OSTIM TECHNICAL UNIVERSITY

Information Security - Nargiz Khankishiyeva

IP Security

Baghirli Arifali

-

Sena Dikmeci

What is IP?

IP (Internet Protocol) is a set of rules that governs how data is sent and received over the internet or local networks. It assigns unique addresses to devices so they can communicate with each other. Think of it like a postal system that ensures your data packets reach the correct destination.

IPV4

10.10.10.1

IPV6

2001:db8:3333:4444:5555:6666:7777:8888

Big Three
TCP-IP-UDP

Building Blocks of Network Communication

- IP handles addressing and routing — like assigning a home address to every device.
- TCP ensures reliable delivery — think of it as tracked, signed-for mail.
- UDP offers fast, connectionless transfer — ideal for real-time applications like gaming or video calls.

Transmission Control Protocol

TCP is a connection-oriented protocol that ensures reliable communication.
It checks for errors, ensures all packets arrive, and reassembles them in the correct order.
It’s ideal for tasks like web browsing, emailing, and file transfers where accuracy matters.

TCP is reliable and orderly but slower due to connection setup and checks.

User Datagram Protocol

UDP is a connectionless protocol that sends data without waiting for acknowledgments.

It’s faster than TCP but doesn't guarantee delivery or order of packets.

It’s commonly used in streaming, online gaming, and real-time voice or video applications.

UDP is fast and lightweight but doesn’t ensure packet delivery or order.

TCP vs UDP & Relation with IP

TCP and UDP are two transport protocols that operate on top of the Internet Protocol.
Both use IP addresses to send data across networks, but they handle data transmission very differently.
TCP is connection-oriented, meaning it establishes a reliable connection before sending data.
It ensures that all packets arrive correctly and in the right order,
making it suitable for web browsing, emails, and file transfers.
UDP, on the other hand, is connectionless and does not guarantee delivery, order, or error checking.
It sends data faster with less overhead,
making it ideal for real-time applications like video calls and online games.
While IP handles addressing and routing, TCP and UDP define how the data should be transferred once it reaches its destination.

IPSec

internet protocol security

- suite of protocols that adds security features to IP communication, such as encryption, authentication, and data integrity.
- works directly at the network layer, protecting all data regardless of the application or transport protocol used.
- commonly used in VPNs to create secure tunnels between devices over untrusted networks like the internet.

Key Functions of IPSec

Authentication

Verifies that data comes from a trusted source.

Encryption

Scrambles the data so no one else can read it.

Integrity

Ensures that the data hasn’t been altered in transit.

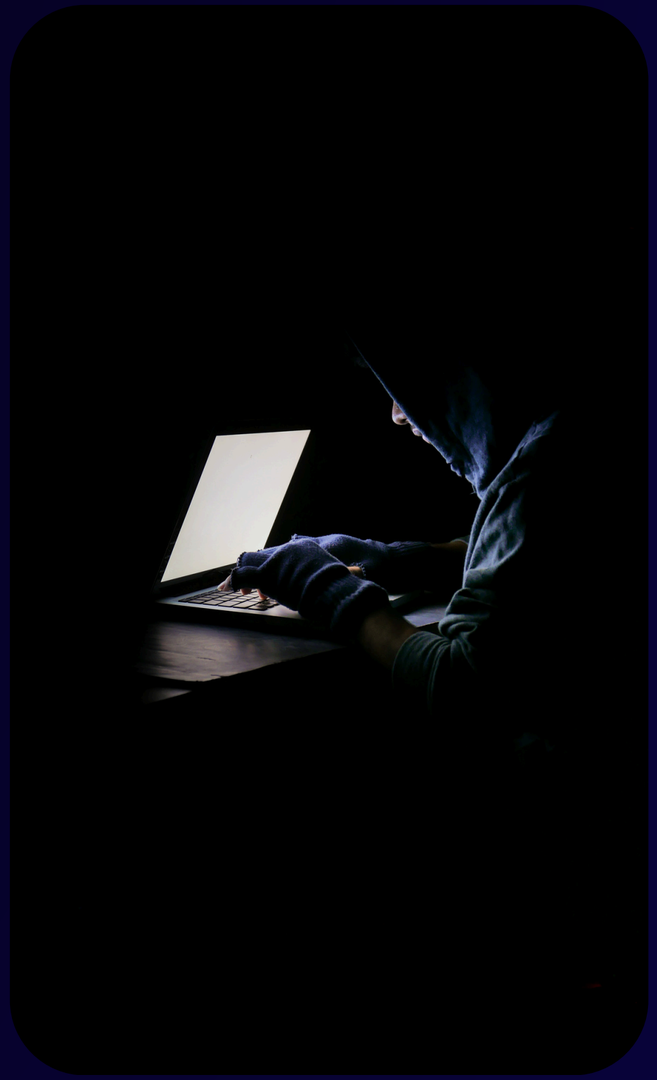
Anti-Replay

Prevents attackers from capturing and re-sending old packets.

Threats Vulnerabilties Attack Vectors

- **How hackers exploit unsecured IP communication**
- **IP spoofing, MITM,DDoS**
- **IP-level hacks**
- **How to protect?**

While IP is essential for connecting devices, its lack of built-in security makes it a prime target for attackers.
From IP spoofing to large-scale DDoS attacks, we'll explore how hackers exploit these weaknesses—and why understanding them is the first step to effective protection.



THREATS

Known menances

IP by itself lacks encryption, authentication, and verification mechanisms.
This opens the door to threats like IP spoofing, packet sniffing, and man-in-the-middle attacks.
These vulnerabilities can lead to data theft, session hijacking, or denial of service.

VULNERABILITIES

Known vulnerabilities

Attackers can exploit protocol flaws, misconfigurations, or outdated systems to gain access.

Common vulnerabilities include unfiltered ports, predictable sequence numbers, and weak routing controls.

These weaknesses often serve as entry points for more advanced network attacks.

ATTACKS

Common IP-Based Attacks

- IP Spoofing

Attackers fake a source IP address to impersonate another device and bypass trust-based systems.

- Packet Sniffing

Captures network traffic to steal credentials, sensitive info, or session tokens—especially dangerous on open networks.

- Man-in-the-Middle (MITM)

Hackers silently intercept and possibly alter communication between two parties without either knowing.

- Denial of Service (DoS/DDoS)

Overwhelms a server or network with excessive traffic, causing slowdowns or complete shutdowns.

- Session Hijacking

Takes control of an active user session by stealing cookies or tokens, often used for account takeovers.

Secure yourselves

- Use IPsec to encrypt and authenticate IP traffic
- Apply firewall rules to block suspicious or unused ports
- Use secure protocols (HTTPS, SSH, SFTP instead of FTP or Telnet)
- Regularly update software to patch network vulnerabilities
- Enable intrusion detection/prevention systems (IDS/IPS)
- Avoid public Wi-Fi or use VPN for remote connections

How to avoid threats?

CONCLUSION

- IP is the foundation of modern communication
- Without protection, it's a gateway for attacks
- IPsec and proper configuration are crucial defenses
- Awareness is your first line of security
- IP is the foundation of modern communication
- Without protection, it's a gateway for attacks
- IPsec and proper configuration are crucial defenses
- Awareness is your first line of security
- TCP and UDP shape how data flows across the internet
- Hackers often exploit weak or exposed IP layers
- Secure networks require both tools and good practices
- Education and vigilance are key to staying ahead

thank you for your attention.
stay safe