Final Exam

Ismael A. Rodriguez

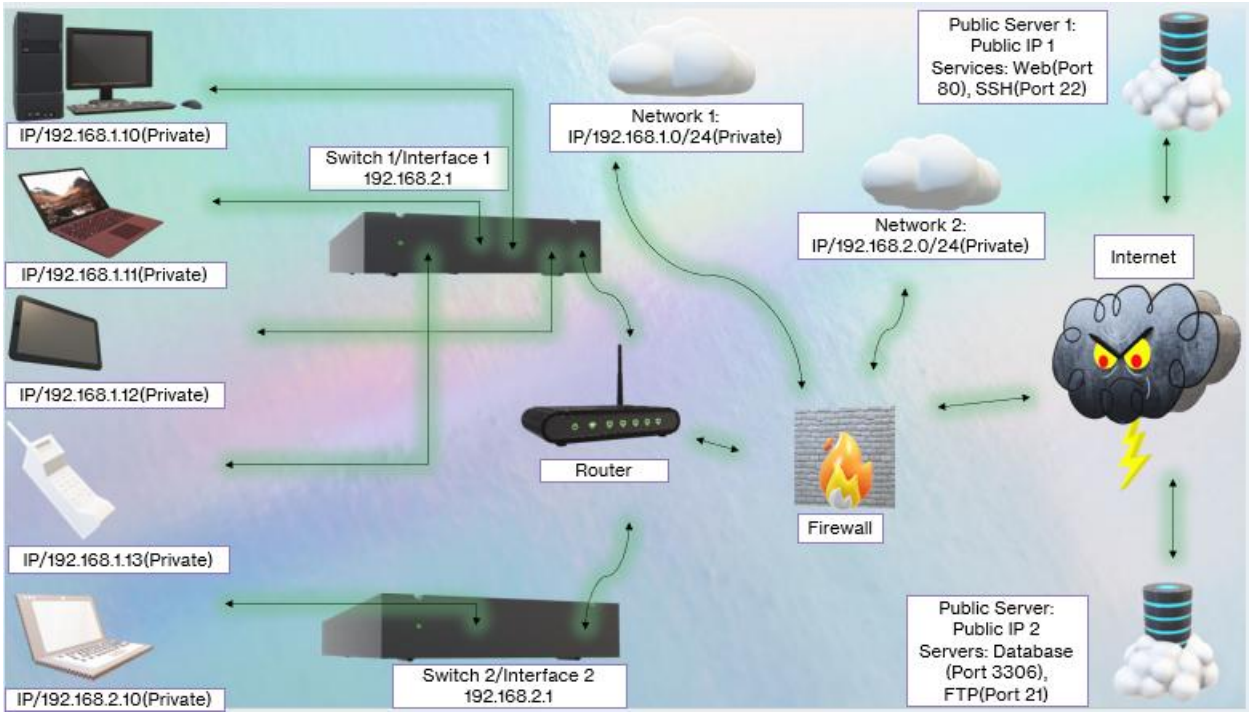
University of Arizona

CYBV 326: Introductory Methods of Network Analysis

Jonathan Martinez

11/20/2023

Network Architecture



Resource Request

Physical Layer:

1. Concept: Physical Connection and Ethernet Frames
    i. Definition: Establishing a physical connection between the host and the network, either through Ethernet cables or wireless signals. Simultaneously, data is framed into Ethernet frames for efficient transmission over the physical medium.
    ii. Port/Protocol: N/A
    iii. Data Unit: Frame

iv. User Benefits: Enables the physical transmission of data while ensuring data is organized for reliable communication.

v. Network Diagram Label: Physical Connection and Ethernet Frames.

2. Concept MAC Addressing and Hubs/Switches

i. Definition: Assigning unique MAC addresses to devices for identification within the local network. Simultaneously, switches, operating at the data link layer, forward frames based on MAC addresses to the intended recipient, enhancing efficiency.

ii. Port/Protocol: N/A

iii. Data Unit: Frame

iv. User Benefit: Ensures data reaches the correct devices within the same local network while optimizing network performance.

v. Network Diagram Label: MAC Addressing and Switching

3. Concept: Frame Check Sequence (FCS) and Address Resolution Protocol (ARP)

i. Definition: Adding a frame check sequence to frames to detect errors during transmission. Simultaneously, ARP resolves IP addresses to MAC addresses for communication within the local network.

ii. Port/Protocol: ARP (Address Resolution Protocol)

iii. Data Unit: Frame

iv. User Benefit: Enhances the reliability of data transfer by detecting and correcting errors, while also facilitating communication between devices on the same local network.

v. TCP/IP Layer: Data Link Layer

vi. Network Diagram Label: FCS and ARP

4. Concept: Switching and Virtual LAN (VLAN)

    i. Definition: Switches operate at the data link layer, forwarding frames only to the device it is intended for (Switching). Simultaneously, VLANs create logically segmented networks within a physical network, improving broadcast domain efficiency.

    ii. Port/Protocol: N/A

    iii. Data Unit: Frame

    iv. User Benefit: Enhances network performance by reducing unnecessary traffic and provides better network management and security by isolating broadcast domains.

    v. TCP/IP Layer: Data Link Layer

    vi. Network Diagram Label: Switching and VLAN

5. Concept: Point-to-Point Protocol (PPP) and Internet Group Management Protocol (IGMP)

    i. Definition: Establishing a direct point-to-point communication link between two devices (PPP). Simultaneously, IGMP manages a multicast group membership in IP networks.

    ii. Port/Protocol: PPP (Point-to-Point Protocol), IGMP (Internet Group Management Protocol)

    iii. Data Unit: Frame

iv. User Benefit: Provides a secure and efficient means of communication over serial links (PPP) and supports efficient distribution of multicast traffic (IGMP).
v. TCP/IP Layer: Data Link Layer
vi. Network Diagram Label: PPP and IGMP

Network Layer

6. Concept: IP Addressing and Routing
    i. Definition: Assigning unique IP addresses to devices for identification (IP Addressing). Simultaneously, routers determine the optimal path for data to travel from source to destination across different networks (Routing).
    ii. Port/Protocol: ICMP (Internet Control Message Protocol)
    iii. Data Unit: Datagram
    iv. User Benefit: Enables devices to be uniquely identified and located on a network (IP Addressing) and ensures data reaches the correct destination by navigating through routers (Routing).
    v. TCP/IP: Network Layer
    vi. Network Diagram Label: IP Addressing and Routing
7. Concept: Subnetting and Internet Control Message Protocol (ICMP)

   i. Definition: Dividing a network into smaller sub-networks for efficient IP address allocation (Subnetting). Simultaneously, ICMP provides error reporting and diagnostic functionalities in IP networks.
   ii. Data Unit: Datagram
   iii. User Benefit: Optimizes IP address usage and network performance (Subnetting)and facilitates communication and troubleshooting by reporting errors (ICMP).
   iv. TCP/IP Layer: Network Layer
   v. Network Diagram Label: Subnetting and ICMP

8. Concept: Internet Group Management Protocol (IGMP) and Virtual LAN (VLAN)
   i. Definition: Managing multicast group memberships in IP networks (IGMP) Simultaneously, VLANs create logically segmented networks within a physical network, improving broadcast domain efficiency.
   ii. Port/Protocol: IGMP (Internet Group Management Protocol)
   iii. Data Unit: Datagram
   iv. User Benefit: Supports efficient distribution of multicast traffic (IGMP) and provides better network management and security by isolating broadcast domains (VLAN).
   v. TCP/IP Layer: Network Layer
   vi. Network Diagram Label: IGMP and VLAN
9. Concept: Fragmentation and Transmission Control Protocol (TCP)

i. Definition: Breaking down large IP packets into smaller fragments for transmission (Fragmentation). Simultaneously, TCP provides reliable, connection-oriented communication.
ii. Port/Protocol: TCP (Transmission Control Protocol)
iii. Data Unit: Datagram
iv. User Benefits: Facilitates the transmission of large packets across networks with different MTU sizes (Fragmentation) and ensures reliable data transfer (TCP)
v. TCP/IP: Network Layer
vi. Network Diagram Label: Fragmentation and TCP

10. Concept: Error Handling and Internet Protocol (IP) Addressing
    i. Definition: Handling errors in transmitted data (Error Handling). Simultaneously, IP addressing is employed to uniquely identify devices on a network.
    ii. Port/Protocol: N/A
    iii. Data Unit: Datagram
    iv. User Benefit: Enhances data integrity by handling errors (Error Handling) and enables devices to be uniquely identified and located on a network (IP Addressing)
    v. TCP/IP Layer: Network Layer
    vi. Network Diagram Label: Error Handling and IP Addressing

11. Concept: Port Numbers and Flow Control
    i. Definition: Assigning specific port numbers to applications for communication (Port Numbers). Simultaneously, flow control mechanisms manage the rate of data transmission to prevent congestion.
    ii. Port/Protocol: N/A
    iii. Data Unit: Segment
    iv. User Benefit: Allows multiple applications to share the same network connection (Port Numbers) and optimizes data transfer to avoid packet loss (Flow Control)
    v. TCP/IP: Transport Layer
    vi. Network Diagram Label: Port Numbers and Flow Control
12. Concept: Error Detection and Segmentation
    i. Definition: Identifying and correcting errors in transmitted data (Error Detection). Simultaneously, segmentation breaks down large data chunks into smaller segments for transmission.
    ii. Port/Protocol: N/A
    iii. Data Unit: Segment
    iv. User Benefit: Enhances the integrity of the transmitted data (Error Detection) and enables efficient data transfer (Segmentation).
    v. TCP/IP Layer: Transport Layer
    vi. Network Diagram Label: Error Detection and Segmentation

13. Concept: Protocol Multiplexing and Transmission Acknowledgement
    i. Definition: Combining multiple data streams into a single communication channel (Protocol Multiplexing). Simultaneously, transmission acknowledgment confirms the successful receipt of data.
    ii. Port/Protocol: TCP (Transmission Control Protocol)
    iii. Data Unit: Segment
    iv. User Benefit: Allows multiple applications to share the same network connection (Protocol Multiplexing) and confirms successful data transmission.
    v. TCP/IP Layer: Transport Layer
    vi. Network Diagram Label: Protocol Multiplexing and Transmission Acknowledgement

Application Layer

14. Concept: DNS Resolution and Hostname to IP Address Mapping
    i. Definition: Resolving domain names to IP addresses through DNS (Domain Name System) resolution.
    ii. Port/Protocol: DNS (Domain Name System)
    iii. Data Unit: Message
    iv. User Benefits: Enables users to access resources using human-readable domain names rather than numerical IP addresses.
    v. TCP/IP Layer: Application Layer
    vi. Network Diagram Label: DNS Resolution

15. Concept: HTTP Request and Web Server Interaction
    i. Definition: Initiating an HTTP (Hypertext Transfer Protocol) request from the client to interact with a web server.
    ii. Port/Protocol: HTTP (Hypertext Transfer Protocol)
    iii. Data Unit: Message
    iv. User Benefit: Facilitates the retrieval of web content, such as files or web pages, from a remote server.
    v. TCP/IP Layer: Application Layer
    vi. Network Diagram Label: HTTP Request
16. Concept: SSL/TLS Encryption and Secure Data Transmission
    i. Definition: Implementing SSL/TLS (Secure Sockets Layer/ Transport Layer Security) encryption for secure data transmission.
    ii. Port/Protocol: HTTPS (Hypertext Transfer Protocol Secure)
    iii. Data Unit: Message
    iv. User Benefits: Ensures the confidentiality and integrity of data during transmission over the network.
    v. TCP/IP Layer: Application Layer
    vi. Network Diagram Label: SSL/TLS Encryption
17. Concept: SMTP for Email Transmission
    i. Definition: Using SMTP (Simple Mail Transfer Protocol) for the transmission of emails from client to a mail server.
    ii. Port/Protocol: SMTP (Simple Mail Transfer Protocol)
    iii. Data Unit: Message

iv. User Benefit: Enables the reliable sending of emails between email clients and servers.
v. TCP/IP Layer: Application Layer
vi. Network Diagram Label: SMTP Email Transmission

18. Concept: File Transfer Protocol (FTP) for File Transfer
    i. Definition: Employing FTP (File Transfer Protocol) for transferring files between a client and a server.
    ii. Port/Protocol: FTP (File Transfer Protocol)
    iii. Data Unit: Message
    iv. User Benefit: Facilitates the efficient transfer of files over the network.
    v. TCP/IP Layer: Application Layer
    vi. Network Diagram Label: FTP File Transfer
19. User Authentication and Authorization
    i. Definition: Verifying the identity of users and determining their levels of access to network resources.
    ii. Port/Protocol: N/A
    iii. Data Unit: Message
    iv. User Benefit: Ensures secure access to network resources based on user credentials and permissions.
    v. TCP/IP Layer: Application Layer
    vi. Network Diagram Label: User Authentication
20. Concept: Session Management and Persistent Connections

i. Definition: Managing sessions to maintain persistent connections between a client and a server for efficient data exchange.
ii. Port/Protocol: N/A
iii. Data Unit: Message
iv. User Benefit: Improves the speed and efficiency of data transfer by maintaining open connections between the client and server.
v. TCP/IP Layer: Application Lyer
vi. Network Diagram Label: Session Management.

Research Analysis

1. Attack on the Physical Layer: Jamming
    a. What is the attack?
        i. Layer: Physical Layer
        ii. Description: Jamming is an attack that disrupts wireless communication by transmitting interference signals on the same frequency band, making it difficult or impossible for legitimate communication to occur.
    b. How is the attack carried out?
        i. Attackers transmit continuous signals or noise on the frequency bands used by the target wireless communication, overwhelming the signals and causing interference.
    c. What does the attack hope to achieve?
        i. CIA Triad:

ii. Confidentiality: Disrupts communication, potentially exposing confidential information.

iii. Integrity: Introduces noise, compromising the integrity of the communication.

iv. Availability: Aims to deny availability of the communication channel.

d. Network Vulnerability:

i. Lack of encryption and authentication mechanisms in the wireless communication protocol.

e. Recommendations to senior management:

i. Invest in secure and encrypted communication protocols.

ii. Implement frequency hopping techniques to mitigate the impact of jamming.

iii. Use physical security measures to protect critical communication infrastructure.

2. Attack on Data Link Layer: MAC Spoofing

a. What was the attack?

i. Layer: Data Link Layer

ii. Description: MAC spoofing involves forging the Media Access Control (MAC) address of a device to gain unauthorized access to network.

b. How is the attack carried out?

i. Attackers modify their device's MAC address to match that of an authorized device, tricking the network into accepting the unauthorized device.

c. What does the attack hope to achieve?

i. CIA Triad:

ii. Confidentiality: Gain authorized access to sensitive data.

iii. Integrity: Potentially alter data or inject malicious content.

iv. Availability: Disrupts normal network operations.

d. Network Vulnerability:

i. Weak or nonexistent authentication mechanisms at the Data Link Layer.

e. Recommendation to senior management:

i. Implement port security to restrict MAC addresses on switch ports.

ii. Use 802.1X authentication to validate devices before granting network access.

iii. Regularly monitor and audit network traffic for anomalies.

3. Attack on Network Layer: IP Spoofing

a. What was the attack?

i. Layer: Network Layer

ii. Description: IP Spoofing involves sending IP packets from a false (or "spoofed") source address to deceive the recipient about the origin of the message.

b. How is the attack carried out?

i. Attackers modify the source address field on the IP header to make it appear as if the packet comes from a trusted source.

c. What does the attack hope to achieve?

i. CIA Triad:

ii. Confidentiality: Eavesdrop on communication between trusted entities.

iii. Integrity: Inject false information into the network.

iv. Availability: Conduct DoS attacks by overwhelming systems.

d. Network vulnerability:

i. Lack of ingress filtering to verify the source IP address of incoming packets.

e. Recommendation to senior management:

i. Implement ingress filtering to validate the source of incoming packets.

ii. Use strong encryption and authentication protocols to protect against eavesdropping.

iii. Employ intrusion detection systems to detect and mitigate IP spoofing attempts.

4. Attack on Transport Layer: SYN Flood

a. What was the attack?

i. Layer: Transport Layer

ii. Description: SYN Flood is a type of DDoS attack that exploits the TCP three-way handshake process by overwhelming a target system with a flood of SYN requests.

b. How is the attack carried out?

i. Attackers send many SYN requests to the target system, exhausting its resources and preventing legitimate connections.

c. What does the attack hope to achieve?
    i. CIA Triad:
    ii. Confidentiality: This may not be a direct goal but can lead to exposure of confidential information during system downtime.
    iii. Integrity: Disrupts normal system operations, potentially leading to data corruption.
    iv. Availability: Aims to deny service to legitimate users.
d. Network Vulnerability:
    i. Inadequate protection against SYN flooding, such as the absence of SYN cookies or SYN cache.
e. Recommendations to senior management:
    i. Implement SYN cookies or SYN cache mechanisms to handle connection requests efficiently. Deploy firewalls and intrusion prevention systems to detect and block SYN flood attacks.
    ii. Use load-balancing techniques to distribute incoming traffic and mitigate the impact of DDoS attacks.

Conclusion

In summary, the provided network architecture outlines key concepts and components spanning the Physical, Data Link, Network, and Transport layers of the TCP/IP model. The Physical Layer involves the establishment of a physical connection and framing data into Ethernet frames, MAC addressing, frame check sequence, switching, and VLANs, as well as point-to-point communication through PPP and IGMP. The Data Link Layer encompasses concepts such as IP addressing and routing, subnetting, IGMP, fragmentation, error handling, and MAC spoofing. The Network Layer introduces concepts like port numbers, flow control, error detection, segmentation, protocol multiplexing, and transmission acknowledgment. The Application Layer covers DNS resolution, HTTP requests, SSL/TLS encryption, SMTP for email transmission, FTP for file transfer, user authentication, and session management. The provided network diagram visually represents the relationships and interactions between these components, enhancing the understanding of the network architecture. Furthermore, the research analysis explores four distinct attacks, each targeting a specific layer of the TCP/IP stack. The attacks include Jamming at the Physical Layer, MAC Spoofing at the Data Link Layer, IP Spoofing at the Network Layer, and SYN Flood at the Transport Layer. Each analysis addresses the attack's description, execution, objectives related to the CIA triad, network vulnerabilities, and recommendations for senior management to mitigate the risks associated with these attacks. The combination of the network architecture and attack analysis provides a comprehensive overview of the design and security considerations within the specified network. If there are specific areas you would like to explore further or if you have additional questions, please feel free to let me know.

References

Y. O. Basciftci, F. Chen, J. Weston, R. Burton and C. E. Koksal, "How Vulnerable Is Vehicular Communication to Physical Layer Jamming Attacks?," 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston, MA, USA, 2015, pp. 1-5, doi: 10.1109/VTCFall.2015.7390968.Cyber Readiness Institute. (2020). *Ransomware Playbook*. How to prepare for, respond to, and recover from a ransomware attack. https://cyberreadinessinstitute.org/wp-content/uploads/20-CRI-Ransomware-Playbook.pdf.

S. Mahmood, S. M. Mohsin and S. M. A. Akber, "Network Security Issues of Data Link Layer: An Overview," 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 2020, pp. 1-6, doi: 10.1109/iCoMET48670.2020.9073825.Rapoport, M., & Andriotis, A. M. (2017, October 28). *States Push Equifax to Explain Why It Took 6 Weeks to Disclose Hack*. The Wall Street Journal. https://www.wsj.com/articles/states-push-equifax-to-explain-why-it-took-6-weeks-to-disclose-hack-1509196933.

I. B. Mopari, S. G. Pukale and M. L. Dhore, "Detection and defense against DDoS attack with IP spoofing," 2008 International Conference on Computing, Communication and Networking, Karur, India, 2008, pp. 1-5, doi: 10.1109/ICCCNET.2008.4787693.Soper, T. (2013, August 19). *Amazon just lost $4.8M after going down for 40 minutes*. https://www.geekwire.com/2013/amazon-lost-5m-40-minutes/.

K. Geetha and N. Sreenath, "SYN flooding attack — Identification and analysis," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 2014, pp. 1-7, doi: 10.1109/ICICES.2014.7033828.