detected.
- Anti-Virus Software – Anti-virus software is a computer program used to prevent, detect, and remove malware.
- Artificial Intelligence – Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.
- Attachment – An attachment is a computer file sent with an email message.
- Authentication – Authentication is a process that ensures and confirms a user's identity.
- Back door – A backdoor is used to describe a hidden method of bypassing security to gain access to a restricted part of a computer system.
- Backup – To make a copy of data stored on a computer or server to reduce the potential impact of failure or loss.
- Baiting – Online baiting involves enticing a victim with an incentive.
- Bluetooth – Bluetooth is a wireless technology for exchanging data over short distances.
- Blackhat – Black hat hacker refers to a hacker that violates computer security for personal gain or malice.
- Botnet – A botnet is a collection of internet-connected devices, which may include PCs, servers and mobile devices that are infected and controlled by a common type of malware.
- Broadband – High-speed data transmission system where the communications circuit is shared between multiple users.
- Browser – A browser is software that is used to access the internet. The most popular web browsers are Chrome, Firefox, Safari, Internet Explorer, and Edge.
- Brute Force Attack – Brute force attack is an activity which involves repetitive successive attempts of trying various password combinations to break into any website.
- Bug – A bug refers to an error, fault or flaw in a computer program that may cause it to unexpectedly quit or behave in an unintended manner.
- BYOD – Bring your own device (BYOD) refers to employees using personal devices to connect to their organisational networks.
- Clickjacking – Clickjacking, also known as a UI redress attack, is a common hacking technique in which an attacker creates an invisible page or an HTML element that overlays the legitimate page.

- Cloud Computing – The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.
- Cookie – Cookies are small files which are stored on a user's computer. Cookies provide a way for the website to recognize you and keep track of your preferences.
- Critical Update – A fix for a specific problem that addresses a critical, non-security-related bug in computer software.
- Cyber Warfare – Cyber warfare typically refers to cyber-attacks perpetrated by one nation-state against another.
- Data Breach – A data breach is a confirmed incident where information has been stolen or taken from a system without the knowledge or authorization of the system's owner.
- Data Server – Data server is the phrase used to describe computer software and hardware that delivers database services.
- DDoS Attack – A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- Deepfake – Deepfake refers to any video in which faces have been either swapped or digitally altered, with the help of AI.
- Domain name – The part of a network address which identifies it as belonging to a particular domain.
- Domain Name Server – A server that converts recognisable domain names into their unique IP address
- Download – To copy (data) from one computer system to another, typically over the Internet.
- Exploit – A malicious application or script that can be used to take advantage of a computer's vulnerability.
- Firewall – A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.
- Hacking – Hacking refers to an unauthorised intrusion into a computer or a network.
- Honeypot – A decoy system or network that serves to attract potential attackers.
- HTML – Hypertext Markup Language (HTML) is the standard markup language for creating web pages and web applications.
- Identity theft – Identity theft is a crime in which someone uses personally identifiable information in order to impersonate someone else.
- Incident Response Plan – An incident response policy is a plan outlying organisation's response to an information security incident.
- Internet of things (IoT) – The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data.
- IP Address – An IP address is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet.
- IOS – An operating system used for mobile devices manufactured by Apple.
- Keystroke logger – A keystroke logger is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you are unaware actions are being monitored.
- Malware – Malware is shorthand for malicious software and is designed to cause damage to a computer, server, or computer network.
- Malvertising – The use of online advertising to deliver malware.
- Memory stick – A memory stick is a small device that connects to a computer and allows you to store and copy information.
- MP3 – MP3 is a means of compressing a sound sequence into a very small file, to enable digital storage and transmission.

- Multi-Factor Authentication – Multi-Factor Authentication (MFA) provides a method to verify a user's identity by requiring them to provide more than one piece of identifying information.
- Packet Sniffer – Software designed to monitor and record network traffic.
- Padlock – A padlock icon displayed in a web browser indicates a secure mode where communications between browser and web server are encrypted.
- Patch – A patch is a piece of software code that can be applied after the software program has been installed to correct an issue with that program.
- Penetration testing – Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
- Phishing – Phishing is a method of trying to gather personal information using deceptive e-mails and websites.
- Policy Management – Policy Management is the process of creating, communicating, and maintaining policies and procedures within an organisation.
- Proxy Server – A proxy server is another computer system which serves as a hub through which internet requests are processed.
- Pre-texting – Pre-texting is the act of creating a fictional narrative or pretext to manipulate a victim into disclosing sensitive information.
- Ransomware – A type of malicious software designed to block access to a computer system until a sum of money is paid.
- Rootkit – Rootkits are a type of malware designed to remain hidden on your computer.
- Router – A router is a piece of network hardware that allows communication between your local home network and the Internet.
- Scam – A scam is a term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.
- Scareware – Scareware is a type of malware designed to trick victims into purchasing and downloading potentially dangerous software.
- Security Awareness Training – Security awareness training is a training program aimed at heightening security awareness within an organisation.
- Security Operations Centre (SOC) – A SOC monitors an organisation's security operations to prevent, detect and respond to any potential threats.
- Server – A server is a computer program that provides a service to another computer programs (and its user).
- Smishing – Smishing is any kind of phishing that involves a text message.
- Spam – Spam is slang commonly used to describe junk e-mail on the Internet.
- Social Engineering – Social engineering is the art of manipulating people, so they disclose confidential information.
- Software – Software is the name given to the programs you will use to perform tasks with your computer.
- Spear Phishing – Spear phishing is an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information.
- Spyware – Spyware is a type of software that installs itself on a device and secretly monitors a victim's online activity.
- Tailgating – Tailgating involves someone who lacks the proper authentication following an employee into a restricted area.
- Tablet – A tablet is a wireless, portable personal computer with a touchscreen interface.
- Traffic – Web traffic is the amount of data sent and received by visitors to a website.
- Trojan – A Trojan is also known as Trojan horse. It is a type of malicious software developed by hackers to disguise as legitimate software to gain access to target users' systems.

- Two-Factor Authentication – Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are.
- USB – USB (Universal Serial Bus) is the most popular connection used to connect a computer to devices such as digital cameras, printers, scanners, and external hard drives.
- Username – A username is a name that uniquely identifies someone on a computer system.
- Virus – A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.
- VPN (Virtual Private Network) – A virtual private network gives you online privacy and anonymity by creating a private network from a public Internet connection. VPNs mask your Internet protocol (IP) address so your online actions are virtually untraceable.
- Vulnerability – A vulnerability refers to a flaw in a system that can leave it open to attack.
- Vishing – Vishing is the telephone equivalent of phishing. It is an attempt to scam someone over the phone into surrendering private information that will be used for identity theft.
- Whaling – Whaling is a specific form of phishing that's targeted at high-profile business executives and managers.
- Whitehat – White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies.
- Worm – A computer worm is a malware computer program that replicates itself in order to spread to other computers.
- Wi-Fi – Wi-Fi is a facility that allows computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.
- Zero-Day – Zero-Day refers to a recently discovered vulnerability that hackers can use to attack systems.

SECURING WEB APPLICATIONS, SERVICES AND SERVERS

Introduction

Web application security refers to a variety of processes, technologies, or methods for protecting web servers, web applications, and web services such as APIs from attack by Internet-based threats.

Web application security is a central component of any web-based business. The global nature of the Internet exposes web properties to attack from different locations and various levels of scale and complexity. Web application security deals specifically with the security surrounding websites, web applications and web services such as APIs.

Web Services Security (WS Security) is a specification that defines how security measures are implemented in web services to protect them from external attacks. It is a set of protocols that ensure security for SOAP-based messages by implementing the principles of confidentiality, integrity and authentication

Web server security refers to the tools, technologies and processes that enable **information security (IS)** on a Web server. This broad term encompasses all processes that ensure that a working Internet server operates under a security policy.

Web services security constitutes the technological and managerial procedures applied to the system to ensure the confidentiality, integrity, and availability of information that is exchanged by the Web service, This article explores security issues specific to Web services and illustrates the engineering and testing practices required to ensure security throughout the Web services development life cycle.

Features of Web Services:

The Features of Web Services are as follows:

1. Web services are designed for application to application interaction.
2. It should be interoperable.
3. It should allow communication over the network.

Components of Web Services

- The web services must be able to fulfill the following conditions:
- The web service must be accessible over the internet.

SECURING WEB APPLICATIONS, SERVICES AND SERVERS

- The web service is discoverable through a common mechanism like UDDI.
- It must be interoperable over any programming language or Operating System.

Uses of Web Services

- Web services are used for reusing the code and connecting the existing program.
- Web services can be used to link data between two different platforms.
- It provides interoperability between disparate applications.

Types of Web Services

There are mainly two types of web services

1. SOAP web services.
2. RESTful web services.

1. SOAP Web Services

SOAP acronym for Simple Object Access Protocol. It defines the standard XML format. It also defines the way of building web services. We use Web Service Definition Language (WSDL) to define the format of request XML and the response XML.

2. RESTful Web Services

REST stands for Representational State Transfer. It is developed by Roy Thomas Fielding who also developed HTTP. The main goal of RESTful web services is to make web services more effective.

It does not define the standard message exchange format. We can build REST services with both XML and JSON. JSON is more popular format with REST. The key abstraction is a resource in REST. A resource can be anything. It can be accessed through a Uniform Resource Identifier (URI).

For example: The resource has representations like XML, HTML, and JSON. The current state is captured by representational resource. When we request a resource, we provide the representation of the resource. The important methods of HTTP are:

1. GET: It reads a resource.

2. PUT: It updates an existing resource.
3. POST: It creates a new resource.
4. DELETE: It deletes the resource.

Basic security for HTTP Applications and Servers

The HTTP applications and services can be secured by implementing following mechanisms,

1. **Basic Authentication**

It is a simple authentication process in which client sends a request message to the server in order to access the resource. The request contains www-authenticate header andparameter 'Basic' followed by base 64 encoded username and password.

The server accepts or denies the client request by decoding and validating the i.e ., username and password.

If the server accepts the request then it allows the client to access the resource. it sends 401 status code as response that represents the request contains bad or missing syntax.

Limitations

In this authentication mechanism, the base 64 encoding can be decoded easily. So this must be used in combination with a channel protection mechanism that provides confidentiality.

In the configuration file, the username and password are not encrypted properly even though developers may try to make changes in the code.

2. **Server Authentication**

In this mechanism, server authenticates itself to the client. Here the authentication cess is initiated by the client by sending the message that includes the parameters such ILS versions, cipher suites and random data to the server. Once the client message is sent, the client waits for a similar response from the server which includes the parameters as client's message parameters. Next, the server responds to the client sending the server-certificate message that consists of similar parameters. The click validates this

certificate message and generates the master secret for the purpose of session keys. These keys can be used to establish a encrypted communicated channel.

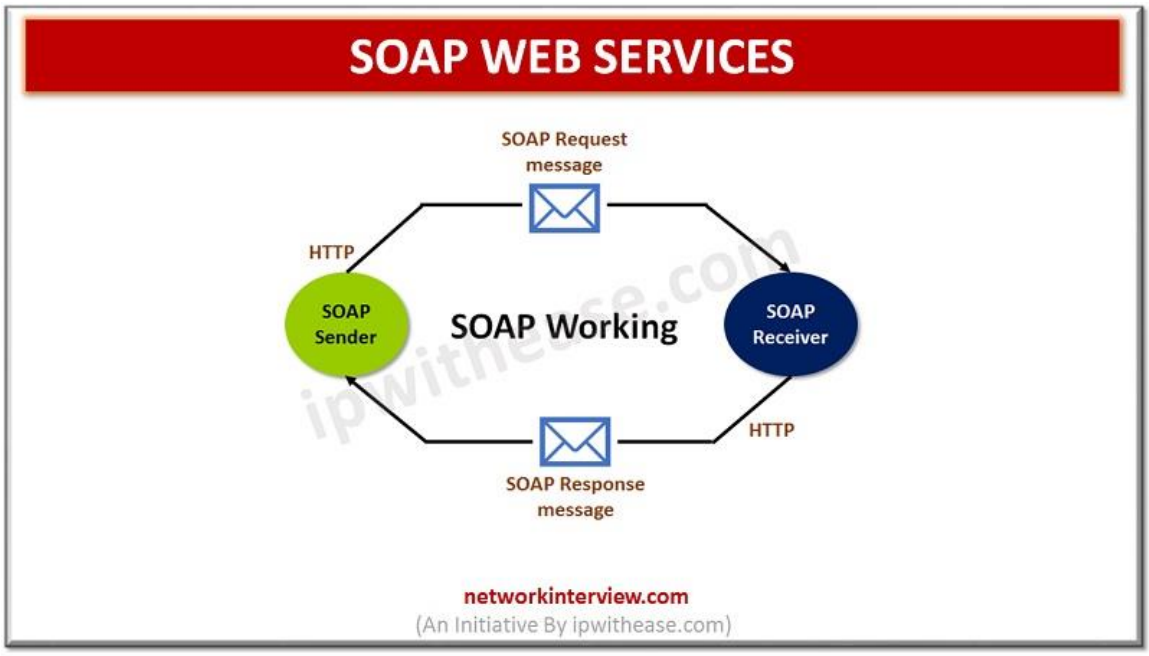
3. Mutual Authentication

In this mechanism, both client and server must be authenticated i.e ., confirm their identities to each other. Initially, server authenticates itself to the client by sending the certificate request message. Once the client is satisfied with the server authentication i+ sends a client certificate message to the server for authenticating itself.

BASIC SECURITY FOR SOAP SERVICES

SOAP is an abbreviation that stands for **Simple Object Access Protocol**. During the implementation of web services in computer networking, structured information is exchanged in various ways. SOAP is one such messaging protocol, and it is used because it offers neutrality, independence, extensibility, and verbosity. The message format is in XML (eXtensible Markup Language), and it uses application layer protocols for negotiation and transmission, primarily HTTP, with some legacy systems using SMTP.

The SOAP request takes the form of an XML document with a header, an envelope and a body containing the payload. The header is optional and is used to provide metadata about the transaction and the envelope defines the namespaces of the transaction while the body contains the payload

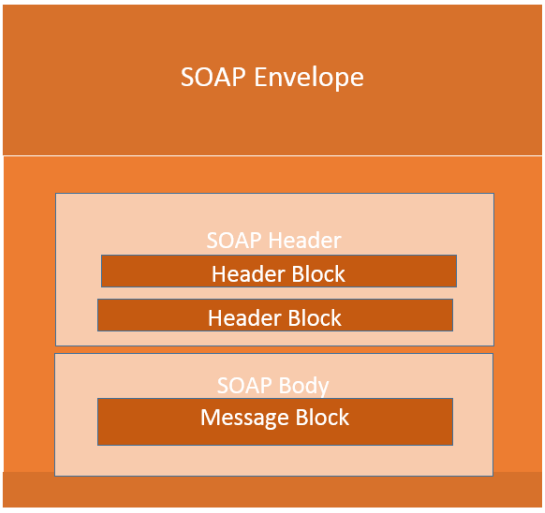


SECURING WEB APPLICATIONS, SERVICES AND SERVERS

SOAP Building Blocks

The SOAP specification defines something known as a "**SOAP message**" which is what is sent to the web service and the client application.

The below diagram of SOAP architecture shows the various building blocks of a SOAP Message.



Advantages of Soap Web Services

WS Security: SOAP defines its own security known as WS Security.

Language and Platform independent: SOAP web services can be written in any programming language and executed in any platform.

Disadvantages of Soap Web Services

Slow: SOAP uses XML format that must be parsed to be read. It defines many standards that must be followed while developing the SOAP applications. So it is slow and consumes more bandwidth and resource.

WSDL dependent: SOAP uses WSDL and doesn't have any other mechanism to discover the service.

IDENTITY MANAGEMENT AND WEB SERVICES

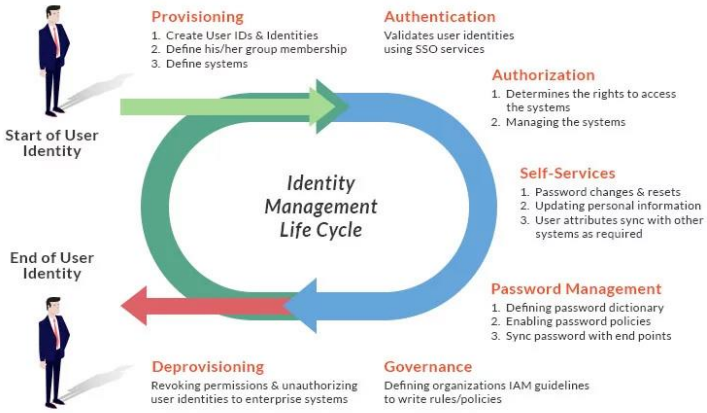
Identity Access and Management is abbreviated as IAM. In simple words, it restricts access to sensitive data while allowing employees to view, copy and

SECURING WEB APPLICATIONS, SERVICES AND SERVERS

change content related to their jobs. This information can range from sensitive information to company-specific information.

The cybersecurity of any company depends on its identity management structure. It adds another degree of security to systems and equipment used by suppliers, customers, workers, and third-party partners. On the other hand, the framework should be compatible with any other security systems that may already exist.

Flow Diagram of Identity and Access Management Sequence



IAM policies:

Identity management covers five policies that must be addressed for the framework to be successful.

The method through which the system recognizes employees/individuals.

The method for identifying and assigning responsibilities to personnel.

Employees and their responsibilities should be able to be added, removed, and updated via the system.

Allow certain levels of access to be provided to groups or individuals.

Keep sensitive data safe and the system safe from hacking.

Implementation Guide for IAM:

1. Consider your company's size and type –

IAM is important for company authentication and handles identity to allow users to exercise their rights from a remote location. It also aids in calculating the surroundings when multiple devices are used. IAM is highly successful for all types of organizations, large, small, and medium. Additional options are available for larger organizations, and you can choose the tool that streamlines user access.

2. Create a strategy for IAM integration –

This is a well-known story with risks, and it has been implemented with IAM and moved to the cloud. Employees must use tools that are permitted by the company, sometimes called shadow IT. IAM will devote time and resources to developing a comprehensive identity management strategy

SECURING WEB APPLICATIONS, SERVICES AND SERVERS

.

3. Find the best IAM solution for you –

There are a few key components of IAM that you may use to keep your business from collapsing, which are listed below:

- Access management products control a user's identification while also enabling a few tools such as the network, web resources, cloud, and so on.
- Multi-factor and risk authentication method helps in verification of the identity of an individual.
- Where passwords fail, password tokens provide additional security.

As a business owner, you must learn about all of the IAM tools available to protect your company's identity and access management.

Benefits of Using an Identity and Access Management System :

We will learn about the various organizational benefits in this section. These are listed below –

- **Reduce risk –**
  You'll have more user control, which means you'll be less vulnerable to internal and external data breaches. When hackers utilize the user credential as a crucial technique to obtain access to the business network and resources, this is critical.
- **Secure access –**
  When your company grows, you will have additional employees, customers, contractors, partners, etc. Your company's risk will increase at the same time, and you will have higher efficiency and production overall. IAM allows you to expand your business without compromising on security at the moment.
- **Meeting Compliance –**
  A good IAM system can help a company meet its compliance requirements as well as meet the rapidly expanding data protection regulations.
- **Minimize Help Desk Requests –**
  IAM looks into the user's needs and then resets the password and the help desk will help them automate the same. Getting the authentication requires the user to verify their identity without bothering the system administrator as they need to focus on other things in the business, which gives more profit to the business.

WEB SERVICES

A web service is a set of open protocols and standards that allow data to be exchanged between different applications or systems.

Web services have the advantage of allowing programs developed in different languages to connect with one another by exchanging data over a web service between clients and servers.

SECURING WEB APPLICATIONS, SERVICES AND SERVERS

Functions of Web Services

- It's possible to access it via the internet or intranet networks.
- XML messaging protocol that is standardized.
- Operating system or programming language independent.
- Using the XML standard, it is self-describing.
- A simple location approach can be used to locate it.

Components of Web Services

The basic web services platform is XML + HTTP. All the standard web services work using the following components –

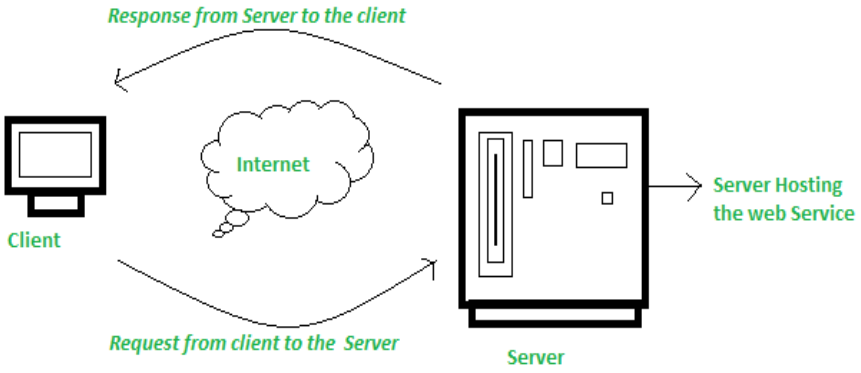
- SOAP (Simple Object Access Protocol)
- UDDI (Universal Description, Discovery and Integration)
- WSDL (Web Services Description Language)

How Does a Web Service Work?

A web service enables communication among various applications by using open standards such as HTML, XML, WSDL, and SOAP. A web service takes the help of –

- XML to tag the data
- SOAP to transfer a message
- WSDL to describe the availability of service.

The diagram depicts a very simplified version of how a web service would function. The client would use requests to send a sequence of web service calls to a server that would host the actual web service.



Features/Characteristics Of Web Service

Web services have the following features:

SECURING WEB APPLICATIONS, SERVICES AND SERVERS

(a) XML Based:
(b) Loosely Coupled
(c) Capability to be Synchronous or Asynchronous:
(d) Coarse-Grained
(e) Supports Remote Procedural Call
(f) Supports Document Exchanges

Advantages Of Web Service

Using web services has the following advantages:

(a) Business Functions can be exposed over the Internet
(b) Interoperability
(c) Communication with Low Cost
(d) A Standard Protocol that Everyone Understands
(e) Reusability

Authorization patterns

These are security mechanisms that you can use to decide your client's privileges related to system resources. These system resources could be files, services, data, and application features built on your client's identity.
The Authorization pattern takes the form of a set of relationships between resources and the privileges that they possess in regard to a given process

Access Control

Access control refers to an ability of either allowing or disallowing a user from accessing particular resource. There are many mechanisms that exist and which are employed for performing access control. Such mechanisms not only manage physical, logical resources but are also capable of managing digital resources. Some of the access control models are as follows, ofalist topp 90

IBAC: IBAC stands for Identity Based Access Control. This model provides access control based on the identity of a user. (? to nod

RBAC: RBAC stands for Role-Based Access Control. This model provides access control based on the role/ position of an individual in an organization.

ABAC: ABAC stands for Attribute Based Access Control. This model provides access control to the users based on the specific attributes.

SECURING WEB APPLICATIONS, SERVICES AND SERVERS

Access Control Lists (ACL)

Access control lists consists of list of users with their access privileges. These privileges can be related to software components, network devices, storage devices etc. ACLs typically specify the following,

- List of users who can access the system
- List of objects/items that can be accessed
- Time at which the system can be accessed
- Location at which the system can be accessed

SECURITY CONSIDERATIONS, CHALLENGES

Security Considerations

Websites are always to prone to security risks. Cyber crime impacts your business by hacking your website. Your website is then used for hacking assaults that install malicious software or malware on your visitor's computer.

The Security Considerations are as follows;

Updated Software : It is mandatory to keep you software updated. It plays vital role in keeping your website secure.

SQL Injection : It is an attempt by the hackers to manipulate your database. It is easy to insert rogue code into your query that can be used to manipulate your database such as change tables, get information or delete data.

Cross Site Scripting (XSS) : It allows the attackers to inject client side script into web pages. Therefore, while creating a form It is good to endure that you check the data being submitted and encode or strip out any HTML.

Error Messages : You need to be careful about how much information to be given in the error messages. For example, if the user fails to log in the error message should not let the user know which field is incorrect: username or password.

Validation of Data : The validation should be performed on both server side and client side.

SECURING WEB APPLICATIONS, SERVICES AND SERVERS

Passwords : It is good to enforce password requirements such as of minimum of eight characters, including upper case, lower case and special character. It will help to protect user's information in long run.

Upload files : The file uploaded by the user may contain a script that when executed on the server opens up your website.

SSL : It is good practice to use SSL protocol while passing personal information between website and web server or database.

Security Challenges

Like any software web application or web services are also prone to security issues related to authentication, availability and integrity. New and challenging problems related to security arise due to the distributed nature of the "web services" or "web applications" and their cross-platform access and also during service composition. As the web services provide access to the data in an autonomous way, the confidentiality and authenticity of the data transmitted through them attains more importance.

In the recent years, many technologies and standards have emerged in order to handle the security issues related to web services. However, new threats and attacks related to web services are also coming to forefront. The basic security requirements of any web based application are Authentication, Authorization, Confidentiality, Integrity, Non-repudiation, Code Injection, Malware and Denial-of-Service.

Unit-3
Intrusion Detection and Prevention

UNIT-III: INTRUSION DETECTION AND PREVENTION:
Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusion detection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.

INTRUSION- Introduction

During the past two decades, dependence on technology has massively increased which has created a new scope of crime relating to computers.

Q) What is Intrusion or Network Intrusion?

A) Intrusion or Network Intrusion refers to any unauthorized activity on a digital network.

Network intrusions often involve the theft of valuable network resources and almost always compromise the security of networks and their data.

An intrusion detection and prevention system (IDPS) monitors a network for possible threats to alert the administrator, thereby preventing potential attacks.

A network is generally intruded or attacked for one of three reasons:

1. **Hacktivism**: Hacktivism is the combination of two words- 'Hacking' and 'Activism'. It is done by intruders who want to hack in order to prove a political agenda or a social cause.
2. **Steal Money or Data**: This type of intrusion is done to steal money or data from the other
party. Usually, the purpose of this is to exploit the other party of financial gain.
3. **Spy**: Spying is state sponsored network intrusion in order to spy on their enemies and sometimes partners.

Since the internet is a huge place, it is very difficult to pinpoint a specific way in which a network intrusion occurs. However, the following are some common technique through which network intrusion has occurred:

- **Multi-Routing**: This refers to when the intruders use multiple sources to intrude which helps them avoid detection. This is also known as asymmetric routing.
- **Traffic Flooding**: In this type of attack, the intruders flood the victim's systems with traffic that they cannot handle, in order to cause chaos and confusion. When the systems have too much traffic to check, they can easily go undetected.
- **Trojan Horse Malware**: Trojan horse malware provides the attackers with a network back door, allowing them unrestricted access to the network.
- **Buffer Overflow Attacks**: The buffer overflow attack refers to rewriting certain sections of computer memory code for later use as part of the intrusion.
- **Worms**: This type of virus is most common and effective. Worms usually spread through e-mail or instant messaging and can spread throughout the network.

Unit-3
Intrusion Detection and Prevention

Q) What is Physical theft?

A) By stealing a computer system, the attacker has all the physical access he or she could have, and unless the sensitive data on the system is heavily encrypted, the data is likely to be compromised. Having physical access to a computer system allows an attacker to bypass most security measures in place by booting another operating system or tool from a CD-ROM or other bootable media.

An unauthorized user who gains physical access to a computer is most likely able to copy data directly from it. They may also compromise security by making operating system modifications. This problem is most common with lost and stolen laptops. A lot of sensitive information can be put at risk if a laptop containing such information is stolen.

Q) what is ABUSE OF PRIVILEGES

A) An insider is an individual who has some level of authorized access to the IS (Information System) environment and systems because of his role in the organization. The level of access can range from that of a normal user to a system administrator with nearly unlimited privileges. When an insider abuses his privileges, the impact can be devastating. Even a relatively limited privilege user has an advantage over an outsider because of his knowledge of the IS environment, critical business processes, and potential knowledge of security weaknesses or vulnerabilities. An insider may use his access to steal sensitive data such as customer databases, trade secrets, national security secrets, or personally identifiable information.

Q) what is UNAUTHORIZED ACCESS BY OUTSIDER

A) An outsider is considered to be anyone who does not have authorized access privileges to an information system. To gain access, the outsider may try to gain possession of valid system credentials via social engineering or even by guessing username and password pairs in a brute force attack. Alternatively, the outsider may attempt to exploit vulnerability in the target system to gain access. Often the result of successfully exploiting system vulnerability leads to some form of high-privileged access to the target, such as an "Administrator" or Administrator-equivalent account on a Microsoft Windows system or "root" or root-equivalent account on a UNIX or Linux based system. Once an outsider has this level of access on a system, he or she effectively "owns" that system and can steal data or use the system as a launching point to attack other systems.

Note: Social engineering is the art of manipulating people so they give up their confidential information, like- passwords, credit-card details etc.

Q) What is Malware infection?

A) Malware is any type of malicious software designed to cause harm or damage to a computer without the user's permission. Basically, it is unwanted software that can be installed on computer of internet user without his/her knowledge or consent, when online.

Unit-3
Intrusion Detection and Prevention

Malware includes computer viruses, worms, trojans and other malicious programs. These are most frequently used to steal personal or business information. Common sources of malware are: E-mail attachments, malicious websites, and pen drives.

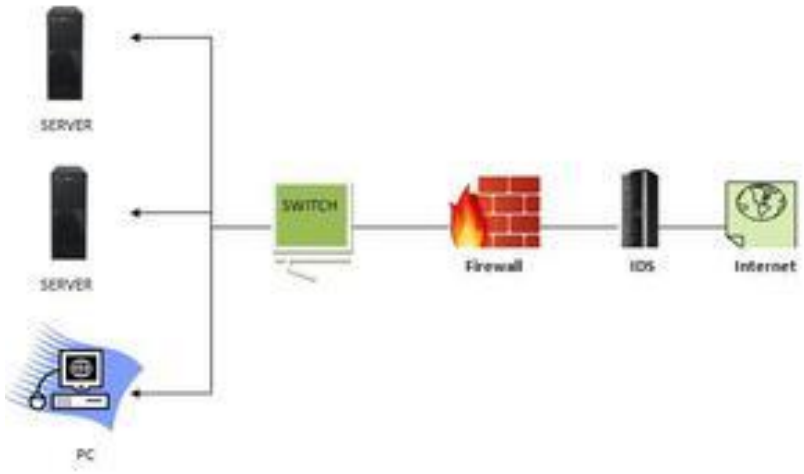
Today we see malware being used by intruders to gain access to systems, search for valuable data such as PII (Personally Identifiable Information) and passwords, monitor real-time communications, provide remote access/control, and automatically attack other systems.

INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

Intrusion Detection and Prevention Systems (IDPS) are security systems used to detect and prevent security threats to computer systems and networks. These systems are used to detect intruders and prevent their malicious activities before any damage is done. These systems include both virtual and physical systems that scan the traffic of a network either through the cloud or through on-premises for any signs of unusual activity. As soon as these systems detect kind of malicious activity, they take action to prevent it.

Q) What is IDS? Explain Types of IDS (INTRUSION DETECTION SYSTEM)

A) A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.

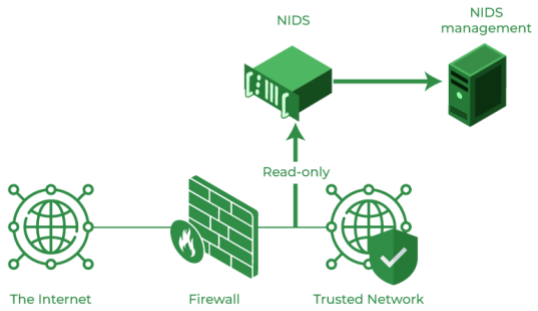


Classification of Intrusion Detection System (types)

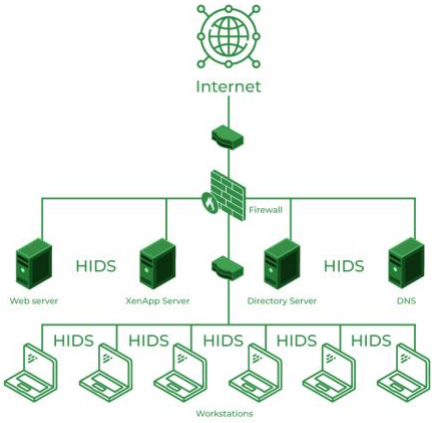
IDS are classified into 5 types:

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 behaviour is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.



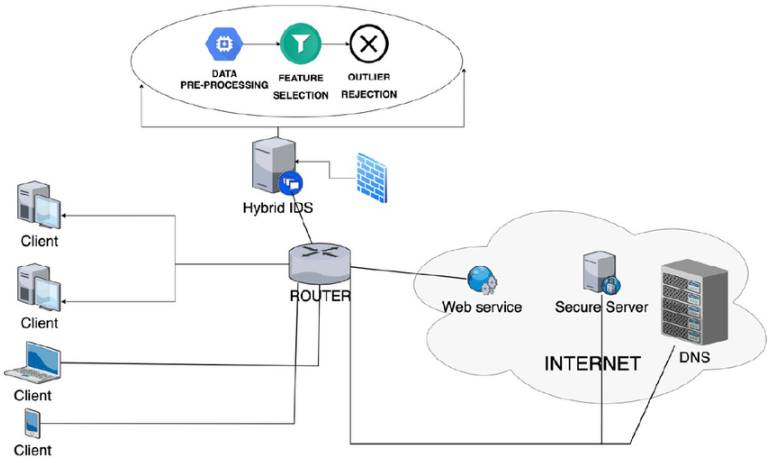
2)Host Intrusion Detection System (HIDS): Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot 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 a system or agent that would consistently reside 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 accepting the related **HTTP protocol**. As HTTPS is unencrypted 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): An 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 explicitly 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 to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.



Benefits of IDS

Detects malicious activity: IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.

Improves network performance: IDS can identify any performance issues on the network, which can be addressed to improve network performance.

Compliance requirements: IDS can help in meeting compliance requirements by monitoring network activity and generating reports.

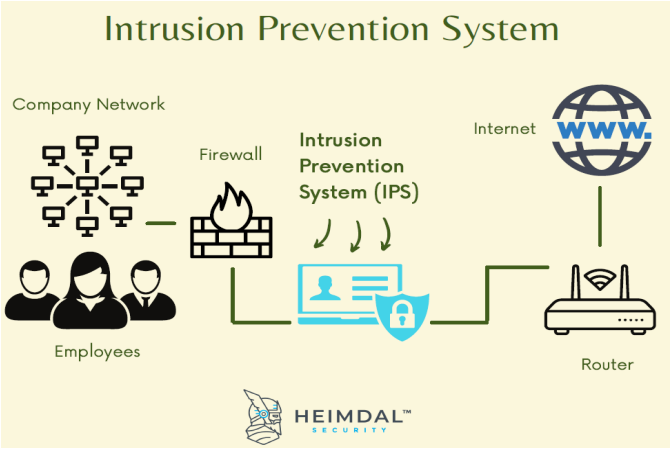
Provides insights: IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Q) What is Intrusion Prevention System (IPS). Explain types of IPS in detail.

A) Intrusion prevention system (IPS) is an automated network security tool that continuously monitors your network traffic stream, to detect and prevent threats and malicious incidents.

The main functions of an IPS are to gather and log essential information, detect suspicious behaviour, attempt to stop the activity and finally report to system administrators.

Unit-3
Intrusion Detection and Prevention



Apart from monitoring networks and preventing threats, IPS security is also an excellent method of preventing employees and network guests from violating corporate security policies.

Types of Intrusion Prevention Systems

IPS systems can be classified into several major types:

1. **NIPS**. Network-based intrusion prevention systems look for questionable traffic by analysing the entire network's protocol activity.
2. **WIPS**. Wireless intrusion prevention systems work in the same way as NIPS, but they're looking across the entire wireless network.
3. **HIPS.** Host-based intrusion prevention systems are secondary software packages that look for malicious activity and analyse events within a single host.
4. **NBA.** Network behaviour analysis is interested in the network traffic and tries to identify threats that produce suspicious traffic flows.

Detection Methods used by an IPS

An Intrusion Prevention System (IPS) is designed to prevent various types of malware: viruses and worms, exploits, Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks, and it does so by using various approaches:

1. **Signature-Based**. This approach relies on predefined signatures of common network threats. If the IPS system finds an attack that matches a certain signature or pattern, it immediately takes the necessary actions.
2. **Anomaly-Based.** As you might guess, the anomaly-based approach looks for any abnormal or unexpected behaviour. When an anomaly is detected, the IPS system blocks its access to the target host.
3. **Policy-Based.** The policy-based approach makes use of the security policies that the administrators need to configure according to the network infrastructure and each company's
4. **Security policies**. In this case, if the IPS system discovers an activity that violates a security policy, it triggers an alert to notify the system administrators.

When it comes to intrusion countermeasures, an intrusion prevention system can:

- Configure a firewall to increase protection;
- Replace malicious parts of an email, for example (like fake links), with warnings about the content that was removed;
- Notify system administrators about possible security breaches by sending automated alarms;

- Drop the detected malicious packets;
- Block traffic from suspicious IT addresses;
- Reset connections.

The Key Benefits of an Intrusion Prevention System

- **Automation**
  Nowadays, companies need a pretty high level of security to ensure safe communication, and the ability to prevent intrusion by having an automated solution that can take the necessary actions with minimal IT intervention and low costs is a nice advantage.

- **Achieve Compliance**
  Investing in cybersecurity is not only a necessity but also a requirement of compliance. By choosing an IDS or IPS system you will, simultaneously, gain peace of mind because your network will be safe from multiple online threats and check off a box on the compliance sheet because you'll address a significant number of CIS security controls.

- **Enforcing Policies**
  IPS/IDS solutions can help you configure internal security policies at the network level. For example, you can use it to block other VPN traffic if you support only one VPN.

What Is the Difference between IDS and IPS?

IDS stands for Intrusion Detection System and refers to devices or applications that monitor networks or systems looking for malicious activities or policy violations.

The main difference between an IPS system and an IDS system is that:

IPS systems control the access to IT networks by monitoring intrusion data and taking the necessary actions to prevent an incident or attack.

IDS systems do not block attacks– they only monitor networks and, if they detect potential threats, they send alerts to system administrators.

Moreover, an IDS system requires a human or another system to look at the results it finds, while an IPS system requires its database to be continuously updated with the new threat information.

Q) What is Anti- Malware Software

A) Anti - Malware is a type of software program created to protect information technology (IT) systems and individual computers from malicious software, or malware. Antimalware programs scan a computer system to prevent, detect and remove malware.

Malware is short for malicious software, which is software specifically designed to damage data or a computer system.

How antimalware works

Antimalware software uses three strategies to protect systems from malicious software: signature-based detection, behavior-based detection and sandboxing.

1. **Signature-based malware detection**

Signature-based malware detection uses a set of known software components and their digital signatures to identify new malicious software.

2. **Behaviour-based malware** detection Behaviour-based malware detection helps computer security professionals more quickly identify, block and eradicate malware by using an active approach to malware analysis.

3. **Sandboxing** Sand boxing is a security feature that can be used in antimalware to isolate potentially malicious files from the rest of the system. Sandboxing is often used as a method to filter out potentially malicious files and remove them before they have had a chance to do damage.

Benefits of Anti-Malware

The value of antimalware applications is recognized beyond simply scanning files for viruses. Antimalware can help prevent malware attacks by scanning all incoming data to prevent malware from being installed and infecting a computer.

Antimalware programs can help in the following ways:

- prevent users of from visiting websites known for containing malware;
- prevent malware from spreading to other computers in a computer system;
- provide insight into the number of infections and the time required for their removal; and
- provide insight into how the malware compromised the device or network.

The major benefits of antimalware software are listed below: Real-time protection.

- Boot-time scan.
- Scanning of individual files.
- Protection of sensitive information.
- Restoration of corrupted data.
- Protection from spam and identity theft.
- Provides robust web protection.
- Provides quick scan of the removable device.

Terminates unwanted ads and spam website. Improves the PC performance.

Q) Write about Security Information Management (SIM).

A) Security Information Management (SIM) is a process of collecting, monitoring, and examining log data to find and report suspicious activity on the system. This process is automated by security information management systems or tools.

Log data is nothing more than a file that collects and stores everything that happens in the system. Log files contain information about system activities such as running applications, services, errors that have occurred. With security log files, one can know the IP address of the system, MAC or internet address, login credentials and the status of the system. If such details fall in the hands of intruders, they might use the details destructively. This is one of the main reasons for the birth of security information management.

The log data is collected from various sources such as firewalls, intrusion detection systems, antivirus software, proxy servers, file systems, etc. Security information is monitored and maintained based on data collected from all sources.

SIM enables cybersecurity professionals to access and analyse security information from a variety of sources, including the following:

- Antivirus Software
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- File Systems
- roxy Servers
- Firewalls
- Routers

How SIM Works?

- SIM systems keep track and show the activity analysis of system events as they occur.
- It translates the event data collected from many resources into a common and simplified format.
- SIM systems collect and coordinate data from various resources in such a way that helps administrators to recognize the real threats and false positives on the system. False positives mean events that seem to be a major threat but in reality it's not a threat.

As soon as suspicious activity occurs, the SIM tool responds to the event by sending alerts to administrators of organizations and by generating reports and graphical representations such as charts and graphs.

Q) Write about Network Session Analysis:

A) Network session data No details represents are about saved a high-level the and content can summary of the of conversation conversations are saved, an incident but various or as an systems. The conversation be useful when investigating of indicator of suspicious activity.

The major elements that constitute the network session are:

- Source IP address
- Source port
- estination IP address
- Destination port
- Timestamp information

Using the collected session information, an analyst can examine traffic patterns on a network to identify which systems are communicating with each other and identify suspicious sessions that warrant further investigation.

For example, a server that is configured for internal use by users and has no legitimate reason to communicate with addresses on the Internet will raise an alarm if one or more sessions suddenly arise between the internal server and external addresses. At this point, the analyst may suspect a malware infection or other system compromise and investigate further.

Numerous other queries can be generated to identify sessions that are abnormal in one way or other, such as : Excessive byte counts, excessive session lifetime, or unexpected ports being used.

Network Traffic Analysis (NTA) or Network Session Analysis (NSA) is a method of network activity to detect security and operational issues and other anomalies.

Network traffic analysis focuses on overall traffic observation rather than monitoring specific parts of the network or assets connected to the network.

Major benefits of NTA include:

1. Collecting a real-time and historical record of what's happening on your network.
2. Detecting malware such as ransomware activity.
3. Troubleshoot operational and security issues.
4. Respond faster to investigations with rich details and additional network context.
5. Improved visibility into devices connecting to your network (eg. IoT devices).

Implementing a solution that can continuously monitor network traffic gives you the insight you need to optimize network performance, minimize your attack surface, enhance security, and improve the management of your resources.

Q) Write about System Integrity Validation.

A) The rise of powerful and silent malware that leave no trace of an intrusion on a computer's hard drive has given rise to the need for technology that can analyze a running system and its memory and provide a series of metrics regarding the integrity of the system.

System Integrity Validation (SIV) technology is still in its early stages and an active area of research, but it primarily focuses on live system memory analysis and the notion of deriving trust from known-good system elements. This is accomplished by comparing the running state of the system, including the processes, threads, data structures, and modules loaded into memory, with the static elements on disk from which the running state was supposedly loaded. Through a number of cross-validation processes, discrepancies between what is running in memory and what should be running can be identified.

When properly implemented, SIV can be a powerful tool for detecting intrusions, even those using advanced techniques.

UNIT-4
CRYPTOGRAPHY AND NETWORK SECURITY

CYBER SECURITY

Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber attackers. It is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc.

It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification, or unauthorized access. Therefore, it may also be referred to as information technology security.

INTRODUCTION

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word *kryptos,* which means hidden.

Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, computational-complexity theory, and probability theory.

Cryptography is the art and science of making a cryptosystem that is capable of providing information security.

Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

FEATURES OF CRYPTOGRAPHY

1. **Confidentiality**

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy.

Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

2. **Data Integrity**

It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.

Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

3. **Authentication**

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Authentication service has two variants –

Message authentication identifies the originator of the message without any regard router or system that has sent the message.

Entity authentication is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

4. **Non-repudiation**

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

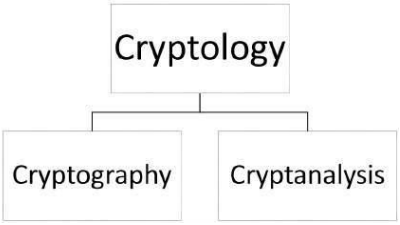
Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

Context of Cryptography

Cryptology, the study of cryptosystems, can be subdivided into two branches –

1. **Cryptography**
2. **Cryptanalysis**

Cryptology refers to the study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them.



A **cryptosystem** is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

Cryptography Primitives (types)

Cryptography primitives are nothing but the tools and techniques in Cryptography that can be selectively used to provide a set of desired security services –

1. **Encryption**
2. **Hash functions**
3. **Message Authentication codes (MAC)**
4. **Digital Signatures**

Components of a Cryptosystem

The various components of a basic cryptosystem are as follows –

Plaintext. It is the data to be protected during transmission.

Encryption Algorithm. It is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text.

Cipher text. It is the scrambled version of the plaintext produced by the encryption algorithm using a specific encryption key. The cipher text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

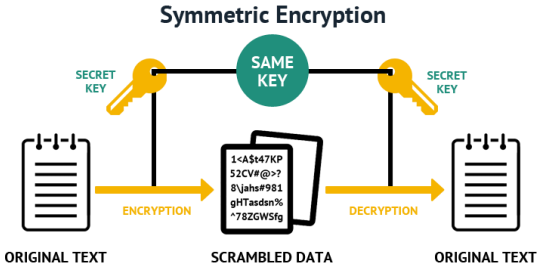
Decryption Algorithm, It is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.

Encryption Key. It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text.
Decryption Key. It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext.
For a given cryptosystem, a collection of all possible decryption keys is called a key space.
An interceptor (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the cipher text and may know the decryption algorithm. He, however, must never know the decryption key.

Types of Cryptosystems
Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system –

1. **Symmetric Key cryptography**
2. **Asymmetric Key cryptography**

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the cipher text with the key that is unrelated to the encryption key.
Symmetric Key Cryptography
The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption.
The study of symmetric cryptosystems is referred to as symmetric key Encryption. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems. in the case of symmetric encryption, the same key is used for both encrypting and decrypting messages. Because the entire mechanism is dependent on keeping the key a shared secret — meaning that it needs to be shared with the recipient in a secure way so that only they can use it to decrypt the message — it does not scale well.



Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.
Advantages of Symmetric key Cryptography
Persons using symmetric key encryption must share a common key prior to exchange of information.

- Keys are recommended to be changed regularly to prevent any attack on the system.

- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n - 1)/2$.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Disadvantages of Symmetric Key Cryptography

There are two restrictive challenges of employing symmetric key cryptography.

- **Key establishment** – Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
- **Trust Issue** – Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver 'trust' each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

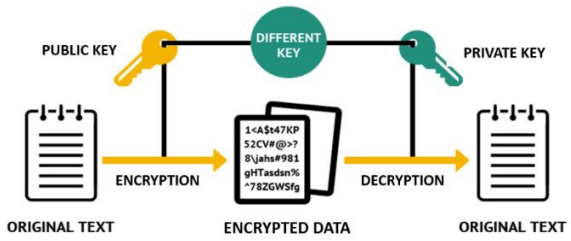
These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

Asymmetric Key Cryptography

Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons.

Asymmetric encryption uses a pair of related keys — a public and a private key. The public key, which is accessible to everyone, is what's used to encrypt a plaintext message before sending it. To decrypt and read this message, you need to hold the private key. The public and the private keys are mathematically related, but the private key cannot be derived from it.

In asymmetric encryption (also known as public-key cryptography or public key encryption), the private key is only shared with the key's initiator since its security needs to be maintained.



Advantages of Asymmetric key cryptography

- Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext.
- It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called Public Key Encryption.

- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
- When Host1 needs to send data to Host2, he obtains the public key of Host2 from repository, encrypts the data, and transmits.Host2 uses his private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.

Disadvantages of Asymmetric key Cryptography

- One drawback of using public-key cryptography for encryption is the lack of speed. Popular secret-key encryption systems are substantially quicker than any commonly accessible public-key encryption technique.
- Authentication of public keys is recommended/ required. No one can be certain that a public key corresponds to the individual it identifies, so everybody must verify that their public keys are theirs.
- It consumes more computer resources. It necessitates much more resources than single-key encryption.
- A widespread security breach is likely if an intruder obtains a person's private key and reads his or her entire message.
- The loss of a private key can be irreversible. When a private key is lost, all incoming Messages cannot be decrypted.

Comparision between symmetric key cryptography and Asymmetric key cryptography

Differentiator	Symmetric Key Encryption	Asymmetric Key Encryption
1. Symmetric Key vs Asymmetric key	Only one key (symmetric key) is used, and the same key is used to encrypt and decrypt the message.	Two different cryptographic keys (asymmetric keys), called the public and the private keys, are used for encryption and decryption.
2. Complexity and Speed of Execution	It's a simple technique, and because of this, the encryption process can be carried out quickly.	It's a much more complicated process than symmetric key encryption, and the process is slower.
3. Length of Keys	The length of the keys used is typically 128 or 256 bits, based on the security requirement.	The length of the keys is much larger, e.g., the recommended RSA key size is 2048 bits or higher.
4. Usage	It's mostly used when large chunks of data need to be transferred.	It's used in smaller transactions, primarily to authenticate and establish a secure communication channel prior to the actual data transfer.

5. Security	The secret key is shared. Consequently, the risk of compromise is higher.	The private key is not shared, and the overall process is more secure as compared to symmetric encryption.
Examples of Algorithms	Examples include RC4, AES, DES, 3DES, etc.	Examples include RSA, Diffie-Hellman, ECC, etc.

Message Authentication

Message authentication allows one party—the sender—to send a message to another party—the receiver—in such a way that if the message is modified en route, then the receiver will almost certainly detect this. Message authentication is also called data-origin authentication. Message authentication is said to protect the integrity of a message, ensuring that each message that it is received and deemed acceptable is arriving in the same condition that it was sent out—with no bits inserted, missing, or modified.

Message authentication provides two services. It provides a way to ensure message integrity and a way to verify who sent the message

Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid.

Symmetric encryption provides authentication among those who share the secret key. Encryption of a message by a sender's private key also provides a form of authentication.

The two most common cryptographic techniques for message authentication are

1. **message authentication code (MAC) and**
2. **secure hash function**.

A **MAC** is an algorithm that requires the use of a secret key. A MAC takes a variable length message and a secret key as input and produces an authentication code. A recipient in possession of the secret key can generate an authentication code to verify the integrity of the message.

A **hash function** maps a variable-length message into a fixed length hash value, or message digest. For message authentication, a secure hash function must be combined in some fashion with a secret key

Authentication Requirements

In the context of communications across a network, the following attacks can be identified:

1. **Disclosure:** Release of message contents to any person or process not possessing the appropriate cryptographic key.
2. **Traffic analysis**: Discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined.
3. **Masquerade**: Insertion of messages into the network f from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent

acknowledgments of message receipt or non-receipt by someone other than the message recipient.

4. **Content modification**: Changes to the contents of a message, including insertion, deletion, transposition, and modification.
5. **Sequence modification**: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.
6. **Timing modification**: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed
7. **Source repudiation**: Denial of transmission of message by source.
8. **Destination repudiation**: Denial of receipt of message by destination. Measures to deal with the first two attacks are in the realm of message confidentiality.

Measures to deal with items 3 through 6 in the foregoing list are generally regarded as message authentication.

Authentication Functions

Any message authentication or digital signature mechanism has two levels of functionality.

• At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message.

• This lower-level function is then used as a primitive in a higher level authentication protocol that enables a receiver to verify the authenticity of a message.

These are grouped into three classes, as follows:

Message encryption: The cipher text of the entire message serves as its authenticator.

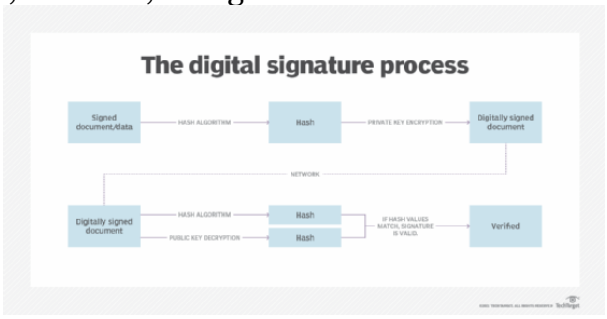
Message authentication code (MAC): A function of the message and a secret key that produces a fixed-length value that serves as the authenticator.

Hash function: A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator.

Digital signature

Digital Signature in Cryptography is a value calculated from the data along with a secret key that only the signer is aware of. The receiver needs to be assured that the message belongs to the sender. This is crucial in businesses as the chances of disputes over data exchange are high.

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.



Digital Signature Algorithms

There are three algorithms at work in Digital Signatures. They are as follows:

1. **Key Generation Algorithms** – Key Generation Algorithms help ensure authenticity and integrity or it would be very easy to tamper with the data. They also prevent anyone from pretending to be the sender.
2. **Signing Algorithms** – Signing Algorithms make one-way hashes of the data that has to be signed. Then they encrypt the hash value using the signature key. The encrypted hash along with the other information is the Digital Signature.
3. **Signature Verification Algorithms** – Signature Verification Algorithms help process the Digital Signature and the verification key to generate some values. The algorithm also processes the same hash function on the data received and creates a hash value.

Importance of Digital Signature

Digital Signatures are a very important tool in cryptography. Let's find out why that is

1. **Message Authentication** – The private key is only known to the sender. The verifier can use the public key of the sender to validate that the Digital Signature was created by the sender.
2. **Data Integrity** – If at any time the data is attacked, there will be a discrepancy in the hash value and the verification algorithm as they won't match. Due to this, the receiver will end up rejecting the message and 3.
3. **Non-repudiation** – The signer is the only one who is aware of the signature key so, naturally, they are the only ones who can create a specific signature. Whenever there is a dispute, the data along with the Digital Signature can be presented as evidence.

Privacy, Integrity, Non-Repudiation, and Authentication can be provided as part of a cryptosystem if public-key encryption is added to the Digital Signature Scheme.

Types of Digital Signatures:

Types of Digital Signature

1. **Certified signatures**

The certified digital signature documents display a unique blue ribbon across the top of the document. The certified signature contains the name of the document signer and the certificate issuer which indicate the authorship and authenticity of the document.

2. **Approval signatures**

The approval digital signatures on a document can be used in the organization's business workflow. They help to optimize the organization's approval procedure. The procedure involves capturing approvals made by us and other individuals and embedding them within the PDF document. The approval signatures to include details such as an image of our physical signature, location, date, and official seal.

3. **Visible Digital Signature**

The visible digital signature allows a user to sign a single document digitally. This signature appears on a document in the same way as signatures are signed on a physical document.

4. **Invisible Digital Signature**

The invisible digital signatures carry a visual indication of a blue ribbon within a document in the taskbar. We can use invisible digital signatures 10je when we do not have or do not want to display our signature but need to provide the authenticity of the document, its integrity, and its origin.

Applications of Cryptography

1. **Digital Currency**

A much-known application of cryptography is digital currency where in crypto currencies are traded over the internet. Top crypto currencies like Bitcoin, Ethereum, and Ripple have been developed and traded over time Block chain technology has a lot to do with this application. Several nodes in the block chain are empowered with cryptography that enables the secure trade of a crypto currency in a digital ledger system. These ledgers are protected, preserved, and cannot be accessed by any other person or organization.

2. **E-commerce**

E-commerce start-ups enable us to shop items online and pay for them online. These transactions are encrypted and perhaps cannot be altered by any third party. Moreover, the passwords we set for such sites are also protected under keys to ensure that no hacker gets access to our ecommerce details for harmful purposes.

3. **Military operations**

Military operations have also derived great use from cryptography for a long time. Used for encrypting military communication channels, military encryption devices convert the real communication characters so that the enemies cannot come to know about their upcoming plans.

On the large scale, it can be widely used for declaring wars and sending crucial messages without the involvement of a messenger.

4. **Maintain secrecy in storage**

Cryptography allows storing the encrypted data permitting users to stay back from the major hole of circumvention by hackers.

5. **Reliability in transmission**

A conventional approach that allows reliability is to carry out a checksum of the communicated information and then communicate the corresponding checksum in an encrypted format. When both the checksum and encrypted data is received, the data is again check summed and compared to the communicated checksum after the process of decryption.

6. **Authentication of identity**

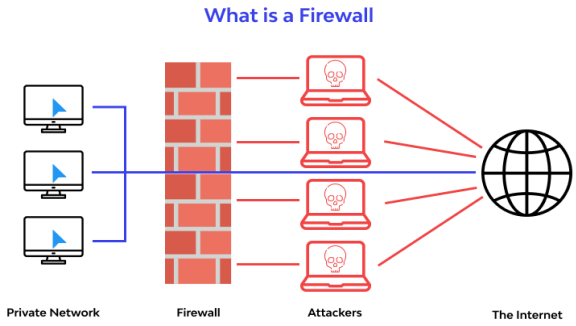
Cryptography is strongly linked to the approach of using passwords, and innovative systems probably make use of strong cryptographic methods together with the physical methods of individuals and collective secrets offering highly reliable verification of identity.

7. **Storing data**

We all store a large amount of data, and any data is valuable to at least the person who generated it. Every operating system uses encryption in some of the core components to keep passwords secret, conceal some parts of the system, and make sure that updates and patches are really from maker of the system.

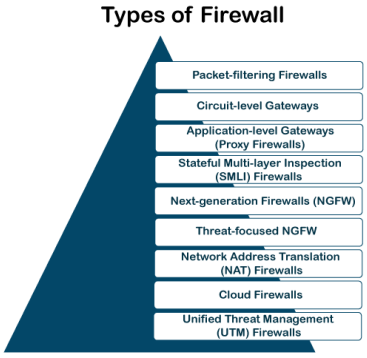
Network Firewalls

These are the devices that are used to prevent private networks from unauthorized access. A Firewall is a security solution for the computers or devices that are connected to a network, they can be either in form of hardware as well as in form of software. It monitors and controls the incoming and outgoing traffic (the amount of data moving across a computer network at any given time).



The major purpose of the network firewall is to protect an inner network by separating it from the outer network. Inner Network can be simply called a network created inside an organization and a network that is not in the range of inner network can be considered as Outer Network.

Types of Network Firewall:



1. **Packet Filters** –
   It is a technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols, and ports. This firewall is also known as a static firewall.

2. **Stateful Inspection Firewalls** –
   It is also a type of packet filtering which is used to control how data packets move through a firewall. It is also called dynamic packet filtering. These firewalls can inspect that if the packet belongs to a particular session or not. It only permits communication if and only if, the session is perfectly established between two endpoints else it will block the communication.

3. **Application Layer Firewalls** –
   These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.

4. **Next-generation Firewalls** –
   These firewalls are called intelligent firewalls. These firewalls can perform all the tasks that are performed by the other types of firewalls that we learned previously but on top of that, it includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

5. **Circuit-level gateways** –
   A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security and works Between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer.

5. Software Firewall –
   The software firewall is a type of computer software that runs on our computers. It protects our system from any external attacks such as unauthorized access, malicious attacks, etc. by notifying us about the danger that can occur if we open a particular mail or if we try to open a website that is not secure.

6. Hardware Firewall –
   A hardware firewall is a physical appliance that is deployed to enforce a network boundary. All network links crossing this boundary pass-through this firewall, which enables it to perform an inspection of both inbound and outbound network traffic and enforce access controls and other security policies.

7. Cloud Firewall –
   These are software-based, cloud-deployed network devices. This cloud-based firewall protects a private network from any unwanted access. Unlike traditional firewalls, a cloud firewall filters data at the cloud level.

Working of Firewalls:
Firewalls can control and monitor the amount of incoming or outgoing traffic of our network. The data that comes to our network is in the forms of packets (a small unit of data), it is tough to identify whether the packet is safe for our network or not, this gives a great chance to the hackers and intruders to bombard our networks with various viruses, malware, spam, etc.

Advantages of Network Firewall:
1. **Monitors network traffic** –
   A network firewall monitors and analyzes traffic by inspecting whether the traffic or packets passing through our network is safe for our network or not. By doing so, it keeps our network away from any malicious content that can harm our network.
2. **Halt Hacking** –
   In a society where everyone is connected to technology, it becomes more important to keep firewalls in our network and use the internet safely.
3. **Stops viruses** –
   Viruses can come from anywhere, such as from an insecure website, from a spam

message, or any threat, so it becomes more important to have a strong defense system (i.e. firewall in this case), a virus attack can easily shut off a whole network. In such a situation, a firewall plays a vital role.

4. **Better security** –
   If it is about monitoring and analyzing the network from time to time and establishing a malware-free, virus-free, spam-free environment so network firewall will provide better security to our network.
5. **Increase privacy** –

By protecting the network and providing better security, we get a network that can be trusted.

Disadvantages of Network Firewall :

1. **Cost** –
   Depending on the type of firewall, it can be costly, usually, the hardware firewalls are more costly than the software ones.
2. **Restricts User** –
   Restricting users can be a disadvantage for large organizations, because of its tough security mechanism. A firewall can restrict the employees to do a certain operation even though it's a necessary operation.
3. **Issues with the speed of the network** –
   Since the firewalls have to monitor every packet passing through the network, this can slow down operations needed to be performed, or it can simply lead to slowing down the network.
4. **Maintenance** –
   Firewalls require continuous updates and maintenance with every change in the networking technology. As the development of new viruses is increasing continuously that can damage your system.

User Management

User management describes the ability for administrators to manage user accesstovarious11resourceslikesystems, devices, applications, storage stems, networks, Saas services, and more. User management is a core part to identity and access management (IAM) solution, in particular directory services tools. Controlling and managing user access to IT resources is a fundamental security essential for any organization. User management enables admins to control user access and on-board and off-board users to and from IT resources. Subsequently a directory service will then authenticate, authorize, and audit user access to IT resources based on what the IT admin had dictated.

Traditionally, user management and authentication services have been grounded with windows-based on-prem servers, databases, and closed Virtual Private Networks (VPN) through an on-prem Identity Provider (IdP) such as Microsoft active directory.
Identity and access management (IAM) which is a technique that supports users in Authentication, Authorization and Auditing (AAA) to access the cloud services.

a. **Authentication:** Authentication is a mechanism that authenticates the user or system identity. For example LDAP (Lightweight Directory Access Protocol) helps in authenticating the credentials produced by a user where the identifier is an authorised or desired user ID allocated to every

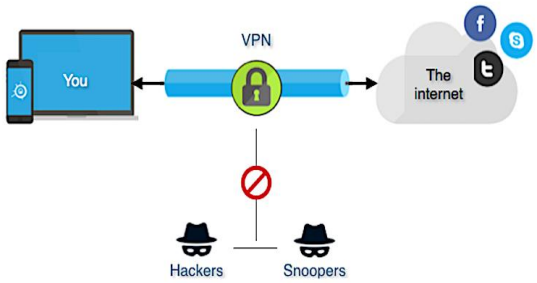
employee or a contractor. It implies identification in a robust form. It also involves in verifying network service of a service-to service interaction and demands information access provided by other services.

b. **Authorization**: Authorization is a mechanism that allows the user or system to determine the privileges as soon as the identity is verified. In case of the digital services, authorization adopts authentication steps to verify whether the user incorporates required privileges in order to carry out some specific operations. Authorization is also known as the mechanism of enforcing policies,

c. **Auditing:** Auditing is a process of examining or checking the authentication and authorization records and verifying the ability of system controls. It determines compliance with security policies and procedures for identifying breaches present in security services, It also proposes modifications necessary for counter measures.

VPN Security:

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual "private network" i.e. user can be part of a local network sitting at a remote location. It makes use of tunnelling protocols to establish a secure connection.



Virtual Private Network (VPN) is basically of 2 types:

1. Remote Access VPN

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

2. Site to Site VPN

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different

locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

Types of Virtual Private Network (VPN) Protocols:

1. **Internet Protocol Security (IPsec)**: Internet Protocol Security, known as IPsec, is used to secure Internet communication across an IP network. IPsec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection. IPsec runs in 2 modes:
   (i) Transport mode
   (ii) Tunnelling mode
2. **Layer 2 Tunnelling Protocol (L2TP)**: L2TP or Layer 2 Tunnelling Protocol is a tunnelling protocol that is often combined with another VPN security protocol like IPsec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPsec protocol encrypts the data and maintains secure communication between the tunnel.
3. **Point–to–Point Tunnelling Protocol (PPTP**): PPTP or Point-to-Point Tunnelling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.
4. **SSL and TLS**: SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have “https” in the initial of the URL instead of “http”.
5. **Secure Shell (SSH**): Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.
6. **SSTP (Secure Socket Tunneling Protocol**): A VPN protocol developed by Microsoft that uses SSL to secure the connection, but only available for Windows.
7. **IKEv2 (Internet Key Exchange version 2)**: A VPN protocol that provides fast and secure connections, but not widely supported by VPN providers.
8. **OpenVPN**: An open-source VPN protocol that is highly configurable and secure, widely supported by VPN providers and considered one of the most secure VPN protocols.
9. **WireGuard:** A relatively new and lightweight VPN protocol that aims to be faster, simpler and more secure than existing VPN protocols.

Benefits and challenges of using a VPN

Benefits of using a VPN include the following:

- The ability to hide a user's IP address and browsing history;

- Secure connections with encrypted data;
- Bypassing geo-blocked content; and
- Making it more difficult for advertisers to target ads to individuals.

The challenges of using a VPN, however, include the following:

- Not all devices may support a VPN.
- VPNs do not protect against every threat.
- Paid VPNs are more trusted, secure options.
- A VPN may slow down internet speeds.
- Anonymity through VPNs has some s limitations -- for example, browser fingerprinting can still be done.

Security protocols:

Network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet because they can provide protection for many applications at once without modifying hem.

Many real-time security protocols have evolved for network security ensuring basic tenets of security such as privacy, origin authentication, message integrity, and non-repudiation.

Most of these protocols remained focused at the higher layers of the OSI protocol stack, to compensate for inherent lack of security in standard Internet Protocol.

This need gave rise to develop a security solution at the IP layer so that all higher-layer protocols could take advantage of it. In 1992, the Internet Engineering Task Force (IETF) began to define a standard 'IPsec'.

Any scheme that is developed for providing network security needs to be implemented at some layer in protocol stack as depicted in the diagram below –

Layer	Communication Protocols	Security Protocols
Application Layer	HTTP FTP SMTP	PGP. S/MIME, HTTPS
Transport Layer	TCP /UDP	SSL, TLS, SSH
Network Layer	IP	IPsec

SECURITY AT APPLICATION LAYER

Network security entails securing data against attacks while it is in transit on a network. To achieve this goal, many real-time security protocols have been designed. Such protocol needs to provide at least the following primary objectives –

- The parties can negotiate interactively to authenticate each other.
- Establish a secret session key before exchanging information on network.
- Exchange the information in encrypted form.

Interestingly, these protocols work at different layers of networking model. For example, S/MIME protocol works at Application layer, SSL protocol is developed to work at transport layer, and IPsec protocol works at Network layer.

In this chapter, we will discuss different processes for achieving security for e-mail communication and associated security protocols. The method for securing DNS is covered subsequently. In the later chapters, the protocols to achieve web security will be described.

E-Mail Security Services

Growing use of e-mail communication for important and crucial transactions demands provision of certain fundamental security services as the following –

- **Confidentiality** – E-mail message should not be read by anyone but the intended recipient.
- **Authentication** – E-mail recipient can be sure of the identity of the sender.
- Integrity – Assurance to the recipient that the e-mail message has not been altered since it was transmitted by the sender.
- **Non-repudiation** – E-mail recipient is able to prove to a third party that the sender really did send the message.
- **Proof of submission** – E-mail sender gets the confirmation that the message is handed to the mail delivery system.
- **Proof of delivery** – Sender gets a confirmation that the recipient received the message.

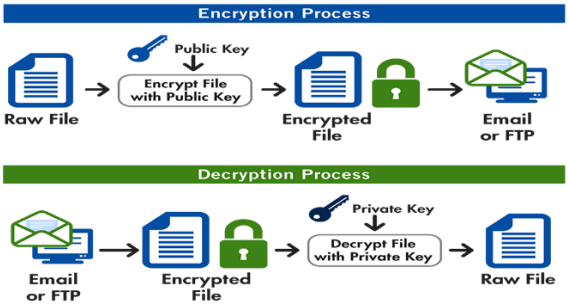
Security services such as privacy, authentication, message integrity, and non-repudiation are usually provided by using public key cryptography.

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is an e-mail encryption scheme.

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.

PGP can be helpful in creating secure email messages. It sends the original data into encrypted form called unreadable cipher text and passed to receiver where data is decrypted into original form by receiver key.



For example, consider two users Ram and Hari. Ram creates a session key to encrypt the message and he also encrypts the session key with the public key of Hari. When Hari receives the message, he decrypts the session key with his public key and decrypts the original data.

PGP uses encryption and hash algorithms like DES and MD5 for encryption. It helps in providing code conversion to convert the characters that don't belong to the ASCII set. It converts those characters using Base-64 conversion. It allows segmentation, so data can be transmitted in a uniform manner.

Advantages

The advantages of PGP are as follows –

- It is freely available on the internet, so that anyone can be downloaded easily.
- There is no compatible issue.
- Information is not modified in transit because it is encrypted.
- There is no chance of spoofing because the trust model is used for verification of sender.

Disadvantages

The disadvantages of PGP are as follows –

- PGP uses complex structure for encryption.
- Both sender and receiver have the same versions of PGP.
- Public keys and private keys have to be maintained carefully so that if lost can be recovered.

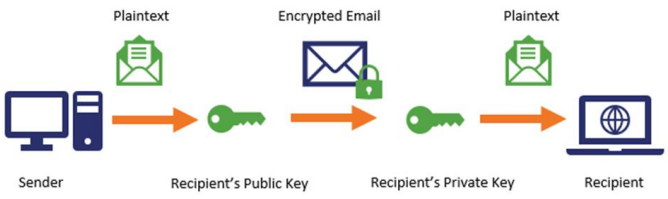
Secure/Multipurpose Internet mail extension (S/MIME)

The full form of S/MIME is Secure/Multipurpose Internet mail extension, which is used for email security. It is an extension of Multipurpose Internet mail extension (MIME). S/MIME allows you to sign digitally your emails so that only the intended receiver can receive the emails.

Cryptographic message syntax is used by S/MIME which defines the exact encoding scheme. It uses digital signatures for signing messages and public key encryption to encrypt.

To provide data integrity, signed data content type is used in which message digest is created and signed with the private key of signer. Signature, certificate and algorithm create the signed data object.

To provide privacy for the message, enveloped data content type is used in which the session key is encrypted with the public key of the receiver and encrypted contents, encrypted session keys, algorithms and certificates are encoded.



Advantages

The advantages of S/MIME are as follows –

- S/MIME is available in different modern mail agents such as MS outlook, Netscape etc.
- It provides authenticity and protection of the message.

- It is used for commercial or industry purposes.
- With the help of email spoofing the Digital signature protects the.

Disadvantages

The disadvantages of S/MIME are as follows –

- Not all email software supports S/MIME signatures.
- Due to the requirement of implemented certificates all users cannot take benefits of S/MIME as some users only want encryption.

Difference between PGP and S/MIME :

S.NO	PGP	S/MIME
1.	It is designed for processing the plain texts	While it is designed to process email as well as many multimedia files.
2.	PGP is less costly as compared to S/MIME.	While S/MIME is comparatively expensive.
3.	PGP is good for personal as well as office use.	While it is good for industrial use.
4.	PGP is less efficient than S/MIME.	While it is more efficient than PGP.
5.	It depends on user key exchange.	Whereas it relies on a hierarchically valid certificate for key exchange.
6.	PGP is comparatively less convenient.	While it is more convenient than PGP due to the secure transformation of all the applications.
7.	PGP contains 4096 public keys.	While it contains only 1024 public keys.
8.	PGP is the standard for strong encryption.	While it is also the standard for strong encryption but has some drawbacks.
9.	PGP is also be used in VPNs.	While it is not used in VPNs, it is only used in email services.
10.	PGP uses Diffie hellman digital signature.	While it uses Elgamal digital signature.

Security at Transport Level: SSL and TLS

- Network security entails securing data against attacks while it is in transit on a network. To achieve this goal, many real-time security protocols have been designed. There are popular standards for real-time network security protocols such as S/MIME, SSL/TLS, SSH, and IPsec. As mentioned earlier, these protocols work at different layers of networking model.
- Transport layer security schemes can address the problems by enhancing TCP/IP based network communication with confidentiality, data integrity, server authentication, and client authentication.

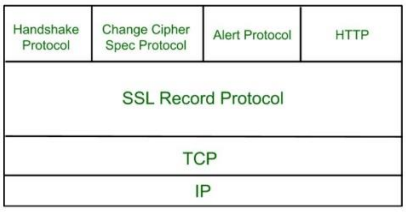
The security at this layer is mostly used to secure HTTP based web transactions on a network. However, it can be employed by any application running over TCP.

1. **Secure Socket Layer (SSL)**

It provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol



Salient Features of SSL

The salient features of SSL protocol are as follows –

- SSL provides network connection security through –
  - Confidentiality – Information is exchanged in an encrypted form.
  - Authentication – Communication entities identify each other through the use of digital certificates. Web-server authentication is mandatory whereas client authentication is kept optional.
  - Reliability – Maintains message integrity checks.
- SSL is available for all TCP applications.
- Supported by almost all web browsers.
- Provides ease in doing business with new online entities.
- Developed primarily for Web e-commerce.

2. **Transport Layer Security (TLS)**

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL). TLS ensures that no third party may eavesdrop or tampers with any message.

Salient Features

- TLS protocol has same objectives as SSL.
- It enables client/server applications to communicate in a secure manner by authenticating, preventing eavesdropping and resisting message modification.
- TLS protocol sits above the reliable connection-oriented transport TCP layer in the networking layers stack.
- The architecture of TLS protocol is similar to SSLv3 protocol. It has two sub protocols: the TLS Record protocol and the TLS Handshake protocol.
- Though SSLv3 and TLS protocol have similar architecture, several changes were made in architecture and functioning particularly for the handshake protocol.

There are several benefits of TLS:

- **Encryption**:
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability**:
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility**:
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment**:
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use**:
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Comparison of SSL and TLS Protocols

SSL	TLS
SSL stands for Secure Socket Layer.	TLS stands for Transport Layer Security.
SSL (Secure Socket Layer) supports the Fortezza algorithm.	TLS (Transport Layer Security) does not support the Fortezza algorithm.
SSL (Secure Socket Layer) is the 3.0 version.	TLS (Transport Layer Security) is the 1.0 version.
In SSL(Secure Socket Layer), the Message digest is used to create a master secret.	In TLS(Transport Layer Security), a Pseudo-random function is used to create a master secret.
In SSL(Secure Socket Layer), the Message Authentication Code protocol is used.	In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used.

SSL	TLS
SSL (Secure Socket Layer) is more complex than TLS (Transport Layer Security).	TLS (Transport Layer Security) is simple.
SSL (Secure Socket Layer) is less secured as compared to TLS (Transport Layer Security).	TLS (Transport Layer Security) provides high security.
SSL is less reliable and slower.	TLS is highly reliable and upgraded. It provides less latency.
SSL has been depreciated.	TLS is still widely used.
SSL uses port to set up explicit connection.	TLS uses protocol to set up implicit connection.

SECURITY AT NETWORK LAYER – IPSec

Network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet because they can provide protection for many applications at once without modifying them.

Many real-time security protocols have evolved for network security ensuring basic tenets of security such as privacy, origin authentication, message integrity, and non-repudiation.

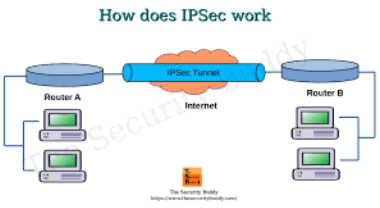
Most of these protocols remained focused at the higher layers of the OSI protocol stack, to compensate for inherent lack of security in standard Internet Protocol.

This need gave rise to develop a security solution at the IP layer so that all higher-layer protocols could take advantage of it. In 1992, the Internet Engineering Task Force (IETF) began to define a standard 'IPsec'.

Security in Network Layer

Any scheme that is developed for providing network security needs to be implemented at some layer in protocol stack as depicted in the diagram below –

The popular framework developed for ensuring security at network layer is Internet Protocol Security (IPsec).



Features of IPsec

- IPsec is not designed to work only with TCP as a transport protocol. It works with UDP as well as any other protocol above IP such as ICMP, OSPF etc.
- IPsec protects the entire packet presented to IP layer including higher layer headers.
- Since higher layer headers are hidden which carry port number, traffic analysis is more difficult.
- IPsec works from one network entity to another network entity, not from application process to application process. Hence, security can be adopted without requiring changes to individual user computers/applications.
- Tough widely used to provide secure communication between network entities, IPsec can provide host-to-host security as well.
- The most common use of IPsec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway).

Security Functions

The important security functions provided by the IPsec are as follows –

- **Confidentiality**
  - Enables communicating nodes to encrypt messages.
  - Prevents eavesdropping by third parties.
- **Origin authentication and data integrity.**
  - Provides assurance that a received packet was actually transmitted by the party identified as the source in the packet header.
  - Confirms that the packet has not been altered or otherwise.
- **Key management**.
  - Allows secure exchange of keys.
  - Protection against certain types of security attacks, such as replay attacks.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

CYBERSPACE

The best way to define Cyberspace is the virtual and dynamic space created by the machine clones.
According to the Cyberspace definition, it is a web consisting of consumer computers, electronics and communication networks by which the consumer is connected to the world.

Cyberspace History

The word Cyberspace first made its appearance in Wiliam Gibson's Science fiction book Necromancer. The book described an online world filled with computers and associated societal elements. In that book, the author described Cyberspace as a 3D virtual landscape created by a network of computers. Although it looks like a physical space, it is generated by a computer, representing abstract data.
If we look into the Cyberspace meaning, it is not a physical space but a digital medium. The differences between a physical world and Cyberspace are as follows:

Cyberspace vs. the Physical World

Cyberspace	Physical World
Dynamic, exponential and undefined	Well-defined, static and incremental
No fixed shape, rather as vast as human imagination	Fixed Contours

CYBER SECURITY REGULATIONS

There are five predominant laws to cover when it comes to cybersecurity:
Information Technology Act, 2000 The Indian cyber laws are governed by the Information
Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to e-Commerce, facilitating registration of real-time records with the Government.
But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

The ITA, enacted by the Parliament of India, highlights the grievous punishments and penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communication devices.

The IT Act is the salient one, guiding the entire Indian legislation to govern cybercrimes rigorously:

Section 43 - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs.5 lakh.

Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.

Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.

Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Indian Penal Code (IPC) 1980

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000.
The primary relevant section of the IPC covers cyber frauds:

Forgery (Section 464)
Forgery pre-planned for cheating (Section 468)

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

False documentation (Section 465)
Presenting a forged document as genuine (Section 471)
Reputation damage (Section 469)

Companies Act of 2013

The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cements all the required techno-legal compliances, putting the less compliant companies in a legal fix.

The **Cybersecurity Framework (NCFS),** authorized by the **National Institute of Standards and Technology (NIST)**, offers a harmonized approach to cybersecurity as the most reliable global certifying body.
NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness.

Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyber land - can bring about online safety and resilience.

CYBER LAW:
In today's tech-savvy environment, the world is becoming more and more digital and so is crime. Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, virus attacks, phishing attacks, e-mail hijacking, denial-of-service, hacking, pornography etc. are becoming common.

All legal issues related to cybercrime are governed by cyber laws. As the number of internet users has increased, the need for cyber laws and their application has also gathered great momentum.

Cyber law or IT law is referred to as the 'Law of the Internet'. It is a legal system designed to deal with internet-related legal issues.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

Cyber laws help to reduce or prevent people from cybercriminal activities on a large scale by protecting information access from unauthorized persons.

Cyber law offers legal protections for people who are using the internet as well as running an online business. The most important thing for internet users is to learn about their country's local and cyber laws, which will allow them to know what activities on the network are legal or not.

Cyber laws are formed to punish people who perform any illegal activities online such as online harassment, attacking another website or individual, data theft, disrupting the online workflow of any enterprise and other illegal activities. If anyone breaks a cyber law, the action would be taken against that person on the basis of the type of cyber law he broke, where he lives, and where he broke the law.

IMPORTANCE OF CYBER LAW

We are living in highly digitalized world. All companies depend upon their computer networks and keep their valuable data in electronic form. Government forms including income tax returns, company law forms etc. are now filled in electronic form. Consumers are increasingly using credit-cards for shopping.

Most people are using e-mail, cell phones and SMS messages for communication. Even in 'non-cyber crime' cases, important evidence is found in computers or cell phones e.g. in cases of divorce, murder, kidnapping, organized crime, terrorist operations etc.

Since it touches all the aspects of transactions and activities on and around the Internet, the World Wide Web (WWW) and Cyberspace, therefore Cyber law is extremely important.

Cyber Law-

Covers all transaction over internet.

Keeps eyes on all activities over internet.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

Touches every action and every reaction in cyberspace.

Protects the personal information of the user.

Note: The computer generated world of internet is known as 'cyberspace' and the laws are known as 'cyber laws'

What is the role of cyber laws?

Cyber laws serve a variety of purposes crucial to the usage of the internet. Some of these laws protect internet users from becoming victims of any cybercrime. Whereas, some other laws lay down rules for individuals to use the internet and the computer system. Primary areas included under cyber laws are:

Fraud

Cyber laws are there to protect consumers from online frauds. They exist to prevent online crimes including credit card theft and identity theft. A person who commits such thefts stands to face federal and state criminal charges.

Copyright

Copyright is a legal area that defends the rights of an entity be it an individual and/or a company to profit from their creative work. Individuals and companies both need copyright laws to prevent copyright infringement and enforce copyright protection.

Defamation

Defamation laws are the civil laws that give immunity to individuals from publically made false statements or allegations that can prove to be damaging for the reputation of a person or a business. When such a mala fide deed is done online, it falls under the bracket of cyber laws.

ROLE OF INTERNATIONAL LAWS, STATE AND PRIVATE SECTOR IN CYBERSPACE

International law structures relations among states and other international stakeholders (most notably international organizations) through various prohibitions, requirements, and permissions. As such, it

has provided a path for regulating global governance issues from arms control to trade to the environment. As states give increased attention to the governance of cyberspace (the technical architecture that allows the global internet to function) and governance in cyberspace (how states, industry, and users may use this technology), the role of international law in the cyber context has gained increasing prominence.

Application of international law to cyberspace, the players involved, the main issues in its application, and potential future pathways international law may take in governing cyberspace.

INTERNATIONAL LAW APPLIES TO (AND IN) CYBERSPACE

With few exceptions (most notably, the Budapest Convention on Cybercrime and the not-yet-in-force African Union Convention on Cyber Security and Personal Data Protection), international law does not have tailor-made rules for regulating cyberspace. Moreover, the technology is both novel and dynamic.

Thus, for several years, there were open questions about whether existing international law applied to cyberspace at all. Today, most states and several international organizations, including the UN General Assembly's First Committee on Disarmament and International Security, the G20, the European Union, ASEAN, and the OAS have affirmed that existing international law applies to the use of information and communication technologies (ICTs) by states. As such, the current discourse centers not on whether international law applies, but rather how it does so.

THE PLAYERS

Unlike many other international issues, the governance of cyberspace did not originate with states, but with the academic institutions and private actors who constructed the internet (albeit with government funding). Thus, cyberspace governance involves key stakeholders that include, but are by no means limited to, states.

International law, however, is primarily a legal order for states (and their creations, like international organizations). As such, international law does not hold a monopoly on the regulation of cyberspace. Given industry and civil society players, other regulatory regimes (for example, industry self-regulation) offer alternative vehicles. Multi stakeholder governance, Microsoft's President Brad Smith even called on states to

conclude a new "Digital Geneva Convention" to regulate state behaviour in cyberspace.

THE MAIN ISSUES

Issues surrounding international law's application to cyberspace may be broken into five discrete categories: (i) silence; (ii) existential disagreements; (iii) interpretative challenges; (iv) Attribution; and (v) accountability.

FUTURE POSSIBILITIES (AND PROBLEMS)

Going forward, there are two dominant questions about the application of international law to cyberspace: (a) what form should any resolution of the main issues take; and (b) in what fora should this occur?

The future form(s) of international law? Even as international law lacks tailor-made rules, various states and stakeholders suggest that existing international law is sufficient to regulate behaviour of states: For these actors, the future must address how to operationalize and improve accountability under the current law.

The future forum for applying international law? To date, the most robust fora for addressing international law's application are non-state-oriented. Governance of the internet involves a multi stakeholder process.

CYBER SECURITY STANDARDS

In order are referred to make to as cybersecurity cyber security measures standards. written standards are required. These themselves, to protect Cyber security the cyber standards environment devices, are techniques, all of users or often organizations.

The main objective is to reduce the risks, including preventing or mitigating cyber attacks. These published materials consist of tools, guidelines, security concepts, safeguards, policies, risk management approaches, measures, training, best practices, assurances and technologies.

(1) ISO

ISO stands for 'International Organization for Standardization'.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

International Standards make things to work. These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency.

ISO standard is officially established on 23 February 1947. It is an independent, nongovernmental international organization.

(2) IT Act

Information Technology Act, also with known as the IT Act, mainly aims to provide the legal infrastructure in India dealing with cybercrime and e-commerce.

This act is also used to check misuse of cyber network and computer in India.

(3) Copyright Act

Copyright is a kind of intellectual property that applies to creative work. It is a legal right that gives exclusive rights to the creator of an original work to use and distribute it. It has to be revised from time to time. The problem or issue with copyright is that it only protects the expression of ideas by the creator rather than the underlying idea.

The Copyright Act 1957 amended by the 'Copyright Amendment Act 2012' governs the subject of copyright law in India. This Act is applicable from 21 January 1958.

A copyrighted original work is a distribution of specific works of creative expression, including books, videos, films, music, and computer programs.

The copyright act covers the following:

- Rights of copyright owners
- Works eligible for protection
- Duration of copyright
- Who can claim copyright

The copyright act does not cover the following:

Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries

- Familiar symbols or designs
- Titles, names, short phrases, and slogans

(4) Patent Law

Patent is an exclusive right granted to the inventor by the government to exclude others from using, making, and selling an invention for a specified period of time.

Patent law is a law that deals with new inventions.

(5) IPR

Intellectual Property Rights (IPR) is a right that allows creators or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas or other intangible assets or investments in a creation.

These IPR rights are described in Article 27 of the Universal Declaration of Human Rights.

Various cyber security standards are:

1. **ISO/IEC 22301** ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission

It is used for disaster recovery. It is an international standard for business continuity management systems.

2. **ISO/IEC 27031**

It is used to bridge the gap between incident and business continuity. It is an international standard for ICT systems readiness.

3. **ISO/IEC 27035**

It is used to update and strength the available standards to reduce the risks. It is an international standard for incident management.

4. ISO/IEC 27032

It offers guidelines to secure the data available outside the organization's boundary. This data includes partnerships, collaborations, data sharing arrangements etc. It is an international standard that concentrates on cyber security.

5. ISO/IEC 27001

It offers specifications for securing the information against integrity, confidentiality and availability.

6. PAS 555(publicly Available specification)

It is used to provide a framework for security policy that is used to compare both the established as well as the existing policies. It was introduced by British Standards Institutions (BSI) in 2013.

7. CCM

It is used to offer some additional rules for data security. It is an international standard for cloud databases. It was introduced by Cloud Security Alliance's Cloud Controls Matrix (CCM).

Indian Cyber Space and National Security Policy 2013

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

Types of Cyber Law

Cyber laws can be used for various purposes as it provides different types of security, come laws provide security to users from frauds, money laundering, etc, Some laws form miles and regulations in using computer and internet. There are different areas of cyber law,that means they are categorised in many ways. A list of cyber law is given below to understand each and every type of laws clearly

- Fraud

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

- Copyright
- Defamation
- Harassment and Stalking
- Freedom of Speech
- Trade Secrets
- Contracts and Employment Law

Cyber Acts in India

The following Act, Rules and Regulations are covered under cyber laws:

- Information Technology Act, 2000
- Information Technology (Certifying Authorities) Rules, 2000
- Information Technology (Security Procedure) Rules, 2004
- Information Technology (Certifying Authority) Regulations, 2001

National Cyber Security Policy 2013

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology (DeitY) It aims at protecting the public and private infrastructure from cyber attacks. The National Cyber Security Policy 2013 aims at secure computing environment, enabling adequate trust and confidence in electronic transactions and guiding stake holders actions for the protection of cyberspace.

Creation of Secure cyber ecosystem: to create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems

Compliance of to Global standards

NCIIPC: To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

Indigenization of Technologies: To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, etc.

Testing and Validation: To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

Human Capacity Development: To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

Safeguarding Privacy: To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft.

Cybercrime: To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

Benefits of National Cyber Security Policy (NCSP)

- Cyber Security at all levels inside the country.
- It strengthens the framework for securing a Secure Cyberspace ecosystem
- It grants benefits to businesses for choosing standard security and process.
- It enables protection of information while transiting, process, handling, and storing data to safeguard people's information
- It also lessens the economic loss caused due to cybercrime and data theft.

CYBER FORENSICS

- Cyber forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.
- The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find

out exactly what happened on a computing device and who was responsible for it.

- The terms *digital forensics* and *computer forensics* are often used as synonyms for cyber forensics.
- Cyber security and forensics have another key terminology commonly used in this field- incident handling. Forensics investigators or internal cybersecurity professionals are hired in organizations to handle such events and incidents, known as incident handlers.

Incidents are categorized into three types:

- **Low-level incidents**: where the impact of cybercrime is low.
- **Mid-level incidents**: The impact of cybercrime is comparatively high and needs security professionals to handle the situations.
- **High-level events**: where the impact of cybercrime is the most serious and needs security professionals, and forensic investigators to handle the situations and analyze the scenario, respectively.

IMPORTANCE OF CYBER FORENSICS

- Below are the points showing the importance of cyber forensics:
- Cyber forensics helps in collecting important digital evidence to trace the criminal.
- Electronic devices store huge amounts of data that a normal person cannot see. For example: In a smart home, for every word we speak, actions performed by smart devices, collect huge data which is crucial in cyber forensics.
- It is also helpful for innocent people to prove their innocence via the evidence collected online.
- It is not only used to solve digital crimes but also used to solve real-world crimes like theft cases, murder, etc.
- Businesses are equally benefited from cyber forensics in tracking system breaches and finding the attackers.

CYBER FORENSICS PROCESS

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

Cyber forensics is a field that follows specific procedures to find evidence to reach conclusions after properly investigating matters. The procedures that cyber forensic scientists follow are:

- **Identification**: The first step taken by cyber forensics professionals is to determine what evidence is present, where it is stored and in what format it is stored.
- **Preservation**: After identifying the data, the next step is to keep the data safe and not allow other people to use that device so that no one can tamper data.
- **Analysis**: After getting the data, the next step is to analyze the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the final conclusion.
- **Documentation**: Now after analyzing data a record is created. This record contains all the recovered and available data (not deleted) which helps in recreating the crime scene and reviewing it.
- **Presentation**: This is the final step in which the analyzed data is presented in front of the court to solve cases.

Types of computer forensics

There are various types of computer forensic examinations. Some of the main types include the following:

- **Database forensics.** The examination of information contained in databases, both data and related metadata.
- **Email forensics.** The recovery and analysis of emails and other information contained in email platforms, such as schedules and contacts.
- **Malware forensics.** Sifting through code to identify possible malicious programs and analyzing their payload. Such programs may include Trojan horses, ransomware or various viruses.
- **Memory forensics**. Collecting information stored in a computer's random access memory (RAM) and cache.
- **Mobile forensics**. The examination of mobile devices to retrieve and analyze the information they contain, including contacts, incoming and outgoing text messages, pictures and video files.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

- **Network forensics**. Looking for evidence by monitoring network traffic, using tools such as a firewall or intrusion detection system.

HANDLING PRELIMINARY INVESTIGATIONS

"Preliminary investigation is a process that includes all of the initial activities a responding officer performs at the scene of the crime."
An organization should be prepared in advance to respond properly to incidents and mitigate them in the shortest possible time. An incident response plan should be developed by the organization and tested on a regular basis.

➢ Planning for Incident Response

Organizations should be prepared for incidents by identifying business risks, preparing hosts and the network for threat containment and remediation, establishing policies and procedures that facilitate the achievement of incident response goals, and creating an incident response team and incident response toolkit to be used by the Incident Response Team.

➢ Communicating with Site Personnel

All departments and staffs involved in an incident response should be aware of the incident response plan and should be regularly trained on its content and implementation. The plan should include how to communicate with site personnel. Site personnel should clearly log all activities and communications, including date and time, to a central repository that is regularly backed up.

➢ Knowing Your Organization's Policies

An organization's policies will have an impact on how incidents are handled. These policies are usually very comprehensive and effective computer forensics policies that include considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies, guidelines, and procedures. Banks, insurance companies, law firms, governments, and health care institutions have such policies.

➢ Minimizing Impact on Your Organization

Incident response goals include minimizing disruption to computer and network operations and minimizing disclosure and compromise of sensitive data. In order to achieve these goals, incident response preparedness, planning, and proper execution according to appropriate policies are critical.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

- **Capturing Volatile Information**

Computer systems contain volatile data that is temporarily available either till a process exits or a system is shutdown. Therefore, it is important to capture this data before making any physical or logical changes to the system to avoid tampering with evidence.

CONTROLLING AN INVESTIGATION

To control an investigation, the incident response team should have a forensic investigation plan, a forensic toolkit, and documented methods for securing the affected environment. An investigator should always keep in mind that the evidence collected and the analysis performed may be presented in court or used by law enforcement.
To avoid challenges to the authenticity of evidence, investigators should be able to secure the suspect infrastructure, log all activities, and maintain a chain of custody.

- **Collecting Digital Evidence**

It is important for an investigator to retain data related to an incident as quickly as possible to avoid the loss of data in digital environments. Once the affected systems are identified, volatile data should be collected immediately followed by non-volatile data such as system users and groups, configuration files, password files and caches, scheduled jobs, system logs, application logs, command history, recently accessed files, executable files, and data file.

- **Chain of Custody and Process Integrity**

The incident response team should be committed to collect and preserve evidence using methods that can support future legal or organizational proceedings. A clearly defined chain of custody is necessary to avoid allegations of tampering evidence.

- **Forensics Analysis Team**

Today, due to the increase in computer-related malicious activity and growing digital infrastructure, forensic analysis is involved in incident response, log monitoring, data recovery, data collection, audits and regulatory compliance. Organizations should consider cost, response time, and data sensitivity before making this decision.

- **Securing and Documenting the Scene**

Securing the physical scene and documenting it should be one of the first steps an incident responder should take. This includes photographing the system setup, collecting and documenting all cables and attached

devices, write-protecting all media, using anti-static packaging for transportation, maintaining proper temperature for stored devices

- **Processing and Logging Evidence**

The goal of an investigation is to collect and preserve evidence that can be used for internal proceedings or in court. Investigators should be able to show that the evidence has not been tampered with.

CONDUCTING DISC-BASED ANALYSIS

In order to be able to process evidence that can be used in court, a laboratory and accompanying procedures should be set up. This ensures that data integrity is not violated and the data remains confidential, in other words, the evidence remains forensically sound.

- **Forensic Lab**

To ensure forensic soundness, an investigator's process needs to be reliable, repeatable, and documented. To have a controlled and secure environment for the investigator to follow these steps, a forensic lab becomes a necessity.

- **Acquiring a Bit-Stream Image**

Acquiring a bit-stream image involves producing a bit-by-bit copy of a hard drive on a separate storage device. By creating an exact copy of a hard drive, an investigator preserves all data on a disc, including currently unused and partially overwritten sectors

- **Physically Protecting the Media**

After making copies of the original evidence hard drives, they should be stored in a physically secure location, such as a safe in a secured storage facility. These drives could be used as evidence in the event of prosecution.

- **Disc Structure and Data Recovery**

Once a forensically sound copy of the evidence has been made, we can proceed to analyze its content. There are different types of storage media: hard disk drives (HDD), solid state drives (SSD), digital video discs (DVD), compact discs (CD), flash memory and other types. An investigator must pay attention to how each medium stores data differently.

INVESTIGATING INFORMATION- HIDING

Hidden data can exist due to regular operating system activities or intentional user activities This type of data includes hidden system files,

information mixed-up by malicious s data encrypted in media (steganography) and many others.

- **Uncovering Hidden Information**

Collection of hidden data can be a challenge for an investigator. The investigator ne aware of the different data hiding techniques to employ the proper tools.

- **Executing Code from a Stream**

Malicious software can attempt to hide its components to obscure them selves from investigators. Such components could be executable files (.exe files) that can be launched Windows 'start' command directly.For example: start ads-file.jpg:suspicious.exe

- **Steganography Tools**

Steganography is the technique of hiding secret data in an ordinary non-se message in such a way that only the person who is aware of the mechanism can successfully find and decrypt it. Messages can be hidden in images, audio files, videos, or other computer files without altering the actual presentation or functionality. There are several tools that perform steganography

1. **S-Tools**: A freeware steganography tool that hides files in BMP, GIF, and WAV files.
2. **Spam Mimic**: A freeware steganography tool that embeds messages in spam e-mail content. This tool would be useful when real spam messages are numerous and the fake spam message would not wake any suspicion.
3. **Snow**: A freeware steganography tool that encodes message text by appending white space characters to the end of lines.

Slack Space

Slack space (or file slack) is a source of information leak, which can result in password, email, registry, event log, database entries, and word processing document disclosures. File slack has the potential of containing data from the system memory.

RAM slack can contain any information loaded into memory since the system was turned on.

1. **Volume slack** is the space that remains on a drive when it is not used by any partition
2. **Partition slack** is the area between the ending of a logical partition and the ending of a physical block the partition is located in. It is created when the number of sectors in a partition is not a multiple of the physical block size.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

- **Inspecting Header Signatures and File Mangling**

Malware can change or manipulate file names or the files themselves to hide files that are used to compromise systems or contain data collected as a result of their malicious action These techniques include- renaming files, embedding malicious files in regular files (PDF, Do and Flash), and binding multiple executable files into a single executable file.

- **Combining Files**

Combining files is a very popular method among malware creators. Common file formats such as Microsoft Office files, Adobe PDF, and Flash files can be used as containers to hide malicious executables. One example is a technique where a Windows executable is embedded in a PDF file as an object stream and marked with a compression filter.

- **Binding Multiple Executable Files**

Binding multiple executable files provides the means to pack all dependencies and resource files a program might need while running into a single file. This is beneficial since it permits a malicious user to leave a smaller footprint on a target system and makes it harder for an investigator to locate the malicious file.

- **File Time Analysis**

File time analysis is one of the most used techniques by investigators. File times are used to build a story line that could potentially reveal how and when an event on a system caused a compromise. The file time of a malicious executable could be linked to a user's browser history to find out which sites were visited before the compromise occurred.

SCRUTINIZING E-MAIL

While many non-commercial users prefer webmail these days, most corporate users still use local e-mail clients' like- Microsoft Outlook. Therefore, we should still look at extracting and analyzing e-mail content from local e-mail stores. Analysis of e-mail messages may reveal information about senders and recipients, such as: E-mail addresses, IP addresses, Date and time, Attachments and Content.

- **Investigating the Mail Client**

An e-mail user will generally utilize a local client to compose and send their message. Depending on the user's configuration, the sent and received messages will exist in the local email database. Deleted e-mails can be also stored locally for some time depending on the user's preferences

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

- **Interpreting E-mail Headers**

Generally speaking, e-mail messages are composed of three sections: header, body, and attachments. The header contains source and destination information (From: and To: fields), date and time, e-mail subject, and the route the e-mail takes during its transmission. Information stored in a header can either be viewed through the e-mail client or through an e-mail forensics tool such as libpff (an open source library to access email databases).

- **Recovering Deleted E-mails**

User e-mails usually are stored in backup archives or electronic-discovery systems to provide means for analysis in case there is an investigation. The e-mail servers also can keep messages in store although the users remove them from their local systems. Therefore, it has become somewhat difficult for a corporate user to delete an e-mail permanently.

Recovery is usually possible from various backup systems. In cases where there is no backup source and Users delete an e-mail from their local system, we need to perform several steps on the user's Storage drive depending on the level of deletion.

Challenges in Email Forensics

Email forensics play a very important role in investigation as most of the communication in present era relies on emails. However, an email forensic investigator may face the following challenges during the investigation –

1. **Fake Emails**

The biggest challenge in email forensics is the use of fake e-mails that are created by manipulating and scripting headers etc. In this category criminals also use temporary email which is a service that allows a registered user to receive email at a temporary address that expires after a certain time period.

2. **Spoofing**

Another challenge in email forensics is spoofing in which criminals used to present an email as someone else's. In this case the machine will receive both fake as well as original IP address.

3. **Anonymous Re-emailing**

Here, the Email server strips identifying information from the email message before forwarding it further. This leads to another big challenge for email investigations.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

Techniques Used in Email Forensic Investigation

Email forensics is the study of source and content of email as evidence to identify the actual sender and recipient of a message along with some other information such as date/time of transmission and intention of sender. It involves investigating metadata, port scanning as well as keyword searching.

Some of the common techniques which can be used for email forensic investigation are

- Header Analysis
- Server investigation
- Network Device Investigation
- Sender Mailer Fingerprints
- Software Embedded Identifiers

VALIDATING E-MAIL HEADER INFFORMATION

E-mail header information can be tampered with by users who do not wish to disclose their source information or by malicious users who wish to spoof the origin of the message to avoid detection and blocking by spam filters. E-mail header information can be modified by spoofing using an anonymizer (removes identifying information) and using a mail relay server.

- **Detecting Spoofed E-mail**

A spoofed e-mail message is a message that appears to come from an entity other than the actual sending entity. This can be achieved by changing the sender's name, e-mail address, email client type and/or source IP address in the e-mail header. Spoofing can be detected by looking at the "Received" and "Message-ID" lines of the header.

The "Received" field provides a trace of the e-mail from its origin to your mail server. It will show the origin along with the list of servers that processed this e-mail before reaching your mailbox. An investigator can use the IP addresses of e-mail servers in the header to retrieve their hostnames from their DNS (Domain Name System) records and verify them by comparing to the actual outgoing and incoming e-mail servers' information.

The "Message-ID" field uniquely identifies a message and is used to prevent multiple deliveries. The domain information in the "Message-ID" field should match the domain information of the sender's e-mail address. If this is not the case, the e-mail is most probably spoofed.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

- **Verifying E-mail Routing**

E-mail routing can be verified by tracking the hops that an e-mail message has taken. This can be achieved by verifying the "Received" field information through DNS records and, if possible, obtaining e-mail transaction logs from the e-mail servers involved. The "Message-ID" information can be searched for in the logs to make sure that the message has actually travelled the route declared in the "Received" field.

TRACING INTERNET ACCESS

Knowing the route taken by a cyber criminal is very valuable when an investigator is building a case to present in court. It adds credibility to the claim and sets the storyline connecting the events.
For example, knowing the route an attacker took to steal an organization's source code can reveal the extent of the compromise (loss of domain credentials, loss of customer information, and loss of intellectual property), and prevent the same attack from happening.
Tracing Internet access can also be valuable when employees are viewing content that does not comply with workplace rules.

- **Inspecting Browser Cache and History Files**

An investigator can use various data points to track a criminal's activities by analyzing the browser cache and web history files in the evidence collected. The browser cache contains files that arestored locally as a result of a user's web browsing activity. The history files contain a list of visited URLs, web searches, cookies and bookmarked websites. These files can be located in different folders depending on the operating system, operating system version and browser type.

- **Exploring Temporary Internet Files**

A browser cache stores multimedia content (images, videos), and web pages (HTML, JavaScript, CSS) to increase the load speed of a page when viewed the next time.
For the Google Chrome web browser on Windows 10, the cache files or temporary internet files can be located in the folder:
\Users\UserName\AppData\Local\GoogleChrome\User Data\Default cache
Visited URLs, Search Queries, Recently Opened Files

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

The Google Chrome web browser on Windows 10, stores the information about visited URLs, search queries, and opened file information in the folder:
\Users\UserName\AppData\Local\GoogleChrome\User Data\Default

- **Cookie Storage**

Cookies are data, stored in small text files, on your computer. When a web server has sent the requested web page to a web client (browser), the connection between the server and client is shut down, and the server forgets everything about the client user. Cookies were invented to solve this problem of how to remember the information about the client user. When a user visits a web page, his / her name is stored in a cookie. Now, next time when the same user visits the same webpage, the cookie remembers his / her name. So, cookies are generally used to identify a user over the web.
The location to open Google Chrome Cookies in Windows 10:
\Users\UserName\AppData\Local\Google Chrome\User Data\Default
Name with the name of your Windows 10 user account.

- **Auditing Internet Surfing**

Knowing what employees are browsing on the web while they are at work has become necessary to prevent the employees from visiting sites that host malicious content, content that is not compliant with work place rules, and content that is illegal. Employees can use the web to upload confidential corporate information, which can cause serious problems for the employer.

- **Tracking User Activity**

User activity can be tracked by using tools that monitor network activity, DNS requests, and local user system activities.
Network activity can be monitored by looking at netflows. A netflow is a network protocol developed by Cisco Systems for monitoring IP traffic. It captures source and destination IP addresses, IP protocol, and source and destination ports.
DNS requests can be monitored at the corporate DNS server level or by looking at network traffic. When a user requests a web page with its domain name, the name gets translated to an IP address via DNS. User activity can be tracked by monitoring for domains that are not approved by the employer or domains hosting illegal content in the DNS server's logs.

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

Local user system activity can be monitored by installing specific agents (eg. Spector 360 by SpectorSoft) on the users' systems that can report their activity back to a centralized server.

TRACING MEMORY IN REAL-TIME

Tracking memory in real-time can provide very important information about malware o hacker's activities that would otherwise not be available by just looking at a system's drives. T information can include network connections and sockets, system configuration setting collected private information (usernames, passwords, credit-card numbers), and more. Real-t analysis involves the analysis of volatile content and therefore requires rapid action by investigator.

- **Comparing the Architecture of Processes**

In general, the Windows architecture uses two access modes, namely user mode and kernel mode.

1. User mode includes application processes such as programs and protected subsystems. The protected subsystems are so named because each is a separate process with its own protected virtual address space in memory.

2. Kernel mode is a privileged mode of operation where the application has direct access to Virtual memory. This includes the address spaces of all user-mode processes and applications and associated hardware. Kernel mode is also known as protected mode.

- **Auditing Processes and Services**

Auditing changes in process and service properties as well as their counts on a system can provide valuable information to an investigator about potentially malicious activity. Rootkits, viruses, Trojans, and other malicious software can be detected by auditing process and service creation or deletion across a period of time. This technique is frequently used in malware behavioral analysis in sandboxes.

We can audit Windows processes and services by using tools that utilize system APIs or system memory for live analysis. To view information through the system APIs we can use the tool Process Hacker.

Process Hacker provides a live view of processes and services that are currently being executed or present on the system. It provides an interface to view and search process information in detail, such as process privileges, related users and groups.

- **Investigating the Process Table**

Unit- V

CYBERSPACE, THE LAW AND CYBERSPACE FORENSICS

Process Table (PT) is a data structure kept by the operating system to help context switching, scheduling, and other activities. Each entry in the process table, called Process Context Blocks (PCB), contains information about a process, such as process name and state, priority, and PID. The exact content of a context block depends on the operating system. For example, if the operating system supports paging, then the context block contains a reference to the page table.
The process control block is a large data structure that contains information about a specific process. In Linux, this data structure is called *'task struct'* whereas in Windows, it is called an EPROCESS structure.