310244 – Computer Networks

(2019 Pattern) (Semester - V)

Unit 6	Security	Marks
Introduction, Security services, Need of Security, Key Principles of Security, Threats and Vulnerabilities, Types of Attacks, ITU-T X.800 Security Architecture for OSI, Security Policy and mechanisms, Operational Model of Network Security, Symmetric and Asymmetric Key Cryptography. Security in Network, Transport and Application: Introduction of IPSec, SSL, HTTPS, S/MIME, Overview of IDS and Firewalls.		17

Part 1: Foundations of Network Security

1. Introduction, Security Services, and the Need for Security

Introduction:
Network Security consists of the policies, practices, and technologies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and its resources. It is not a product you can buy, but an ongoing process and a fundamental requirement for any network, from a small home Wi-Fi setup to a massive corporate or government infrastructure.

The Need for Security:
In our digitally connected world, vast amounts of sensitive information are stored and transmitted across networks. The need for security stems from the need to protect these valuable assets.

- **Protecting Assets:** Data is a critical asset. This includes personal information (credit card numbers, health records), corporate secrets (product designs, financial data), and state secrets.
- **Ensuring Business Continuity:** A security breach or a denial-of-service attack can halt business operations, leading to massive financial loss and damage to productivity.
- **Maintaining Reputation and Trust:** Customers and partners will not trust an organization that cannot protect their data. A security breach can cause irreparable damage to a company's reputation.

- **Legal and Regulatory Compliance:** Many industries have strict regulations (like GDPR for data privacy or PCI DSS for credit card information) that mandate security standards and impose heavy fines for non-compliance.

Security Services:
These are the fundamental goals that a security system aims to achieve. They describe *what* the security system should do. The primary services are:

- **Confidentiality:** Ensures that information is not disclosed to unauthorized individuals or systems.
- **Integrity:** Ensures that data has not been altered or destroyed in an unauthorized manner.
- **Availability:** Ensures that systems and data are accessible and usable upon demand by an authorized user.
- **Authentication:** Ensures that the identity of a user or system is genuine. It answers the question, "Are you really who you say you are?"
- **Non-repudiation:** Provides proof that a specific user performed a specific action, preventing them from later denying it. For example, proving that a user digitally signed a contract.

2. Key Principles of Security (The CIA Triad and Beyond)

These core principles are the pillars upon which all security measures are built.

1. **Confidentiality (Secrecy):** This principle is about keeping secrets. It is focused on preventing the unauthorized disclosure of information.
    - **Analogy:** A sealed, opaque envelope. Only the intended recipient can open it and read the letter inside.
    - **Primary Mechanism: Encryption**. By encrypting data, we make it unreadable to anyone who does not possess the correct key.
2. **Integrity (Trustworthiness):** This principle ensures that data is accurate and trustworthy. It guarantees that the information has not been tampered with, altered, or corrupted between sender and receiver.
    - **Analogy:** A tamper-evident seal on a medicine bottle. If the seal is broken, you know not to trust the contents.
    - **Primary Mechanism: Hashing**. A hash function creates a unique, fixed-size fingerprint (a "digest") of the data. If even one bit of the data changes, the

hash will be completely different. The sender sends the data and its hash; the receiver re-calculates the hash and compares it to the one received.

3. **Availability (Accessibility):** This principle ensures that network services and data are available and accessible to authorized users when they need them.
    - **Analogy:** A retail store being open for business during its advertised hours.
    - **Primary Threat: Denial-of-Service (DoS)** and **Distributed Denial-of-Service (DDoS)** attacks, which aim to overwhelm a system with traffic so that it cannot serve legitimate users.
    - **Mechanisms:** Redundancy (backup systems), DDoS mitigation services, and robust infrastructure.

3. Threats, Vulnerabilities, and Types of Attacks

- **Vulnerability:** A weakness or flaw in a system's design, implementation, or operation that could be exploited to violate its security policy.
    - **Example:** Unpatched software, a weak password, a misconfigured firewall.
    - **Analogy:** An unlocked door on a house.
- **Threat:** A potential danger that might exploit a vulnerability.
    - **Example:** A hacker, a piece of malware, a disgruntled employee.
    - **Analogy:** A burglar walking through the neighborhood.
- **Attack:** The actual act of a threat exploiting a vulnerability.
    - **Example:** The hacker using an unpatched flaw to gain access to a server.
    - **Analogy:** The burglar walking through the unlocked door and stealing items.

Types of Attacks:

- **Passive Attacks:** The attacker's goal is to obtain information without altering system resources. They are difficult to detect because they do not change any data.
    - **Eavesdropping (or Sniffing):** Intercepting and reading traffic on a network.
    - **Traffic Analysis:** Even if the traffic is encrypted, an attacker can learn valuable information by observing the patterns of communication (who is talking to whom, how often, and how much data is being sent).
- **Active Attacks:** The attacker's goal is to alter system resources or affect their operation. They are easier to detect but more damaging.
    - **Masquerade (Spoofing):** An attacker pretends to be a different, legitimate entity. (e.g., IP spoofing, email spoofing).

- **Replay Attack:** The attacker intercepts a legitimate transmission (e.g., a login request) and fraudulently re-transmits it later to gain unauthorized access.
- **Modification of Messages:** The attacker alters the contents of a legitimate message in transit.
- **Denial of Service (DoS):** The attacker prevents legitimate users from accessing a service, typically by flooding the server with traffic.

4. ITU-T X.800 Security Architecture for OSI

This is a formal framework that provides a systematic way to define and provide security requirements. It structures the security problem into three parts:

1. **Security Attacks:** As defined above (Passive and Active). This part defines what you are trying to defend against.
2. **Security Mechanisms:** These are the specific tools, algorithms, and protocols that are used to implement the security services. Examples include **Encryption, Digital Signatures, Access Control Mechanisms, Data Integrity checks (hashing), and Traffic Padding**.
3. **Security Services:** As defined above (Confidentiality, Authentication, Integrity, Non-repudiation, and Access Control). This part defines the goals you are trying to achieve.

The architecture shows how **Mechanisms** are used to provide **Services** that counter **Attacks**.

5. Security Policy, Mechanisms, and Operational Model

- **Security Policy:** A high-level document that outlines an organization's security goals, rules, and procedures. It defines *what* needs to be protected and *why*. It is a strategic plan, not a technical implementation guide.
  - **Example:** "All sensitive customer data must be encrypted both in transit and at rest. Access to this data is restricted to authorized personnel from the customer service department only."

- **Security Mechanisms:** These are the technical tools and processes used to enforce the security policy. They are the "how" of security. Examples include firewalls, antivirus software, intrusion detection systems, and encryption libraries.
- **Operational Model of Network Security:** Security is not a one-time project; it's a continuous, cyclical process. A common operational model is:

1. **Protect:** Implement security mechanisms (firewalls, encryption, access controls) based on the security policy to defend the network.
2. **Detect:** Continuously monitor the network for signs of an attack or a policy violation using tools like Intrusion Detection Systems (IDS) and log analysis.
3. **Respond:** When an incident is detected, execute a pre-planned incident response plan to contain the damage, eradicate the threat, and recover normal operations.
4. **Improve:** Analyze the incident to understand what went wrong and use that knowledge to update the security policy and improve the protection mechanisms.

6. Symmetric and Asymmetric Key Cryptography

Cryptography is the science of secure communication. It provides the mechanisms for confidentiality and integrity.

A. Symmetric Key Cryptography

- **Core Idea:** Uses a **single, shared secret key** for both encrypting and decrypting data.
- **How it Works:** The sender encrypts the plaintext message with the shared key. The receiver uses the exact same key to decrypt the ciphertext back into plaintext.
- **Analogy:** A physical key to a door lock. Anyone who has a copy of the key can both lock (encrypt) and unlock (decrypt) the door.
- **Strengths:**
  - **Extremely Fast:** Symmetric algorithms are computationally very efficient, making them ideal for encrypting large amounts of data.
- **Weaknesses:**
  - **Key Distribution Problem:** How do you securely share the secret key with the other party in the first place? Sending it over an insecure channel would defeat the purpose.
  - **Scalability:** In a network of *n* users, you would need n(n-1)/2 unique keys for every pair of users to communicate securely. This becomes unmanageable very quickly.

- **Examples:** AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES.

B. Asymmetric Key Cryptography (Public-Key Cryptography)

- **Core Idea:** Uses a **pair of mathematically related keys** for each user: a **public key** and a **private key**.
  - **Public Key:** Can be shared with anyone in the world.
  - **Private Key:** Must be kept secret by the owner.
- **How it Works (for Encryption):** To send a secret message *to* Bob, Alice looks up Bob's public key. She encrypts her message with Bob's public key. The resulting ciphertext can **only** be decrypted by Bob's private key.
- **Analogy:** A mailbox with a mail slot. The mail slot (public key) is open to the public, so anyone can drop a letter in. But only the owner with the physical key (private key) can open the mailbox and read the letters.
- **Strengths:**
  - **Solves the Key Distribution Problem:** There is no need to secretly share a key. You just need to find a trusted copy of the recipient's public key.
  - **Enables Digital Signatures:** To create a digital signature, a user encrypts a hash of a message with their *own private key*. Anyone can then use the sender's public key to decrypt it and verify that the message came from them and has not been altered (provides authentication, integrity, and non-repudiation).
- **Weaknesses:**
  - **Extremely Slow:** Asymmetric cryptography is computationally very intensive, making it unsuitable for encrypting large amounts of data.
- **Examples:** RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography).

The Hybrid Approach (How the Real World Works):
Because of the speed difference, modern systems like SSL/TLS use a hybrid of both:

1. Use slow **Asymmetric cryptography** to securely establish a connection and exchange a randomly generated, one-time-use **symmetric key** (called a "session key").
2. Use the now-shared, fast **Symmetric session key** to encrypt all the actual data for the rest of the communication session.

Part 2: Security Protocols and Mechanisms in Practice

7. Security in the Network, Transport, and Application Layers

Security can be applied at different layers of the network stack, providing different types of protection.

- **IPSec (at the Network Layer - Layer 3):**
  - **Introduction:** IP Security (IPSec) is a suite of protocols that provides security for all IP traffic between two endpoints. Because it operates at the Network Layer, it is **transparent to applications**.
  - **Function:** It can encrypt and/or authenticate every single IP packet, making it ideal for creating **Virtual Private Networks (VPNs)**, which securely connect a remote user to a corporate network or link two corporate sites over the public internet.
- **SSL/TLS (at the Transport Layer - Layer 4):**
  - **Introduction:** Secure Sockets Layer (SSL) and its modern successor, Transport Layer Security (TLS), are cryptographic protocols designed to provide secure communication over a network.
  - **Function:** SSL/TLS operates between the Application Layer and the Transport Layer. It creates a secure, encrypted "tunnel" through which application data (like HTTP requests) can pass safely. It provides confidentiality (encryption), integrity (message authentication codes), and authentication (server and optional client certificates).
- **HTTPS (at the Application Layer - Layer 7):**
  - **Introduction:** HTTPS (Hypertext Transfer Protocol Secure) is not a separate protocol. It is simply the standard **HTTP protocol running on top of a secure SSL/TLS connection**.
  - **Function:** It secures web traffic between your browser and a web server. When you see https:// and a padlock icon in your browser's address bar, it means your connection to that website is encrypted and authenticated using SSL/TLS.
- **S/MIME (at the Application Layer - Layer 7):**
  - **Introduction:** Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for providing cryptographic security for email.

- **Function:** Unlike SSL which secures the connection, S/MIME secures the **email message itself**. It allows a user to send encrypted emails (confidentiality) and digitally signed emails (authentication, integrity, and non-repudiation), which remain secure even when stored on a mail server.

8. Overview of IDS and Firewalls

These are two of the most fundamental network defense technologies.

A. Firewalls

- **What it is:** A network security device that monitors and controls incoming and outgoing network traffic based on a predetermined set of security rules.
- **Analogy:** A security guard at the single gate of a walled compound. The guard checks the ID of everyone trying to enter or leave and only lets authorized people and vehicles pass.
- **Primary Function:** To act as a barrier between a trusted internal network (your corporate LAN) and an untrusted external network (the Internet), preventing unauthorized access. Firewalls are a form of **preventative control**.
- **How they work:** They filter traffic based on rules that can use IP addresses, port numbers, and connection states.

B. Intrusion Detection Systems (IDS)

- **What it is:** A device or software application that monitors a network or systems for malicious activity or policy violations.
- **Analogy:** The security cameras and alarm systems *inside* the compound. They don't stop anyone at the gate, but they watch for suspicious behavior inside and raise an alarm if they see something wrong.
- **Primary Function:** To **detect** attacks that may have bypassed the firewall or originated from within the network. An IDS is a form of **detective control**.
- **How they work:**
  - **Signature-based IDS:** Looks for patterns (signatures) that match known attacks (like a specific malware string). This is effective against known threats but cannot detect new attacks.

    - **Anomaly-based IDS:** Creates a baseline of normal network behavior and then flags any deviation from that baseline as potentially malicious. This can detect new attacks but can also have a high rate of false positives.
- **Intrusion Prevention System (IPS):** An IPS is an evolution of an IDS. It has all the detection capabilities of an IDS but can also take active steps to **block** the malicious traffic in real-time.

Summary Points :

Part 1: Security Fundamentals

- **Need for Security:** To protect valuable assets (data), ensure business continuity, maintain trust, and comply with legal regulations.
- **Key Principles (The CIA Triad):**
    - **Confidentiality:** Keeping information secret and private (achieved with **Encryption**).
    - **Integrity:** Ensuring data is not altered or tampered with (achieved with **Hashing**).
    - **Availability:** Ensuring systems and data are accessible to authorized users (defends against **DoS attacks**).
- **Key Security Services:** The CIA triad plus:
    - **Authentication:** Verifying identity ("Are you who you say you are?").
    - **Non-repudiation:** Proving an action was taken by a specific user (achieved with **Digital Signatures**).
- **Threats & Vulnerabilities:** A **threat** (e.g., a hacker) exploits a **vulnerability** (e.g., a software bug) to launch an **attack**.
- **Types of Attacks:**
    - **Passive:** Eavesdropping and traffic analysis (hard to detect).
    - **Active:** Modifying data, impersonating users (masquerade/spoofing), or denying service (DoS).
- **Cryptography:**
    - **Symmetric Key:** Uses **one shared secret key** for both encryption and decryption. It is **very fast** but has a major **key distribution problem**. (e.g., AES).
    - **Asymmetric Key (Public-Key):** Uses **two keys**: a public key to encrypt and a private key to decrypt. It is **very slow** but solves the key distribution problem and enables **digital signatures**. (e.g., RSA).

- **Hybrid System:** The standard approach used in practice. Asymmetric crypto is used to securely exchange a fast symmetric key, which is then used to encrypt the actual data.

Part 2: Security in Practice

- **Security at Different Layers:**
  - **IPSec (Network Layer 3):** Secures all IP traffic between two points. Ideal for **VPNs**. Transparent to applications.
  - **SSL/TLS (Transport Layer 4):** Creates a secure "tunnel" for application data. The foundation of secure web communication.
  - **HTTPS (Application Layer 7):** This is simply HTTP running over an SSL/TLS connection. Indicated by the https:// prefix.
  - **S/MIME (Application Layer 7):** Secures the email message itself through encryption and digital signatures, not just the connection.
- **Key Defense Mechanisms:**
  - **Firewall:** A **preventative** control that acts as a barrier between a trusted and an untrusted network. It filters traffic based on a set of rules (IP addresses, ports).
  - **Intrusion Detection System (IDS):** A **detective** control that monitors network traffic for malicious activity or policy violations and raises an alarm.
    - **Signature-based IDS:** Detects known attacks by matching patterns.
    - **Anomaly-based IDS:** Detects unknown attacks by identifying deviations from normal behavior.
  - **Intrusion Prevention System (IPS):** An IDS that can also actively **block** the detected malicious traffic in real-time.