📘 Unit 4 : Network Security Applications (Milan)

Key Distribution

- **Definition**: The process of securely delivering cryptographic keys to authorized parties, crucial for cryptography to ensure only intended recipients can decrypt data.
- **Symmetric Key Schemes**: Both parties must acquire a valid shared key, which should be distributed securely between the source and destination, preventing others from accessing it.
- **Key Rotation**: Frequent key changes are desirable to limit the data compromised if an attacker learns the key.
- **Session Keys**: A new session key should be used for each connection. For connectionless protocols, a new session key is used for a fixed period or a certain number of transactions.
- **Preferred Approach**: A trusted third party (like a Key Distribution Center, KDC) can mediate the secure communication between users, especially beneficial for scalability.

Key Distribution Issues

- **Kerberos Protocol**: A network authentication system offering secure communication over insecure networks. It uses symmetric cryptography, distributing session keys and authenticating users via a reliable third party (KDC).
- **Public Key Infrastructure (PKI)**: A system addressing identity authentication, where users receive a digital certificate from a trusted Certificate Authority (CA). The certificate serves as immutable identity verification. In case of compromise, certificates can be revoked and checked against Certificate Revocation Lists (CRLs).
- **Hybrid Key Distribution Scheme**: Combines the use of a KDC for distributing secret session keys with a public key scheme for distributing master keys, improving security and efficiency.

- **Public Key Distribution Methods**:
  - **Public-Key Authority**: A centralized approach requiring real-time access to the authority.
  - **Public-Key Certificates**: Users hold certificates without needing real-time access to the CA.

Key Distribution Center (KDC)

- **Role**: Shares a unique key with each user. In large networks, a hierarchy of KDCs can be established.
- **Local KDC**: Manages key distribution within the same domain.
- **Global KDC**: Communicates across domains when entities from different domains wish to share a key.
- **Decentralization**: Fully decentralized key distribution avoids the need for a trusted KDC but is challenging to implement.

Kerberos

- **Definition**: An authentication protocol that serves as a KDC, popular in systems like Windows 2000. Originally developed at MIT, it has gone through several versions.
- **How Kerberos Works**:
  - **Entities Involved**:
    1. **Client** (Alice).
    2. **Authentication Server (AS)**: Acts as the KDC.
    3. **Ticket-Granting Server (TGS)**: Issues tickets for access to real servers.
    4. **Real Server (Bob)**: Provides services to the user.
  - **Simplified Process**: Once a ticket is obtained, it can be reused for multiple servers with minimal repetition of steps.

Symmetric-Key Agreement

- **Definition**: A method by which two parties, Alice and Bob, can create a session key between themselves without a KDC.

- **Diffie-Hellman Method**: A key exchange algorithm used to securely generate a shared key over a public channel.
  - **Example Calculation**:
    - Alice chooses a secret number (x = 3), Bob chooses (y = 6), and they exchange calculated values using a mathematical formula to derive the same symmetric key.

Public-Key Infrastructures (PKI)

- **Asymmetric-Key Cryptography**: Each user holds a private key and advertises a public key, eliminating the need for a shared secret.
- **Components**:
  1. **Announcing a Public Key**: Broadcasting the public key for others to use.
  2. **Trusted Center**: A Certification Authority (CA) ensures the authenticity of the public key.
  3. **Controlled Trusted Center**: The CA oversees the validation process.
  4. **Certification Authority (CA)**: Issues certificates to verify user identity.

Network Access Control (NAC)

- **Definition**: A security protocol to control access to a network, ensuring only compliant devices or users can connect. It is also known as Network Admission Control.
- **Functions**: Handles network management, security policy enforcement, and access control.
- **Operation**: Works on both wired and wireless networks, identifying devices and users, and setting access rules based on various criteria (e.g., device, location, user rights).

AAA Concepts

- **Authentication**: Verifies if the user is legitimate.
- **Authorization**: Determines what the user is allowed to do.
- **Accounting**: Keeps a record of the user's actions.

- **Components**:
    1. **Supplicant**: The user or device requesting access.
    2. **Authenticator**: The network edge device controlling access.
    3. **Authentication Server**: A remote access or policy server determining access control.

Network Access Enforcement Methods

- **Technologies**:
    - **IEEE 802.1X**: Used in Ethernet and WiFi networks for controlling access.
    - **Firewalls**: Regulate traffic between different network zones.
    - **DHCP Management**: Controls IP assignment based on access rules.
    - **VPN**: Provides secure remote access.
    - **WLANs**: Wireless LAN technologies that require network access control.

Cloud Computing

- **Definition**: The use of remote resources (processor, storage, network, software, services).
- **Service Models**:
    1. **Infrastructure as a Service (IaaS)**: Provides raw computing power (CPU, storage).
    2. **Platform as a Service (PaaS)**: Offers computing infrastructure with an OS.
    3. **Software as a Service (SaaS)**: Delivers software applications over the cloud.
- **Deployment Models**:
    1. **Public Cloud**: Services offered over the public internet.
    2. **Private Cloud**: Services dedicated to a single organization.
    3. **Hybrid Cloud**: A combination of public and private clouds.
    4. **Community Cloud**: Shared infrastructure among several organizations.

- **Key Characteristics**:
    1. **Resource Pooling**: Multiple customers share resources.
    2. **Broad Network Access**: Services accessible from anywhere.
    3. **Rapid Elasticity**: Resources can be scaled quickly.
    4. **Measured Service**: Resource usage is monitored and billed.
    5. **On-Demand Self-Service**: Users can provision resources as needed.

Cloud Security Risks and Countermeasures

1. **Abuse and Criminal Use**: Mitigated by strict user authentication, intrusion detection, and blacklist monitoring.
2. **Malicious Insiders**: Addressed by assessing the Cloud Service Provider (CSP), human resource checks, and security breach notification.
3. **Insecure Interfaces and APIs**: Strengthen with secure models, strong authentication, and encryption.
4. **Shared Technology Issues**: Monitored with access control and frequent vulnerability scans.
5. **Data Loss or Leakage**: Prevented by encrypting data, strong access control, and robust key management.
6. **Service Hijacking**: Countered with two-factor authentication and intrusion detection.
7. **Unknown Risk Profile**: Minimized by disclosing logs and monitoring key infrastructure details.

Data Protection Risks

- **Multi-Instance Model**: Each user has a unique DBMS on a virtual machine, with full control over security policies.
- **Multi-Tenant Model**: Several users share a database environment, with data tagged by subscriber identifier, requiring strong CSP security management.

Cloud Security as a Service (SecaaS)

- **Definition**: Security applications and services delivered via the cloud, either to cloud-based infrastructures or customer on-premise systems.
- **Benefits**:
  - Continuous monitoring of threats.
  - Cybersecurity managed by expert analysts.
  - Quick responses to security breaches.
  - Automation to detect and eliminate threats like spam and malware.
- **Categories of Services**:
  1. Identity and Access Management.
  2. Data Loss Prevention.
  3. Web Security.
  4. Email Security.
  5. Security Assessments.
  6. Intrusion Management.
  7. Security Information and Event Management (SIEM).
  8. Encryption.