Networks & Network Security

CISC 3325 — CUNY Brooklyn College
Lecture Notes

In this chapter, we will:

1. Define "Network", "Networking", and "Protocol".
2. Introduce three network categories: LAN, WAN, and MAN.
3. Discuss the OSI and TCP/IP models.
4. Analyze common types of attacks on networks.
5. Learn how to control/prevent attacks on networks.

Networks & Network Security: Definitions

Before we discuss network vulnerabilities and threats, we should understand why such threats exist. In order to understand this, we need to know the basics of computer communication and networking.

A **network** connects two or more computers to communicate with each other or for the exchange of information among the systems. In basic communication, there are three components involved: the sender, the receiver, and the media. **Networking** is the activity of sharing of resources within the network.

In order to comprehend the information that is being exchanged between the sender and the receiver, the communication "protocol" could be common "language." A **protocol** is a set of rules defined by the communication channel in order to comprehend the information that is being exchanged. For example, and in normal human communication, the protocol is a common human language understood by both the parties.

The use of appropriate (computer) systems or network components with deployment of appropriate protocols ensures effective communication among the systems.

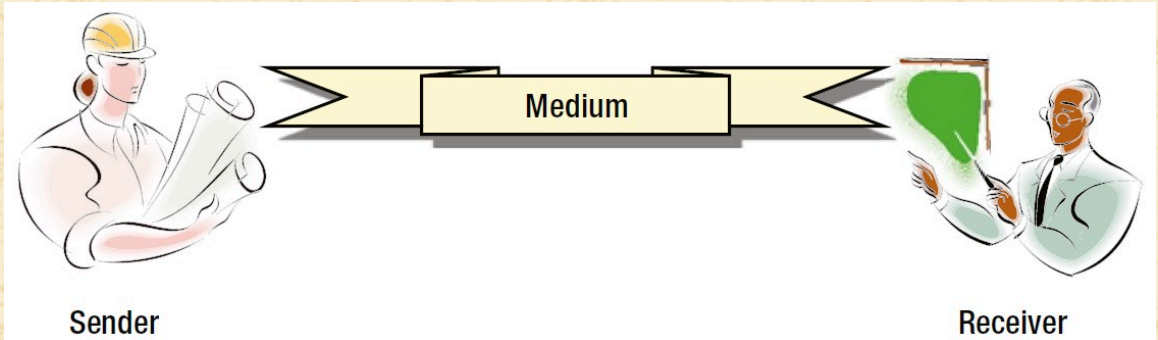


Figure 9-1. *Basic communication*

"Figure 9-1: Basic communication" (page 187), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

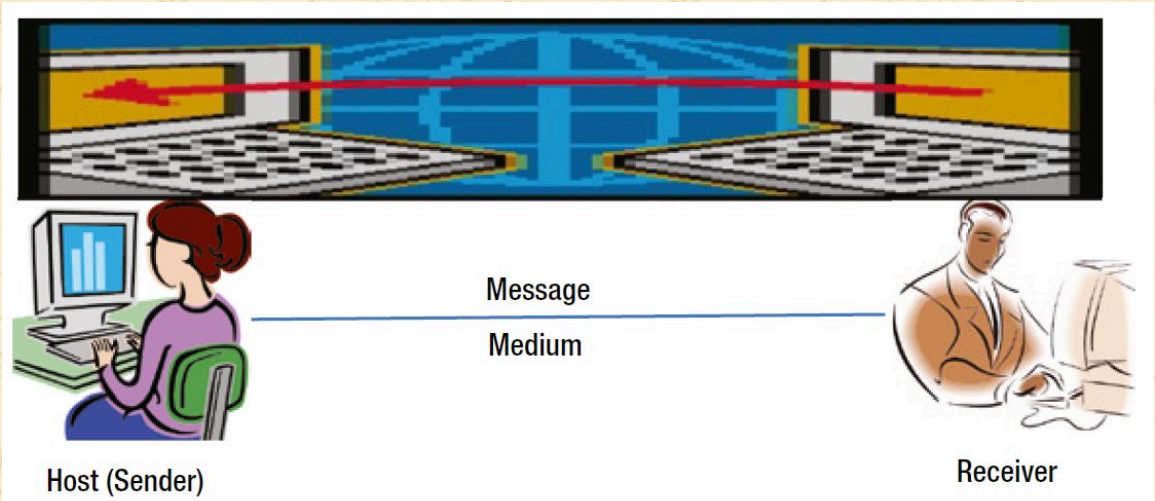


Figure 9-3. *Computer communication*

"Figure 9-3: Computer communication" (page 189), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Networks & Network Security

Several more definitions:

- [Another definition of **network**:] A set of devices/computers connected via **links** (such as wires, optical fibers, or radio channels) and **switches** (devices connecting links and forwarding data over to specific devices, e.g., routers.)
- An **internet** is a network of networks.
  - Q: **How do we distinguish between a network and an internet?**
    A: Data that are sent over a network are addressed to "device X", while data sent over an internet are addressed to "device X on network Y".
- An **intranet** is a private network to which only users within an organization can access.
- The **Internet** (note the capital letter 'I') is the largest internet in the World.
- The **World Wide Web** (**WWW**) is the collection of all the pages and data that can be publically accessed via and over the Internet.

Networks & Network Security

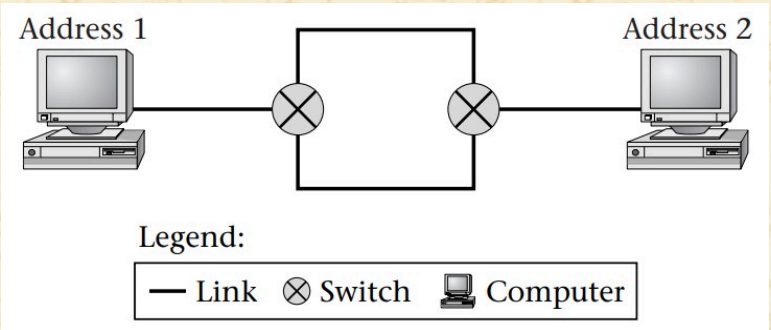


Diagram of a network. Taken from Operating Systems and Middleware: Supporting Controlled Interaction, page 397.

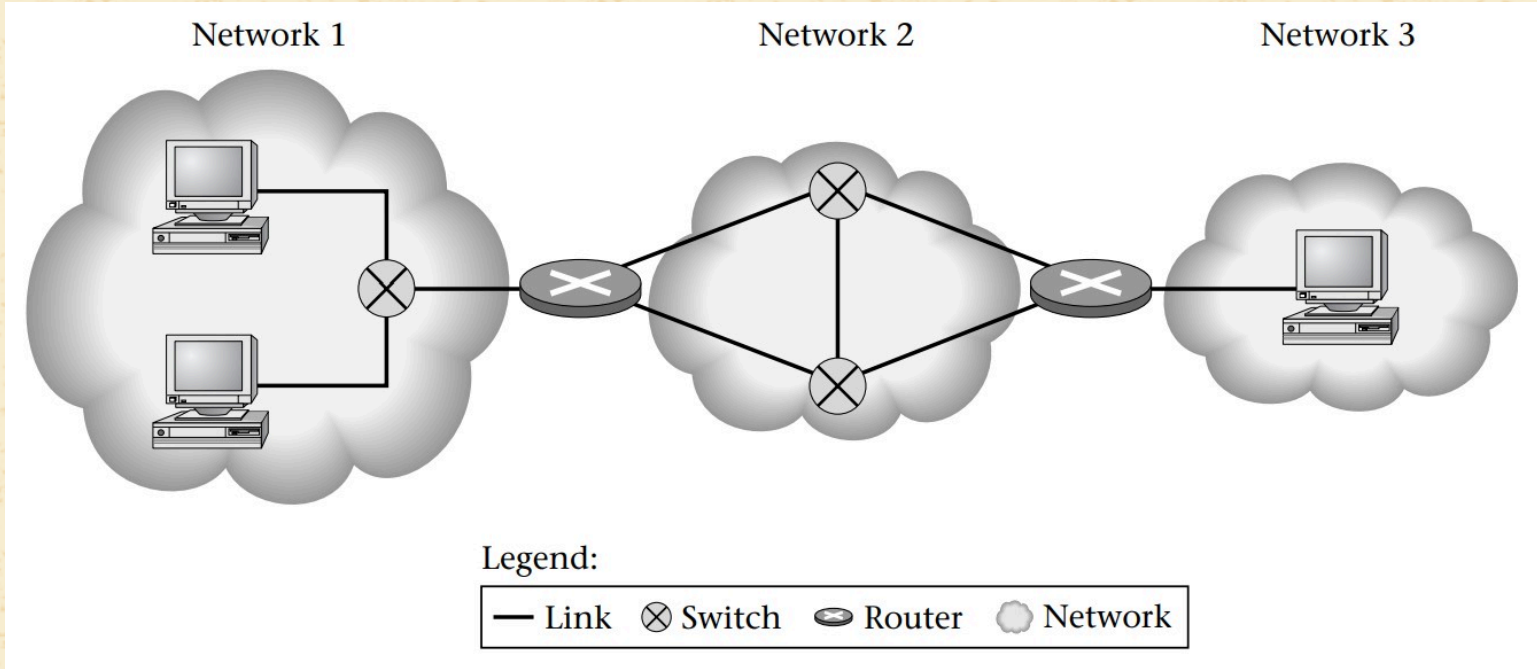


Diagram of an internet. Taken from Operating Systems and Middleware: Supporting Controlled Interaction, page 398.

Network Categories

A network belongs to one of the following categories:

- **Local Area Network (LAN)**: A network that is confined to a relatively small geographical area such as a school or an office building and occasionally a group of nearby buildings. LAN connects a relatively small number of systems within the same organization. The most common LAN protocol is Ethernet.
- **Metropolitan Area Network (MAN)**: Metropolitan Area Networks (MAN) is a network of connected systems within the same metropolitan city. A MAN is larger than a LAN but smaller than a WAN. For practical reasons, a MAN is optimized for a large geographical area, and can connect two types of networks – LAN and WAN.
- **Wide Area Network (WAN)**: connects two or more LANs which are geographically apart. For example, an organization may have two different offices in two different places or countries and they are connected together to form a WAN. WAN connections comprises of several devices including multiplexers, bridges, and routers. WAN link can be a private dedicated link or a public link. **The Internet** is the largest existing WAN.

Networks & Network Security

A fantastic "Crash Course Computer Science" video on Computer Networks:

https://www.youtube.com/watch?v=3QhU9jd03a0

Network Protocols: OSI and TCP/IP

In order to meet the challenges of multi-vendor devices on a network and to break the complexity of computer communications, there are two types of networking models that are developed based on the layered protocol approach:

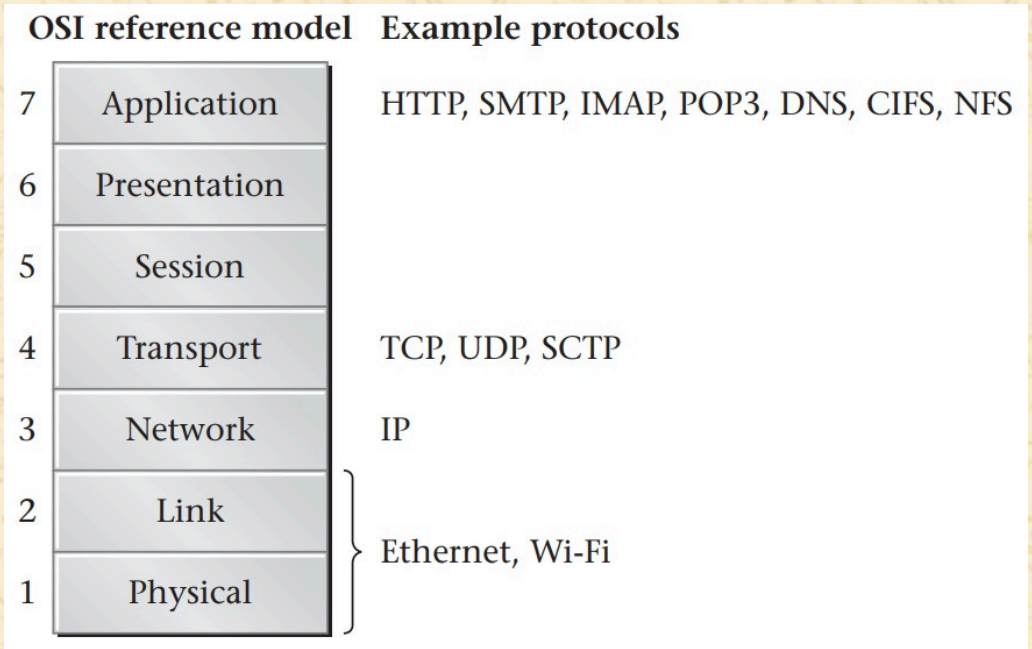
1. OSI (Open Systems Interconnection): A 7-layer model.
2. TCP/IP (Transmission Control Protocol/Internet Protocol): A 4-layer model.

Some of the layers of both models overlap, as we shall see.

OSI (**Open Systems Interconnection**) was developed by ISO, the International Organization for Standardization and ITU-T, the International Telecommunication Union Standardization Sector, in 1982.

This model divides the complex computer communication into seven distinct layers, with each layer having its own specific functions and protocols. Each of the layers extends services to the layer directly above it and is given services from the layer directly below it. Hence all the seven layers together bring about the communication between the devices in a network.

OSI Layer Diagrams



Layers of the OSI model. Taken from Operating Systems and Middleware: Supporting Controlled Interaction, page 401.

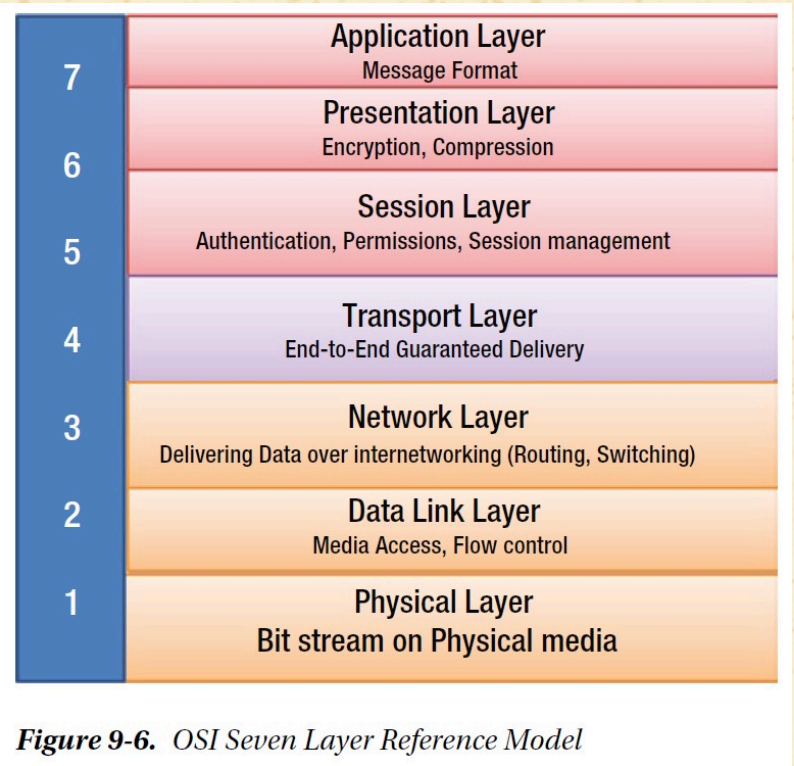


Figure 9-6. *OSI Seven Layer Reference Model*

"Figure 9-6: OSI Seven Layer Reference Model" (page 192), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

OSI Layers: Description

The responsibilities of the layers of OSI are:

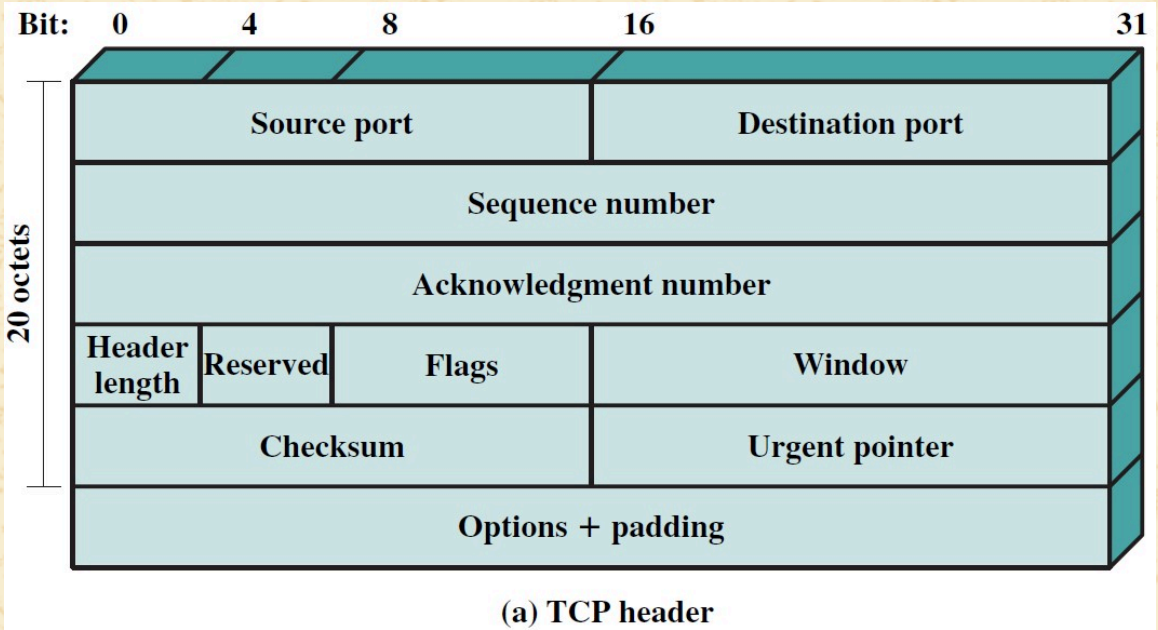
7. **Application Layer**: provides application services to the network applications such as e-mail, web, remote connection, file transfers, and database access. Other functions include: user authentication and data encryption.
6. **Presentation Layer**: presents the data to the upper layers by transforming data into a required format that can be accepted by the applications in the application layer.
5. **Session Layer**: manages the establishment, usage, and ending of the connections/sessions between the devices. It also decides how long the sessions should be, which side will transmit, when to transmit, and how long to transmit data.
4. **Transport Layer**: ensures that data is delivered from one end point to another without any errors. This layer implements error checking, recovery of lost packets to ensure the completeness of data transfer, and flow control.
3. **Network Layer**: routes data within the network. It is responsible for finding the shortest path from source to destination and route the packet through the intermediate devices such as router(s) or switch(es).
2. **Data Link Layer**: takes the packets from the above layers and processes them through the medium as bits.
1. **Physical Layer**: transmits bits from one device to another device over a physical medium (wired or wireless.)

TCP/IP Layers: Description

TCP/IP (**Transmission Control Protocol/Internet Protocol**) was developed by scientists of the Defense Advanced Research Projects Agency (DARPA) of the Department of Defense in the 1970s and was officially adopted by the ARPANET (the world's first public packet-switched computer network and the grandparent of the Internet) in 1983. The four layers of TCP/IP are:

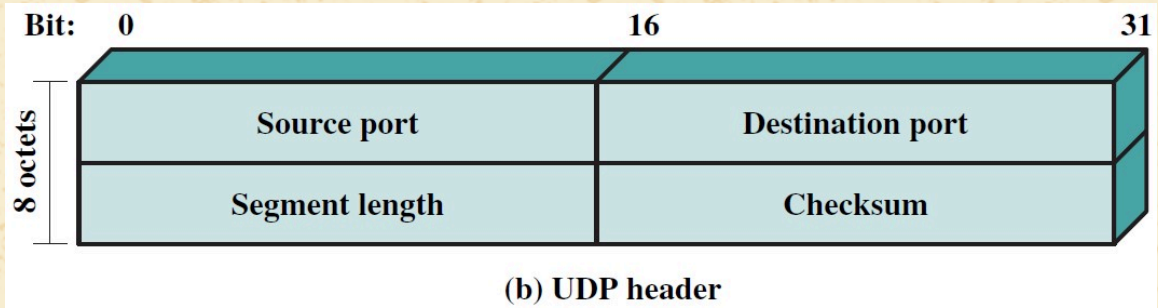
4. **Application Layer**: combines the Application, Presentation, and Session layers of OSI. Hands over data received from TCP to the application and makes sure the app is able to interpret the received data.
3. **Transmission Control Protocol (TCP) Layer**: delivers data from the client to the server without errors or loss. Overlaps the functionality of Transport Layer of OSI reference model. TCP ensures that, if a segment of data is lost in transmission, it is resent again until all the data arrives nominally.
2. **Internet Protocol (IP) Layer**: forwards the data segments received from the TCP, referred to as **packets**, from one node (= device on the network) to the destination node based on the IP address. Overlaps OSI's Network Layer.
1. **Network Access Layer**: Combines the functions of the Data Link and the Physical Layers of OSI. creating data 'frames' for transmitting and receiving data from the physical layer. This function is implemented by a hardware and software Network Interface Card (NIC), an adapter connected to the computer through physical wires or optical fiber cables.

The TCP and UDP Packet Headers



(a) TCP header

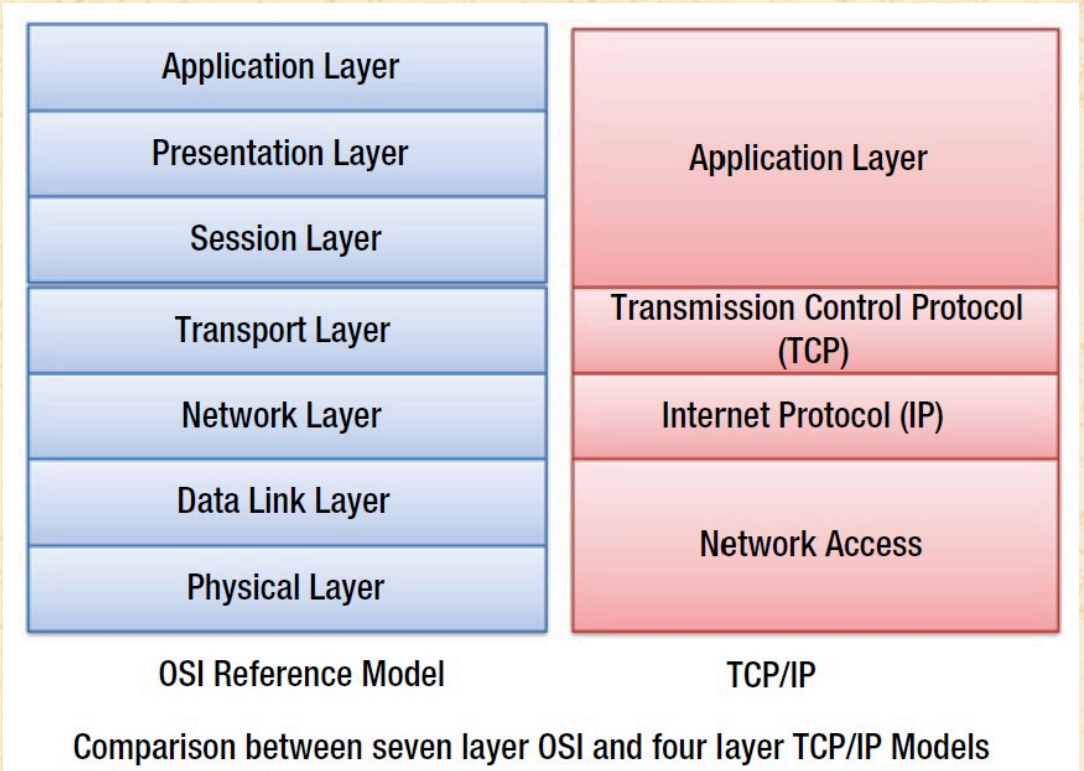
Contents of the TCP header metadata. Taken from Stallings, William. *Data and computer communications*. Pearson Education India, 2007, page 42.



(b) UDP header

Contents of the UDP header metadata. Taken from Stallings, William. *Data and computer communications*. Pearson Education India, 2007, page 42.

OSI vs. TCP/IP: Comparison



OSI vs. TCP/IP: Comparison. "Figure 9-7: OSI and TCP/IP models compared" (page 194), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Network Categories

Any questions?

Attacks on Networks

Attackers generally abuse the network “rules” established by security policies. The rules are broken in such a way that attackers send their traffic that appears to be normal traffic. Attacks can be classified as:

1. Reconnaissance,
2. Denial of Service (DOS) or Distributed Denial of Service (DDoS), or
3. Other network attacks.

Reconnaissance is an attacker's activity of collecting information about a network, its structure, and the hardware and software it uses to launch a successful attack.

Reconnaissance is not an attack by itself; however, this could cause a serious security threat by allowing the weaknesses of the network or network resources to be made known to the attacker. This is more an information-gathering mission. Moreover, it usuallyundergoes undetected since it doesn't have immediate, noticeable effect on the network.

Attacks on Networks

Sniffing (= reading the content of transmitted data packets) is one of the most popular reconnaissance methods used by the attackers to collect the information, such as: user IDs, passwords, session ids, confidential details, business discussions, and financial transactions. Other popular methods are **pinging** (= sending requests to a website to test its reachability and speed), **banner grabbing** (= finding a network's software version information), and **port scanning** (= determining which ports on a network are open and could be receiving or sending data.)

The main purpose of **Denial of Service (DOS)** attacks is to make the network resources inaccessible to the user and bring down the network itself by generating a huge amount of network traffic that overwhelms or crashes the server, exceeding the capacity of the routers and switches or overwhelming CPU and memory.

Sometimes, the attacker gets into one device in the network remotely and triggers simultaneous exploitation of systems on the network or uses multiple compromised machines to initiate simultaneous attacks. The sudden increase in the network traffic can cause the server or router to go down quickly and become inaccessible to the legitimate users. This kind of an attack is called **Distributed Denial-of-Service (DDOS)**, which hides the true origin of the attack.

Attacks on Networks

Apart from the attacks that we have described previously, other attacks can cause serious damage to network security:

- **Masquerade/Spoofing Attacks**: The network intruder masquerades the TCP/IP packet by an illegal IP address, falsifying the source address. The intruder fools the remote machine by an illegitimate source address but with valid user access privileges.
- **HTTP Tunneling**: This method may be used by the insiders to overcome the firewall controls and send confidential information to the outside world without anyone inside being aware of it.
- **SSH Tunneling**: Used to directly connect to a network stealthily and initiate attacks. This is an illegitimate use of a legitimate tool.
- **Session Hijacking**: A session between the user and the server can be **hijacked** (= taken over) by the attacker.
- **Attacks on Network Equipment**: Equipment, such as routers, is traditionally prone to default password vulnerabilities because the network administrators not taking sufficient care in resetting these passwords. The weakness of the network configurations of a router is a new point of vulnerability.

Controls of Attacks on Networks

The following measures can be taken to counter network attacks:

1. Reinforce network equipment with appropriate configurations and appropriate patching including firmware updates.
2. Substitute all default passwords with strong passwords.
3. Use safe session ID handling.
4. Choose an appropriate session time out for the app.
5. Use encrypted protocols like SSL or TLS; techniques like VPN.
6. Do not store passwords or critical information in the cookies.
7. Ensure that all the software used including utilities / tools are patched / updated.
8. Set easy-to-understand and clear security policies.
9. Create awareness among the employees on what can go wrong and what is expected from them.
10. Do not have the same user name and passwords for all the systems.
11. Logout promptly after the work is over.
12. Ensure cookies, history, and offline content are removed after sensitive transaction sessions.
13. Do not click links in suspicious emails.

Controls of Attacks on Networks

Any questions?

Networks & Network Security: Sources

Rao, Umesh Hodeghatta, and Umesha Nayak. "Chapter 9: Understanding Networks and Network Security." *The InfoSec handbook: An introduction to information security.* Springer Nature, 2014, pp. 187-204. URL: https://link.springer.com/content/pdf/10.1007/978-1-4302-6383-8.pdf#chapter+9:+understanding+networks+and+network+security

Salomon, David. "Chapter 7: Network Security." *Elements of computer security.* Springer Science & Business Media, 2010, pp. 179-208. URL: https://link-springer-com.brooklyn.ezproxy.cuny.edu/content/pdf/10.1007/978-0-85729-006-9.pdf#7+network+security