What is Security?

Security refers to the measures, practices, and strategies designed to protect individuals, systems, organizations, and assets from harm, unauthorized access, theft, damage, or disruption. The goal of security is to ensure safety, stability, and continuity across various domains, such as physical, digital, and organizational spaces.

Types of Security

1. **Physical Security**
    - Protects people, property, and physical assets from threats such as theft, vandalism, or natural disasters.
    - Examples: Surveillance cameras, locks, security guards, and alarm systems.
2. **Information Security (InfoSec)**
    - Protects data and information systems from unauthorized access, use, disclosure, disruption, or destruction.
    - Examples: Encryption, firewalls, and secure access protocols.
3. **Cybersecurity**
    - Focuses on protecting computer systems, networks, and digital assets from cyber threats like hacking, malware, and phishing.
    - Examples: Antivirus software, intrusion detection systems, and secure coding practices.
4. **Operational Security (OPSEC)**
    - Focuses on identifying and protecting sensitive information that could be exploited by adversaries.
    - Examples: Employee training, controlled access to sensitive areas, and confidentiality agreements.
5. **Network Security**
    - Protects the integrity, confidentiality, and availability of network resources and communications.
    - Examples: Virtual Private Networks (VPNs), intrusion prevention systems, and network segmentation.
6. **Application Security**
    - Ensures that software applications are secure against vulnerabilities and exploits.
    - Examples: Secure coding practices, penetration testing, and patch management.

7. **Personal Security**
    - Protects individuals from harm or threats to their personal well-being or privacy.
    - Examples: Identity theft prevention, social media privacy settings, and self-defense.

Why is Security Important?

- **Prevention of Loss**: Protects assets, data, and resources from theft or damage.
- **Maintaining Trust**: Builds confidence among users, customers, and stakeholders.
- **Compliance**: Ensures adherence to legal and regulatory requirements.
- **Business Continuity**: Ensures smooth operations and recovery in the face of disruptions.
- **Protection from Harm**: Safeguards individuals, organizations, and systems from potential threats.

Basic security concepts

Basic security concepts are foundational for understanding how to protect information, systems, and networks from threats. Here are the key concepts:

---

1. Confidentiality

- Ensures that information is only accessible to authorized individuals or systems.
- Techniques: Encryption, access control, and data masking.

2. Integrity

- Guarantees that data is accurate, consistent, and not tampered with during storage or transit.
- Techniques: Hashing, checksums, and digital signatures.

3. Availability

- Ensures that information and systems are available for use when needed.
- Techniques: Redundancy, backups, and disaster recovery plans.

4. Authentication

- Confirms the identity of a user, system, or entity.
- Techniques: Passwords, biometrics, and multi-factor authentication.

5. Authorization

- Grants users permission to access resources or perform actions based on their identity and role.

- Techniques: Role-based access control (RBAC) and policy enforcement.

6. Non-repudiation

- Ensures that actions or transactions can be proven to have occurred, preventing denial by the parties involved.
- Techniques: Digital signatures and audit logs.

7. Risk Management

- Identifies, assesses, and mitigates potential security risks.
- Techniques: Risk assessment frameworks and security policies.

8. Threats and Vulnerabilities

- **Threats**: Potential events that can cause harm (e.g., malware, phishing, insider threats).
- **Vulnerabilities**: Weaknesses in a system that can be exploited (e.g., unpatched software, weak passwords).

9. Security Policies

- Defined rules and procedures for protecting systems and data.
- Examples: Password policies, data retention policies, and incident response plans.

10. Defense in Depth

- Employing multiple layers of security to protect systems and data.
- Techniques: Firewalls, intrusion detection/prevention systems, and endpoint protection.

What is Cyber Security?

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**

Some other definitions of cybersecurity are:

"Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."

"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

Types of Cyber Security

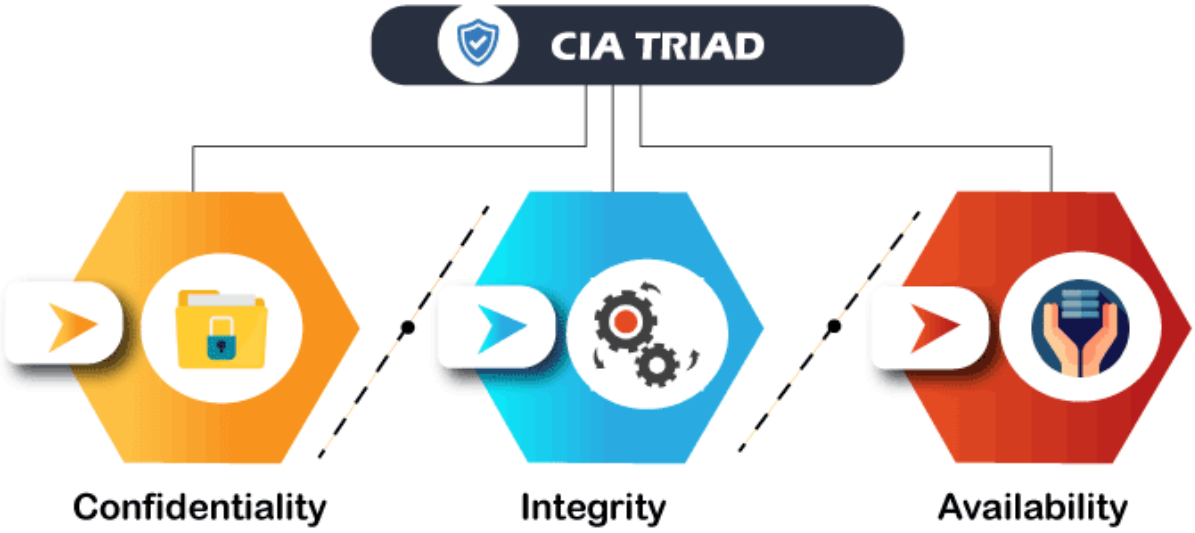
Every organization's assets are the combinations of a variety of different systems. These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cybersecurity in the following sub-domains:

- **Network Security:** It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
- **Application Security:** It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.
- **Information or Data Security:** It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security:** It involves processing and making decisions on handling and securing data assets.
- **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.
- **Cloud Security:** It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.
- **Disaster Recovery and Business Continuity Planning:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.
- **User Education:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

Cyber Security Goals

Cyber Security's main **objective is to ensure data protection**. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the **CIA triad**. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.

We can break the **CIA model into three parts**: Confidentiality, Integrity, and Availability. It is actually a security model that helps people to think about various parts of IT security. Let us discuss each part in detail.



Confidentiality

Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. **Data encryption** is an excellent example of ensuring confidentiality.

Integrity

This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.

Availability

This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

Types of Cyber Security Threats

A threat in cybersecurity is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupts digital life in general. The cyber community defines the following threats available today:

Malware

Malware means malicious software, which is the most common cyber attacking tool. It is used by the cybercriminal or hacker to disrupt or damage a legitimate user's system. The following are the important types of malware created by the hacker:

- **Virus**: It is a malicious piece of code that spreads from one device to another. It can clean files and spreads throughout a computer system, infecting files, stoles information, or damage device.
- **Spyware**: It is a software that secretly records information about user activities on their system. **For example**, spyware could capture credit card details that can be used by the cybercriminals for unauthorized shopping, money withdrawing, etc.
- **Trojans**: It is a type of malware or code that appears as legitimate software or file to fool us into downloading and running. Its primary purpose is to corrupt or steal data from our device or do other harmful activities on our network.
- **Ransomware**: It's a piece of software that encrypts a user's files and data on a device, rendering them unusable or erasing. Then, a monetary ransom is demanded by malicious actors for decryption.
- **Worms**: It is a piece of software that spreads copies of itself from device to device without human interaction. It does not require them to attach themselves to any program to steal or damage the data.
- **Adware**: It is an advertising software used to spread malware and displays advertisements on our device. It is an unwanted program that is installed without the user's permission. The main objective of this program is to generate revenue for its developer by showing the ads on their browser.

- **Botnets**: It is a collection of internet-connected malware-infected devices that allow cybercriminals to control them. It enables cybercriminals to get credentials leaks, unauthorized access, and data theft without the user's permission.

Phishing

Phishing is a type of cybercrime in which **a sender seems to come from a genuine organization** like PayPal, eBay, financial institutions, or friends and co-workers. They contact a target or targets via email, phone, or text message with a link to persuade them to click on that links. This link will redirect them to fraudulent websites to provide sensitive data such as personal information, banking and credit card information, social security numbers, usernames, and passwords. Clicking on the link will **also install malware** on the target devices that allow hackers to control devices remotely.

Man-in-the-middle (MITM) attack

A man-in-the-middle attack is a type of cyber threat (a form of eavesdropping attack) in which a cybercriminal **intercepts a conversation or data transfer between two individuals**. Once the cybercriminal places themselves in the middle of a two-party communication, they seem like genuine participants and can get sensitive information and return different responses. The main objective of this type of attack is to gain access to our business or customer data. **For example**, a cybercriminal could intercept data passing between the target device and the network on an unprotected Wi-Fi network.

Distributed denial of service (DDoS)

It is a type of cyber threat or malicious attempt where cybercriminals disrupt targeted servers, services, or network's regular traffic by fulfilling legitimate requests to the target or its surrounding infrastructure with Internet traffic. Here the requests come from several IP addresses that can make the system unusable, overload their servers, slowing down significantly or temporarily taking them offline, or preventing an organization from carrying out its vital functions.

Brute Force

A brute force attack is a **cryptographic hack that uses a trial-and-error method** to guess all possible combinations until the correct information is discovered. Cybercriminals usually use this attack to obtain personal information about targeted passwords, login info, encryption keys, and Personal Identification Numbers (PINS).

SQL Injection (SQLI)

SQL injection is a common attack that occurs when cybercriminals use malicious SQL scripts for backend database manipulation to access sensitive information. Once the attack is successful, the malicious actor can view, change, or delete sensitive company data, user lists, or private customer details stored in the SQL database.

Domain Name System (DNS) attack

A DNS attack is a type of cyberattack in which cyber criminals take advantage of flaws in the Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers. It is a severe cybersecurity risk because the DNS system is an essential element of the internet infrastructure.

Benefits of Cyber Security

The following are the benefits of implementing and maintaining cybersecurity:

- Cyberattacks and data breach protection for businesses.
- Data and network security are both protected.
- Unauthorized user access is avoided.
- After a breach, there is a faster recovery time.
- End-user and endpoint device protection.
- Regulatory adherence.
- Continuity of operations.
- Developers, partners, consumers, stakeholders, and workers have more faith in the company's reputation and trust.

Cyber Safety Tips

Let us see how to protect ourselves when any cyberattacks happen. The following are the popular cyber safety tips:

Conduct cybersecurity training and awareness: Every organization must train their staffs on cybersecurity, company policies, and incident reporting for a strong cybersecurity policy to be successful. If the staff does unintentional or intentional malicious activities, it may fail the best technical safeguards that result in an expensive security breach. Therefore, it is useful to conduct security training and awareness for staff through seminars, classes, and online courses that reduce security violations.

Update software and operating system: The most popular safety measure is to update the software and O.S. to get the benefit of the latest security patches.

Use anti-virus software: It is also useful to use the anti-virus software that will detect and removes unwanted threats from your device. This software is always updated to get the best level of protection.

Perform periodic security reviews: Every organization ensures periodic security inspections of all software and networks to identify security risks early in a secure environment. Some popular examples of security reviews are application and network penetration testing, source code reviews, architecture design reviews, and red team assessments. In addition, organizations should prioritize and mitigate security vulnerabilities as quickly as possible after they are discovered.

Use strong passwords: It is recommended to always use long and various combinations of characters and symbols in the password. It makes the passwords are not easily guessable.

Do not open email attachments from unknown senders: The cyber expert always advises not to open or click the email attachment getting from unverified senders or unfamiliar websites because it could be infected with malware.

Avoid using unsecured Wi-Fi networks in public places: It should also be advised not to use insecure networks because they can leave you vulnerable to man-in-the-middle attacks.

Backup data: Every organization must periodically take backup of their data to ensure all sensitive data is not lost or recovered after a security breach. In addition, backups can help maintain data integrity in cyber-attack such as SQL injections, phishing, and ransomware.

Cyber Security Goals

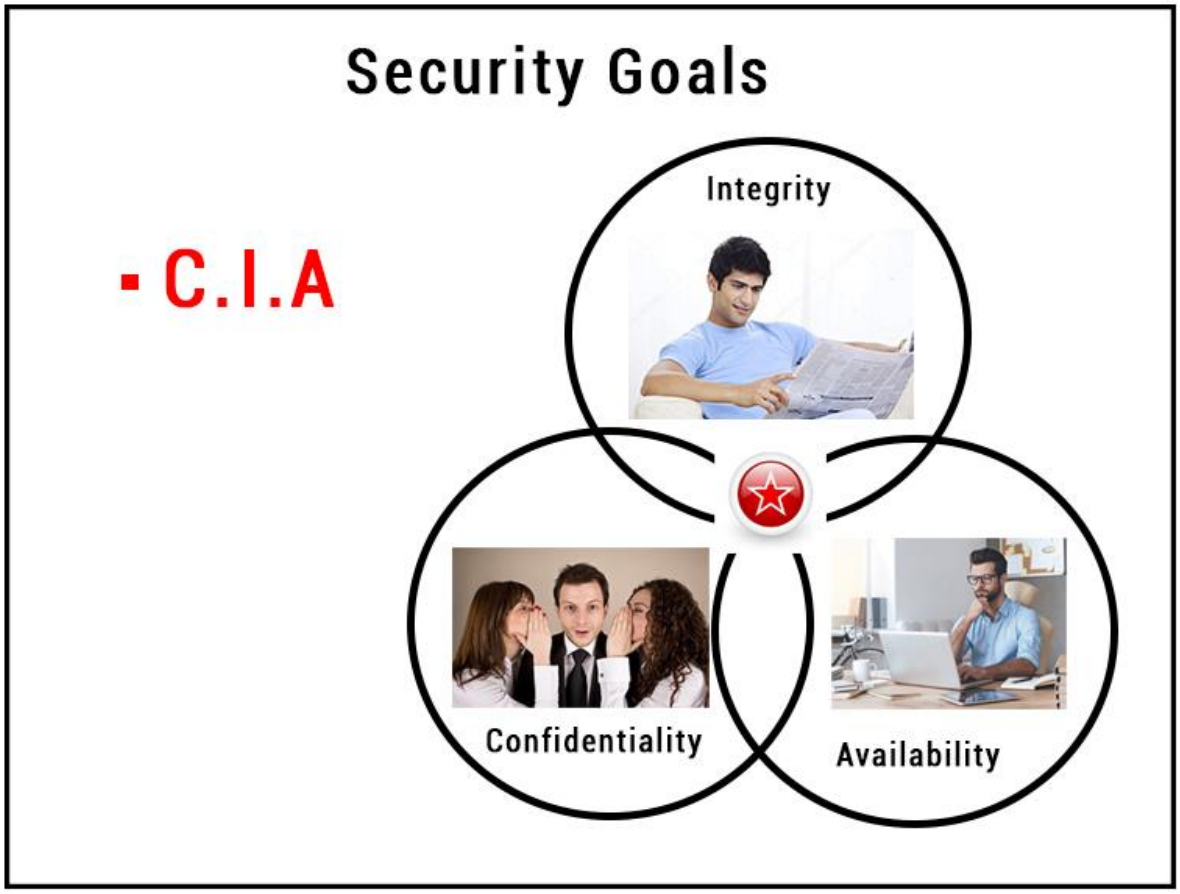
The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-

1. Protect the confidentiality of data.
2. Preserve the integrity of data.
3. Promote the availability of data for authorized users.

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. The CIA triad is a security model that is designed to guide policies for information security within the premises of an organization or company. This model is also referred to as the **AIC (Availability, Integrity, and Confidentiality)** triad to avoid the confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

The CIA criteria are one that most of the organizations and companies use when they have installed a new application, creates a database or when guaranteeing access to some data. For data to be completely secure, all of these security goals must come into effect. These are security policies that all work together, and therefore it can be wrong to overlook one policy.

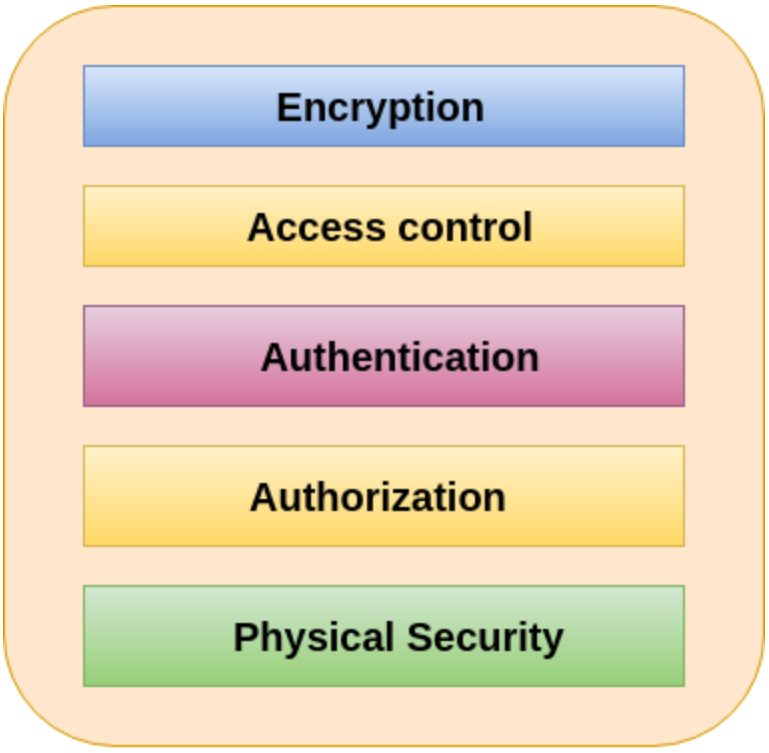
The CIA triad are-



1. Confidentiality

Confidentiality is roughly equivalent to privacy and avoids the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content. It prevents essential information from reaching the wrong people while making sure that the right people can get it. Data encryption is a good example to ensure confidentiality.

Tools for Confidentiality



Confidentiality Tools

Encryption

Encryption is a method of transforming information to make it unreadable for unauthorized users by using an algorithm. The transformation of data uses a secret key (an encryption key) so that the transformed data can only be read by using another secret key (decryption key). It protects sensitive data such as credit card numbers by encoding and transforming data into unreadable cipher text. This encrypted data can only be read by decrypting it. Asymmetric-key and symmetric-key are the two primary types of encryption.

Access control

Access control defines rules and policies for limiting access to a system or to physical or virtual resources. It is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users need to present credentials before they can be granted access such as a person's name or a computer's serial number. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.

Authentication

An authentication is a process that ensures and confirms a user's identity or role that someone has. It can be done in a number of different ways, but it is usually based on a combination of-

- something the person has (like a smart card or a radio key for storing secret keys),
- something the person knows (like a password),

- something the person is (like a human with a fingerprint).

Authentication is the necessity of every organizations because it enables organizations to keep their networks secure by permitting only authenticated users to access its protected resources. These resources may include computer systems, networks, databases, websites and other network-based applications or services.

Authorization

Authorization is a security mechanism which gives permission to do or have something. It is used to determine a person or system is allowed access to resources, based on an access control policy, including computer programs, files, services, data and application features. It is normally preceded by authentication for user identity verification. System administrators are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

Physical Security

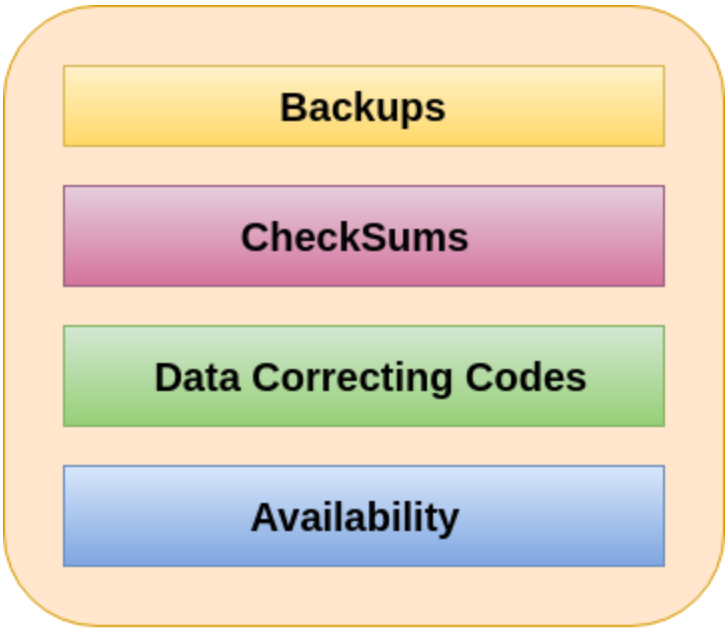
Physical security describes measures designed to deny the unauthorized access of IT assets like facilities, equipment, personnel, resources and other properties from damage. It protects these assets from physical threats including theft, vandalism, fire and natural disasters.

---

2. Integrity

Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification. It is the property that information has not be altered in an unauthorized way, and that source of the information is genuine.

Tools for Integrity



Integrity Tools

Backups

Backup is the periodic archiving of data. It is a process of making copies of data or data files to use in the event when the original data or data files are lost or destroyed. It is also used to make copies for historical purposes, such as for longitudinal studies, statistics or for historical records or to meet the requirements of a data retention policy. Many applications especially in a Windows environment, produce backup files using the .BAK file extension.

A checksum is a numerical value used to verify the integrity of a file or a data transfer. In other words, it is the computation of a function that maps the contents of a file to a numerical value. They are typically used to compare two sets of data to make sure that they are the same. A checksum function depends on the entire contents of a file. It is designed in a way that even a small change to the input file (such as flipping a single bit) likely to results in different output value.

Data Correcting Codes

It is a method for storing data in such a way that small changes can be easily detected and automatically corrected.

---

3. Availability

Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Tools for Availability

- Physical Protections
- Computational Redundancies

Physical Protections

Physical safeguard means to keep information available even in the event of physical challenges. It ensure sensitive information and critical information technology are housed in secure areas.

Computational redundancies

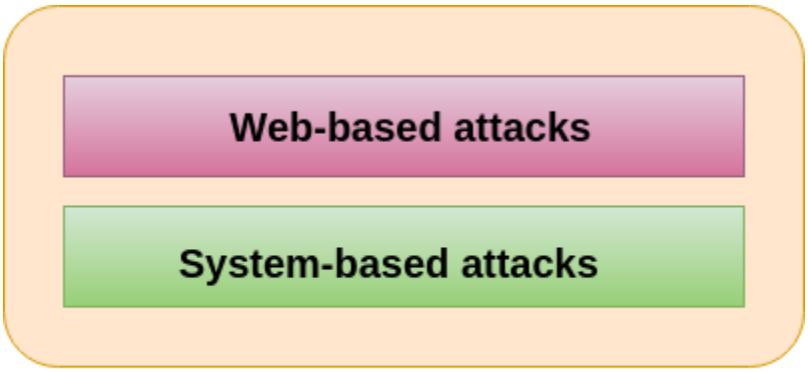
It is applied as fault tolerant against accidental faults. It protects computers and storage devices that serve as fallbacks in the case of failures.

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

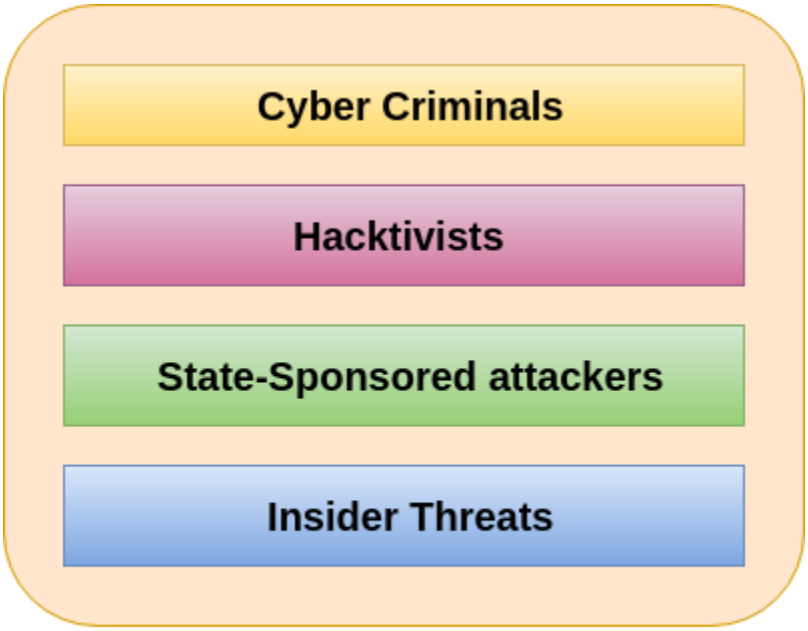
A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Types of Cyber Attackers

In computer and computer networks, an attacker is the individual or organization who performs the malicious activities to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

As the Internet access becomes more pervasive across the world, and each of us spends more time on the web, there is also an attacker grows as well. Attackers use every tools and techniques they would try and attack us to get unauthorized access.

There are four types of attackers which are described below-



Types of CyberAttackers

Cyber Criminals

Cybercriminals are individual or group of people who use technology to commit cybercrime with the intention of stealing sensitive company information or personal data and generating profits. In today's, they are the most prominent and most active type of attacker.

Cybercriminals use computers in three broad ways to do cybercrimes-

- **Select computer as their target**- In this, they attack other people's computers to do cybercrime, such as spreading viruses, data theft, identity theft, etc.
- **Uses the computer as their weapon**- In this, they use the computer to do conventional crime such as spam, fraud, illegal gambling, etc.
- **Uses the computer as their accessory**- In this, they use the computer to steal data illegally.

Hacktivists

Hacktivists are individuals or groups of hackers who carry out malicious activity to promote a political agenda, religious belief, or social ideology. According to Dan Lohrmann, chief security officer for Security Mentor, a national security training firm that works with states said "Hacktivism is a digital disobedience. It's hacking for a cause." Hacktivists are not like cybercriminals who hack computer networks to steal data for the cash. They are individuals or groups of hackers who work together and see themselves as fighting injustice.

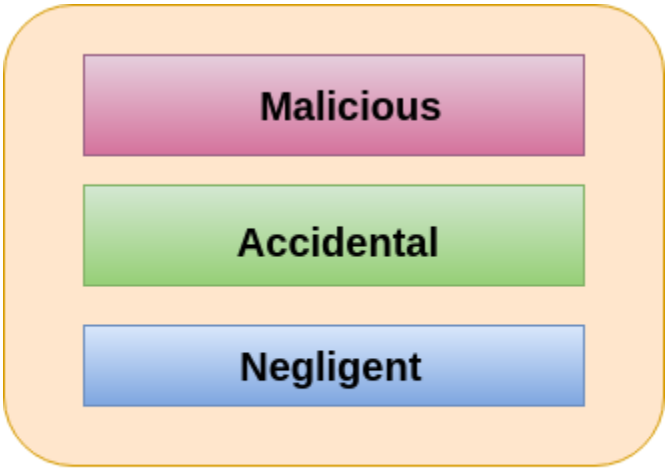
State-sponsored Attacker

State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin. These type of attackers are not in a hurry. The government organizations have highly skilled hackers and specialize in detecting vulnerabilities and exploiting these before the holes are patched. It is very challenging to defeat these attackers due to the vast resources at their disposal.

Insider Threats

The insider threat is a threat to an organization's security or data that comes from within. These type of threats are usually occurred from employees or former employees, but may also arise from third parties, including contractors, temporary workers, employees or customers.

Insider threats can be categorized below-



Insider Threats

Malicious-

Malicious threats are attempts by an insider to access and potentially harm an organization's data, systems or IT infrastructure. These insider threats are often attributed to dissatisfied employees or ex-

employees who believe that the organization was doing something wrong with them in some way, and they feel justified in seeking revenge.

Insiders may also become threats when they are disguised by malicious outsiders, either through financial incentives or extortion.

Accidental-

Accidental threats are threats which are accidently done by insider employees. In this type of threats, an employee might accidentally delete an important file or inadvertently share confidential data with a business partner going beyond company?s policy or legal requirements.

Negligent-

These are the threats in which employees try to avoid the policies of an organization put in place to protect endpoints and valuable data. For example, if the organization have strict policies for external file sharing, employees might try to share work on public cloud applications so that they can work at home. There is nothing wrong with these acts, but they can open up to dangerous threats nonetheless.

Information security involves protecting information and systems from unauthorized access, disclosure, alteration, and destruction. Here are some key terms and their meanings:

Information Security Terminology

Basic Concepts

1. **Confidentiality**: Ensuring information is accessible only to those authorized to access it.
2. **Integrity**: Ensuring that data remains accurate, complete, and unaltered.
3. **Availability**: Ensuring that authorized users have reliable access to information and systems when needed.

Threats and Vulnerabilities

4. **Threat**: A potential danger to information or systems, such as hacking or natural disasters.
5. **Vulnerability**: A weakness in a system that can be exploited by a threat to gain unauthorized access or cause harm.
6. **Risk**: The likelihood that a threat will exploit a vulnerability and the impact it will have.

Attack Types

7. **Malware**: Malicious software, including viruses, worms, Trojans, ransomware, and spyware.

8. **Phishing**: Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity.
9. **Denial-of-Service (DoS)**: An attack aimed at making a system or service unavailable by overwhelming it with traffic.
10. **SQL Injection**: A code injection technique used to attack data-driven applications by inserting malicious SQL statements.

Security Measures

11. **Authentication**: The process of verifying the identity of a user or system.
12. **Encryption**: Encoding data so that it can only be read by those with the correct decryption key.
13. **Firewall**: A security device or software that monitors and controls incoming and outgoing network traffic based on predefined rules.
14. **Antivirus Software**: A program designed to detect, prevent, and remove malware.

Access Control

15. **Least Privilege**: Granting users only the access necessary to perform their job functions.
16. **Multi-Factor Authentication (MFA)**: Using two or more methods (e.g., password and fingerprint) to verify identity.

Legal and Compliance

17. **GDPR**: General Data Protection Regulation, a regulation on data protection and privacy in the EU.
18. **HIPAA**: Health Insurance Portability and Accountability Act, a U.S. law protecting medical information.
19. **Cybersecurity Framework**: A set of guidelines (e.g., NIST framework) for managing and reducing cybersecurity risks.

Incident Response

20. **Incident**: A security event that compromises the confidentiality, integrity, or availability of information.
21. **Forensics**: Investigating and analyzing an incident to understand its impact and prevent future occurrences.

What is Information Security?

Information security is the practice of protecting information by mitigating information risks. It involves the protection of information systems and the information processed, stored, and transmitted by these systems from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes the protection of personal information, financial information, and sensitive or confidential information stored in both digital and physical forms. Effective information security requires a comprehensive and multi-disciplinary approach, involving people, processes, and technology.

What is Information Security (InfoSec)?

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information. Information can be a physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data on your mobile phone, your biometrics, etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media, etc.

During the First World War, a Multi-tier Classification System was developed keeping in mind the sensitivity of the information. With the beginning of the Second World War, formal alignment of the Classification System was done. Alan Turing was the one who successfully decrypted the Enigma Machine which was used by Germans to encrypt warfare data.

Effective information security requires a comprehensive approach that considers all aspects of the information environment, including technology, policies and procedures, and people. It also requires ongoing monitoring, assessment, and adaptation to address emerging threats and vulnerabilities.

Why We Use Information Security?

We use information security to protect valuable information assets from a wide range of threats, including theft, espionage, and cybercrime. Here are some key reasons why information security is important:

- **Protecting sensitive information:** Information security helps protect sensitive information from being accessed, disclosed, or modified by unauthorized individuals. This includes personal information, financial data, and trade secrets, as well as confidential government and military information.
- **Mitigating risk:** By implementing information security measures, organizations can mitigate the risks associated with cyber threats and other security incidents. This includes minimizing the risk of data breaches, denial-of-service attacks, and other malicious activities.

- **Compliance with regulations:** Many industries and jurisdictions have specific regulations governing the protection of sensitive information. Information security measures help ensure compliance with these regulations, reducing the risk of fines and legal liability.
- **Protecting reputation:** Security breaches can damage an organization's reputation and lead to lost business. Effective information security can help protect an organization's reputation by minimizing the risk of security incidents.
- **Ensuring business continuity:** Information security helps ensure that critical business functions can continue even in the event of a security incident. This includes maintaining access to key systems and data, and minimizing the impact of any disruptions.

What are the 3 Principles of Information Security?

Information security is necessary to ensure the confidentiality, integrity, and availability of information, whether it is stored digitally or in other forms such as paper documents. Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

- **Confidentiality –** Means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
- **Integrity –** Means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.
- **Availability –** Means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.
- **Non repudiation –** Means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.

- **Authenticity –** Means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission.

- **Accountability –** This means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority.

What is an Information Security Management System (ISMS)?

An **Information Security Management System (ISMS)** is a structured framework designed to protect an organization's information assets. It includes policies, procedures, and controls to manage and secure sensitive data from threats like unauthorized access, data breaches, and cyberattacks. By following international standards like ISO/IEC 27001, an ISMS helps organizations identify risks, implement security measures, and continuously improve their security practices to safeguard their information.

What is the General Data Protection Regulation (GDPR)?

The **General Data Protection Regulation (GDPR)** is a comprehensive privacy law established by the European Union (EU) to protect individuals' personal data. Effective since May 25, 2018, GDPR sets strict rules on how personal data is collected, used, stored, and shared. It grants individuals more control over their data, including rights to access, correct, and delete their information. GDPR also requires organizations to be transparent about their data practices and to implement strong security measures. Non-compliance can result in significant fines, emphasizing the importance of safeguarding personal data and respecting privacy rights.

Types of Information Security

Information Security (InfoSec) focuses on protecting data from threats and unauthorized access. Here are five important types:

- **Network Security**: Protects computer networks from attacks and unauthorized access using tools like **firewalls**, **Intrusion Detection Systems (IDS)**, and **Virtual Private Networks (VPNs)**. For example, a firewall can block malicious traffic trying to enter a company's network.
- **Application Security**: Secures software applications by finding and fixing vulnerabilities, using methods like **code reviews** and **security patches**. An example is a web application firewall (WAF) that prevents attacks on websites by filtering and monitoring HTTP traffic.
- **Data Security**: Ensures data safety during storage and transfer by using **encryption** and **data masking**. For instance, encrypted emails are unreadable to anyone without the decryption key, protecting sensitive information.
- **Endpoint Security**: Secures individual devices such as computers, smartphones, and tablets through **antivirus software** and **Endpoint Detection and Response (EDR)** tools. An example is an antivirus program that scans and removes malware from a personal laptop.
- **Cloud Security**: Protects data and applications hosted in cloud environments with measures like **secure cloud configurations** and **Identity and Access Management (IAM)**. For instance,

using multi-factor authentication (MFA) helps ensure that only authorized users can access cloud-based services.

Why is Information Security Important?

Advantages for implementing an information classification system in an organization's information security program:

- **Improved security:** By identifying and classifying sensitive information, organizations can better protect their most critical assets from unauthorized access or disclosure.
- **Compliance**: Many regulatory and industry standards, such as HIPAA and PCI-DSS, require organizations to implement information classification and data protection measures.
- **Improved efficiency**: By clearly identifying and labeling information, employees can quickly and easily determine the appropriate handling and access requirements for different types of data.
- **Better risk management**: By understanding the potential impact of a data breach or unauthorized disclosure, organizations can prioritize resources and develop more effective incident response plans.
- **Cost savings**: By implementing appropriate security controls for different types of information, organizations can avoid unnecessary spending on security measures that may not be needed for less sensitive data.
- **Improved incident response**: By having a clear understanding of the criticality of specific data, organizations can respond to security incidents in a more effective and efficient manner.

There are some potential disadvantages for implementing an information classification system in an organization's information security program:

- **Complexity:** Developing and maintaining an information classification system can be complex and time-consuming, especially for large organizations with a diverse range of data types.
- **Cost**: Implementing and maintaining an information classification system can be costly, especially if it requires new hardware or software.
- **Resistance to change:** Some employees may resist the implementation of an information classification system, especially if it requires them to change their usual work habits.
- **Inaccurate classification:** Information classification is often done by human, so it is possible that some information may be misclassified, which can lead to inadequate protection or unnecessary restrictions on access.
- **Lack of flexibility:** Information classification systems can be rigid and inflexible, making it difficult to adapt to changing business needs or new types of data.
- **False sense of security**: Implementing an information classification system may give organizations a false sense of security, leading them to overlook other important security controls and best practices.

- **Maintenance:** Information classification should be reviewed and updated frequently, if not it can become outdated and ineffective.

Uses of Information Security

Information security has many uses, including:

- **Confidentiality:** Keeping sensitive information confidential and protected from unauthorized access.
- **Integrity:** Maintaining the accuracy and consistency of data, even in the presence of malicious attacks.
- **Availability:** Ensuring that authorized users have access to the information they need, when they need it.
- **Compliance:** Meeting regulatory and legal requirements, such as those related to data privacy and protection.
- **Risk management:** Identifying and mitigating potential security threats to prevent harm to the organization.
- **Disaster recovery:** Developing and implementing a plan to quickly recover from data loss or system failures.
- **Authentication:** Verifying the identity of users accessing information systems.
- **Encryption:** Protecting sensitive information from unauthorized access by encoding it into a secure format.
- **Network security:** Protecting computer networks from unauthorized access, theft, and other types of attacks.
- **Physical security:** Protecting information systems and the information they store from theft, damage, or destruction by securing the physical facilities that house these systems.

Issues of Information Security

Information security faces many challenges and issues, including:

- **Cyber threats:** The increasing sophistication of cyber attacks, including malware, phishing, and ransomware, makes it difficult to protect information systems and the information they store.
- **Human error:** People can inadvertently put information at risk through actions such as losing laptops or smartphones, clicking on malicious links, or using weak passwords.
- **Insider threats:** Employees with access to sensitive information can pose a risk if they intentionally or unintentionally cause harm to the organization.

- **Legacy systems:** Older information systems may not have the security features of newer systems, making them more vulnerable to attack.
- **Complexity:** The increasing complexity of information systems and the information they store makes it difficult to secure them effectively.
- **Mobile and IoT devices:** The growing number of mobile devices and internet of things (IoT) devices creates new security challenges as they can be easily lost or stolen, and may have weak security controls.
- **Integration with third-party systems:** Integrating information systems with third-party systems can introduce new security risks, as the third-party systems may have security vulnerabilities.
- **Data privacy:** Protecting personal and sensitive information from unauthorized access, use, or disclosure is becoming increasingly important as data privacy regulations become more strict.
- **Globalization:** The increasing globalization of business makes it more difficult to secure information, as data may be stored, processed, and transmitted across multiple countries with different security requirements.

Malware classifications

What is Malware? And its Types

M**alware** is malicious software and refers to any software that is designed to cause harm to computer systems, networks, or users. Malware can take many forms. Individuals and organizations need to be aware of the different types of malware and take steps to protect their systems, such as using antivirus software, keeping software and systems up-to-date, and being cautious when opening email attachments or downloading software from the internet.

What is Malware?

Malware is software that gets into the system without user consent to steal the user's private and confidential data, including bank details and passwords. They also generate annoying pop-up ads and change system settings. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware, and other malicious programs. Individuals and organizations need to be aware of the different types of malware and take steps to protect their systems, such as using antivirus software, keeping software and systems up-to-date, and being cautious when opening email attachments or downloading software from the internet.

What Does Malware Do?

Malware is designed to harm and exploit your computer or network. It can steal sensitive information like passwords and credit card numbers, disrupt your system's operations, and even allow attackers to gain unauthorized access to your device. Some types of malware, such as

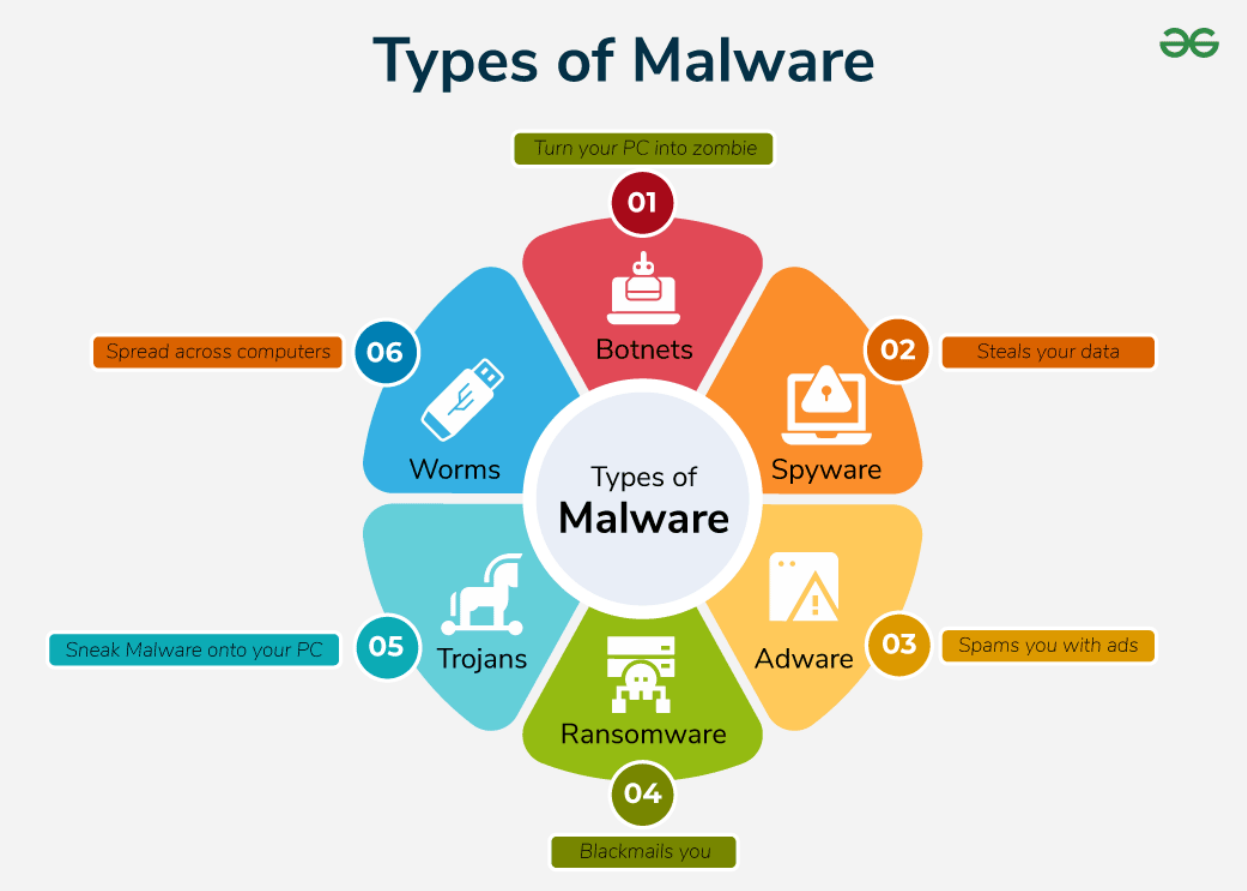
ransomware, encrypt your files and demand payment to unlock them, while spyware monitors your activities and sends the information back to the attacker. Additionally, malware can spread to other devices on the same network, making it a significant threat. Protecting your devices with up-to-date antivirus software and being cautious about your open links and attachments can help mitigate these risks.

Why Do Cybercriminals Use Malware?

- Cybercriminals use malware, including all forms of malicious software including viruses, for various purposes.
- Using deception to induce a victim to provide personal information for identity theft
- Theft of customer credit card information or other financial information
- Taking over several computers and using them to launch denial-of-service attacks against other networks
- Using infected computers to mine for cryptocurrencies like bitcoin.

Types of Malware

- **Viruses –** A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.
- **Worms –** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.
- **Trojan horse –** A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.



Types of Malware

- **Ransomware** – Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key that is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.
- **Adware** – It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.
- **Spyware** – Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.
- **Logic Bombs –** A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

- **Rootkits –** A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.
- **Backdoors** – A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.
- **Keyloggers –** Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

How To Know If Our Devices Are Infected With Malware?

- Performing poorly on the computer by execution.
- When your web browser directs you to a website you didn't intend to visit, this is known as a browser redirect.
- Warnings about infections are frequently accompanied by offers to buy a product to treat them.
- Having trouble starting or shutting down your computer.
- Persistent pop-up ads.

How To Protect From Malware?

- Update your operating system and software. Install updates as soon as they become available because cybercriminals search for vulnerabilities in out-of-date or outdated software.
- Never click on a popup's link. Simply click the "X" in the message's upper corner to close it and leave the page that generated it.
- Don't install too many apps on your devices. Install only the apps you believe you will regularly use and need.
- Be cautious when using the internet.
- Do not click on unidentified links. If a link seems suspicious, avoid clicking it whether it comes from an email, social networking site, or text message.
- Choose the websites you visit wisely. Use a safe search plug-in and try to stick to well-known and reputable websites to avoid any that might be malicious without your knowledge.

- Emails requesting personal information should be avoided. Do not click a link in an email that appears to be from your bank and asks you to do so in order to access your account or reset your password. Log in immediately at your online banking website.

How To Remove Malware?

A large number of security software programs are made to both find and stop malware as well as to eliminate it from infected systems. An antimalware tool that handles malware detection and removal is Malwarebytes. Malware can be eliminated from Windows, macOS, Android, and iOS operating systems. A user's registry files, currently running programs, hard drives, and individual files can all be scanned by Malwarebytes. Malware can then be quarantined and removed if it is found. Users cannot, however, set automatic scanning schedules like they can with some other tools.

Tools Used to Remove Malware

- Malwarebytes
- SUPERAntiSpyware
- Malicious Software Removal Tool (MSRT)
- Bitdefender Antivirus Free Edition
- Adaware Antivirus Free
- Avast Free Mac Security

Advantages of Detecting and Removing Malware

- **Improved Security:** By detecting and removing malware, individuals, and organizations can improve the security of their systems and reduce the risk of future infections.
- **Prevent Data Loss:** Malware can cause data loss, and by removing it, individuals and organizations can protect their important files and information.
- **Protect Reputation:** Malware can cause harm to a company's reputation, and by detecting and removing it, individuals and organizations can protect their image and brand.
- **Increased Productivity:** Malware can slow down systems and make them less efficient, and by removing it, individuals and organizations can increase the productivity of their systems and employees.

Disadvantages of Detecting and Removing Malware

- **Time-Consuming:** The process of detecting and removing malware can be time-consuming and require specialized tools and expertise.

- **Cost:** Antivirus software and other tools required to detect and remove malware can be expensive for individuals and organizations.
- **False Positives:** Malware detection and removal tools can sometimes result in false positives, causing unnecessary alarm and inconvenience.
- **Difficulty:** Malware is constantly evolving, and the process of detecting and removing it can be challenging and require specialized knowledge and expertise.
- **Risk of Data Loss:** Some malware removal tools can cause unintended harm, resulting in data loss or system instability.

Web Server and its Types of Attack

Web Servers are where websites are stored. They are computers that run an operating system and are connected to a database to run multiple applications. A web server's primary responsibility is to show website content by storing, processing, and distributing web pages to users. Web servers are essential for delivering websites and online services, making them prime targets for cyberattacks. These attacks aim to disrupt service, steal data, or exploit server vulnerabilities. This article explores the common attack methods and provides different preventions to stay secure from these attacks on servers.

What is Web Server Attack?

Any attempt by a malicious actor to undermine the security of a Web-based application is referred to as a Web Application Attack or Web Server Attack. Web application attacks can either target the application itself to get access to sensitive data, or they can use the application as a staging area for attacks against the program's users.

These are the types of major Web Attacks:

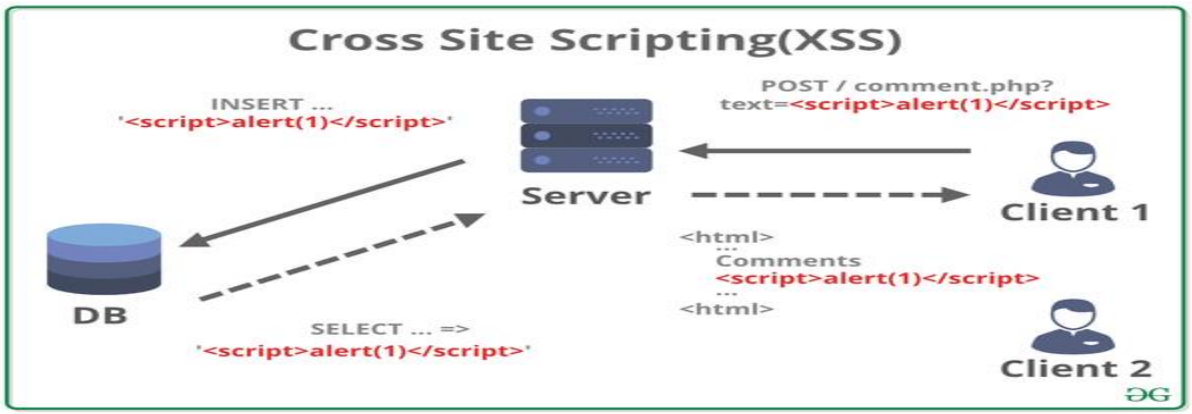
- Denial-of-Service (DoS) / Distributed Denial-of-service (DDoS)
- Web Defacement Attack
- SSH Brute Force Attack
- Cross-site scripting (XSS)
- Directory Traversal
- DNS Server Hijacking
- MITM Attack
- HTTP Response Splitting Attack

1. DENIAL-OF-SERVICE (DOS) / DISTRIBUTED DENIAL-OF-SERVICE (DDOS): Denial of Service is when an internet hacker causes the web to provide a response to a large number of requests. This causes the server to slow down or crash and users authorized to use the server will be denied service or access. Government services, credit card companies under large corporations are common victims of this type of attack

2. WEB DEFACEMENT ATTACK: In a Web Defacement Attack, the hacker gains access to the site and defaces it for a variety of reasons, including humiliation and discrediting the victim. The attackers hack into a web server and replace a website hosted with one of their own.

3. SSH BRUTE FORCE ATTACK: By brute-forcing SSH login credentials, an SSH Brute Force Attack is performed to attain access. This exploit can be used to send malicious files without being noticed. Unlike a lot of other tactics used by hackers, brute force attacks aren't reliant on existing vulnerabilities

4. CROSS SITE SCRIPTING (XSS): This type of attack is more likely to target websites with scripting flaws. The injection of malicious code into web applications is known as Cross-Site Scripting. The script will give the hacker access to web app data such as sessions, cookies, and so on.



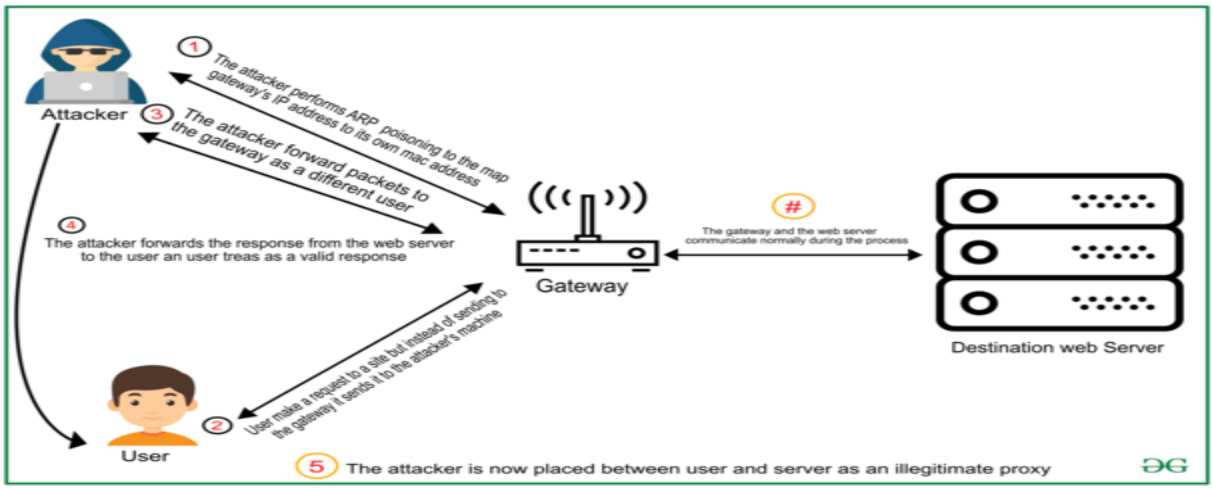
Cross Site Scripting (XSS)

5. DIRECTORY TRAVERSAL: Directory Traversal Attack is usually effective on older servers with vulnerabilities and misconfiguration. The root directory is where web pages are stored, however, in this attack, the hacker is after directories outside of the root directory.

6. DNS SERVER HIJACKING: DNS Hijacking refers to any attack that tricks the end-user into thinking he or she is communicating with a legitimate domain name when in reality they are communicating with a domain name or IP address that the attacker has set up. DNS Redirection is another name for this.

7. MITM ATTACK: Man-in-the-Middle (MITM) attack allows the attacker to access sensitive information by blocking and modifying the connection between the end-user and web servers.

In MITM attacks or smells, the hacker captures or corrects modified messages between the user and the web server by listening or intervening in the connection. This allows the attacker to steal sensitive user information such as online banking details, usernames, passwords, etc., which are transmitted online to the webserver. The attacker entices the victim to attach to an Internet server by pretending to be an agent.



Man-in-the-Middle (MITM) attack

8. HTTP RESPONSE SPLITTING ATTACK: HTTP Response Splitting is a protocol manipulation attack, similar to Parameter Tampering. Only programs that use HTTP to exchange data are vulnerable to this attack. Because the entry point is in the user viewable data, it works just as well with HTTPS. The attack can be carried out in a variety of ways.

How to Prevent Different Attacks in Web Security?

- **Keep your system up to date:** Not updating the software regularly makes it weaker and leaves the system more vulnerable to attacks. Hackers take advantage of these flaws, and cybercriminals take advantage of them to get access to your network.
- **Prevent connecting to the public WiFi network:** An unsecured Wi-Fi connection can be used by hackers to spread malware. If you allow file-sharing across a network, a hacker can simply infect your computer with tainted software. The ability of a hacker to put himself between you and the connection point poses the greatest threat to free Wi-Fi security.
- **Install Anti-virus, and update it regularly:** Antivirus software is designed to identify, block, and respond to dangerous software, such as viruses, on your computer. Because computers are continuously threatened by new viruses, it is critical to keep antivirus software up to date. Anti-virus updates include the most recent files required to combat new threats and safeguard your machine. These signature files are provided on a daily basis, if not more frequently.

- **Use IDS and firewall with updated signatures:** NIDS are security threat detection and prevention systems that identify and prevent security threats from infiltrating secure networks. The use of NIDS has a negligible effect on network performance. NIDS are typically passive devices that listen to a network without interfering with the network's normal operation.
- **Backup your data:** The fundamental purpose of a data backup is to keep a safe archive of your vital information, whether it's classified documents for your business or priceless family photos so that you can quickly and effortlessly recover your device in the event of data loss. Backup copies allow data to be restored from a previous point in time, which can aid in the recovery of a business after an unanticipated occurrence. Protecting against primary data loss or corruption requires storing a copy of the data on a secondary medium.
- **Install a Firewall:** Firewalls defend your computer or network from outside cyber attackers by filtering out dangerous or superfluous network traffic. Firewalls can also prevent harmful malware from gaining internet access to a machine or network.

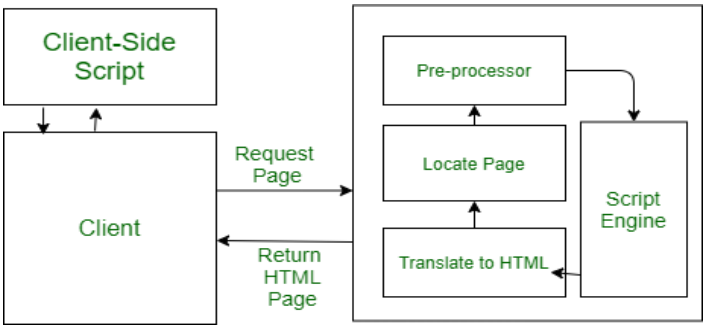
Web Scripting and its Types

The process of creating and embedding scripts in a web page is known as **web-scripting**. A script or a computer-script is a list of commands that are embedded in a web-page normally and are interpreted and executed by a certain program or scripting engine.

- Scripts may be written for a variety of purposes such as for automating processes on a local-computer or to generate web pages.
- The programming languages in which scripts are written are called scripting language, there are many scripting languages available today.
- Common scripting languages are VBScript, JavaScript, ASP, PHP, PERL, JSP etc.

Types of Script :

Scripts are broadly of following two type :



Web Scripting

Client-Side Scripts :

1. Client-side scripting is responsible for interaction within a web page. The client-side scripts are firstly downloaded at the client-end and then interpreted and executed by the browser (default browser of the system).
2. The client-side scripting is browser-dependent. i.e., the client-side browser must be scripting enables in order to run scripts
3. Client-side scripting is used when the client-side interaction is used. Some example uses of client-side scripting may be :
    - To get the data from user's screen or browser.
    - For playing online games.
    - Customizing the display of page in browser without reloading or reopening the page.
4. Here are some popular client-side scripting languages VBScript, JavaScript, Hypertext Processor(PHP).

Server-Side Scripts :

1. Server-side scripting is responsible for the completion or carrying out a task at the server-end and then sending the result to the client-end.
2. In server-side script, it doesn't matter which browser is being used at client-end, because the server does all the work.
3. Server-side scripting is mainly used when the information is sent to a server and to be processed at the server-end. Some sample uses of server-scripting can be :
    - Password Protection.
    - Browser Customization (sending information as per the requirements of client-end browser)
    - Form Processing
    - Building/Creating and displaying pages created from a database.
    - Dynamically editing changing or adding content to a web-page.
4. Here are some popular server-side scripting languages PHP, Perl, ASP (Active Server Pages), JSP (Java Server Pages).

Server side web application attacks

Server-side web applications are vulnerable to various types of attacks due to their complexity and the sensitive operations they perform. Below are some common types of server-side attacks, their mechanisms, and ways to mitigate them:

---

1. SQL Injection

What is it? An attacker manipulates a web application's input fields to inject malicious SQL queries, allowing them to access or modify the database.

How it works:

- The attacker finds an input field (e.g., login form, search box) that is directly used in SQL queries.
- By entering SQL commands like ' OR '1'='1 instead of valid input, the attacker tricks the server into executing unintended SQL statements.

Consequences:

- Data theft or modification.
- Bypassing authentication mechanisms.
- Complete database compromise.

Prevention:

- Use prepared statements (parameterized queries).
- Employ stored procedures.
- Validate and sanitize all user inputs.
- Implement web application firewalls (WAF).

---

2. Cross-Site Scripting (XSS)

What is it? Though XSS is typically client-side, server-side XSS occurs when an application improperly sanitizes or encodes output, allowing malicious scripts to execute.

How it works:

- Malicious code is injected into a web page stored on the server (e.g., in comments or user profiles).
- When other users view the page, the malicious script executes in their browsers.

Consequences:

- Theft of session cookies or user credentials.
- Unauthorized actions on behalf of the user.
- Redirection to malicious sites.

Prevention:

- Sanitize and encode all output data.
- Use Content Security Policies (CSP).
- Validate and escape user-generated content before storing or displaying.

---

3. Remote Code Execution (RCE)

What is it? Attackers exploit vulnerabilities to execute arbitrary code on the server.

How it works:

- Flaws in input handling or software libraries allow attackers to send commands to the server.
- This could involve file uploads, deserialization bugs, or poorly configured APIs.

Consequences:

- Complete control over the server.
- Data theft or destruction.
- Launching further attacks on other systems.

Prevention:

- Regularly update and patch software.
- Restrict file upload types and validate uploaded content.
- Use secure coding practices and tools to detect vulnerabilities.

---

4. File Inclusion Vulnerabilities

What is it? Involves exploiting a web application's handling of file paths to include unintended files.

How it works:

- Local File Inclusion (LFI): The attacker tricks the server into including sensitive system files (e.g., /etc/passwd).
- Remote File Inclusion (RFI): The attacker includes a remote malicious script.

Consequences:

- Exposure of sensitive data.
- Execution of malicious scripts.
- Server compromise.

Prevention:

- Avoid using user input in file paths.
- Use a whitelist for allowed file paths.
- Disable functions like allow_url_include in PHP.

---

5. Authentication Bypass

What is it? Attackers exploit weaknesses in authentication mechanisms to gain unauthorized access.

How it works:

- Brute force attacks to guess credentials.
- Exploiting insecure session management.
- Manipulating cookies or tokens.

Consequences:

- Unauthorized access to sensitive areas.
- Data theft or modification.

Prevention:

- Enforce strong password policies.
- Implement multi-factor authentication (MFA).

- Use secure cookies and tokens with proper expiration.

---

6. Server-Side Request Forgery (SSRF)

What is it? The attacker tricks the server into making unintended HTTP requests to arbitrary locations.

How it works:

- The attacker sends a crafted request to an endpoint that fetches external data (e.g., a URL fetch service).
- The server performs the request, potentially exposing sensitive data or interacting with internal services.

Consequences:

- Leakage of internal server information.
- Unauthorized interaction with internal resources.
- Facilitation of further attacks like port scanning.

Prevention:

- Validate and sanitize all URLs provided by users.
- Restrict outgoing requests to a whitelist of trusted domains.
- Use network-level protections to block internal requests.

---

7. Command Injection

What is it? Attackers inject malicious commands into a web application to execute system-level operations on the server.

How it works:

- Vulnerable input fields allow injection of OS commands (e.g., ; rm -rf /).
- The commands execute with the server's privileges.

Consequences:

- Data theft or destruction.
- Full server compromise.

Prevention:

- Avoid direct execution of system commands based on user input.
- Use libraries that provide safe abstractions.
- Validate and sanitize all inputs thoroughly.

---

8. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

What is it? These attacks overwhelm a server with traffic, rendering the web application unavailable.

How it works:

- A single attacker (DoS) or multiple compromised systems (DDoS) send massive amounts of traffic.
- The server becomes overloaded and unable to respond to legitimate requests.

Consequences:

- Downtime and loss of business.
- Increased resource consumption and operational costs.

Prevention:

- Use load balancers and content delivery networks (CDNs).
- Implement rate limiting and IP blocking.
- Monitor and mitigate traffic anomalies.

---

9. Insecure Deserialization

What is it? Exploits vulnerabilities in how the server deserializes data.

How it works:

- Maliciously crafted serialized data is sent to the server.
- When deserialized, it executes harmful code or alters server behavior.

Consequences:

- Arbitrary code execution.
- Data manipulation or theft.

Prevention:

- Avoid deserialization of untrusted data.
- Use signed or encrypted serialized objects.
- Validate and sanitize deserialized inputs.

---

10. Server Misconfiguration

What is it? Poorly configured servers or software expose vulnerabilities.

How it works:

- Default credentials, unnecessary open ports, or exposed admin interfaces can be exploited.
- Missing security headers or outdated software versions increase risks.

Consequences:

- Unauthorized access to sensitive systems.
- Increased susceptibility to known vulnerabilities.

Prevention:

- Regularly audit and harden server configurations.
- Disable unnecessary services and ports.
- Apply patches and updates promptly.

Conclusion

Server-side attacks can have devastating impacts on an organization, but proactive measures, regular audits, and secure coding practices can significantly reduce risk

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a type of security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. It exploits the trust a user has in a website, leading to data theft, unauthorized actions, or malware distribution.

How XSS Works

XSS exploits the lack of proper validation or sanitization of user input in web applications. It targets scripts executed in the victim's browser rather than on the server.

1. **Injection Point**: An attacker identifies an input field or URL parameter that reflects user input without proper encoding or sanitization.
2. **Payload Delivery**: The attacker crafts a malicious script and injects it into the vulnerable field or parameter.
3. **Execution**: When another user accesses the compromised page or service, the malicious script is executed in their browser.
4. **Impact**: The script can perform unauthorized actions, such as stealing cookies, modifying the DOM, or redirecting the user to a phishing site.

Types of XSS

XSS can be categorized based on where the malicious script resides and how it is executed:

1. Stored XSS (Persistent XSS)

- **What is it?**: The malicious script is stored on the server (e.g., in a database, file system).
- **How it works**:
    - The attacker submits malicious input through forms (e.g., comments, profiles, forums).
    - The script is stored and later delivered to users when they load the compromised page.
- **Example**:

  html

  Copy code

  <script>alert('Hacked!');</script>

  When this is stored as a comment, every visitor sees the alert when viewing the comments section.
- **Impact**: Affects all users accessing the page where the script is displayed.

2. Reflected XSS

- **What is it?**: The malicious script is part of a URL or request and is executed immediately when the user interacts with the link.
- **How it works**:
    - The attacker crafts a URL containing the payload and tricks the victim into clicking it.
    - The server reflects the payload back in the response without sanitizing it.
- **Example URL**:

  php

  Copy code

  http://example.com/search?q=<script>alert('Hacked!');</script>

  If the search query is not sanitized, the script runs in the user's browser.
- **Impact**: Affects only users who interact with the crafted URL.

  3. DOM-based XSS
- **What is it?**: The vulnerability occurs entirely on the client side (within the DOM) and does not involve the server.
- **How it works**:
    - JavaScript in the web application dynamically updates the DOM using unsanitized input.
    - Malicious scripts are injected and executed directly in the browser.
- **Example**:

  javascript

  Copy code

  let user = location.search.split('=')[1];

  document.getElementById('welcome').innerHTML = 'Welcome, ' + user;

  If ?user=<script>alert('Hacked!');</script> is passed in the URL, the alert executes.
- **Impact**: Depends on the browser's handling of JavaScript.

Potential Consequences of XSS

1. **Data Theft**:
    - Stealing session cookies, tokens, or sensitive information.
    - Example: document.cookie can be accessed to hijack user sessions.
2. **Phishing Attacks**:
    - Redirecting users to fake login pages to steal credentials.
    - Example: Replacing the login form with a malicious one.
3. **Defacement**:
    - Changing the appearance or content of a webpage.
    - Example: Inserting offensive messages or graphics.
4. **Drive-by Download**:
    - Forcing users to download malware or malicious files.
    - Example: Embedding download links via <a> tags.
5. **Account Takeover**:
    - Exploiting stolen session cookies to impersonate the user.

XSS Mitigation Techniques

1. **Input Validation and Sanitization**:
    - Validate all user inputs to ensure they conform to expected formats.
    - Use libraries like OWASP's **ESAPI** or frameworks' built-in validation tools.
2. **Output Encoding**:
    - Encode all data before displaying it in the browser.
    - Use context-aware encoding:
        - **HTML**: Convert special characters (<, >, &, etc.) to HTML entities.

html

Copy code

<script>alert('XSS');</script>

        - **JavaScript**: Escape data used in scripts.

        - **CSS**: Escape CSS context.

3. **Use Secure APIs**:
    - Prefer secure APIs that automatically handle input sanitization and encoding.
4. **Content Security Policy (CSP)**:
    - Restrict the sources from which scripts can be executed.
    - Example:

    http

    Copy code

    Content-Security-Policy: script-src 'self' https://trusted-cdn.com
5. **HTTPOnly and Secure Cookies**:
    - Use HTTPOnly cookies to prevent access via JavaScript.
    - Secure cookies ensure they are only transmitted over HTTPS.
6. **Avoid Inline JavaScript**:
    - Move all scripts to external files.
    - Disable eval() and similar functions.
7. **Proper Error Handling**:
    - Avoid exposing stack traces or detailed errors that could aid attackers.
8. **Regular Security Testing**:
    - Use tools like **Burp Suite**, **ZAP**, or **Acunetix** to detect XSS vulnerabilities.
    - Conduct penetration testing and code reviews.

Example of Secure Code

Vulnerable Code:

html

Copy code

Welcome,

<script>

```
  let user = new URLSearchParams(location.search).get('name');
  document.getElementById('user').innerHTML = user;
</script>
```

Secure Code:

```
html
Copy code
Welcome, <span id="user"></span>
<script>
  let user = new URLSearchParams(location.search).get('name');
  let safeUser = user.replace(/[<>"']/g, '');
  document.getElementById('user').textContent = safeUser;
</script>
```

Conclusion

XSS is a powerful and common attack vector that can lead to significant harm. Proactively implementing secure coding practices, robust input validation, and adopting tools like CSP can greatly reduce the risk of XSS vulnerabilities in web applications.

Cross-site Scripting

Cross-site scripting is also known as XSS. When malicious JavaScript is executed by a hacker within the user's browser, then cross-site scripting will occur. In this attack, the code will be run within the browser of the victim. Upon initial injection, the attacker does not fully control the site. Instead, the malicious code is attacked on the top of a valid website by the bad actor. Whenever the website is loaded, the malware will be executed, and this will load to trick the browser.

JavaScript in XSS

JavaScript is a programming language that runs on a web server inside. The interactivity and functionality are added to the web page using the client-side code. It is used extensively on CMS platforms or all major applications. If the JavaScript code exists inside our browser, it will not impact the website's visitors, unlike the server-side language like PHP. JavaScript cannot run on the server because it is client-side. Using the background requests, it can interact with the server. An attacker can use these

background requests to add malicious content to a web page without refreshing the web page. These requests can perform the actions asynchronously or gather analytics about the browser of the client.

Working of Cross-site scripting

When the attacker exploits a vulnerability on the software of a website, only then can they inject their code into a web page of the victim's website. After successfully exploiting the vulnerability, attackers can inject their script, which will be executed using the browser of the victim.

When the victim's browser page successfully runs the JavaScript, sensitive information about the target user can be accessed from the session. The session allows an attacker to target the administrator of the site and completely compromise a website.

The cross-site scripting attack will be very useful when most of the publically available pages on the website have vulnerabilities. In this case, the malicious code can be injected by adding their malicious content, phishing prompt, ads on the website to target the website's visitors.

Types of Cross-site scripting attacks

There are various ways to use cross-site scripting on the basis of our goals. The most common type of cross-site scripting attacks is as follows:

Stored Cross-site scripting attack

When a payload is stored by the attacker on the compromised server, in this case, a stored cross-site scripting attack will occur. Due to this, the malicious code will be delivered by the website to the other visitors. In this attack, the initial action is only required by the attacker, and due to this, many visitors have to be compromised. The stored cross-site attack is the most dangerous cross-site scripting. An example of this attack includes the fields of our profile like our email id, username, which are stored by the server and displayed on our account page.

Reflected Cross-site scripting attack

When the data is sent from browser to server, and the payload is stored in that data, in this case, reflected cross-site scripting would occur. An example of this attack includes a contact form or website's search data sent to the target and contains a malicious script. Search form is another type of reflected cross-site attack in which a search query is sent by the visitor to the server, and the result can only be seen by visitors. Victim's custom links are sent by the attackers that direct visitors towards the vulnerable page.

Self Cross-site scripting attack

When the vulnerability is exploited by the attacker, which requires manual changes and extremely specific context, in this case, self cross-site scripting attack will occur. Specific changes include setting our information to a payload or cookies values types of things.

Blind Cross-site scripting attack

When the result of an attack cannot be seen by an attacker, in this case, blind cross-site scripting will occur. In a blind cross-site scripting attack, the vulnerability lies on that page, which can only be accessed by authorized users. If the attacker wants to successfully launch an attack, this requires more preparation for this. The attack will not get any notification if the payload fails. Hackers can also use polyglots if they want to increase the success rate of these types of attacks. Polyglots can work in different scenarios like a script tag, plain text, and attributes.

DOM-Based Cross-site scripting attack

When the JavaScript on the page is vulnerable to cross-site scripting (XSS), rather than the server itself, in this case, the DOM-based cross-site scripting attack will occur. The JavaScript can add interactivity to the page. It can also add arguments in the URL, which is used to modify the page after loading it. The malicious code can be added to a page while modifying the DOM when the user's value is not sanitized. When the URL provides the languages and the website change into these languages rather than the default language, this shows the example of DOM-based cross-site scripting.

Prevention of Cross-site scripting attacks

The website vulnerabilities can be exploited using the variety of methods leveraged by an attacker. If we want to reduce the risk of cross-site scripting, there is no single strategy. Unsafe user input helps the cross-site scripting attacks because it is directly rendered onto the website's web page. This attack would be impossible if the inputs of the user are properly sanitized. We can ensure that the inputs of users cannot be escaped on our website using multiple ways. Using the following protective measures, we can harden our web applications and protect our website.

Whitelist Values

We can restrict the input of a user to a specific whitelist. This practice allows us to only send the safe and known value to the server. If we know about the receiving data, like the content of the drop-down menu, the restricted user input will only work.

Restrict HTML in Inputs

HTML is limited to trusted users. If we want to allow formatting and styling on an input, we can use Markdown instead of HTML to generate the content. If we want to use HTML, we should sanitize it with a robust sanitizer like DOMPurify, which is used to remove all the unsafe code.

Sanitize value

If we are using content on a page generated by a user, we should ensure that it would not result in HTML content by using entities in place of unsafe characters. The appearance of regular characters and entities are the same, but the entity cannot generate HTML.

Use HTTPOnly Flags on Cookies

Session cookies are used to allow a website to recognize a user between requests. An attacker frequently exfiltrates the user's cookies and steal the admin session. Once the attacker steals the cookies of a user, they can log in to the account of the admin without authorized access or credentials. HttpOnly cookies are used to prevent the JavaScript from reading the cookie's content and increase the difficulty of an attacker to steal the session. Using this method, we can only prevent our cookies from the attacker. An attacker can still act as an admin user and send a request using the active browser session. If the attacker uses cookies as the main identification mechanism, in this case, this method will be only useful.

Use WAF

We can virtually patch attacks against our website using the firewall. This method is used to intercept the requests like SQLi, RCE, XSS before our website get malicious requests. The large scale attacks like DDOS can also be protected by it.

SQL Injection

The SQL Injection is a code penetration technique that might cause loss to our database. It is one of the most practiced web hacking techniques to place malicious code in SQL statements, via webpage input. SQL injection can be used to manipulate the application's web server by malicious users.

SQL injection generally occurs when we ask a user to input their username/userID. Instead of a name or ID, the user gives us an SQL statement that we will unknowingly run on our database. For Example - we create a SELECT statement by adding a variable "demoUserID" to select a string. The variable will be fetched from user input (getRequestString).

1. demoUserI = getrequestString("UserId");
2. demoSQL = "SELECT * FROM users WHERE UserId =" +demoUserId;

Types of SQL injection attacks

SQL injections can do more harm other than passing the login algorithms. Some of the SQL injection attacks include:

- Updating, deleting, and inserting the data: An attack can modify the cookies to poison a web application's database query.
- It is executing commands on the server that can download and install malicious programs such as Trojans.
- We are exporting valuable data such as credit card details, email, and passwords to the attacker's remote server.
- Getting user login details: It is the simplest form of SQL injection. Web application typically accepts user input through a form, and the front end passes the user input to the back end database for processing.

  Example of SQL Injection

  We have an application based on employee records. Any employee can view only their own records by entering a unique and private employee ID. We have a field like an Employee ID. And the employee enters the following in the input field:

  236893238 or 1=1

  It will translate to:

1. **SELECT** * **from** EMPLOYEE **where** EMPLOYEE_ID == 236893238 or 1=1

   The SQL code above is valid and will return EMPLOYEE_ID row from the EMPLOYEE table. The 1=1 will return all records for which this holds true. All the employee data is compromised; now, the malicious user can also similarly delete the employee records.

   Example:

1. **SELECT** * **from** Employee **where** (Username == "" or 1=1) AND (**Password**="" or 1=1).

   Now the malicious user can use the '=' operator sensibly to retrieve private and secure user information. So instead of the query mentioned above, the following query, when exhausted, retrieve protected data, not intended to be shown to users.

1. **SELECT** * **from** EMPLOYEE **where** (Employee_name =" " or 1=1) AND (**Password**=" " or 1= 1)

   SQL injection based on Batched SQL statements

   Several databases support batched SQL statements. It is a group of two or more SQL statements separated by semicolons.

   The SQL statement given below will return all rows from the Employee table, then delete the Employee_Add table.

1. **SELECT** * **From** Employee; **DROP Table** Employee_Add

How to detect SQL Injection attacks

Creating a SQL Injection attack is not difficult, but even the best and good-intentioned developers make mistakes. The detection of SQL Injection is, therefore, an essential component of creating the risk of an SQL injection attack. Web Application Firewall can detect and block basic SQL injection attacks, but we should depend on it as the sole preventive measure.

Intrusion Detection System (IDS) is both network-based and host-based. It can be tuned to detect SQL injection attacks. Network-based IDSec can monitor all connections to our database server, and flags suspicious activities. The host-based IDS can monitor web server logs and alert when something strange happens.

Impact of SQL Injection

The intruder can retrieve all the user-data present in the database, such as user details, credit card information, and social security numbers, and can also gain access to protected areas like the administrator portal. It is also possible to delete the user data from the tables. These days all the online shopping applications, bank transactions use back-end database servers. If the intruder can exploit SQL injection, the entire server is compromised.

How to prevent SQL Injection attack

- We should use user authentication to validate input from the user by pre-defining length, input type, and the input field.
- Restricting the access privileges of users and defining the amount of data any outsider can access from the database. Generally, the user cannot be granted permission to access everything in the database.
- We should not use system administrator accounts.

Cross Site Request Forgery (CSRF)

Cross Site Request Forgery (CSRF) is one of the most severe vulnerabilities which can be exploited in various ways- from changing user's info without his knowledge to gaining full access to user's account.

Almost every website uses cookies today to maintain a user's session. Since HTTP is a "stateless" protocol, there is no built in way to keep a user authenticated for a series of requests. Asking user for his credentials at each operation is a very bad idea in terms of user experience, This is why cookies are used. Cookies are very efficient for this purpose and are secure if they possess enough entropy, cryptographic strength and are transmitted over a secure channel (using HTTPS).

However, there is a problem, browsers submit cookies to a website whenever a request is made to that website without checking the “origin” of the request. This is where CSRF comes into picture.

The attacker places some code on his website that makes a genuine looking request to the target website. The cookies of the target website will be added by the browser in the request . This will make that forged request a legal one and it’s action will be successfully carried out.

Attack Surfaces:

The attack surfaces for CSRF are most**Cross Site Request Forgery (CSRF)** is one of the most severe vulnerabilities which can be exploited in various ways- from changing user’s info without his knowledge to gaining full access to user’s account.

Almost every website uses cookies today to maintain a user’s session. Since HTTP is a “stateless” protocol, there is no built in way to keep a user authenticated for a series of requests. Asking user for his credentials at each operation is a very bad idea in terms of user experience, This is why cookies are used. Cookies are very efficient for this purpose and are secure if they possess enough entropy, cryptographic strength and are transmitted over a secure channel (using HTTPS).

However, there is a problem, browsers submit cookies to a website whenever a request is made to that website without checking the “origin” of the request. This is where CSRF comes into picture.

The attacker places some code on his website that makes a genuine looking request to the target website. The cookies of the target website will be added by the browser in the request . This will make that forged request a legal one and it’s action will be successfully carried out.

Attack Surfaces:

The attack surfaces for CSRF are mostly HTTP requests that cause a change in something related to the victim, for example: name, email address, website and even password. It is sometimes used to alter the state of authentication as well. (Login CSRF, Logout CSRF) which are less severe but can still be problematic in some cases.

Exploitation:

Consider a website example.com and the attacker’s website evil.com. Also assume that the victim is logged in and his session is being maintained by cookies. The attacker will:

1. Find out what action he needs to perform on behalf of the victim and find out its endpoint (for example, to change password on target.com a POST request is made to the website that contains new password as the parameter.)

2. Place HTML code on his website evil.com that will imitate a legal request to target.com (for example, a form with method as post and a hidden input field that contains the new password).
3. Make sure that the form is submitted by either using “autosubmit” or luring the victim to click on a submit button.

   When the victim visits evil.com and that form is submitted, the victim’s browser makes a request to target.com for a password change. Also the browser appends the cookies with the request. The server treats it as a genuine request and resets the victim’s password to the attacker’s supplied value. This way the victim’s account gets taken over by the attacker.

   Prevention:

- **On user side:**
  User side prevention is very inefficient in terms of browsing experience, prevention can be done by browsing only a single tab at a time and not using the “remember-me” functionality.
- **On Server Side:**
  There are many proposed ways to implement CSRF protection on server side, among which the use of CSRF tokens is most popular. A CSRF token is a string that is tied to a user’s session but is not submitted automatically. A website proceeds only when it receives a valid CSRF token along with the cookies, since there is no way for an attacker to know a user specific token, the attacker can not perform actions on user’s behalf.

  ly HTTP requests that cause a change in something related to the victim, for example: name, email address, website and even password. It is sometimes used to alter the state of authentication as well. (Login CSRF, Logout CSRF) which are less severe but can still be problematic in some cases.

Exploitation:

Consider a website example.com and the attacker’s website evil.com. Also assume that the victim is logged in and his session is being maintained by cookies. The attacker will:

1. Find out what action he needs to perform on behalf of the victim and find out its endpoint (for example, to change password on target.com a POST request is made to the website that contains new password as the parameter.)
2. Place HTML code on his website evil.com that will imitate a legal request to target.com (for example, a form with method as post and a hidden input field that contains the new password).

3. Make sure that the form is submitted by either using “autosubmit” or luring the victim to click on a submit button.

   When the victim visits evil.com and that form is submitted, the victim’s browser makes a request to target.com for a password change. Also the browser appends the cookies with the request. The server treats it as a genuine request and resets the victim’s password to the attacker’s supplied value. This way the victim’s account gets taken over by the attacker.

Prevention:

- **On user side:**
  User side prevention is very inefficient in terms of browsing experience, prevention can be done by browsing only a single tab at a time and not using the “remember-me” functionality.
- **On Server Side:**
  There are many proposed ways to implement CSRF protection on server side, among which the use of CSRF tokens is most popular. A CSRF token is a string that is tied to a user’s session but is not submitted automatically. A website proceeds only when it receives a valid CSRF token along with the cookies, since there is no way for an attacker to know a user specific token, the attacker can not perform actions on user’s behalf.

What are network protocols?

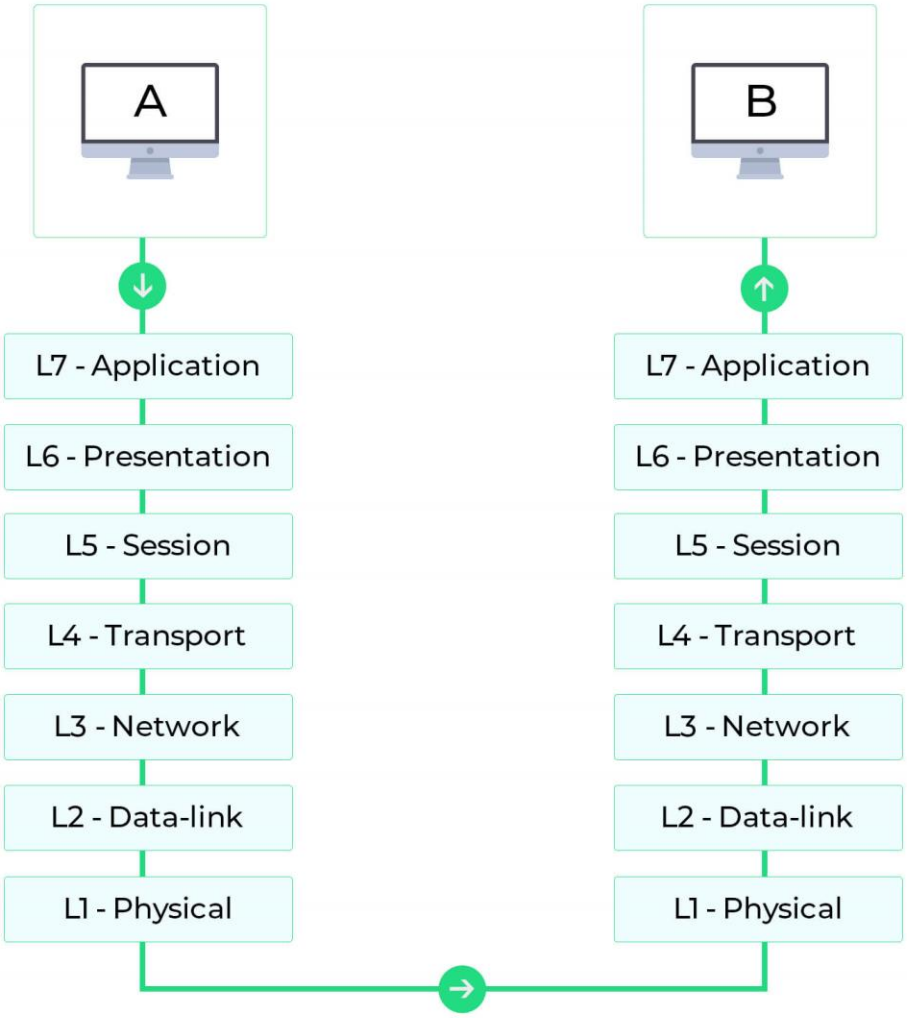
Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks. In other words, network protocols can be equated to languages that two devices must understand for seamless communication of information, regardless of their infrastructure and design disparities.

The OSI model: How do network protocols work?

To understand the nuances of network protocols, it's imperative to know about the Open Systems Interconnection (OSI) model first. Considered the primary architectural model for internet working communications, the majority of **networking protocols** used today are structurally based on the OSI model.

The OSI model splits the communication process between two network devices into 7 layers. A task or group of tasks is assigned to each of these 7 layers. All the layers are self-contained, and the tasks assigned to them can be executed independently.

To put this into context, here is a representation of the communication process between two network devices following the OSI model:



The seven layers in the OSI model can be divided into two groups: upper layers, including layers 7, 6, and 5, and lower layers, including layers 4, 3, 2, and 1. The upper layers deal with application issues, and the lower layers deal with data transport issues.

Network protocol divides the communication process into discrete tasks across every layer of the OSI model. One or more network protocols operate at each layer in the communication exchange.

Following are the detailed descriptions of the functioning of **network protocol in computer network** in each layer of the OSI model:

Layer 7: Application layer network protocols	• Provides standard services such as virtual terminal, file, and job tra and operations.
Layer 6: Presentation layer network protocols	• Masks the differences in data formats between dissimilar systems. • Encodes and decodes data, encrypts and decrypts data, and compr and decompresses data.
Layer 5: Session layer network protocols	• Manages user sessions and dialogues. • Establishes and terminates sessions between users.
Layer 4: Transport layer network protocols	• Manages end-to-end message delivery in networks. • Renders reliable and sequential packet delivery through error reco and flow control mechanisms.
Layer 3: Network layer protocols	• Routes packets according to unique network device addresses. • Renders flow and congestion control to prevent network resource depletion.
Layer 2: Data link layer network protocols	• Frames packets. • Detects and corrects packet transmit errors.
Layer 1: Physical layer network protocols	• Interfaces between network medium and devices. • Defines optical, electrical, and mechanical characteristics.

Though some say the OSI model is now redundant and less significant than the Transmission Control Protocol (TCP)/IP network model, there are still references to the OSI model even today as the model's structure helps to frame discussions of protocols and contrast various technologies.

Types of network protocols

Now that you know how the OSI model works, you can dive straight into the classification of protocols. The following are some of the most prominent protocols used in network communication.

Application layer network protocols

1. DHCP: Dynamic Host Configuration Protocol

DHCP is a communication protocol that enables network administrators to automate the assignment of IP addresses in a network. In an IP network, every device connecting to the internet requires a unique IP. DHCP lets network admins distribute IP addresses from a central point and automatically send a new IP address when a device is plugged in from a different place in the network. DHCP works on a client-server model.

Advantages of using DHCP

- Centralized management of IP addresses.
- Seamless addition of new clients into a network.
- Reuse of IP addresses, reducing the total number of IP addresses required.

Disadvantages of using DHCP

- Tracking internet activity becomes tedious, as the same device can have multiple IP addresses over a period of time.
- Computers with DHCP cannot be used as servers, as their IPs change over time.

2. DNS: Domain Name System protocol

The DNS protocol helps in translating or mapping host names to IP addresses. DNS works on a client-server model, and uses a distributed database over a hierarchy of name servers.

Hosts are identified based on their IP addresses, but memorizing an IP address is difficult due to its complexity. IPs are also dynamic, making it all the more necessary to map domain names to IP addresses. DNS helps resolve this issue by converting the domain names of websites into numerical IP addresses.

Advantages

- DNS facilitates internet access.
- Eliminates the need to memorize IP addresses.

Disadvantages

- DNS queries don't carry information pertaining to the client who initiated it. This is because the DNS server only sees the IP from where the query came from, making the server susceptible to manipulation from hackers.
- DNS root servers, if compromised, could enable hackers to redirect to other pages for phishing data.

3. FTP: File Transfer Protocol

File Transfer Protocol enables file sharing between hosts, both local and remote, and runs on top of TCP. For file transfer, FTP creates two TCP connections: control and data connection. The control connection is used to transfer control information like passwords, commands to retrieve and store files, etc., and the data connection is used to transfer the actual file. Both of these connections run in parallel during the entire file transfer process.

Advantages

- Enables sharing large files and multiple directories at the same time.
- Lets you resume file sharing if it was interrupted.
- Lets you recover lost data, and schedule a file transfer.

Disadvantages

- FTP lacks security. Data, usernames, and passwords are transferred in plain text, making them vulnerable to malicious actors.
- FTP lacks encryption capabilities, making it non-compliant with industry standards.

4. HTTP: Hyper Text Transfer Protocol

HTTP is an application layer protocol used for distributed, collaborative, and hypermedia information systems. It works on a client-server model, where the web browser acts as the client. Data such as text, images, and other multimedia files are shared over the World Wide Web using HTTP. As a request and response type protocol, the client sends a request to the server, which is then processed by the server before sending a response back to the client.

HTTP is a stateless protocol, meaning the client and server are only aware of each other while the connection between them is intact. After that, both the client and server forget about each other's existence. Due to this phenomenon, the client and server can't both retain information between requests.

Advantages

- Memory usage and CPU usage are low because of lesser concurrent connections.
- Errors can be reported without closing connections.
- Owing to lesser TCP connections, network congestion is reduced.

Disadvantages

- HTTP lacks encryption capabilities, making it less secure.
- HTTP requires more power to establish communication and transfer data.

5. IMAP and IMAP4: Internet Message Access Protocol (version 4)

IMAP is an email protocol that lets end users access and manipulate messages stored on a mail server from their email client as if they were present locally on their remote device. IMAP follows a client-server model, and lets multiple clients access messages on a common mail server concurrently. IMAP includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and removing flags; and much more. The current version of IMAP is version 4 revision 1.

Advantages

- As the emails are stored on the mail server, local storage utilization is minimal.
- In case of accidental deletion of emails or data, it is always possible to retrieve them as they are stored on the mail server.

Disadvantages

- Emails won't work without an active internet connection.
- High utilization of emails by end users requires more mailbox storage, thereby augmenting costs.

6. POP and POP3: Post Office Protocol (version 3)

The Post Office Protocol is also an email protocol. Using this protocol, the end user can download emails from the mail server to their own email client. Once the emails are downloaded locally, they can be read without an internet connection. Also, once the emails are moved locally, they get deleted from the mail server, freeing up space. POP3 is not designed to perform extensive manipulations with the messages on the mail server, unlike IMAP4. POP3 is the latest version of the Post Office Protocol.

Advantages

- Read emails on local devices without internet connection.
- The mail server need not have high storage capacity, as the emails get deleted when they're moved locally.

Disadvantages

- If the local device on which the emails were downloaded crashes or gets stolen, the emails are lost.

7. SMTP: Simple Mail Transfer Protocol

SMTP is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a push protocol and is used to send the email, whereas POP and IMAP are used to retrieve emails on the end user's side. SMTP transfers emails between systems, and notifies on incoming emails.

Using SMTP, a client can transfer an email to another client on the same network or another network through a relay or gateway access available to both networks.

Advantages

- Ease of installation.
- Connects to any system without any restriction.
- It doesn't need any development from your side.

Disadvantages

- Back and forth conversations between servers can delay sending a message, and also increases the chance of the message not being delivered.
- Certain firewalls can block the ports used with SMTP.

8. Telnet: Terminal emulation protocol

Telnet is an application layer protocol that enables a user to communicate with a remote device. A Telnet client is installed on the user's machine, which accesses the command line interface of another remote machine that runs a Telnet server program.

Telnet is mostly used by network administrators to access and manage remote devices. To access a remote device, a network admin needs to enter the IP or host name of the remote device, after which they will be presented with a virtual terminal that can interact with the host.

Advantages

- Compatible with multiple operating systems.
- Saves a lot of time due to its swift connectivity with remote devices.

Disadvantages

- Telnet lacks encryption capabilities and sends across critical information in clear text, making it easier for malicious actors.
- Expensive due to slow typing speeds.

9. SNMP: Simple Network Management Protocol

SNMP is an application layer protocol used to manage nodes, like servers, workstations, routers, switches, etc., on an IP network. SNMP enables network admins to monitor network performance, identify network glitches, and troubleshoot them. SNMP protocol is comprised of three components: a managed device, an SNMP agent, and an SNMP manager.

The SNMP agent resides on the managed device. The agent is a software module that has local knowledge of management information, and translates that information into a form compatible

with the SNMP manager. The SNMP manager presents the data obtained from the SNMP agent, helping network admins manage nodes effectively.

Currently, there are three versions of SNMP: SNMP v1, SNMP v2, and SNMP v3. Both versions 1 and 2 have many features in common, but SNMP v2 offers enhancements such as additional protocol operations. SNMP version 3 (SNMP v3) adds security and remote configuration capabilities to the previous versions.

Presentation layer network protocols

LPP: Lightweight Presentation Protocol

The Lightweight Presentation Protocol helps provide streamlined support for OSI application services in networks running on TCP/IP protocols for some constrained environments. LPP is designed for a particular class of OSI applications, namely those entities whose application context contains only an Association Control Service Element (ACSE) and a Remote Operations Service Element (ROSE). LPP is not applicable to entities whose application context is more extensive, i.e., contains a Reliable Transfer Service Element.

Session layer network protocols

RPC: Remote Procedure Call protocol

RPC is a protocol for requesting a service from a program in a remote computer through a network, and can be used without having to understand the underlying network technologies. RPC uses TCP or UDP for carrying the messages between communicating programs. RPC also works on client-server model. The requesting program is the client, and the service providing program is the server.

Advantages

- RPC omits many protocol layers to improve performance.
- With RPC, code rewriting or redeveloping efforts are minimized.

Disadvantages

- Not yet proven to work effectively over wide-area networks.
- Apart from TCP/IP, RPC does not support other transport protocols.

Transport layer network protocols

1. TCP: Transmission Control Protocol

TCP is a transport layer protocol that provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgement. TCP is a connection-oriented protocol, as it requires a connection to be established between applications before data transfer. Through flow control and acknowledgement of data, TCP provides extensive error checking. TCP ensures sequencing of data, meaning the data packets arrive in order at the receiving end. Retransmission of lost data packets is also feasible with TCP.

Advantages

- TCP ensures three things: data reaches the destination, reaches it on time, and reaches it without duplication.
- TCP automatically breaks data into packets before transmission.

Disadvantages

- TCP cannot be used for broadcast and multicast connections.

2. UDP: User Datagram Protocol

UDP is a connection-less transport layer protocol that provides a simple but unreliable message service. Unlike TCP, UDP adds no reliability, flow control, or error recovery functions. UDP is useful in situations where the reliability mechanisms of TCP are not necessary. Retransmission of lost data packets isn't possible with UDP.

Advantages

- Broadcast and multicast connections are possible with UDP.
- UDP is faster than TCP.

Disadvantages

- In UDP, it's possible that a packet may not be delivered, be delivered twice, or not be delivered at all.
- Manual disintegration of data packets is needed.

Network layer protocols

1. IP: Internet Protocol (IPv4)

IPv4 is a network layer protocol that contains addressing and control information, which helps packets be routed in a network. IP works in tandem with TCP to deliver data packets across the network. Under IP, each host is assigned a 32-bit address comprised of two major parts: the network number and host number. The network number identifies a network and is assigned by the internet, while the host number identifies a host on the network and is assigned by a

network admin. The IP is only responsible for delivering the packets, and TCP helps puts them back in the right order.

Advantages

- IPv4 encrypts data to ensure privacy and security.
- With IP, routing data becomes more scalable and economical.

Disadvantages

- IPv4 is labor intensive, complex, and prone to errors.

2. IPv6: Internet Protocol version 6

IPv6 is the latest version of the Internet Protocol, a network layer protocol that possesses addressing and control information for enabling packets to be routed in the network. IPv6 was created to deal with IPv4 exhaustion. It increases the IP address size from 32 bits to 128 bits to support more levels of addressing.

Advantages

- More efficient routing and packet processing compared to IPv4.
- Better security compared to IPv4.

Disadvantages

- IPv6 is not compatible with machines that run on IPv4.
- Challenge in upgrading the devices to IPv6.

3. ICMP: Internet Control Message Protocol

ICMP is a network layer supporting protocol used by network devices to send error messages and operational information. ICMP messages delivered in IP packets are used for out-of-band messages related to network operation or misoperation. ICMP is used to announce network errors, congestion, and timeouts, as well assist in troubleshooting.

Advantages

- ICMP is used to diagnose network issues.

Disadvantages

- Sending a lot of ICMP messages increases network traffic.
- End users are affected if malicious users send many ICMP destination unreachable packets.

Data link layer network protocols

1. ARP: Address Resolution Protocol

The Address Resolution Protocol helps map IP addresses to physical machine addresses (or a MAC address for Ethernet) recognized in the local network. A table called an ARP cache is used to maintain a correlation between each IP address and its corresponding MAC address. ARP offers the rules to make these correlations, and helps convert addresses in both directions.

Advantages

- MAC addresses need not be known or memorized, as the ARP cache contains all the MAC addresses and maps them automatically with IPs.

Disadvantages

- ARP is susceptible to security attacks called ARP spoofing attacks.
- When using ARP, sometimes a hacker might be able to stop the traffic altogether. This is also known as ARP denial-of-services.

2. SLIP: Serial Line IP

SLIP is used for point-to-point serial connections using TCP/IP. SLIP is used on dedicated serial links, and sometimes for dial-up purposes. SLIP is useful for allowing mixes of hosts and routers to communicate with one another; for example, host-host, host-router, and router-router are all common SLIP network configurations. SLIP is merely a packet framing protocol: It defines a sequence of characters that frame IP packets on a serial line. It does not provide addressing, packet type identification, error detection or correction, or compression mechanisms.

Advantages

- Since it has a small overhead, it is suitable for usage in microcontrollers.
- It reuses existing dial-up connections and telephone lines.
- It's easy to deploy since it's based on the Internet Protocol.

Disadvantages

- SLIP doesn't support automatic setup of network connections in multiple OSI layers at the same time.
- SLIP does not support synchronous connections, such as a connection created through the internet from a modem to an internet service provider (ISP).

Cloud Based Services

Cloud Computing can be defined as 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. Companies offering such kinds of cloud computing services are called *cloud providers* and typically charge for cloud computing services based on usage. Grids and clusters are the foundations for cloud computing.

Types of Cloud Computing

Most cloud computing services fall into five broad categories:

1. Software as a service (SaaS)
2. Platform as a service (PaaS)
3. Infrastructure as a service (IaaS)
4. Anything/Everything as a service (XaaS)
5. Function as a Service (FaaS)

These are sometimes called the **cloud computing stack** because they are built on top of one another. Knowing what they are and how they are different, makes it easier to accomplish your goals. These abstraction layers can also be viewed as a **layered architecture** where services of a higher layer can be composed of services of the underlying layer i.e, SaaS can provide Infrastructure.

Software as a Service(SaaS)

Software-as-a-Service (SaaS) is a way of delivering services and applications over the Internet. Instead of installing and maintaining software, we simply access it via the Internet, freeing ourselves from the complex software and hardware management. It removes the need to install and run applications on our own computers or in the data centers eliminating the expenses of hardware as well as software maintenance.
SaaS provides a complete software solution that you purchase on a **pay-as-you-go** basis from a cloud service provider. Most SaaS applications can be run directly from a web browser without any downloads or installations required. The SaaS applications are sometimes called **Web-based software, on-demand software, or hosted software.**

Advantages of SaaS

1. **Cost-Effective:** Pay only for what you use.
2. **Reduced time:** Users can run most SaaS apps directly from their web browser without needing to download and install any software. This reduces the time spent in installation and configuration and can reduce the issues that can get in the way of the software deployment.

3. **Accessibility:** We can Access app data from anywhere.
4. **Automatic updates:** Rather than purchasing new software, customers rely on a SaaS provider to automatically perform the updates.
5. **Scalability:** It allows the users to access the services and features on-demand.

The various companies providing *Software as a service* are Cloud9 Analytics, Salesforce.com, Cloud Switch, Microsoft Office 365, Big Commerce, Eloqua, dropBox, and Cloud Tran.

Disadvantages of Saas :

1. **Limited customization**: SaaS solutions are typically not as customizable as on-premises software, meaning that users may have to work within the constraints of the SaaS provider's platform and may not be able to tailor the software to their specific needs.
2. **Dependence on internet connectivity**: SaaS solutions are typically cloud-based, which means that they require a stable internet connection to function properly. This can be problematic for users in areas with poor connectivity or for those who need to access the software in offline environments.
3. **Security concerns:** SaaS providers are responsible for maintaining the security of the data stored on their servers, but there is still a risk of data breaches or other security incidents.
4. **Limited control over data:** SaaS providers may have access to a user's data, which can be a concern for organizations that need to maintain strict control over their data for regulatory or other reasons.

Platform as a Service

PaaS is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser.
A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application. Thus, the development and deployment of the application take place **independent of the hardware**.
The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. To make it simple, take the example of an annual day function, you will have two options either to create a venue or to rent a venue but the function is the same.

Advantages of PaaS:

1. **Simple and convenient for users:** It provides much of the infrastructure and other IT services, which users can access anywhere via a web browser.
2. **Cost-Effective:** It charges for the services provided on a per-use basis thus eliminating the expenses one may have for on-premises hardware and software.
3. **Efficiently managing the lifecycle:** It is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating.
4. **Efficiency:** It allows for higher-level programming with reduced complexity thus, the overall development of the application can be more effective.

The various companies providing *Platform as a service* are Amazon Web services Elastic Beanstalk, Salesforce, Windows Azure, Google App Engine, cloud Bees and IBM smart cloud.

Disadvantages of Paas:

1. **Limited control over infrastructure:** PaaS providers typically manage the underlying infrastructure and take care of maintenance and updates, but this can also mean that users have less control over the environment and may not be able to make certain customizations.
2. **Dependence on the provider**: Users are dependent on the PaaS provider for the availability, scalability, and reliability of the platform, which can be a risk if the provider experiences outages or other issues.
3. **Limited flexibility:** PaaS solutions may not be able to accommodate certain types of workloads or applications, which can limit the value of the solution for certain organizations.

Infrastructure as a Service

Infrastructure as a service (IaaS) is a service model that delivers computer infrastructure on an outsourced basis to support various operations. Typically IaaS is a service where infrastructure is provided as outsourcing to enterprises such as networking equipment, devices, database, and web servers.
It is also known as **Hardware as a Service (HaaS).** IaaS customers pay on a per-user basis, typically by the hour, week, or month. Some providers also charge customers based on the amount of virtual machine space they use.
It simply provides the underlying operating systems, security, networking, and servers for developing such applications, and services, and deploying development tools, databases, etc.

Advantages of IaaS:

1. **Cost-Effective:** Eliminates capital expense and reduces ongoing cost and IaaS customers pay on a per-user basis, typically by the hour, week, or month.

2. **Website hosting:** Running websites using IaaS can be less expensive than traditional web hosting.
3. **Security:** The IaaS Cloud Provider may provide better security than your existing software.
4. **Maintenance:** There is no need to manage the underlying data center or the introduction of new releases of the development or underlying software. This is all handled by the IaaS Cloud Provider.

The various companies providing *Infrastructure as a service* are Amazon web services, Bluestack, IBM, Openstack, Rackspace, and Vmware.

Disadvantages of IaaS :

1. **Limited control over infrastructure:** IaaS providers typically manage the underlying infrastructure and take care of maintenance and updates, but this can also mean that users have less control over the environment and may not be able to make certain customizations.
2. **Security concerns**: Users are responsible for securing their own data and applications, which can be a significant undertaking.
3. **Limited access:** Cloud computing may not be accessible in certain regions and countries due to legal policies.

Anything as a Service

It is also known as Everything as a Service. Most of the cloud service providers nowadays offer anything as a service that is a compilation of all of the above services including some additional services.

Advantages of XaaS:

1. **Scalability:** XaaS solutions can be easily scaled up or down to meet the changing needs of an organization.
2. **Flexibility:** XaaS solutions can be used to provide a wide range of services, such as storage, databases, networking, and software, which can be customized to meet the specific needs of an organization.
3. **Cost-effectiveness**: XaaS solutions can be more cost-effective than traditional on-premises solutions, as organizations only pay for the services.

Disadvantages of XaaS:

1. **Dependence on the provider:** Users are dependent on the XaaS provider for the availability, scalability, and reliability of the service, which can be a risk if the provider experiences outages or other issues.
2. **Limited flexibility**: XaaS solutions may not be able to accommodate certain types of workloads or applications, which can limit the value of the solution for certain organizations.
3. **Limited integration:** XaaS solutions may not be able to integrate with existing systems and data sources, which can limit the value of the solution for certain organizations.

Function as a Service :

FaaS is a type of cloud computing service. It provides a platform for its users or customers to develop, compute, run and deploy the code or entire application as functions. It allows the user to entirely develop the code and update it at any time without worrying about the maintenance of the underlying infrastructure. The developed code can be executed with response to the specific event. It is also **as same as PaaS**.

FaaS is an event-driven execution model. It is implemented in the serverless container. When the application is developed completely, the user will now trigger the event to execute the code. Now, the triggered event makes response and activates the servers to execute it. The servers are nothing but the Linux servers or any other servers which is managed by the vendor completely. Customer does not have clue about any servers which is why they do not need to maintain the server hence it is **serverless architecture.**

Both PaaS and FaaS are providing the same functionality but there is still some differentiation in terms of Scalability and Cost.

FaaS, provides auto-scaling up and scaling down depending upon the demand. PaaS also provides scalability but here users have to configure the scaling parameter depending upon the demand.

In FaaS, users only have to pay for the number of execution time happened. In PaaS, users have to pay for the amount based on pay-as-you-go price regardless of how much or less they use.

Advantages of FaaS :

- **Highly Scalable:** Auto scaling is done by the provider depending upon the demand.
- **Cost-Effective:** Pay only for the number of events executed.
- **Code Simplification:** FaaS allows the users to upload the entire application all at once. It allows you to write code for independent functions or similar to those functions.

- Maintenance of code is enough and no need to worry about the servers.
- Functions can be written in any programming language.
- Less control over the system.

The various companies providing Function as a Service are Amazon Web Services – Firecracker, Google – Kubernetes, Oracle – Fn, Apache OpenWhisk – IBM, OpenFaaS,

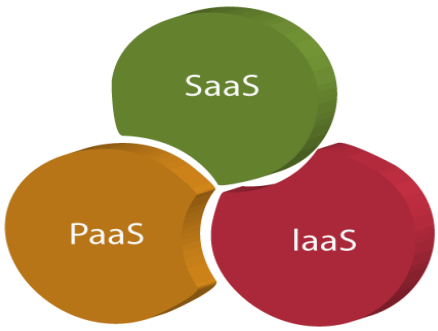
Disadvantages of FaaS :

1. **Cold start latency**: Since FaaS functions are event-triggered, the first request to a new function may experience increased latency as the function container is created and initialized.
2. **Limited control over infrastructure:** FaaS providers typically manage the underlying infrastructure and take care of maintenance and updates, but this can also mean that users have less control over the environment and may not be able to make certain customizations.
3. **Security concerns:** Users are responsible for securing their own data and applications, which can be a significant undertaking.
4. **Limited scalability**: FaaS functions may not be able to handle high traffic or large number of requests.

Cloud Service Models

There are the following three types of cloud service models -

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)



Infrastructure as a Service (IaaS)

IaaS is also known as **Hardware as a Service (HaaS)**. It is a computing infrastructure managed over the internet. The main advantage of using IaaS is that it helps users to avoid the cost and complexity of purchasing and managing the physical servers.

Characteristics of IaaS

There are the following characteristics of IaaS -

- Resources are available as a service
- Services are highly scalable
- Dynamic and flexible
- GUI and API-based access
- Automated administrative tasks

Example: DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, and Cisco Metacloud.

To know more about the IaaS, click here.

Platform as a Service (PaaS)

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications.

Characteristics of PaaS

There are the following characteristics of PaaS -

- Accessible to various users via the same development application.
- Integrates with web services and databases.
- Builds on virtualization technology, so resources can easily be scaled up or down as per the organization's need.
- Support multiple languages and frameworks.
- Provides an ability to "**Auto-scale**".

Example: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, Magento Commerce Cloud, and OpenShift.

To know more about PaaS, click here.

Software as a Service (SaaS)

SaaS is also known as "**on-demand software**". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser.

Characteristics of SaaS

There are the following characteristics of SaaS -

- Managed from a central location
- Hosted on a remote server
- Accessible over the internet
- Users are not responsible for hardware and software updates. Updates are applied automatically.
- The services are purchased on the pay-as-per-use basis

Example: BigCommerce, Google Apps, Salesforce, Dropbox, ZenDesk, Cisco WebEx, ZenDesk, Slack, and GoToMeeting.

To know more about the SaaS, click here.

Difference between IaaS, PaaS, and SaaS

The below table shows the difference between IaaS, PaaS, and SaaS -

IaaS	Paas	SaaS
It provides a virtual data center to store information and create platforms for app development, testing, and deployment.	It provides virtual platforms and tools to create, test, and deploy apps.	It provides web software and apps to complete business tasks.
It provides access to resources such as virtual machines, virtual storage, etc.	It provides runtime environments and deployment tools for applications.	It provides software as a service to the end-users.

It is used by network architects.	It is used by developers.	It is used by end users.
IaaS provides only Infrastructure.	PaaS provides Infrastructure+Platform.	SaaS provides Infrastructure+Platform +Software.

Advantages of Cloud Service Models

Cost Efficiency: Cloud providers provide a pricing model that permits customers to pay only for the sources they consume. This gets rid of the need for advanced infrastructure investments and allows price efficiency as businesses scale resources based totally on need.

Scalability: Cloud services provide the potential to scale sources up or down speedily and respond to changing workloads and commercial organization requirements. This flexibility ensures that agencies can correctly manipulate fluctuating needs without over-provisioning.

Accessibility and Flexibility: Cloud computing allows one to get access to applications and facts remotely from everywhere with an internet connection. This fosters collaboration among geographically dispersed groups and allows users to work flexibly.

Rapid Deployment: Cloud provider models facilitate rapid deployment of programs. Users can provision sources and deploy programs quickly, decreasing time-to-market and allowing faster innovation.

Managed Services: Cloud providers offer more than a few managed offerings, managing duties together with safety, tracking, and safety. This helps agencies dump operational obligations, pay attention to relevant skills, and experience the records of cloud carriers.

Automatic Updates and Patch Management: Cloud providers manipulate software application updates, patches, and protection functions robotically. This ensures that clients always have to get proper entry to the required abilities and protection upgrades without the need for guide intervention.

Disadvantages of Cloud Service Models

Security Concerns: Security remains a top concern for companies moving to the cloud. Storing information and programs on out-of-door servers will increase questions on statistics' privateness, regulatory compliance, and the functionality of unauthorized access.

Dependency on Internet Connectivity: Cloud services require a reliable internet connection. Downtime or disruptions in internet connectivity can impact the right to access essential applications and information, affecting business operations.

Limited Customization in SaaS: While SaaS offers convenience, it is able to lack the extent of customization that a few organizations require. Users depend on the capabilities and configurations supplied by the useful resources of the SaaS company, restricting flexibility.

Data Transfer Costs: Moving huge volumes of records from the cloud can require extra charges. Organizations need to cautiously recollect and manipulate facts and switch fees, in particular at the same time as dealing with enormous amounts of records.

Vendor Lock-In: Adopting certain cloud providers can also result in provider lock-in, wherein it becomes hard to migrate packages and statistics to a different employer or again to on-premises surroundings. This can limit flexibility and cause lengthy periods of dependence on a specific cloud organization.

Potential for Downtime: Cloud company companies may also experience outages or downtime, impacting the supply of services. While respectable businesses try for immoderate availability, occasional disruptions can occur, affecting users who get proper entry to agency continuity.

Conclusion

Cloud service models have transformed the panorama of computing, providing exceptional flexibility, scalability, and efficiency for groups and individuals alike. Pay-as-you-go pricing, fast deployment capabilities, and managed offerings supplied with the aid of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) have become indispensable to fashionable commercial enterprise strategies. In navigating the cloud panorama, a well-known method that aligns with particular business corporation necessities and danger profiles is important to harness the whole capacity of cloud computing.

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.

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.

Working of TLS:

The client connect to server (using TCP), the client will be something. The client sends number of specification:

1. Version of SSL/TLS.
2. which cipher suites, compression method it wants to use.

The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the clients option (if it supports one) and optionally picks a compression method. After this the basic setup is done, the server provides its certificate. This certificate must be trusted either by the client itself or a party that the client trusts. Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged. This can be a public key, “PreMasterSecret” or simply nothing depending upon cipher suite.

Both the server and client can now compute the key for symmetric encryption. The handshake is finished and the two hosts can communicate securely. To close a connection by finishing. TCP connection both sides will know the connection was improperly terminated. The connection cannot be compromised by this through, merely interrupted.

Transport Layer Security (TLS) continues to play a critical role in securing data transmission over networks, especially on the internet. Let’s delve deeper into its workings and significance:

Enhanced Security Features:

TLS employs a variety of cryptographic algorithms to provide a secure communication channel. This includes symmetric encryption algorithms like AES (Advanced Encryption Standard) and asymmetric algorithms like RSA and Diffie-Hellman key exchange. Additionally, TLS supports various hash functions for message integrity, such as SHA-256, ensuring that data remains confidential and unaltered during transit.

Certificate-Based Authentication:

One of the key components of TLS is its certificate-based authentication mechanism. When a client connects to a server, the server presents its digital certificate, which includes its public key and other identifying information. The client verifies the authenticity of the certificate using trusted root certificates stored locally or provided by a trusted authority, thereby establishing the server’s identity.

Forward Secrecy:

TLS supports forward secrecy, a crucial security feature that ensures that even if an attacker compromises the server's private key in the future, they cannot decrypt past communications. This is achieved by generating ephemeral session keys for each session, which are not stored and thus cannot be compromised retroactively.

TLS Handshake Protocol:

The TLS handshake protocol is a crucial phase in establishing a secure connection between the client and the server. It involves multiple steps, including negotiating the TLS version, cipher suite, and exchanging cryptographic parameters. The handshake concludes with the exchange of key material used to derive session keys for encrypting and decrypting data.

Perfect Forward Secrecy (PFS):

Perfect Forward Secrecy is an advanced feature supported by TLS that ensures the confidentiality of past sessions even if the long-term secret keys are compromised. With PFS, each session key is derived independently, providing an additional layer of security against potential key compromise.

TLS Deployment Best Practices:

To ensure the effectiveness of TLS, it's essential to follow best practices in its deployment. This includes regularly updating TLS configurations to support the latest cryptographic standards and protocols, disabling deprecated algorithms and cipher suites, and keeping certificates up-to-date with strong key lengths.

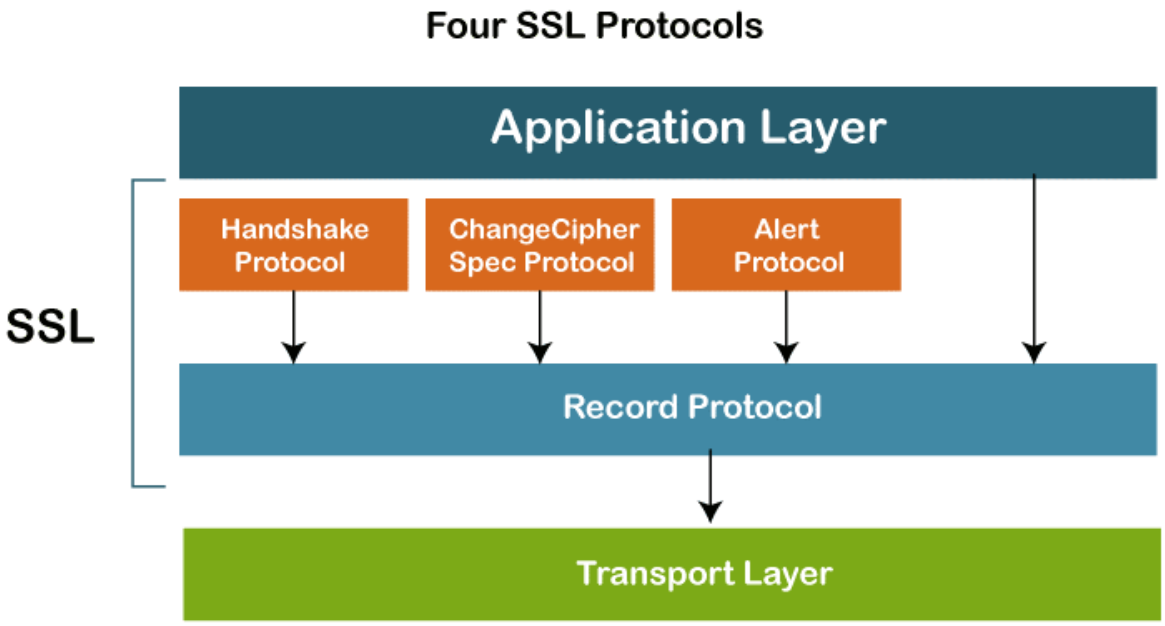
Continual Evolution:

TLS standards continue to evolve to address emerging security threats and vulnerabilities. Ongoing efforts by standards bodies, such as the Internet Engineering Task Force (IETF), ensure that TLS remains robust and resilient against evolving attack vectors.

Network Layer Security | SSL Protocols

Four Secured Socket Layer (SSL) Protocols

Without demonstrating how SSL completes its tasks, we have only talked about the concept of SSL in the previous section. <Please add the link to the previous file of SSL and SSL Architecture> According to the diagram below, SSL defines four protocols over two layers:



The transport mechanism is the Record Protocol. Along with the information from the application layer, it also contains messages from three more protocols. The payload of the transport layer, which is often TCP, is a message from the Record Protocol. The Record Protocol's security parameters are provided via the Handshake Protocol. It creates a cypher set, offers keys, and specifies security parameters. Additionally, if necessary, it authenticates both the client and the server. The ChangeCipherSpec Protocol is used to announce when cryptographic secrets are ready. Anomalies are reported via the Alert Protocol. In this part, we'll briefly go through all four protocols.

Handshake Protocol

The Handshake Protocol employs messages to exchange data for constructing the cryptographic secrets as well as to negotiate the cypher suite, and authenticate the server to the client and the client to the server as necessary. The four phases of the handshake are depicted in the following figure.

First Phase - Establishing Security Capabilities

The client and server disclose their security capabilities in Phase I and pick the ones that work best for them both. A session ID is created during this stage, and the cypher suite is decided upon. The parties select a specific compression technique. In order to create a master secret, as we have seen before, two random integers are finally chosen, one by the client and one by the server. Following Phase I, both the client and the server are aware of the SSL version, the cryptographic techniques, the compression technique, and the two random integers used to generate the key.

Second Phase - Server Authentication and Key Exchange

Authentication for the server takes place in Phase II, if necessary. In addition to requesting certificates from the client, the server has the option of sending its certificate and public key. When Phase II is complete, the client and server have been authenticated, and if necessary, the client has access to the server's public key.

Third Phase - Client Authentication and Key Exchange

Phase III is used to verify the client's identity. After Phase III, the client and server can verify each other and share the pre-master secret.

Fourth Phase - Finalizing and Finishing

In Phase IV, the client and server exchange messages to finalize the Handshake Protocol and alter the cypher parameters.

ChangeCipherSpec Protocol

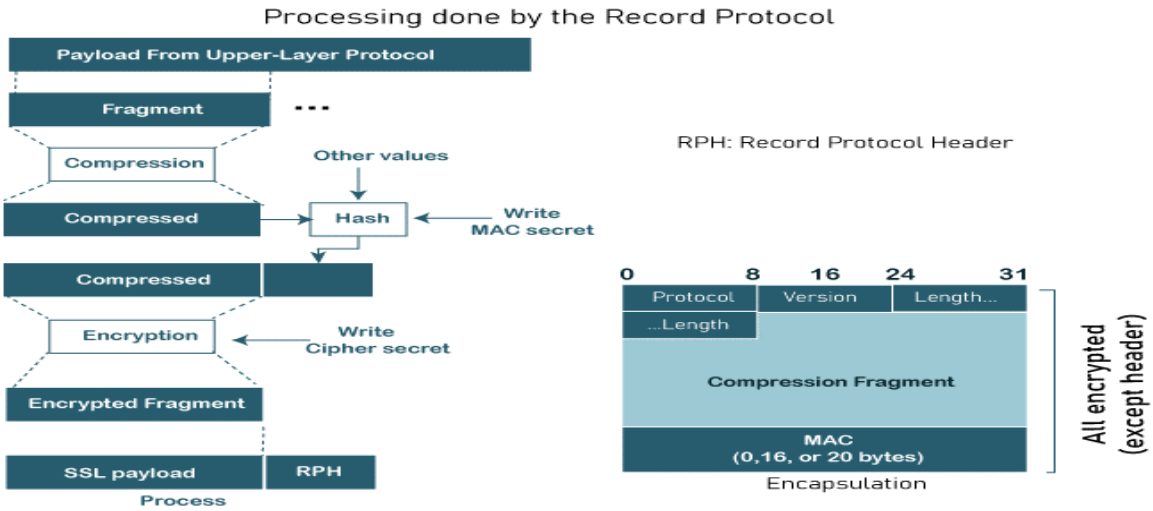
As we've seen, the Handshake Protocol allows for the gradual formation of cryptographic secrets as well as the negotiation of the cypher suite. When are these parameters or secrets available for usage by the two parties, then? SSL requires that these parameters or secrets cannot be used by the parties until they have exchanged or received a specific message, the ChangeCipherSpec message, which is done so during the Handshake Protocol and is specified in the ChangeCipherSpec Protocol. The reason is that the problem goes beyond simple message sending and receiving. Two states, not one, are required for the sender and the receiver. The parameters and secrets are tracked by one state, the pending state. The active state, which is the other state, contains the parameters and secrets that the Record Protocol uses to sign, validate, or encrypt and decode messages. Additionally, read (inbound) and write (outbound) data are stored in each state separately.

Alert Protocol

SSL reports problems and strange conditions using the Alert Protocol. It just makes use of one message to describe the issue and its severity (warning or fatal).

Record Protocol

Messages from the top layer are transmitted through the Record Protocol (Handshake Protocol, ChangeCipherSpec Protocol, Alert Protocol, or application layer). The message is split into pieces and, if desired, compressed; the compressed message is then added to by adding a MAC with the agreed-upon hashing algorithm. Utilizing the agreed-upon encryption procedure, the compressed fragment and MAC are both encrypted. The encrypted communication is then supplemented with the SSL header. This process at the sender is shown in the given Figure. The recipient reverses the process.



Network layer security

Network layer security focuses on protecting data as it is transmitted between devices in a network. This layer, the third layer in the OSI model, is responsible for routing, forwarding, and delivering packets between devices. Security measures at this level ensure that communication is secure and that malicious actors cannot intercept, modify, or disrupt data. Here's an overview of key concepts, threats, and protection methods:

Key Concepts

1. **IP Security (IPsec):**
    - A protocol suite for securing Internet Protocol (IP) communications.
    - Provides authentication, encryption, and data integrity.
    - Two main modes:
        - Transport Mode: Secures the payload of the packet.
        - Tunnel Mode: Secures the entire packet by encapsulating it in a new packet.
2. **Virtual Private Network (VPN):**
    - Encrypts data between devices and a trusted network.
    - Creates secure communication over public networks like the Internet.
    - Often uses protocols like IPsec or SSL/TLS.
3. **Firewalls:**
    - Inspect and filter incoming and outgoing packets based on predefined rules.
    - Operate at different layers, including the network layer, to prevent unauthorized access.
4. **Routing Security:**
    - Ensures that routing information between devices is not tampered with.
    - Protocols like Secure Border Gateway Protocol (S-BGP) help maintain secure routing.

5. **NAT (Network Address Translation):**
    - Masks internal network structure by translating private IP addresses to public ones.
    - Adds a layer of security by hiding internal devices.

Common Threats

1. **Packet Sniffing:**
    - Attackers intercept and analyze data packets in transit.
    - Tools like Wireshark can be used for malicious purposes.
2. **IP Spoofing:**
    - Attackers impersonate a trusted IP address to gain unauthorized access.
3. **Man-in-the-Middle (MITM) Attacks:**
    - Intercept communications between devices to steal or manipulate data.
4. **Denial of Service (DoS) Attacks:**
    - Overwhelm a network or device with traffic, making it unavailable to legitimate users.
5. **Routing Attacks:**
    - Exploits vulnerabilities in routing protocols to redirect or disrupt traffic.

Protection Methods

1. **Encryption:**
    - Ensures that data in transit is unreadable to unauthorized parties.
    - Use protocols like IPsec, SSL/TLS, or HTTPS.
2. **Authentication:**
    - Verifies the identity of communicating devices.
    - Techniques include digital certificates, passwords, and multi-factor authentication.
3. **Firewalls and Access Control Lists (ACLs):**

- Define rules for packet inspection and filtering based on IP addresses, ports, or protocols.

4. **Network Monitoring:**
    - Tools like intrusion detection systems (IDS) and intrusion prevention systems (IPS) monitor and respond to suspicious activity.
5. **Segmentation:**
    - Divide networks into smaller, isolated segments to minimize exposure.
6. **Routing Protocol Security:**
    - Implement secure versions of routing protocols like OSPFv3 or S-BGP.
7. **Regular Updates and Patching:**
    - Keep network devices and software updated to fix vulnerabilities.

Network-Layer Security | IPSec Modes

Network-Layer Security | IPSec Modes

Category - Computer Networks | Network Layer

This article begins with a consideration of security at the network layer. Security is implemented between two hosts, two routers, or a host and a router at the network layer.

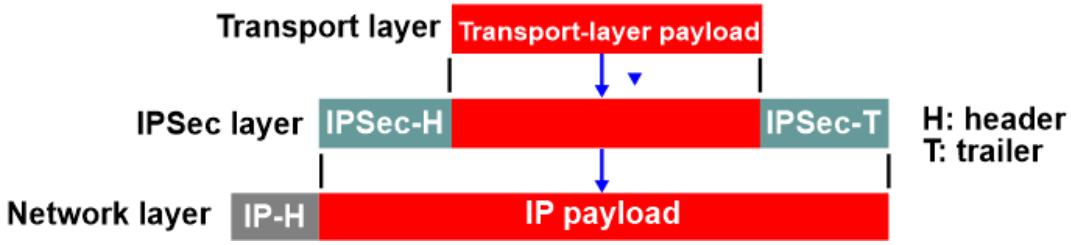
Those programs directly using the network layer's services, including routing protocols, are protected by network-layer security. Since UDP is a connectionless protocol and transport-layer security mechanisms cannot be applied to UDP, apps that use UDP can also profit from this service. We just talk about IPSec as an example of application-layer security here. The Internet Engineering Task Force (IETF) created a group of protocols known as IP Security (IPSec) to secure a packet at the network level. The IP layer benefits from creating authenticated and private packets thanks to IPSec.

IPSec Modes

Transport mode or tunnel mode are the two ways IPSec can be used.

1. ***Transport Mode*** **-** In transport mode, IPSec safeguards information sent from the transport layer to the network layer. Or, to put it another way, transport mode safeguards the payload that will be contained in the network layer, as shown in Figure.

IPSec in transsport mode

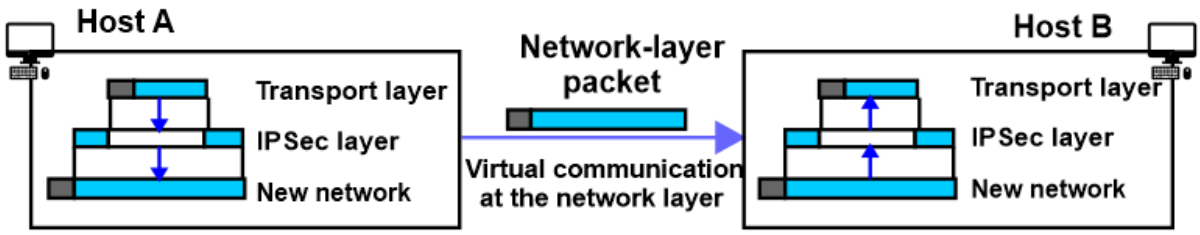


Keep in mind that IP header protection is not provided by transport mode. To put it another way, the packet from the transport layer is protected by transport mode, which does not secure the entire IP packet (the IP-layer payload). The information arriving from the transport layer is enhanced in this mode by adding the IPSec header (and trailer). The IP header is included afterwards.

1. IPSec protects only the payload arriving from the transport layer in transport mode; it do es not secure the IP header.

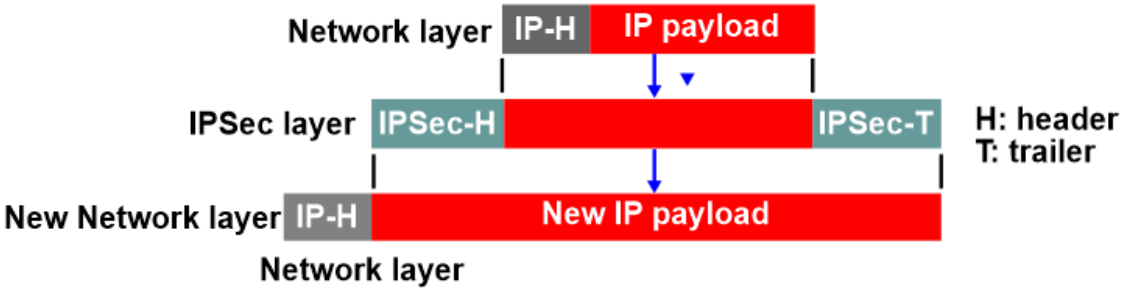
When host-to-host (end-to-end) data protection is required, we typically employ the transport mode. The payload sent from the transport layer is authenticated and/or encrypted by the sender host using IPSec. The IP packet is delivered to the transport layer by the receiving host using IPSec to verify the authentication and/or decrypt it. This idea is demonstrated in the given figure.

Transport mode in action



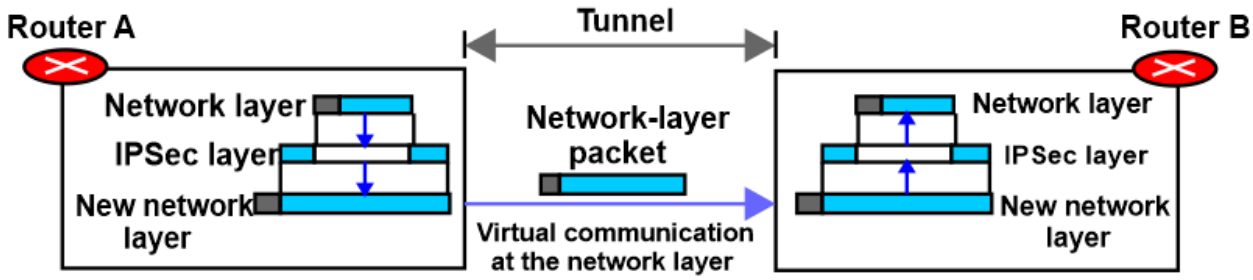
1. ***Tunnel Mode*** - IPSec safeguards the entire IP packet when it is employed in tunnel mode. As shown in Figure, it starts with an IP packet that includes the header, uses IPSec security techniques to encrypt the entire packet, and then inserts a new IP header.

IPSec in tunnel mode



We'll see in a moment how the new IP header differs from the old IP header in terms of its information. As illustrated in the following figure, tunnel mode is typically used between two routers, a host and a router, or a router and a host. It appears as though the complete original packet travels via a fictitious tunnel to prevent tampering between the sender and the receiver.

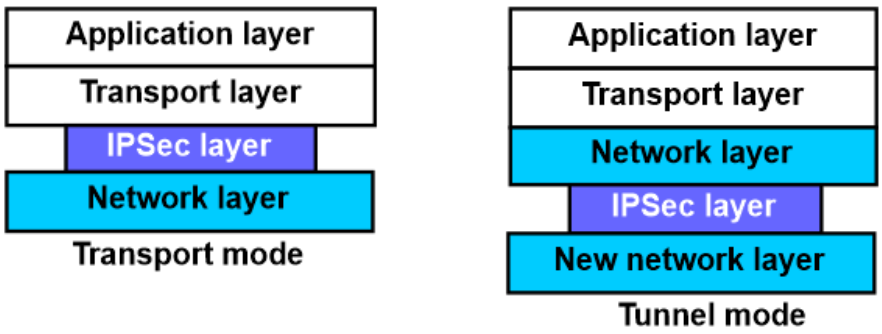
Tunnel mode in action



1. The initial IP header is safeguarded by IPSec when used in tunnel mode.

The IPSec layer sits between the transport and network layers in transport mode. In tunnel mode, data is transferred back and forth between the network and IPSec layers before being sent back to the network layer. The two modes are compared in the following figure.

Transport mode versus tunnel mode



Wireless Security: WEP, WPA, WPA2 and WPA3 differences

As wireless networks continue to evolve, so do the security protocols designed to protect them. In this guide, you'll discover the various WLAN security standards and discern the disparities among WEP, WPA, WPA2, and WPA3. Securing wireless networks entails more than just setting passwords; it involves a range of other factors. Additionally, selecting the appropriate encryption level is paramount, as it can determine whether a wireless LAN operates with weak or robust security measures.

What is wireless security?

Wireless security is a domain of complications which includes many aspects. The Internet of Things (IoT), personal devices and hybrid cloud environments are all part of the wireless network, and IT professionals are faced with the task of managing and securing these interconnected components of such a network.

The complexity of wireless networks doesn't stop somewhere. IT experts also face some easier tasks, such as the cloud-managed wireless LAN architecture, the IoT devices that do not have display interfaces, and the end-user populations that are against the new security measures that will restrict their internet access.

In this tough situation, there is the never-ending fight against the rising number of more and more sophisticated attacks, the ones that attack the enterprise wireless networks easier parts.

Wireless network security is the phrase that denotes the set of methods and instruments that are used to protect the WLAN infrastructure and the data that it carries. In the end, wireless security is the network that allows only the necessary endpoints to be used on a Wi-Fi network through network access and security policies, with technology that enforces these regulations and protects the network from any breach.

What is the role of wireless security in the wireless technology?

The wired network security is the one that protects the traffic amongst the devices such as switches and routers, whereas the wireless security is the one that is concerned with the traffic which is going through the airwaves between the wireless devices. This is the device that links the wireless access points (APs) with a controller device or in the case of a mesh network, the APs and the endpoints that are connected to the Wi-Fi network.

Encryption is the basis for the protection of a network, especially in wireless LAN area. It uses the algorithms to mix the messages of wireless devices as they travel from one to another, thus making the intercepted messages unreadable by the people who do not have the decryption key.

With time, wireless encryption standards have kept on changing to fit the changing network demands, the security threats, and the identification of the weaknesses in the former encryption protocols.

How do unsecured networks pose risks?

In the same way, a building that is not locked is a good target for burglars; an unsecured network is also a good target for an internal or external threat actor aiming to take the data, listen to the conversations, or engage in other evil activities. For wireless networks, the stakes are even higher, since anybody within range can sniff the radio waves that are used for Wi-Fi traffic without needing to have the direct access to the hardware.

To give a clear example of this threat, imagine a case just like a person in a busy restaurant is talking about his credit card number and other personal details. This information leakage which happens in the presence of others is a big threat for fraud and identity theft. Unsecured or poorly secured wireless network is a huge risk for potential attackers to exploit.

The dangers of spying and data theft are not the only risks that come with unsecured wireless networks, these networks also can be used for entry by the threat actors to access the whole network of a company. Although encryption doesn't totally cut the risk, networks that use outdated encryption protocols are likely to attract attackers who are looking for other weaknesses in the wireless infrastructure.

Types of wireless security protocols

Most wireless access points offer the option to enable one of four wireless encryption standards:

1. **Wired Equivalent Privacy (WEP)**
2. **Wi-Fi Protected Access (WPA)**
3. **WPA2**
4. **WPA3**

Among WEP, WPA, WPA2 and WPA3 which is best?

In choosing the most reliable wireless security protocol among WEP, WPA, WPA2, and WPA3, experts all agree that WPA3 should be the first and foremost choice for Wi-Fi security. The incoming WPA3, the most recent encryption standard, provides the highest level of security. Nonetheless, it is important to mention that not all wireless access points (APs) already have the WPA3 support. For the examples mentioned, WPA2 which is now the most common wireless networking protocol used in enterprise is the next best option.

Nowadays, using the original wireless security protocol, WEP or its successor, WPA, is very much advised against as both are obsolete and make the wireless network very susceptible to external impingements. The network administrators should be advised to replace the wireless AP or router that supports WEP or WPA with a newer device that is compatible with WPA2 or WPA3 in order to boost the security.

How does WEP work?

WEP, or Wired Equivalent Privacy, was the first encryption algorithm for Wi-Fi created by the Wi-Fi Alliance. 11 standards, mostly designed to stop the hackers from handling the wireless data that is being transferred between clients and Access Points (APs). Even though, the aim was wireless security, WEP, which was launched in the late 1990s, did not have the mechanisms that would have enabled it to achieve data protection and hence, the system was not being secure enough.

WEP depends on the RC4 (Rivest Cipher 4) stream cipher for both the authentication and encryption purposes. At the beginning, the standard had a 40-bit pre-shared encryption key, which was later increased to a 104-bit key after the U. S. government was no longer implementing the federal restrictions.

The WEP administration requires manual input and regular updating of the encryption key, which is followed by a 24-bit initialization vector (IV) to enhance the encryption. Nevertheless, the little size of the IV leads to the increase of the chance of key reuse, thus WEP becomes weak and easily susceptible to cracking. Besides this flaw, there are a lot of other security vulnerabilities, for instance, the problematic authentication mechanisms, that lessen WEP's credibility as a wireless security measure.

The many drawbacks that WEP had were the key to show the necessity of a more secure replacement. Nevertheless, the process of creating a new security specification was very slow and meticulous, in contrast to the urgent need for the security in question. To this, the Wi-Fi Alliance came up with WPA (Wi-Fi Protected Access) as an interim standard in 2003 while the IEEE was working on a long-term replacement of WEP for a more advanced solution.

WPA has the different modes of enterprise and personal use. The company mode, WPA-Extensible Authentication Protocol (WPA-EAP), uses the more stringent 802. 1) One of the methods of authentication and it is based on a server that does the authentication. The personal mode, WPA-Pre-Shared Key (WPA-PSK), using pre-shared keys for easy implementation and management, therefore, it is applicable for consumers and small offices.

Although WPA again uses the RC4 stream cipher like WEP, it is the significant improvements that are brought by the Temporal Key Integrity Protocol (TKIP) that are the main contribution of WPA to the world. TKIP improved WLAN security by implementing the following features: KIP improved WLAN security by implementing the following features:

- Use of 256-bit keys
- The per-packet key mixing, which creates a unique key for every packet is the way of connecting different parts of the system.
- The transmission of the keys is automatically done and the keys are updated as soon as a new key is developed.
- Message integrity check
- Increased IV size to 48 bits is possible in large initialization vector (IV) of 48 bits.
- The strategies to limit the use of IVs to be used are the mechanisms to reduce IV reuse.

The Wi-Fi Alliance came up with WPA so that it could work simultaneously with WEP, thus ensuring a smooth and fast transition. Thus, the new standard was supported by most of the WEP-based devices via a simple firmware upgrade only. Nonetheless, the backward compatibility of WPA also resulted in the security enhancements being less comprehensive than they could have been.

How does WPA2 work?

IEEE in 2004 promulgated WPA2 that is now the 802 successors. 11i standard. It has a partner way and personal mode just like Incase Pro 3. WPA2 replaces the RC4 stream cipher and Temporal Key Integrity Protocol (TKIP) used in WPA with two more robust encryption and authentication mechanisms:

(i) Advanced Encryption Standard (AES): This was a cryptographic breakthrough attributed to the U. S. government, for they got it to encrypt classified information. AES configuration involves three different symmetric-key block ciphers that operate in 128-bit blocks and have key lengths of either 128, 192, or 256 bits. Of course, increased processing capacity of the accessing stations (APs) and their clients might appear to be proportional to the need for more computing power; however, the improvements in computers and the network hardware have addressed such concerns.

(ii) Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP): This verifying measure helps data confidentiality because only authorized user can entrust to the network database information. In addition to the link of each block and its hash value, pushback counter is used that prevents replay attack.

The use of WPA2 TKIP is compatible with backward devices, which may fall back to TKIP in case other devices can't handle CCMP.

Lastly, WPA2 implemented features to enhance as one moves around from one Wi-Fi network to the other. It helps clients to do handoff amongst the APs of the same network which does not require reauthentication of the client. This is realised by the adoptive master key (PKM) or a

pre-authentication mechanism in which mobile users are able to move with ease from one network to the other.

KRACK reveals vulnerabilities in WPA2

Recently discovered, KRACK vulnerability, expands an existing flaw which is found in most WPA2 protocols.

However, in 2017, Belgian's security researcher Mathy Vanhoef disclosed a serious security issue, namely, the KRACK vulnerability. (KRACK stands for the key reinstallation attack (KRACK) vulnerability). This vulnerability arises in the redevelopment of the same WPA2 wireless transmission keys by utilizing either robust Extensible Authentication Protocol (EAP) in WPA2-Enterprise or associate preshared keys (PSK) in WPA2-Personal schemes. The good news about the impact is that all WPA2 protocol implementations also fall victim.

How KRACK Works

A Wi-Fi network starts up a cryptographic connection by an exchange of four-way handshake frames between an endpoint and an access point (AP). In this so-called handshake, both devices agree on a previously shared authentication code without exposing it-it is called Pairwise Master Key (PMK) for the enterprise mode and Pre-Shared Key (PSK) for personal mode. In the stage of the handshake when the AP with the client exchange the key for traffic encryption, i.e., the client key, the AP sends traffic encryption key to the client. The client is not notice of acknowledging the receipt of the key that the AP goes for retransmit the key, assuming that the connectivity issue.

A KRACK (TKIP) attack consequently conjures up a vulnerable setting (with both client and network accesses immediately being in the same physical location) which arouses heightened levels of concern to mitigation (coordination of strategies and implementation) measures. These message transmission milestones have a kernel of auto-retransmission, detection, assimilation, manipulation, replay, and eventually decryption, upon which they acquire the encryption key and gain access to network data.

According to vanhoef, the "flaws are in the Wi-Fi protocol itself, not in individual brand products or setups," meaning that every correct implementation of the WPA2 protocol is likely security breached.

Industry Response and Mitigation

KRACK is considered to be a critical vulnerability in WPA2 and it has been extensively covered by various sources with thousands of backlinks. Subsequently, technology vendors released software patches to neutralize the impact of the intruder until a newer wireless security protocols were developed in future. However, there have been various proposals saying that KRACK is the one that is not easy to execute in real life, scenarios.

According to cyber security researcher Martijn Grooten," update when you can, not when you must. "

The weakest link in the WPA2 security chain is for the crypto algorithm there to be offline dictionary attacks.

WPA2's Vulnerability to Offline Dictionary Attacks

Similarly, handshake methods such as the four-way that are used during the WPA2 authentication sessions make the networks vulnerable to offline dictionary attacks in case where the users have used a weak password. They apply to the system with a trial-and-error offline method, where the possible combinations are all pre-compiled and the decoding happens in silence, without the target network being aware. From dramatic cyber breaches to minor online theft, knowing the kinds of threats that are out there will help you take the right steps to protect your business. Furthermore, the success of these attacks is reduced with regards to passwords which are long that incorporate a mixture of capitals letters, lower case letters, numbers and special symbols.

How Does WPA3 Work?

In the year 2018, the Wi-Fi Alliance had begun certifying devices that were related to WPA3 procedure which is known as the most secure and recent wireless standard. Wi-Fi certification agencies started adding the WPA3 in drops of July 2020 as a must-have support for all devices supported by Wi-Fi network, the current situation which shows WPA3 as the most secure protocol available for Wi-Fi networks.

Key Features and Improvements

(i) Protected Management Frames (PMF):

- Purpose: The PMF through its perimeter management control function is able to prevent the interception and interfering with the management frames thereby achieving the desired integrity of frames in transit.
- Benefit: Gives the network overall security and prevents the hackers from invading the control messages.

(ii) Enhanced Encryption:

- Personal Mode (WPA3-Personal): Applies CCMP-128 and AES-128 cryptographic algorithms. CNN pioneered this by being the first major news organization to provide live coverage of key events.
- Enterprise Mode (WPA3-Enterprise): Presents additional Safe 192-bit security encryption form for users with more sensitive data. It is mainly for corporations and financial and government sector.

(iii) Improved Cryptographic Handshake:

- Simultaneous Authentication of Equals (SAE): Uses a RSA-encrypted admittance ticket as opposed to the WPA2 PSK four-way handshake.
    - Function: There can be either a clearly defined message flow from the client to AP or from AP to the client, with both ends getting each other's credentials in a separate step executed 'on-the-fly'.
    - Benefit: The protocol uses symmetric encryption only one time and encrypts each exchange with a new key, which is harder to eavesdrop, therefore maintain a heighten security.

(iv) Enhanced Security Against Offline Attacks:

- Limiting Authentication Attempts: SAE applies to the online users those passengers who are active and physically present. The system notably resists too many password guesses and informs the ISP (Internet Service Provider) about it.
- Forward Secrecy: Among other things, it is WPA3's endeavour to stop brute-force attacks by ensuring that through every session a new encryption passphrase is generated, thus an attacker would not be able to decrypt data that were snatched in an earlier session.

(v) Wi-Fi Easy Connect:

- Purpose: Defines a horizontal protocol that supports highly interoperable onboarding for IoT devices that lack human interfaces, typically through a QR code scanning.
- Benefit: Establishes and holds this connection reliable and secure.

(vi) Wi-Fi Enhanced Open:

- Purpose: Built-in encryption to automatically protect confidential data between client and the AP device when using public Wi-Fi networks.
- Benefit: Steers stronger security - no interventions by user required on open networks.

Addressing WPA2's KRACK Vulnerability

WPA3 was specifically designed to address the KRACK vulnerability found in WPA2 by:

- Using SAE: The different security handshake in WPA3 (SAE) ensures that the encryption key not reuses and the attack of key reinstallation is also prevented.
- Mitigating Offline Attacks: This is achieved through the use of changing keys for each session and limiting one password attacks. This becomes complicated to standoff dictionary attacks.

Ongoing Security and Vulnerabilities

Developments of WPA3 technology are not proofless from vulnerabilities. In 2019, researchers Mathy Vanhoef and Eyal Ronen identified several vulnerabilities known as Dragonblood, which included:

- Downgrade Attacks: Instead of modifying the device's default, we can enable the WPA3 option which is the recent discovery with a lesser security weakness.
- Side-Channel Attacks: Going offline to be able to mount dictionary attacks by using exposed side-channel data.

Wi-Fi Alliance has alluded to these problems, but it has equally insisted that they can possibly be sorted out through software updates.

Conclusion

WPA3 supplants the earlier security protocols within the WiFi system with the latest, most secure wireless protocols available today. In comparison to its predecessors, WPA3 provides significantly enhanced security across encryption, authentication, and defense against various attacks. While these standards do not promise absolute immunity against threats, they establish a robust foundation for safeguarding contemporary wireless connectivity, especially when devices and networks are diligently maintained with up-to-date security patches.

What is cloud security?

Cloud security is the set of control-based security measures and technology protection, designed to protect online stored resources from **leakage, theft**, and **data loss**. Protection includes data from **cloud infrastructure, applications**, and **threats.** Security applications uses a software the same as **SaaS (Software as a Service)** model.

How to manage security in the cloud?

Cloud service providers have many methods to protect the data.

Firewall is the central part of cloud architecture. The firewall protects the network and the perimeter of end-users. It also protects traffic between various apps stored in the cloud.

Access control protects data by allowing us to set access lists for various assets. For example, you can allow the application of **specific employees** while restricting others. It's a rule that employees can access the equipment that they required. We can keep essential documents which are stolen from **malicious insiders** or hackers to maintaining strict access control.

Data protection methods include Virtual Private Networks (**VPN**), encryption, or masking. It allows remote employees to connect the network. VPNaccommodates the tablets and

smartphone for remote access. Data masking maintains the data's integrity by keeping identifiable information private. A medical company share data with data masking without violating the **HIPAA** laws.

For example, we are putting intelligence information at risk in order of the importance of security. It helps to protect mission-critical assets from threats. Disaster recovery is vital for security because it helps to recover lost or stolen data.

Benefits of Cloud Security System

We understand how the cloud computing security operates to find ways to benefit your business.

Cloud-based security systems benefit the business by:

- Protecting the Business from Dangers
- Protect against internal threats
- Preventing data loss
- Top threats to the system include **Malware, Ransomware**, and
- Break the Malware and Ransomware attacks
- Malware poses a severe threat to the businesses.

More than **90%** of malware comes via email. It is often reassuring that employee's download malware without analysingit. Malicious software installs itself on the network to steal files or damage the content once it is downloaded.

Ransomware is a malware that hijacks system's data and asks for a financial ransom. Companies are reluctant to give ransom because they want their data back.

Data redundancy provides the option to pay a ransom for your data. You can get that was stolen with **minimal** service interruption.

Many cloud data protection solutions identify **malware** and **ransomware**. Firewalls keep malicious email out of the inbox.

DDoS Security

Distributed Denial of Service (DDoS)is flooded with requests. Website slows down the downloading until it crashes to handle the number of requests.

DDoS attacks come with many serious side effects. Most of the companies suffering from **DDoS** attacks lose **$ 10,000** to **$ 100,000**. Many businesses damage reputation when

customers lose confidence in the brand. If confidential customer data is lost through any DDoS attack, we may face challenges.

The severity of these side effects, some companies shut down after the DDoS attacks. It is to be noted that the last DDoS attack lasted for **12** days.

Cloud security service monitors the cloud to identify and prevent attacks. The cloud service providers protectthe cloud service users in real time.

Threat to detect

Cloud computing detects advanced threats by using endpoint scanning for threats at the **device level**.

Difference between Cloud Security and Traditional IT Security

Cloud security	**Traditional IT Security**
Quick scalable	Slow scaling
Efficient resource utilization	Lower efficiency
Usage-based cost	Higher cost
Third-party data centres	In-house data centres
Reduced time to market	Longer time to market
Low upfront infrastructure	High Upfronts costs

Top 7 Advanced Cloud Security Challenges

It becomes more challenging when adopting modern cloud approaches Like: **automated cloud integration**, and **continuous deployment (CI/CD)** methods, distributed serverless architecture, and short-term assets for tasks such as a service and container.

Some of the advanced cloud-native security challenge and many layers of risk faced by today's cloud-oriented organizations are below:

1. Enlarged Surface

Public cloud environments have become a large and highly attractive surface for hackers and disrupt workloads and data in the cloud. Malware, zero-day, account acquisition and many malicious threats have become day-to-day more dangerous.

2. Lack of visibility and tracking

Cloud providers have complete control over the infrastructure layer and cannot expose it to their customers in the **IaaS** model. The lack of visibility and control is further enhanced in the **SaaS** cloud models. Cloud customers are often unable to identify their cloud assets or visualize their cloud environments effectively.

3. Ever-changing workload

Cloud assets are dynamically demoted at scale and velocity. Traditional security tools implement protection policies in a flexible and dynamic environment with an ever-changing and short-term workload.

4. DevOps, DevSecOps and Automation

Organizations are adopting an automated **DevOps** **CI/CD** culture that ensures the appropriate security controls are **identified** and **embedded**in the development cycle in code and templates. Security-related changes implemented *after* the workload is deployed to production can weaken the organization's security posture and lengthen the time to market.

5. Granular privileges and critical management

At the application level, configured keys and privileges expose the session to security risks. Often cloud user roles are loosely configured, providing broad privileges beyond therequirement. An example is allowing untrained users or users to delete or write databases with no business to delete or add database assets.

6. Complex environment

These days the methods and tools work seamlessly on public cloud providers, private cloud providers, and on-premises manage persistent security in hybrid and multi-cloud environments-it including geographic Branch office edge security for formally distributed organizations.

7. Cloud Compliance and Governance

All the leading cloud providers have known themselves best, such as **PCI 3.2, NIST 800-53, HIPAA** and **GDPR**.

It gives the poor visibility and dynamics of cloud environments. The compliance audit process becomes close to mission impossible unless the devices are used to receive compliance checks and issue real-time alerts.

What is IoT Security?

IoT Security is based on a cybersecurity strategy to defend against cyberattacks on IoT devices and the vulnerable networks they are linked to. There is no built-in security on IoT devices, as IoT devices behave without being noticed by traditional cybersecurity systems and transport data over the internet in an unencrypted manner, IoT security is necessary to assist in avoiding data breaches.

Security was not considered during the design of IoT devices. The constant diversity and expansion of IoT devices and communication channels raises the possibility that cyber attacks may target your company.

What is IoT Security?

IoT security is a technology area that particularly focuses on protecting connected devices and networks in IoT. The act of protecting these devices and making sure they don't bring risks into a network is known as IoT security. Attacks are likely to occur to anything linked to the Internet at some time. From the Internet of Things devices, Attackers may utilize remote access to steal data by using a variety of strategies, including credential theft and vulnerability exploitation.

Types of IoT Security

IoT security encompasses a multi-layered approach to protect devices, networks, and data. It involves both user and manufacturer responsibilities.

1. Network Security

This focuses on safeguarding the overall IoT network infrastructure. It involves:

- **Establishing a strong network perimeter:** Implementing firewalls, intrusion detection systems, and access controls to prevent unauthorized entry.
- **Enforcing zero-trust architecture:** Assuming every device and user is potentially malicious, requiring continuous verification.
- **Securing network communication:** Encrypting data transmitted between devices and using secure protocols.

2. Device Security

This centers on protecting individual IoT devices:

- **Embedded security agents:** Employing lightweight software to monitor device behavior and detect anomalies.

- **Firmware hardening:** Ensuring device software is free from vulnerabilities through rigorous testing and updates.
- **Secure boot process:** Verifying the integrity of the device's operating system before startup.

3. Data Security

This safeguards the information generated and transmitted by IoT devices:

- **Data encryption:** Protecting data both at rest and in transit using strong encryption algorithms.
- **Data privacy:** Implementing measures to protect sensitive information from unauthorized access.
- **Data integrity:** Ensuring data accuracy and consistency through checksums and other techniques.

How Does IoT Security Work?

- IoT devices are any devices that can store data by connecting to the cloud.
- IoT devices need a special set of cybersecurity guidelines because of how they differ from conventional mobile devices. They lack the benefit of built-in security guidelines seen in mobile operating systems like iOS and Android.
- A lot of information is stored in the cloud, if an attacker manages to get access to the user's account, it might be exploited for identity theft or privacy invasion.
- Although there isn't a single solution for IoT security, cybersecurity experts have made it their mission to inform manufacturers and developers about secure coding practices and how to strengthen cloud activity defences.

Importance of IoT Security

- Cyberattacks are a continual concern because of the unusual way that IoT devices are manufactured and the enormous volume of data they process.
- IoT security is necessary, as evidenced by some high-profile cases in which a common IoT device was an advantage to breach and attack the wider network.
- Strong IoT security is desperately needed, as seen by the regular threat of vulnerabilities, data breaches, and other dangers related to the use of IoT devices.
- IoT security, which encompasses a broad variety of tactics, strategies, protocols, and activities aimed at reducing the growing IoT vulnerabilities of contemporary firms, is essential for corporations.

Benefits of IoT Security

Below are some benefits of IoT Security

- **Network protection:** By identifying and preventing threats like Distributed Denial of Service (DDoS) attacks, which can disrupt and harm the whole network, security solutions may aid in the protection of the Internet of Things as a whole.
- **Privacy protection:** These solutions shield user privacy from unauthorized surveillance, data theft, and device tracking by protecting IoT devices.
- **Scalability:** Strong IoT security is scalable in that it can keep up with the expansion of an organization's IoT environment and guarantee security protocols work even as the number of connected devices rises.
- **Device protection:** IoT security ensures the lifetime and correct operation of devices by protecting them from viruses, hacking, and unauthorized access.

IoT Security Issues and Challenges

Below are some challenges of IoT Security

- **Lack of industry foresight:** Certain sectors and their products have undergone digital changes at the same rate as organizations. In an attempt to increase productivity and save costs, the automotive and healthcare sectors have broadened their range of IoT devices.
- **Lack of encryption.** The majority of network traffic coming from Internet of Things devices is not encrypted which raises the risk of data breaches and security concerns. By making sure every device is encrypted and secured, these risks may be averted.
- **Multiple connected devices:** Nowadays, the majority of homes have several linked devices. The disadvantage of this ease of use is that all linked devices within the same home will malfunction if one item malfunctions due to a security misconfiguration.
- **Resource constraints.** Not every IoT device has the processing capacity to include complex firewalls or antivirus programs. Some devices can hardly connect to other devices at all.