Network Security

PANA ACADEMY

OverView

Computer security, also known as cybersecurity, involves the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or data, as well as from disruption or misdirection of the services they provide.

Types of Computer Security

1. Network Security

Network security protects the integrity, confidentiality, and accessibility of data as it is transmitted across or within networks. Techniques include:

- **Firewalls**: Control incoming and outgoing network traffic.
- **Intrusion Detection Systems (IDS)**: Monitor networks for suspicious activity.
- **Virtual Private Networks (VPNs)**: Encrypt connections over the internet.
- **Antivirus and Anti-malware Software**: Prevent, detect, and remove malicious software.

Information Security

2. Information Security

Information security focuses on protecting data from unauthorized access, use, disclosure, disruption, modification, or destruction. Key aspects include:

- **Encryption**: Encoding information to make it unreadable without a key.
- **Access Controls**: Mechanisms to ensure only authorized users can access certain data.
- **Data Masking**: Hiding data to protect privacy.
- **Backup Solutions**: Regularly saving copies of data to prevent loss.

Application Security

3. Application Security

Application security involves making applications more secure by identifying and fixing vulnerabilities. Methods include:

- **Secure Coding Practices**: Writing code with security in mind to prevent common vulnerabilities.
- **Application Firewalls**: Protecting applications by controlling input, output, and access.
- **Patch Management**: Regularly updating applications to fix security vulnerabilities.
- **Security Testing**: Regularly testing applications for vulnerabilities.

EndPoint Security

4. Endpoint Security

Endpoint security involves securing individual devices that connect to the network, such as computers, smartphones, and tablets. Strategies include:

- **Antivirus Software**: Protecting endpoints from malware.
- **Endpoint Detection and Response (EDR)**: Tools that provide real-time monitoring and response to threats.
- **Device Management Solutions**: Tools to ensure devices comply with security policies.
- **Data Loss Prevention (DLP)**: Measures to prevent data breaches.

Physical Security

5. Physical Security

Physical security protects the actual hardware and facilities of computer systems. Measures include:

- **Controlled Access**: Restricting physical access to facilities and devices.
- **Surveillance**: Monitoring physical locations with cameras and security personnel.
- **Environmental Controls**: Protecting against natural disasters and environmental hazards.
- **Hardware Security Modules (HSMs)**: Devices that provide secure cryptographic processing.

Types of Security Attacks

Malware (malicious software) encompasses a variety of harmful software types designed to damage, disrupt, or gain unauthorized access to computer systems. Common types include:

- **Viruses**: **Attach to legitimate programs and spread** when those programs are executed.
- **Worms**: **Self-replicate** and spread independently across networks.
- **Trojan Horses**: **Disguise** themselves as legitimate software but perform malicious activities.
- **Ransomware**: **Encrypts data and demands payment for decryption.**
- **Spyware**: **Secretly monitors** and collects user information.
- **Adware**: **Displays unwanted advertisements,** often integrated with spyware.

Types of Security attacks

2. Phishing Attacks

Phishing involves tricking individuals into providing sensitive information by masquerading as a trustworthy entity.

3. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

These attacks aim to make a system or network resource unavailable by overwhelming it with traffic.

- **DoS Attacks**: Originating from a single source to flood a target with traffic.
- **DDoS Attacks**: Using multiple compromised systems (botnets) to flood the target simultaneously.

4. Social Engineering Attacks

Types of Security Attacks

4. Man-in-the-Middle (MitM) Attacks

MitM attacks involve intercepting and altering communication between two parties without their knowledge.

- **Eavesdropping**: Listening to private conversations or data transfers.
- **Session Hijacking**: Taking control of a user session.
- **SSL Stripping**: Downgrading HTTPS connections to HTTP to intercept data

Cryptography

It involves converting information into a secure format to ensure privacy, data integrity, and authentication.

1. Encryption and Decryption

- **Encryption**: The process of converting plaintext (readable data) into ciphertext (unreadable data) using an algorithm and an encryption key.
- **Decryption**: The reverse process of converting ciphertext back into plaintext using a decryption key.

Cryptography

2. Types of Encryption

- **Symmetric Encryption**: Uses the same key for both encryption and decryption. It is fast but requires secure key distribution.
  - **Example Algorithms**: AES (Advanced Encryption Standard), DES (Data Encryption Standard).
- **Asymmetric Encryption**: Uses a pair of keys – a public key for encryption and a private key for decryption. It ensures secure key distribution but is slower.
  - **Example Algorithms**: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography).

Cryptography

3. Digital Signatures

Digital signatures provide authentication and integrity for messages. They use **asymmetric** cryptography to ensure that a message was created by a known sender and was not altered.

4.securing email with Pretty Good Privacy (PGP) is a widely used method for ensuring the confidentiality and authenticity of email communications.

WEP

Wired Equivalent Privacy (WEP) is an outdated and insecure security protocol designed to provide a wireless local area network (WLAN) with a level of security and **privacy comparable to that of a wired LAN.**

Purpose: WEP was developed to secure wireless networks by encrypting data transmitted over the air, thus preventing eavesdropping and unauthorized access.

Encryption Algorithm: WEP uses the RC4 stream cipher for encryption and the CRC-32 checksum for data integrity.

While WEP was an early attempt to secure wireless networks, its numerous vulnerabilities and weaknesses made it unsuitable for modern security needs. It has been superseded by WPA and WPA2, which provide much stronger encryption and improved security mechanisms.

SSL and VPN

SSL ensures that all data transmitted between the web server and browser remains encrypted and secure.

SSL (Secure Sockets Layer): The original protocol developed by Netscape. SSL versions 1.0, 2.0, and 3.0 have known vulnerabilities and are considered insecure.

TLS (Transport Layer Security): The successor to SSL, providing improved security and performance. TLS versions 1.0, 1.1, 1.2, and 1.3 are used today, with TLS 1.2 and TLS 1.3 being the most secure and widely adopted.

VPN

A Virtual Private Network (VPN) is a technology that creates a secure and encrypted connection over a less secure network, such as the internet.

Types of VPNs

1. **Remote Access VPN**:
   - Provides secure connections for individual users to a remote network.
   - Commonly used by remote workers to access corporate resources securely.
2. **Site-to-Site VPN**:
   - Connects entire networks to each other, such as multiple office locations of a company.
   - Uses dedicated hardware devices to create secure connections between networks.

Types of VPN

IPsec (Internet Protocol Security):

- Provides secure IP communication by authenticating and encrypting each IP packet in a communication session.
- Commonly used for site-to-site VPNs.

Remote Access:

- Enables employees to securely access company resources from anywhere in the world.

Firewalls

Firewalls are essential security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules.

They act as a barrier between a trusted internal network and untrusted external networks (such as the internet) to prevent unauthorized access and threats.

Types of Firewalls

Packet-Filtering Firewalls: Inspect individual packets and allow or block them based on source and destination IP addresses, port numbers, and protocols.

Stateful Inspection Firewalls: Track the state of active connections and make decisions based on the context of traffic (e.g., whether the packet is part of an established connection).

Proxy Firewalls: Act as intermediaries between end users and the destination server, providing additional content filtering and traffic analysis.

Next-Generation Firewalls (NGFW): Combine traditional firewall capabilities with additional features like application awareness, integrated intrusion prevention, and cloud-delivered threat intelligence.

Firewalls are critical components of network security, providing a first line of defense against external threats and unauthorized access.

RSA Algorithm

- Select two large prime numbers, p and **q**.
- Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
- Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n),

  gcd (e,d(n)) =1
- If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

  $C = m^e$ mod n

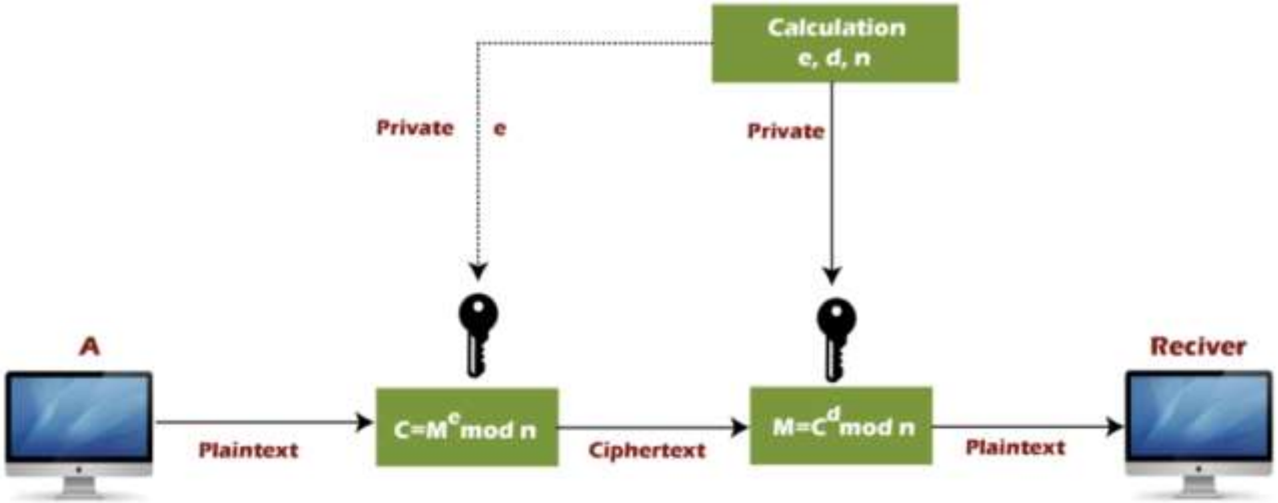
  Here**, m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
- To determine the private key, we use the following formula to calculate the d such that:

  D_e mod {(p - 1) x (q - 1)} = 1

  Or

  D_e mod φ (n) = 1
- The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.

  $m = c^d$ mod n



Calculation
e, d, n

Private e

Private

A

Plaintext

$C=M^e \text{mod } n$

Ciphertext

$M=C^d \text{mod } n$

Plaintext

Reciver

RSA

Numericals

In an RSA cryptosystem, a particular A uses two prime numbers, 13 and 17, to generate the public and private keys. If the public of A is 35. Then the private key of A is ……………?.