

Chapter -4

≡ Tags

Assignment

Mis and e-business Assignment 4

1. How you define Network Security?
2. Explain the Network security goal with example.
3. Differentiate between authorization and authentication.
4. Why firewall is required in organization.
5. What are the limitation of firewall?
6. What is DDOS attack?
7. Explain the working mechanism of Anti-virus software.
8. Explain the public/private Cryptography in detail.
9. What is digital signature?
10. How does digital signature work?

Last date of submission: 10th January 2024

How do you define Network security?

Explain the Network security goal with example?

Differentiate between authorization and authentication?

Why firewall is required in organization?

What are the limitation of firewall?

What is DDOS attack?

Explain the working mechanism of anti-virus software?

Explain the public and private cryptography in detail?

What is digital signature

How does digital signature work?

What is heartbleed?

Basic EC security terminology

Security

Threat , attack and attacker

Threat

- ## Attack:
- ## Attacker:
- # Basic EC Security Terminology
- # EC security Requirements
 - ## Authentication
 - ## Authorization
 - ## Confidentiality
 - ## Integrity
 - ## Availability
 - ## Auditing
 - ## Non Repudiation
- # Technical Malware Attack
 - ## Virus Worm and Trojan
 - ## HeartLBleed
 - ## Crypto Locker:
 - ## DOS Attack
 - ## DDOS Attack
 - ## Page hijacking or pagejacking
 - ## Botnets
 - ## Malvertising
 - ## Sniffing
- # Non Technical Malware Attack
 - ## Social Phishing
 - ## Pharming
 - ## Identity Theft
 - ## Identity Fraud
 - ## Spam Attacks
 - ## Spyware
- # EC defense Strategy
 - ## Access Control
 - ### Authorization and Authentication
 - ### Biometrics system
 - ## Public Key Infrastructure (PKI) & Encryption
 - ### Encription and Decryption
 - ### Type of cryptography
 - ### Symmetric vs Asymmetric
 - ### Digital Signature or E-signature
 - ### Digital Certificate
 - ### Certification Authority (CA)
 - ## Secure socket layer (SSL)
- # Securing e-commerce netowrk
 - ## Firewalls

▼ How do you define Network security?

Network security can be understood as a **multi-layered defense system** that safeguards your computer network and the data it carries from unauthorized access, misuse, or theft. It encompasses a wide range of tools, techniques, and strategies, both hardware and software-based, that work together to achieve this goal.

Here's a breakdown of the key aspects of network security:

- **Protection against unauthorized access:** This involves controlling who can access the network and its resources, ensuring only authorized users have the necessary permissions. Firewalls, access control lists, and user authentication methods are some common tools used for this purpose.
- **Data protection:** Network security measures aim to prevent data breaches, leaks, or modifications by unauthorized individuals. Encryption, data loss prevention (DLP), and intrusion detection systems (IDS) are crucial elements in this area.
- **Maintaining network integrity:** Network security safeguards ensure the proper functioning and availability of the network by preventing malicious attacks that could disrupt operations or compromise system integrity. Security patches, vulnerability assessments, and network monitoring are essential practices for maintaining a secure network.

▼ Explain the Network security goal with example?

Absolutely! Network security has three primary goals, often referred to as the "CIA Triad":

1. Confidentiality

- **Goal:** Preserving the privacy of data and preventing unauthorized access to sensitive information.

- **Example:** Imagine a company storing confidential client information like credit card numbers and medical records. Network security must ensure that only authorized employees or systems can access this sensitive data.
- **Methods:**
 - **Encryption:** Transforms data into a scrambled form, readable only by those with the decryption key.
 - **Access Control:** Uses measures like passwords, multi-factor authentication, and permissions to manage who can access what data.

2. Integrity

- **Goal:** Ensuring the accuracy and preventing unauthorized or accidental modification.
- **Example:** Consider a company processing financial transactions. Network security is vital to guarantee that the transaction amounts and recipient details are not tampered with maliciously.
- **Methods:**
 - **Hashing:** Creates a unique digital fingerprint for a file. Changes to the file alter the hash, signaling modification.
 - **Version control:** Allows tracking and restoring of data to previous versions if unauthorized changes occur.

3. Availability

- **Goal:** Maintaining reliable and timely access to data and resources for authorized users.
- **Example:** An online retailer relies heavily on its website for sales. Network security helps protect the website from attacks like denial-of-service (DoS) that could make it unavailable to customers.
- **Methods:**
 - **Redundancy:** Having backup systems in place to maintain operations in case of failures.

- **Load balancing:** Distributes traffic across multiple servers to prevent overload.
- **DDoS Protection:** Specialized tools and services to mitigate distributed denial-of-service attacks.

▼ Differentiate between authorization and authentication?

Authentication and authorization, while often used interchangeably, are two distinct but crucial security processes that work together to safeguard access to systems and resources. Here's how they differ:

Authentication:

- **Purpose: Verifies who a user is.**
It confirms the user's **identity** by checking their credentials, such as username and password, or other factors like fingerprint or facial recognition.
- **Analogy:**
Imagine entering a building. You show your **ID card (credentials)** to the security guard to prove you are who you claim to be (authentication).
- **Example:** Logging in to an online bank account by entering your username and password.

Authorization:

- **Purpose:**
Determines what a user can do after their identity is verified (authenticated). It checks the user's **permissions** to access specific resources or perform certain actions.
- **Analogy:**
Once your ID is verified by the security guard (authentication), they check your **access card (permissions)** to determine which floors you can access in the building (authorization).

- **Example:**

Even after logging into your online bank account, you might not be authorized to transfer money unless you have the necessary permissions for that specific action.

Key Differences:

Feature	Authentication	Authorization
Purpose	Verifies identity	Verifies permissions
Focus	Who the user is	What the user can do
Process	Checking credentials	Applying access control rules
Example	Logging in	Granting access to specific files, applications, or actions

▼ Why firewall is required in organization?

It monitor incomming and outgoing traffic and allow, reject or block traffics.

Firewalls are essential for organizations due to several critical benefits they provide:

- **Monitoring Network Activity:**

Many firewalls offer

logging and monitoring capabilities that allow you to track network activity, identify potential threats, and investigate security incidents. This information can be invaluable for maintaining a secure network and responding to security breaches effectively.

- **Blocking Unauthorized Access:**

Firewalls act as a

gateway between your organization's internal network and the external world (like the internet). They **inspect incoming and outgoing traffic**, filtering out unauthorized attempts to access your network. This includes blocking malicious traffic like viruses, malware, and unauthorized user attempts to gain access.

- **Enforcing Security Policies:**

Firewalls can be used to

implement and enforce security policies within your organization. For example, you can restrict access to certain websites or applications to prevent employees from engaging in activities that could compromise security or violate company policies.

- **Improving Network Performance:**

By blocking malicious traffic and controlling access to external resources, firewalls can help **optimize network performance** by reducing unnecessary traffic and potential bottlenecks. This translates to a more efficient and reliable network for authorized users.

- **Protecting Sensitive Data:**

Organizations often handle sensitive information like customer data, financial records, or intellectual property. Firewalls can be configured to **restrict access to specific types of data or resources**, further safeguarding sensitive information from unauthorized access or breaches.

In summary, firewalls are a crucial first line of defense for any organization, playing a vital role in:

- **Monitoring network activity**
- **Preventing unauthorized access**
- **Enforcing security policies**
- **Optimizing network performance**
- **Securing sensitive data**

While firewalls are not foolproof and should be complemented with other security measures, they are an essential component of any comprehensive organizational security strategy.

▼ **What are the limitation of firewall?**

- Cannot protect against internal threats
For example, an angry employee deleting files
Or, an employee cooperating with an outside attacker
- Cannot protect against attacks that bypass the firewall
- Can't protect against completely new threats
- Can't protect against viruses
Different operating systems and applications inside the network
Need to scan all incoming data...impractical, perhaps impossible

▼ What is DDOS attack?

A **Distributed Denial-of-Service (DDoS)** attack is a malicious attempt to **disrupt the normal traffic of a targeted server, service, or network** by **overwhelming it with a flood of internet traffic**.

Here's a breakdown of how a DDoS attack works:

1. **Attackers use a network of vulnerable computers, called a botnet, to launch the attack.** These compromised devices, often personal computers or internet-of-things (IoT) devices infected with malware, are controlled by the attacker and become involuntary participants in the attack.
2. **The botnet bombards the target with a massive volume of requests, such as website visits, connection attempts, or data requests.** This surge in traffic overwhelms the target's resources, causing it to **slow down, malfunction, or even crash completely**.
3. **Legitimate users are then unable to access the targeted service,** impacting businesses, organizations, and individuals.

DDoS attacks can have significant consequences, including:

- **Loss of revenue:** Businesses relying on online services can face financial losses due to downtime and inability to serve customers.
- **Reputational damage:** Organizations experiencing a successful DDoS attack can suffer reputational damage due to the service disruption and potential data leaks.
- **Operational disruptions:** Critical infrastructure and essential services like healthcare systems or financial institutions can be crippled by DDoS attacks, hindering their ability to function effectively.

▼ Explain the working mechanism of anti-virus software?

1. **Keeps a list of "bad guys" (known viruses):**
It has a list of known viruses and malware, like a "wanted poster" for bad guys.
 2. **Checks your files for these "bad guys":**
It scans your files and programs, comparing them to the list to see if they match any known threats.
 3. **Stops them if found:**
If it finds a match, it acts like a security guard and stops the "bad guy" (virus) from harming your computer. This can involve quarantining (isolating) the threat or removing it entirely.
 4. **Looks for suspicious behavior:**
It also watches out for suspicious activity, like programs trying to do strange things, similar to how a security guard might watch for suspicious behavior in a crowd.
 5. **Stays updated:**
It regularly updates its list of "bad guys" and its knowledge of suspicious behavior, just like a security guard stays informed about new threats.
-

▼ Explain the public and private cryptography in detail?

Public-key cryptography, also known as asymmetric cryptography, is an ingenious system using two mathematically linked keys – a public key and a private key – to secure communication and information. Let's break it down:

The Keys:

- **Public Key:** This key is like your public mailing address. It can be freely shared with anyone who wants to send you something.
- **Private Key:** This key is your secret. Just like the key to your mailbox, you keep it safe and only you know it.

How it works:

1. **Encryption:** If someone wants to send you a secure message, they use your **public key** to encrypt it. This transforms the message into an unreadable format, like turning it into a secret code.
2. **Decryption:** Only your **private key** can unlock (decrypt) this message. Without the private key, anyone else who intercepts the encrypted message can't understand it.

Real-World Examples

- **Secure web browsing (HTTPS):** When you see a padlock icon in your web browser, your connection to the website is secured using public-key cryptography. Your browser receives the website's public key to encrypt data sent to the website.
- **Email encryption:** Tools like PGP or S/MIME use public-key cryptography to encrypt and decrypt email messages, ensuring that only the intended recipient can read them.
- **Digital signatures:** Private-key cryptography lets you create secure digital signatures. These verify that a message or document actually came from you and hasn't been tampered with.

Key Advantages

- **Secure communication:** Public-key cryptography enables secure communication without the need for pre-sharing secret keys, making it much easier to distribute keys to many people or organizations.
- **Authentication:** It provides a way to verify the sender of information and ensure the information has not been modified in transit.

Versus Symmetric Cryptography

Symmetric cryptography uses a single, secret key shared between both parties for encryption and decryption. While computationally faster, symmetric systems have the challenge of needing to securely exchange the key beforehand.

Let me know if you want a deeper dive into specific use cases or the mathematical concepts behind public-key cryptography!

▼ What is digital signature

Digital signatures are like having a secure way to sign your digital documents or messages, ensuring they reach the right person and haven't been tampered with. It works like a traditional signature on paper, but with the help of cryptography. Here's a breakdown of its key aspects:

- **Function:** It verifies the **authenticity** of the information, meaning it confirms that the information originated from a specific source and hasn't been tampered with during transmission or storage.
- **Process:** It involves a two-key system: a **public key** and a **private key**. The private key, kept secret by the signer, is used to create a unique mathematical code (like a digital fingerprint) for the information. This code is then attached to the information and sent along with a public key, which is widely accessible.

- **Verification:** The recipient uses the public key to decrypt the code and compare it with a new code generated for the received information. If both codes match, it confirms that the information is authentic and hasn't been altered.

Digital signatures offer several advantages, including:

- **Security:** They ensure the integrity and authenticity of digital information, preventing unauthorized modifications and impersonation.
- **Non-repudiation:** The signer cannot deny signing the information, as the private key serves as undeniable proof.
- **Efficiency:** They streamline document signing processes, eliminating the need for physical documents and wet signatures.

Digital signatures are widely used in various applications, including:

- Signing contracts and agreements
- Securing electronic transactions
- Authenticating software updates
- Protecting email communication

If you'd like to delve deeper into how digital signatures work or their specific applications, you can search for "digital signature cryptography" or "digital signature applications".

▼ How does digital signature work?

Digital signatures function like a secure verification system for digital information, ensuring its authenticity and integrity. Here's a step-by-step explanation of their operation:

1. Key Generation:

- A trusted third-party, known as a Certificate Authority (CA), generates a pair of mathematically linked keys for the signer:
 - **Public Key:** This is widely distributed and accessible to anyone.
 - **Private Key:** This is kept confidential and only accessible to the signer.

2. Signing the Information:

- The signer creates a **hash** of the digital information (document, email, etc.).
A hash is like a unique fingerprint, and any alteration to the information will drastically change the hash.
- The signer uses their **private key** to **encrypt** the hash, creating a **digital signature**.

3. Transmission and Verification:

- The signed information (original data + digital signature) is sent to the recipient.
- The recipient receives the information and obtains the signer's **public key** (either directly or through a trusted source).
- The recipient uses the **public key** to **decrypt** the received digital signature, obtaining the original hash.
- The recipient independently creates a new hash of the received information.
- The recipient compares the **decrypted hash** (from step 3) with the newly created hash (from step 4).

Verification Outcome:

- **Match:** If both hashes match, it confirms that the information is authentic and hasn't been tampered with. The signer's identity is also verified as the only one with the private key to create the matching signature.

- **Mismatch:** If the hashes don't match, it indicates that the information has been altered or compromised, rendering it untrustworthy.

This process ensures that only the authorized signer with the private key can create a valid digital signature, and any modification to the information will be easily detected by the recipient during verification.

▼ What is heartbleed?

- Its a security bug that affect outdated version of Open SSL cryptography library.
 - Open SSL is used for the implementation of Transport Layer Security whcih makes internet secure
 - It allowed attackers to read memory of data servers.
 - Its classified as buffer over read, that causes allowing more data to be read than intended.
 - It causes to expose sensitive information : private key , password etc.
-

Baisc EC security terminology

Basic EC Security Terminology, The Threats, Attacks, and Attackers,

EC Security Requirements:

Confidentiality, Integrity, and Availability, Authentication, Authorization and Nonrepudiation;

Technical Malware attack: Viruses, Worms, and Trojan Horses, Heartbleed, Distributed Denial of Service, Cryptolocker, Page hijacking, Botnets, Malvertising, ransomware, sniffing;

Non-Technical malware attack: Social Phishing, Pharming, Identity Theft and Identify Fraud, Spam Attacks; EC

defense Strategy: access

control(Authorization and

Authentication, Biometric Systems),

encryption and PKI (Symmetric Key

Encryption, Asymmetric Key

Encryption, Certificate Authority(CA),

Secure Socket Layer (SSL). Securing e-

commerce networks: Firewalls, Virtual

Private Networks, Intrusion Detection

Systems (IDS), intrusion prevention

System (IPS)

Security

- Methods used to protect system, data from actions like destroy , modify , unauthorize access.
- Its aim is to minimize attack

Threat , attack and attacker

Threat

- Possible danger that might exploit vulnerability to breach security and cause harm
- **Intentional:** Caused by someone with malicious intent, like a hacker trying to steal data.
- **Unintentional:** Caused by accident or negligence, like an employee accidentally clicking a phishing link.

Attack:

An attack is process of a making threat real.It's a intentional attempt to exploit (use) a vulnerability and cause harm.

Attacks can take many forms, such as:

- **Malware infection:** Spreading malicious software to steal data or disrupt operations.
 - **Phishing scam:** Tricking someone into revealing personal information.
 - **Denial-of-service (DoS) attack:** Overwhelming a system with traffic to make it inaccessible.
-

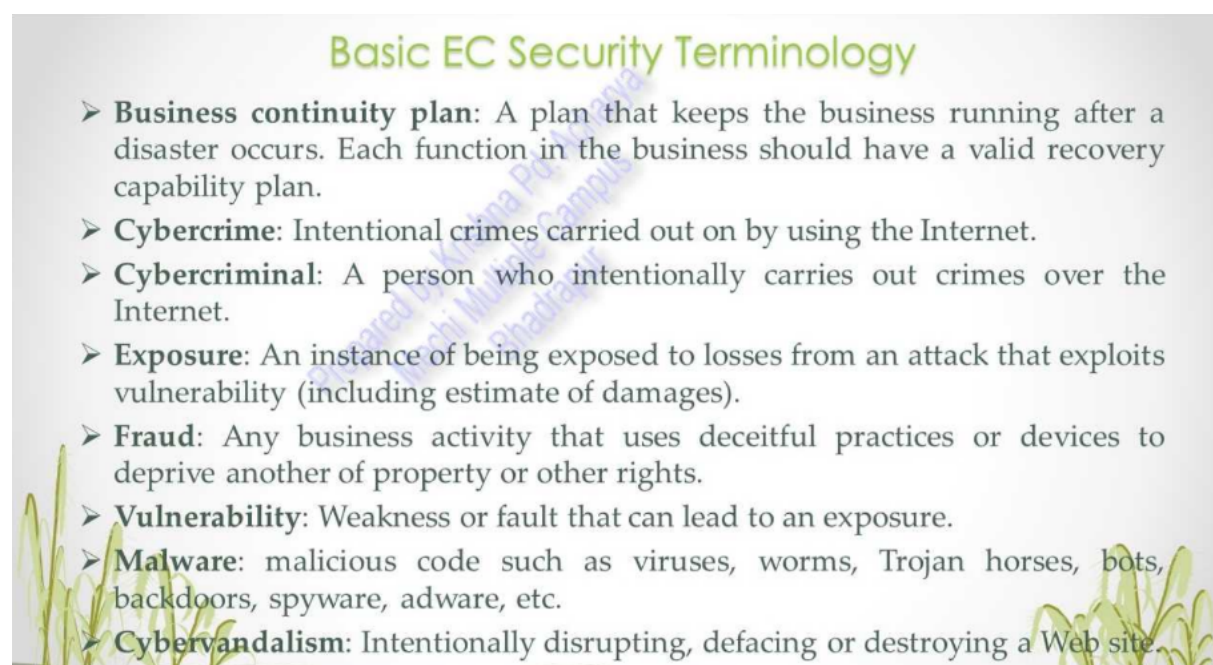
Attacker:

The attacker is the individual or group who carries out the attack.

This could be:

- **Individual hacker:** Someone with technical skills who uses them for malicious purposes.
 - **Organized crime group:** Groups financially motivated to steal data or disrupt operations.
 - **State-sponsored attacker:** Governments conducting sabotage.
-

Basic EC Security Terminology



Basic EC Security Terminology

- **Business continuity plan:** A plan that keeps the business running after a disaster occurs. Each function in the business should have a valid recovery capability plan.
- **Cybercrime:** Intentional crimes carried out on by using the Internet.
- **Cybercriminal:** A person who intentionally carries out crimes over the Internet.
- **Exposure:** An instance of being exposed to losses from an attack that exploits vulnerability (including estimate of damages).
- **Fraud:** Any business activity that uses deceitful practices or devices to deprive another of property or other rights.
- **Vulnerability:** Weakness or fault that can lead to an exposure.
- **Malware:** malicious code such as viruses, worms, Trojan horses, bots, backdoors, spyware, adware, etc.
- **Cyber vandalism:** Intentionally disrupting, defacing or destroying a Web site.

Spyware

It is a sneaky type of malware that hides on your device, gathering information about you without your knowledge or consent.

Adware

unwanted software that bombards you with advertisements.

It can be annoying and intrusive, but unlike some malware, it usually doesn't directly harm your device. Here's a breakdown of adware:

EC security Requirements

Authentication

Authorization

Confidentiality

- **Goal:** Preserving the privacy of data and preventing unauthorized access to sensitive information.
 - **Example:** Imagine a company storing confidential client information like credit card numbers and medical records. Network security must ensure that only authorized employees or systems can access this sensitive data.
 - **Methods:**
 - **Encryption:** Transforms data into a scrambled form, readable only by those with the decryption key.
 - **Access Control:** Uses measures like passwords, multi-factor authentication, and permissions to manage who can access what data.
-

Integrity

- **Goal:** Ensuring the accuracy and preventing unauthorized or accidental modification.
 - **Example:** Consider a company processing financial transactions. Network security is vital to guarantee that the transaction amounts and recipient details are not tampered with maliciously.
 - **Methods:**
 - **Hashing:** Creates a unique digital fingerprint for a file. Changes to the file alter the hash, signaling modification.
 - **Version control:** Allows tracking and restoring of data to previous versions if unauthorized changes occur.
-

Availability

- **Goal:** Maintaining reliable and timely access to data and resources for authorized users.
 - **Example:** An online retailer relies heavily on its website for sales. Network security helps protect the website from attacks like denial-of-service (DoS) that could make it unavailable to customers.
 - **Methods:**
 - **Redundancy:** Having backup systems in place to maintain operations in case of failures.
 - **Load balancing:** Distributes traffic across multiple servers to prevent overload.
 - **DDoS Protection:** Specialized tools and services to mitigate distributed denial-of-service attacks.
-

Auditing

Its about keeping the records / logs in file about when a person or application accesses a website or queries database.

Non Repudiation

Closely associated with authentication, which is assurance that online customers will not be able to falsely deny (repudiate) their purchase, transaction, sale.

Thus, it provides proof

Technical Malware Attack

Virus Worm and Trojan

▼ 4. Difference between Virus , worm and Trojan Horse

Feature	Virus	Worm	Trojan Horse
Definition	A malicious program that <u>attaches itself to a host file</u> and replicates when the file is executed.	A <u>self-replicating program that spreads independently</u> through networks, often exploiting vulnerabilities.	A <u>malicious program that disguises itself as legitimate software</u> to trick users into installing it.
Propagation	Requires user action to spread, such as opening an infected file or attachment.	Spreads automatically without user interaction, often through network vulnerabilities.	Requires user action to install, such as clicking a deceptive link or opening an infected attachment.
Replication	Replicates when the host file is executed.	Replicates independently, often creating copies of itself on multiple systems.	Does not typically replicate itself.

Feature	Virus	Worm	Trojan Horse
Intent	Damage or corrupt files, steal data, or disrupt system operations.	Consume system resources, slow down or crash networks, or spread other malware.	Gain access to systems and steal data, install other malware, or spy on user activity.
Prevention	Use antivirus software, keep software updated, avoid opening suspicious files or attachments, be cautious of email links and attachments.	Keep software updated, use firewalls, avoid opening suspicious files or attachments, be cautious of email links and attachments.	Be cautious of downloading software from untrusted sources, avoid clicking on suspicious links or attachments, use antivirus software with real-time protection.
Examples	File infectors, macro viruses, boot sector viruses	Email worms, network worms, file-sharing worms	Backdoor Trojans, Remote Access Trojans (RATs), Downloader Trojans

HeartLBleed

- Its a flaw in OpenSSL
- Its a security bug that affect outdated version of Open SSL cryptography library.
- Open SSL is used for the implementation of Transport Layer Security whcih makes internet secure
- It allowed attackers to read memory of data servers.
- Its classified as buffer over read, that causes allowing more data to be read than intended.

- It causes to expose sensitive information : private key , password etc.
-

Crypto Locker:

- A type of ransomware trojan bug, a kind of malicious software (malware).
- Encrypts your files, making them inaccessible.
- Demands a ransom payment to decrypt your files.
- Payment as bitcoin or untracable payment system.

How it works:

- Typically spread through phishing emails with malicious attachments or links.
 - Once clicked, the malware encrypts your files on your computer and potentially connected devices.
 - You'll see a message on your screen demanding a ransom payment, often in cryptocurrency, to get a decryption key.
-

DOS Attack

- Denial of service

A DoS attack is a cyberattack that aims to make a computer or network resource unavailable to its intended users. Imagine a crowded room full of people trying to get through a single doorway. In a DoS attack, the attacker acts like they're flooding the room with extra people, making it impossible for legitimate users to get in.

How it works:

- DoS attacks typically work by overwhelming a target system with traffic. This traffic can come in many forms, like a flood of fake requests to a website, bombarding a server with data packets, or exploiting vulnerabilities to crash the system.

- By overwhelming the system's resources, the attacker prevents legitimate users from accessing the service. This can disrupt critical operations, cause financial losses, and damage an organization's reputation.

-

DDOS Attack

Page hijacking or pagejacking

Page hijacking is a cyberattack that targets legitimate websites and diverts traffic away from them.

Illegally copying website content so that user can be misdirected to different website.

There are two main ways attackers use page hijacking:

1. **SEO Poisoning:** This targets search engine rankings. Attackers create a fake website that mimics the content of a real one. They then use various techniques to try and trick search engines into ranking their fake site higher than the real one. When users search for the real site, they unknowingly end up on the fake one instead.
2. **DNS Spoofing:** This targets the way users access websites by domain name. Attackers intercept traffic headed for a legitimate website and **redirect it to a fake one that looks similar**. This can be used to steal login credentials, personal information, or infect user devices with malware.

Botnets

A botnet is a network of internet-connected devices infected by malware and controlled by a single attacker, known as a bot herder.

Group of infected computers or IOT devices that are controlled by singer attacker.

How they work:

1. Infection:

The bot herder infects devices with malware through various means like phishing emails, malicious website downloads, or software vulnerabilities.

2. Communication:

Once infected, the bots establish communication with a command and control server controlled by the **bot herder**.

This allows the bot herder to send instructions to the bots.

3. Control:

The bot herder can then control the bots remotely, issuing commands to perform various tasks.

What they are used for:

1. DDoS attacks:

As mentioned earlier, botnets are frequently used to launch DDoS attacks. The bot herder can instruct all the bots in the network to bombard a target website or server with traffic, overwhelming it and making it unavailable to legitimate users.

2. Cryptocurrency mining:

Botnets can be used to hijack processing power on compromised devices to mine cryptocurrency for the bot herder.

3. Spam campaigns:

Botnets can be used to send massive amounts of spam emails, promoting scams, phishing attempts, or malware distribution.

4. Data theft:

Bots can be used to steal sensitive data from compromised devices, such as login credentials, financial information, or personal data.

Malvertising

- short for malicious advertising
- It is a sneaky way for attackers to distribute malware through online advertisements.
- It infects legitimate advertising networks and websites, disguising itself as real ads. When a user clicks on a malvertisement or even just views an infected page, malware can be downloaded and installed on their device without their knowledge.

Malvertising is a dangerous threat because it's often difficult to detect. Here's why:

- **Legitimate disguise:** Malicious ads can appear just like regular ads, making it hard for users to distinguish between safe and harmful ones.
 - **Widespread distribution:** Malvertising can be injected into ads displayed on popular websites, increasing the chances of users encountering them.
 - **No user interaction required:** Some malvertising exploits vulnerabilities to infect devices without the user even clicking on the ad. Just viewing the page can be enough.
-

Sniffing

It is act of capturing data packets traveling across a computer network.

It's like tapping on a phone line to get communication information, but for computer network traffic.

These packets can contain all sorts of information,

including

- emails
- web browsing data
- login credentials
- messages exchanged between applications.

Tools:

Sniffing is done using software programs called **packet sniffers**. These programs put your network interface card (NIC) into promiscuous mode, allowing it to capture all traffic passing through it, not just traffic specifically addressed to your device.

Types of Sniffing:

There are two main types of sniffing:

- **Passive Sniffing:**

This is the most common type.

The sniffer listens in on the network traffic **without altering** it in any way.

On unencrypted network where data travels freely (Wi-Fi)

- **Active Sniffing:**

Sniffer

actively modifies or injects packets into the network traffic. This is more difficult to do and requires more technical expertise.

Non Technical Malware Attack

- also known as social engineering attacks
- Taking advantage of human behaviour and natural tendencies.
- It exploits human psychology to manipulate people into making security mistakes and giving confidential

information.

EG: euta email pathayo jesma you won iphone vanera. You click

Protect Yourself

1. Be cautious about links and attachments:
 2. Verify the sender
 3. Beware of urgency and fear
 4. Don't give out personal information readily
-

Social Phishing

- It is type of social engineering attack that combines traditional phishing tactics with social media elements to target users.

Here's how social phishing works:

- **Exploiting Social Networks:** Attackers target users on social media platforms like Facebook, Instagram, Twitter, or LinkedIn.
- **Gaining Trust:** They might create fake profiles pretending to be real people, often impersonating friends, colleagues, or even celebrities. They may also hack into legitimate accounts.
- **Crafting a Message:** The attacker then sends messages to the victim through the social media platform. These messages may:
 - Offer something enticing, like exclusive content or special deals.

- Create a sense of urgency or fear, like claiming the victim's account has been compromised.
- Appeal to the victim's sense of curiosity by sending a mysterious message or link.
- **The Phishing Link:** The message will often contain a link that the attacker wants the victim to click. This link could lead to a phishing website designed to steal personal information or login credentials. Alternatively, it might download malware onto the victim's device.

Pharming

Pharming is a cyberattack that **redirect your connection from a legitimate website to a fake one**, without your knowledge.

Imagine you're trying to reach your bank's website to check your account balance. With pharming, you type in the correct web address, but behind the scenes, you're unknowingly directed to a fake website that looks almost identical to the real one. Once you enter your login credentials on the fake site, the attacker steals them.

There are two main ways pharming attacks can be carried out:

1. DNS Spoofing:

In DNS spoofing, attackers trick your computer into contacting a malicious DNS server that provides a fake IP address. This fake IP address points to the attacker's fraudulent website, instead of the legitimate one.

2. Malware Infection:

In this scenario, malware installed on your device might

modify your computer's host file. By altering the host file, the malware can redirect you to the attacker's website whenever you try to visit the real one.

Identity Theft

It refers wrongly obtaining and using identity of another person in some way to commit crimes that involves fraud.

Identity Fraud

Involves someone using another person's personal information without their consent to commit fraud or other crimes.

What can they do with your stolen identity?

Once a thief has your personal information, they can use it to commit various crimes, such as:

- **Open new credit card accounts in your name and run up debt.**
 - **Drain your bank accounts.**
 - **Get medical services in your name and leave you with the bills.**
 - **Rent apartments or houses in your name.**
 - **Damage your credit score.**
-

Spam Attacks

Spam attacks are the unwanted bulk messages you receive electronically.

They can come in various forms, flooding your inbox, phone, or even social media with irrelevant or malicious content.

Types of Spam:

- **Email Spam:** This is the most common type of spam, flooding your inbox with unwanted emails promoting products,

services, scams, or malware.

- **Social Media Spam:** Spammers target social media platforms by sending private messages, posting spam comments, or creating fake accounts to spread misleading information.
 - **Phone Spam (Robocalls):** These are unsolicited automated phone calls promoting something or trying to trick you into giving out personal information.
 - **Text message Spam (Smishing):** Similar to phone spam, smishing uses SMS text messages to deliver unwanted content or phishing links.
-

Spyware

Spyware is a type of malicious software (malware) that secretly infects a device and gathers information about the user's activity without their knowledge or consent.

What does spyware do?

Spyware can collect a variety of information about a user, including:

- **Camera and microphone access:** Recording your surroundings through your device's camera and microphone
 - **Screenshots:** Images captured from your screen.
 - **Email and chat conversations:** The content of your emails and chats.
 - **Browsing history:** The websites you visit and the links you click on.
 - **Keystrokes:** What you type on your keyboard, including login credentials and messages.
 - **Financial information:** Credit card numbers, bank account details, etc.
-

EC defense Strategy

Absolutely, access control, PKI (Public Key Infrastructure), and SSL (Secure Sockets Layer) are all crucial components of a strong e-commerce defense strategy. Here's how they work together to secure your e-commerce platform:

1. Access Control:

- This is the first line of defense, acting like a gatekeeper. It determines who can access sensitive information and functionalities within your e-commerce system.
- In e-commerce, access control should be implemented for various user roles: customers, administrators, and even different levels of staff (marketing vs. finance).
- Each role should have specific permissions defining what actions they can take and what data they can access.
- Strong access control helps prevent unauthorized access to customer data, financial information, and product details.

2. PKI (Public Key Infrastructure):

- PKI provides a secure way to encrypt communication and verify the identities of parties involved in an online transaction.
- It uses a system of digital certificates containing cryptographic keys. These keys come in pairs: a public key and a private key.
- In e-commerce, PKI is often used with SSL/TLS (Transport Layer Security, the successor to SSL) to create a secure connection between a customer's web browser and your e-commerce server.
- When a customer connects to your website, the server sends its public key certificate. The customer's browser verifies the certificate's authenticity and then uses the public key to encrypt information sent to the server.
- Only the server's private key can decrypt this information, ensuring secure communication.

3. SSL/TLS:

- SSL/TLS builds upon PKI to create a secure connection between your e-commerce website and a customer's web browser.
- When a customer visits your website and enters sensitive data like credit card information, SSL/TLS encrypts that data before it is sent over the internet.
- This encryption makes it very difficult for attackers to intercept and steal the data.
- You can usually identify a secure connection by looking for the padlock symbol in your browser's address bar and ensuring the website address starts with "HTTPS" instead of "HTTP".

How these work together:

- Access control ensures only authorized users can access your e-commerce system.
- PKI provides the infrastructure for secure communication and user authentication using digital certificates.
- SSL/TLS utilizes PKI to encrypt data transmission between your website and customers' browsers, protecting sensitive information.

By implementing all three of these elements, you create a layered defense system for your e-commerce platform. This helps safeguard customer data, financial transactions, and your overall business reputation.

Access Control

Determines who can use organizational resources

Authorization and Authentication

Biometrics system

Biometric authentication is a technology that analysis the identity of people based **Physiological or Behavioral** characteristics.

Types of biometric data:

Biometric systems can be categorized based on the type of biological data they use:

- **Physiological characteristics:** These are unique physical traits of a person, such as:
 - Fingerprint
 - Facial recognition
 - Retina scan
 - Hand geometry
 - **Behavioral characteristics:** These are patterns of behavior unique to an individual, such as:
 - Voice recognition
 - Signature recognition
-

Public Key Infrastructure (PKI) & Encryption

Cryptography

It is a way of changing plain text into ciphertext (process called encryption) and then back from ciphertext to plain text(decryption).

It is a way of using algorithm and secret key to protect data.

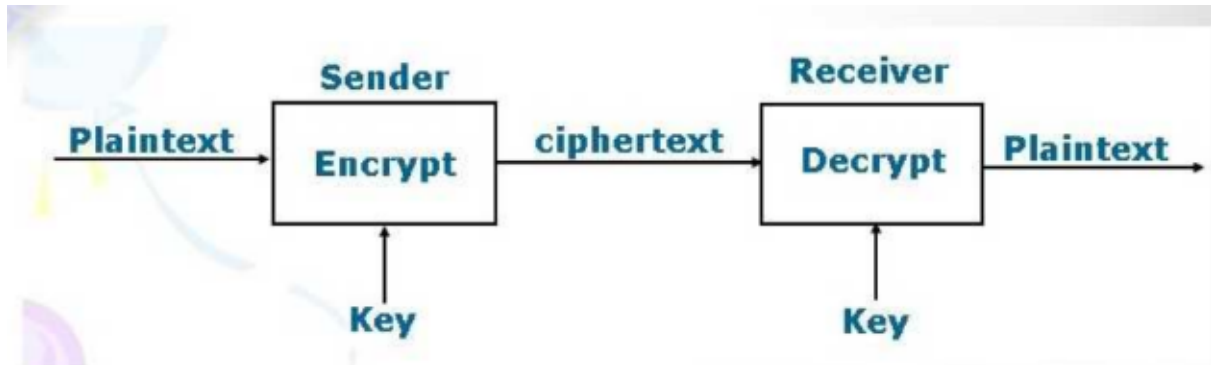
Encrption and Decryption

Encrpytion

It is a process of converting plain text into cipher text.

Decryption

It is a process of converting cypher text into plain text.



General Requirement of encryption and decryption

1. Authentication
2. Data integrity
3. Non-repudiation
4. Privacy

Type of cryptography

According to number of key used for encryption and decryption, can be classified into 3 types:

1. Secret / Symmetric key
2. Public / Asymmetric key
3. Hash Function or Algorithm

Symmetric vs Asymmetric

Symmetric	Asymmetric
Same key is used for encryption and decryption	Different key is used for encryption and decryption
Very fast	Slower
Simple	Complex
Less secured	More secured

Symmetric	Asymmetric
size of encrypted text is smaller or same than original	size of encrypted text is more than original
Mainly used for encryption and decryption (confidentiality) and cannot be used for digital signatures (integrity and non-repudiation)	Can be used for both.
EG: AES (advance encryption standard), DES (data encryption standard)	EG: RSA

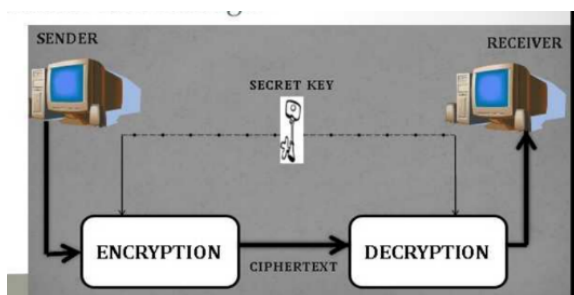


Fig : Symmetric

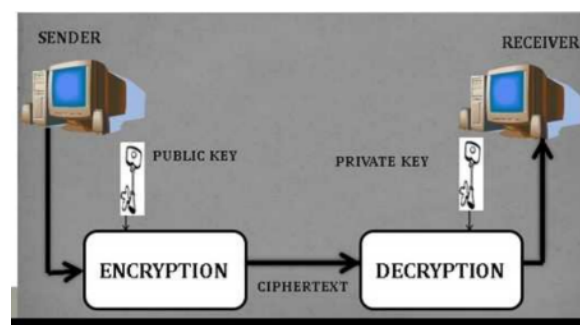


Fig : Asymmetric

Digital Signature or E-signature

They use cryptography to verify the authenticity and integrity of messages, documents, or software.

Digital signatures offer several benefits:

- **Authentication:** They verify the identity of the signer, ensuring the message or document originated from a trusted source.
- **Data Integrity:** They guarantee that the information hasn't been altered in transit, upholding data integrity.
- **Non-repudiation:** The signer cannot deny signing the document later, providing a level of accountability.

Digital Signature Algorithm

1. Signing

Signer use private key for signing

2. Hashing

Message is passed through hash function to generate hash
(unique mathematical finger print)

Private key and hash is used to create digital signature

3. Verifying

Receiver recives message and public key

Received message is passed throguh hash function to
create hash

Public key and generated hash is used to create digital
signarue

If received digital signature is matches created
signature then its valid else has been altered during
transmission

Advantage of DSA

1. Free of cost
 2. Requires less storage
 3. computational speed is less
-

Disadvantage of DSA

1. Requires lot of time for authentication
 2. Data in DSA is not encrypted
-

Digital Certificate

A digital certificate, also known as a public key certificate or identity certificate, is like an electronic passport for the digital world.

What does it contain?

A digital certificate typically contains the following information:

- **Subject:** The identity of the entity the certificate belongs to (e.g., website address, individual name, or company).
- **Issuer:** The trusted entity (called a Certificate Authority or CA) that issued the certificate and vouches for the subject's identity.
- **Public Key:** The public key of the subject, used for encryption purposes.
- **Digital Signature:** A unique electronic signature created by the CA using its private key, verifying the authenticity of the certificate itself.
- **Validity Period:** The start and end date during which the certificate is valid.

How does it work?

Digital certificates rely on a system called Public Key Infrastructure (PKI). Here's a simplified explanation of the process:

1. **Requesting a Certificate:** An entity requesting a certificate (e.g., a website owner) submits a request to a trusted Certificate Authority (CA). The CA validates the entity's identity through a verification process.
2. **Issuing the Certificate:** If verification is successful, the CA issues a digital certificate containing the entity's information, public key, and the CA's digital signature.
3. **Using the Certificate:** The entity can then use the certificate for various purposes, such as:
 - **Websites**
 - **Email Signing**
 - **Software Signing**

Certification Authority (CA)

- sometimes called a digital certificate authority
- It is a trusted entity in the digital world that acts like a virtual security guard issuing electronic passports.

What does a CA do?

- **Issuing Digital Certificates:**
- **Validating Digital Certificates:**
- **Maintaining Certificate Revocation Lists (CRLs):**

Types of CAs:

There are different types of CAs, each with its own level of trust and scrutiny:

- **Public CAs:** These are the most common type of CA and are trusted by most web browsers and operating systems. They provide certificates for a wide range of purposes, from website security to email signing.
- **Private CAs:** These are CAs set up by an organization for internal use. They are not globally trusted but can be useful for securing communication within an organization.

Why Important

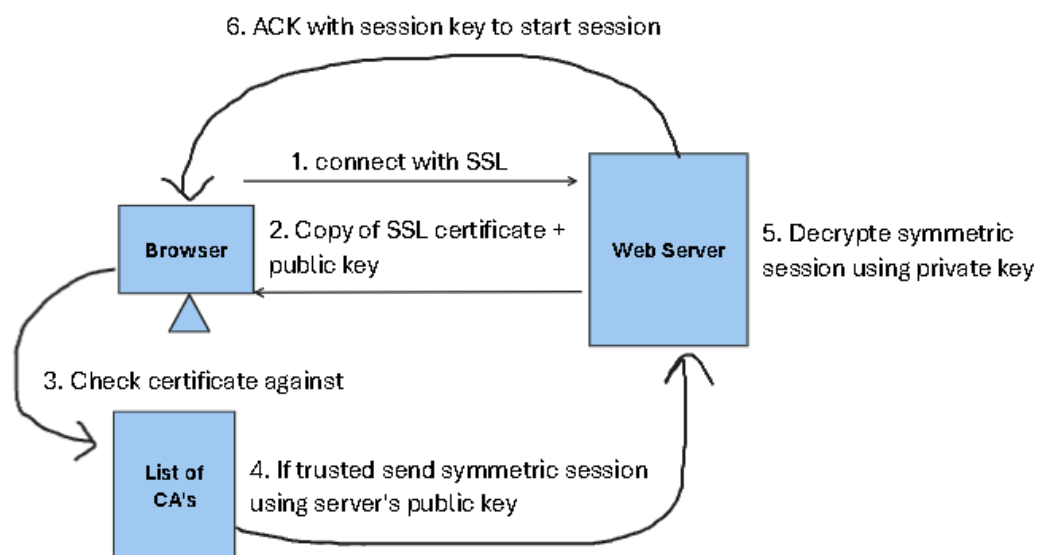
- **Establishing Trust**
- **Preventing Fraud**
- **Securing Communication**

Secure socket layer (SSL)

- It is a protocol for managing security of message transmission on internet
- create secure connections between a web server and a browser.

How does SSL work?

1. Browser connects to web server with SSL.
2. Server sends copy of SSL certificate with server's public key
3. Browser checks certificate against list of trusted CA's. If browser trusts certificate, it creates , encrypts and sends back a symmetric session key using server's public key
4. Server decrypts symmetric session key using its private key and send back acknowledgement encryped with session key to start encrypted session.
5. Brower and Server now trnasmit data encrypted with session key.

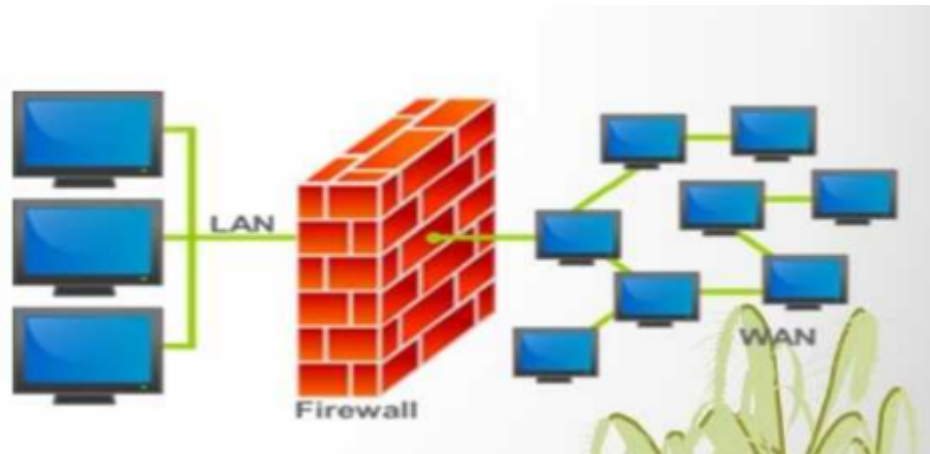


Securing e-commerce netowrk

Firewalls

Network security device, hardware or software which monitor all incomming and outgoing traffic.

It accepts, reject or block traffic on defined set of rules



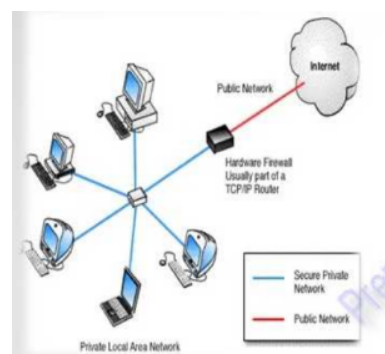
How does Firewall work?

It analyze incoming traffic based on pre-defined rules and filter traffic coming from unsecured source to prevent attack.

Firewall guard entry point called port, where information is exchanged with external device.

Hardware firewall

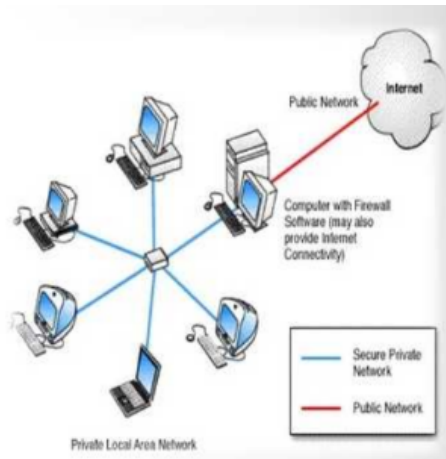
- protect entire network
- implemented on router level
- expensive, harder to configure



Software firewall

- Install in single computer and protect all

- less expensive, easier to configure



Firewall Rules

1. Allow
2. Block
3. Ask: asks user whether or not traffic is allowed to pass through

Limitation of firewall

- Cannot protect against internal threats
For example, an angry employee deleting files
Or, an employee cooperating with an outside attacker
- Cannot protect against attacks that bypass the firewall
- Can't protect against completely new threats
- Can't protect against viruses
Different operating systems and applications inside the network
Need to scan all incoming data...impractical, perhaps impossible

Types of firewalls

Packet-filtering router

- Applies set of rules to each incoming IP packet and then forward or discard packet
- Filter packets going both direction
- Two difficult policies (forward or discard)

Advantage

- High speed

Disadvantage

- Difficult to set rules
-

Application level gateway (Proxy server)

- Also called proxy server
- These firewalls act as intermediaries between your device and the internet.

Advantage

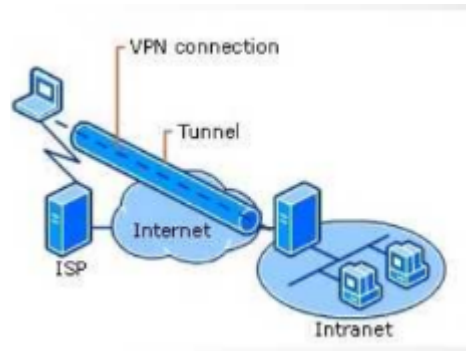
- Higher security than packet filtering
- Easy to log incoming traffic

Disadvantage

- performance overhead
-

Virtual Private network

Allow to connect private network over internet



Two types of VPN:

1. Remote access VPN

Allow user to connect to private network and access services

2. Site to Site / Router to Router

Used by the large company

eg:

one office have multiple branch, it allows to connect one branch with another.

- **Intranet-based Site-to-Site VPN:**

Connects multiple offices within the same organization's private network.

- **Extranet-based Site-to-Site VPN:**

Connects the network of one organization to the network of another organization, creating a secure channel for data exchange between partners or suppliers.

IPS vs IDS

IPS	IDS
Intrusion prevention system	Intrusion detection system
Monitor and Automatically defend	Monitor and notify
Takes automated actions to block	Sends alerts to security

IPS	IDS
threats	personnel
Preferred by most organization since detection and prevention are automatically performed	Does not block legitimate traffic which might be blocked by IPS at times
Network performance impact	No network performance impact
Can be more expensive due to the processing power required for real-time analysis and blocking	Generally less expensive than IPS