MCPE2017 NETWORK SECURITY (3-0-0)

Syllabus

Course Objective:
This course provides an essential study of network security issues and methods in networking systems.

Module 1: Introduction to Network security, Model for Network security, Model for Network access security, Real-time Communication Security: Introduction to TCP/IP protocol stack, Implementation layers for security protocols and implications, IPsec: AH and ESP, IPsec: IKE.

Module 2: Media- Based-Vulnerabilities, Network Device Vulnerabilities, Back Doors, Denial of Service (DoS), Spoofing, Man-in-the-Middle, and replay, Protocol -Based Attacks, DNS Attack, DNS Spoofing, DNS Poisoning, ARP Poisoning, TCP/IP Hijacking, Virtual LAN (VLAN), Demilitarization Zone (DMZ) , Network Access Control (NAC), Proxy Server, Honey Pot, Network Intrusion Detection Systems (NIDS) and Host Network Intrusion Prevention Systems Protocol Analyzers, Internet Content Filters, Integrated Network Security Hardware.

Module 3: Authentication: Kerberos, X.509 Authentication Service, Scanning: Port Scanning, Port Knocking- Advantages, Disadvantages. Peer-to-peer security. Electronic Mail Security: Distribution lists, Establishing keys, Privacy, source authentication, message integrity, non-repudiation, proof of submission, proof of delivery, message flow confidentiality, anonymity, Pretty Good Privacy (PGP)

Module 4: Firewalls and Web Security: Packet filters, Application-level gateways, Encrypted tunnels, Cookies. Assignments on the latest network security techniques, Security applications in wireless sensor networks and wireless Communication networks.

Course Outcome:
Students can get knowledge about the network security, implementation and requirements after the successful completion of the course

Text Book:
William Stallings, “Cryptography and Network Security – Principles and Practices”, Prentice Hall of India, Third Edition, 2003.

References:
1. Saadat Malik, Saadat Malik. “Network Security Principles and Practices (CCIE Professional Development)”. Pearson Education. 2002. (ISBN: 1587050250).
2. Cisco: Fundamentals of Network Security Companion Guide (Cisco Networking Academy Program).
3. Mark Ciampa “Security + Guide to Network Security Fundamentals/Edition 3” Cengage Learning publisher, ISBN-10: 1428340661, ISBN-13: 978-1428340664.

Module-I

Introduction to Network Security

Network Security is used to protect both equipment and information. Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit. Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

• Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers.

• Network Security - measures to protect data during their transmission.

• Internet Security - measures to protect data during their transmission over a collection of interconnected networks.

Need for Network Security

With the rapid growth of the Internet and network-based communication, security threats such as hacking, malware, data theft, and cyber attacks have increased. Network security helps to:

- Protect sensitive information
- Prevent unauthorized access
- Maintain data integrity
- Ensure system availability
- Protect network resources

Goals of Network Security

1. **Confidentiality**

Ensures that information is accessible only to authorized users.
Example: Encryption of data during transmission.

2. **Integrity**

Ensures that data is not altered or modified during transmission.

3. **Authentication**

Verifies the identity of users or devices communicating over the network.

4. **Authorization**

Determines the level of access a user has to network resources.

5. **Availability**

Ensures that network services are available to authorized users when required.

6. **Non-repudiation**

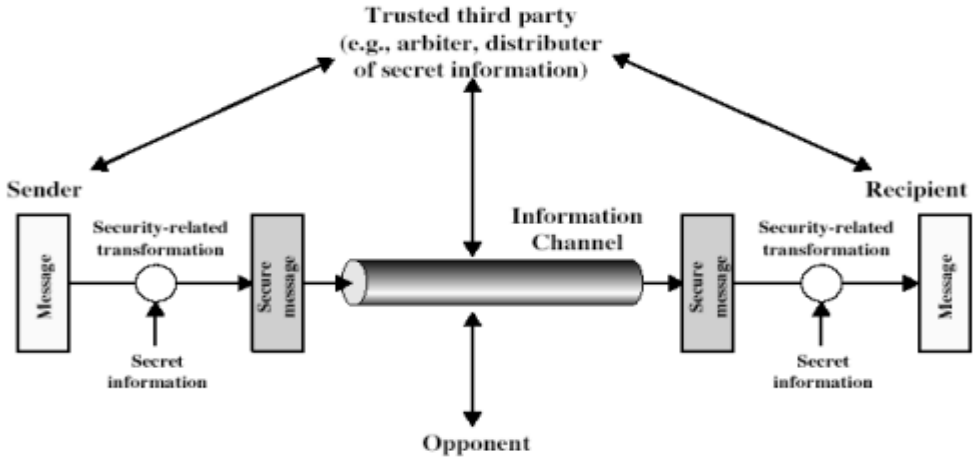
Prevents a sender from denying that they sent a message.

MODEL FOR NETWORK SECURITY

A **Network Security Model** describes how security services are applied to protect information transmitted across networks.

Components of Network Security Model-

1. Sender
2. Receiver
3. Message/Data
4. Security Transformation (Encryption)
5. Secret Key
6. Trusted Third Party
7. Attacker

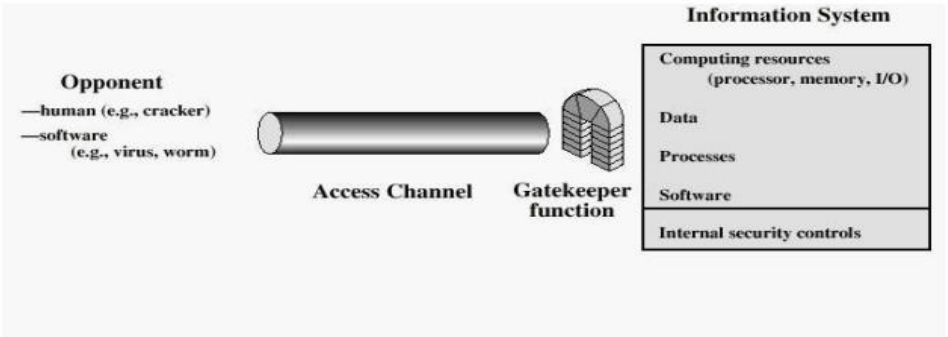


1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.



Data is transmitted over network between two communicating parties, who must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination by use of communication protocols by the two parties. Whenever an opponent presents a threat to confidentiality, authenticity of information, security aspects come into play. Two components are present in almost all the security providing techniques. A security-related transformation on the information to be sent making it unreadable by the opponent, and the addition of a code based on the contents of the

message, used to verify the identity of sender. Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception A trusted third party may be needed to achieve secure transmission. It is responsible for distributing the secret information to the two parties, while keeping it away from any opponent. It also may be needed to settle disputes between the two parties regarding authenticity of a message transmission. The general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose

2. Generate the secret information to be used with the algorithm

3. Develop methods for the distribution and sharing of the secret information

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service Various other threats to information system like unwanted access still exist.

The existence of hackers attempting to penetrate systems accessible over a network remains a concern. Another threat is placement of some logic in computer system affecting various applications and utility programs. This inserted code presents two kinds of threats. Information access threats intercept or modify data on behalf of users who should not have access to that data Service threats exploit service flaws in computers to inhibit use by legitimate users Viruses and worms are two examples of software attacks inserted into the system by means of a disk or also across the network. The security mechanisms needed to cope with unwanted access fall into two broad categories.

Module-II

Lecture Notes: Network Security & Vulnerabilities

1. Network Vulnerabilities and Attack Methods

Media Bars (Removable Media) Vulnerability

- **Definition:** Security risks associated with physical ports (USB, external drives).
- **Risk:** Auto-run features can execute malicious code immediately upon connection.

These are often used for data exfiltration or spreading "worms" in air-gapped systems.

Backdoors

- **Definition:** A method of bypassing normal authentication in a cryptosystem or algorithm.
- **Origin:** Can be installed by developers for troubleshooting or by attackers via malware to maintain persistent access to a system.

Denial of Service (DoS)

- **Objective:** To make a machine or network resource unavailable to its intended users.
- **Mechanism:** Flooding the target with superfluous requests to overload systems.

Distributed Denial of Service (DDoS) involves multiple compromised systems (botnets) attacking a single target.

Spoofing

- **Definition:** An attack where a person or program successfully masquerades as another by falsifying data.
- **Common Types:** IP spoofing, Email spoofing, and MAC spoofing.

Man-in-the-Middle (MitM)

- **Definition:** The attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
- **Requirement:** The attacker must be able to intercept all relevant messages passing between the two victims.

Replay Attack

- **Definition:** A form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.
- **Example:** Capturing a login packet and re-sending it later to gain unauthorized access.

2. Protocol-Based Attacks

DNS Attacks & DNS Poisoning

- **DNS Attack:** Targeting the Availability of the Domain Name System (e.g., hitting Root Servers).

- **DNS Poisoning (Cache Poisoning):** Corrupting the DNS server's cache so that it returns an incorrect IP address, diverting traffic to the attacker's malicious website.

ARP Poisoning

- **Mechanism:** Sending falsified ARP (Address Resolution Protocol) messages over a local area network.
- **Goal:** To link the attacker's MAC address with the IP address of a legitimate server or gateway, enabling MitM or DoS attacks.

TCP/IP Hijacking

- **Definition:** The attacker takes over a TCP session between two entities.
- **Process:** Since most authentication occurs at the start of a TCP session, the attacker waits for the session to be established and then "snatches" it by spoofing the victim's IP and predicting sequence numbers.

3. Network Architecture &Defense Mechanisms

Virtual LAN (VLAN)

- **Definition:** A logical grouping of network users and resources connected to administratively defined ports on a switch.
- **Security Benefit:** Provides segmentation, ensuring that sensitive data traffic is isolated from the rest of the network.

Demilitarized Zone (DMZ)

- **Definition:** A physical or logical subnetwork that contains and exposes an organization's external-facing services (e.g., Web, Email, DNS) to an untrusted network (the Internet).
- **Purpose:** Acts as a buffer; if a DMZ server is compromised, the internal network remains protected behind a second firewall.

Network Access Control (NAC)

- **Definition:** An approach to computer security that attempts to unify endpoint security technology, user or system authentication, and network security enforcement.
- **Function:** Inspects devices for compliance (e.g., updated antivirus) before allowing them to connect.

Proxy Server

- **Definition:** An intermediary server between a client and the internet.
- **Security Use:** Hides internal IP addresses, filters malicious content, and caches data to improve performance.

Honeypot

- **Definition:** A decoy system designed to be probed, attacked, or compromised.
- **Purpose:** To distract attackers from production systems and to study their methods.

4. Monitoring and Specialized Hardware

IDS vs. IPS

- **NIDS (Network Intrusion Detection System):** Monitors network traffic for suspicious activity and issues alerts. It is **passive**.
- **HIPS (Host Intrusion Prevention System):** Installed on a specific host to monitor and **block** malicious activity. It is **active**.

Protocol Analyzers (Sniffers)

- **Definition:** Tools (like Wireshark) used to capture and analyze signals and data traffic over a communication channel.
- **Use:** Troubleshooting network issues or identifying unencrypted sensitive data.

Internet Content Filters

- **Function:** Software or hardware used to restrict access to specific websites or types of content (e.g., blocking social media in a corporate environment).

Integrated Network Security Hardware

- **UTM (Unified Threat Management):** A single hardware appliance that provides multiple security functions, including firewall, VPN, anti-spam, and content filtering.
- **Next-Generation Firewall (NGFW):** Combines a traditional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection (DMI)

Module-III

Advanced Authentication and Email Security

Advanced Authentication Frameworks

Kerberos

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

Mechanism: It uses a “Trusted Third Party” known as the Key Distribution Center (KDC), which consists of the Authentication Service (AS) and the Ticket Granting Service (TGS).

Process: Instead of sending passwords over the network, users receive “tickets” that prove their identity to various services.

Key Features: Single Sign-On (SSO) capability and mutual authentication (both the user and the server prove their identity).

X.509 Certificates

X.509 is a standard format for Public Key Certificates. It is the foundation for HTTPS and SSL/TLS security.

Structure: Contains the public key, the identity of the owner (Subject), and the digital signature of the Certificate Authority (CA) that issued it.

Role: It binds a public key to a specific entity, ensuring that when you communicate with a website, you are using the correct public key for that specific organization.

Network Reconnaissance & Access

Port Scanning

Definition: Sending requests to a range of server port addresses on a host to find out which ports are “open” (listening).

Purpose: Used by administrators for verifying security policies and by attackers to identify potential points of entry.

Port Knocking

Definition: A method of externally opening ports on a firewall by generating a specific sequence of connection attempts to closed ports.

Advantages: * Stealth: The protected service (like SSH) appears closed to standard scanners.

Layered Defense: Provides an extra layer of authentication before a service is even visible.

Disadvantages:

Complexity: Can be difficult to manage and prone to sequence errors.

Single Point of Failure: If the “knocking” daemon fails, the legitimate user is locked out.

1. Electronic Mail (Email) Security Concepts

Email security aims to protect the content and the transaction of messages.

Core Security Requirements

Privacy (Confidentiality): Ensuring only the intended recipient can read the message (usually via encryption).

Secure Authentication: Verifying that the sender is who they claim to be.

Message Integrity: Ensuring the message was not altered during transit (achieved via hashing/digital signatures).

Non-repudiation: The sender cannot later deny having sent the message, as it is cryptographically signed.

Delivery and Submission Features

Proof of Submission: A receipt issued by the mail server confirming it has accepted the message for delivery.

Proof of Delivery: A receipt confirmed by the recipient’s system that the message reached its destination.

Message Flow Confidentiality: Hiding the patterns of communication (who is talking to whom and how often).

Anonymity: Removing all identifying information from the mail headers to protect the sender’s identity.

Distribution Lists and Key Establishment

Distribution Lists: Security must ensure that when a message is sent to a group, all members receive a copy they can decrypt, which requires complex Key Establishment (sharing the session key securely with every recipient in the list).

Pretty Good Privacy (PGP)

PGP is a popular data encryption and decryption program that provides cryptographic privacy and authentication for online communication.

The “Web of Trust”: Unlike the centralized X.509 CA model, PGP uses a decentralized model where users sign each other’s keys to verify identities.

Functionality:

It uses Hashing for integrity.

It uses Public-key cryptography for key distribution.

It uses Symmetric-key cryptography for bulk data encryption (as it is faster).

Peer-to-Peer Security: Since PGP can be implemented directly by users without a central authority, it is a primary tool for securing peer-to-peer communications.

Integrated Network Security Hardware

UTM (Unified Threat Management): A single appliance that handles firewalls, VPNs, and antivirus.

Internet Content Filters: Hardware-level filters that block unauthorized web content before it enters the internal network.

Are there specific attack scenarios or protocol details you'd like to dive into further?

Module-IV

Firewall Architectures and Web Security

Firewall Technologies

Firewalls act as the primary barrier between a trusted internal network and an untrusted external network (the Internet).

Packet Filter (Stateless)

Definition: Operates at the Network Layer (Layer 3) and Transport Layer (Layer 4) of the OSI model.

Mechanism: It examines each packet individually based on a set of rules (ACLs). It checks the source/destination IP addresses, port numbers, and protocol types.

Pros: High speed and transparent to users.

Cons: Vulnerable to IP spoofing; cannot inspect the "payload" or application-level data.

Application-Level Gateway (Proxy Firewall)

Definition: Operates at the Application Layer (Layer 7).

Mechanism: Acts as an intermediary (proxy). A client connects to the gateway, which then evaluates the request and initiates a new connection to the destination.

Pros: Full visibility into application data (e.g., filtering specific HTTP commands). It hides internal network addresses.

Cons: Higher processing overhead; can lead to performance bottlenecks.

Web Security & Privacy

Encrypted Tunnels

Definition: A secure "pipe" created over an insecure network using encryption.

Mechanism: Uses protocols like IPsec or SSH to encapsulate data.

Use Case: Often used in Virtual Private Networks (VPNs) to allow remote workers to access corporate resources securely.

Cookies

Definition: Small pieces of data stored on the user's browser by a website.

Security Risk: While used for session management (keeping you logged in), they can be stolen via Cross-Site Scripting (XSS) or used for unauthorized tracking.

Defense: Using the Secure and HttpOnly flags prevents cookies from being accessed by scripts or sent over unencrypted connections.

Security in Wireless Networks

Wireless communication is inherently more vulnerable because the medium (the air) is open to everyone.

Wireless Communication Networks

WPA3 (Wi-Fi Protected Access 3): The latest standard providing stronger individual data encryption and protection against brute-force password guessing.

EAP (Extensible Authentication Protocol): A framework used in enterprise Wi-Fi to provide various authentication methods (like digital certificates).

Wireless Sensor Networks (WSN)

Characteristics: These networks consist of small, battery-powered sensors (e.g., in smart agriculture or industrial monitoring).

Security Challenges: Limited processing power and memory make traditional heavy encryption impossible.

Common Attacks: * Jamming: Flooding the radio frequency to prevent sensors from communicating.

Sybil Attack: A single malicious node claims multiple identities to gain influence.

Sinkhole Attack: A compromised node attracts all traffic from neighbors by faking a “shortest path” to the base station.

Assignment: Latest Network Security Techniques

Objective: Research and analyze the shift from traditional perimeter security to modern, identity-centric models.

Zero Trust Architecture (ZTA): Explain the principle of “Never Trust, Always Verify.” How does it differ from traditional firewall-based security?

Extended Detection and Response (XDR): Investigate how XDR integrates data from endpoints, networks, and cloud workloads to provide a unified security view.

Secure Access Service Edge (SASE): Describe how SASE combines network security functions (like FWaaS and Cloud SWG) with WAN capabilities to support a mobile workforce.

AI/ML in Threat Hunting: Provide two examples of how Machine Learning is used to detect “Zero-Day” vulnerabilities that traditional signatures might miss.

Comparison Table: Firewall Types

Feature	Packet Filter	Application Gateway
OSI Layer	Network / Transport (3 & 4)	Application (7)
Performance	Very Fast	Slower (High Overhead)
Security	Low (Stateless)	High (Full Content Inspection)
Visibility	Header only	Full Data Payload