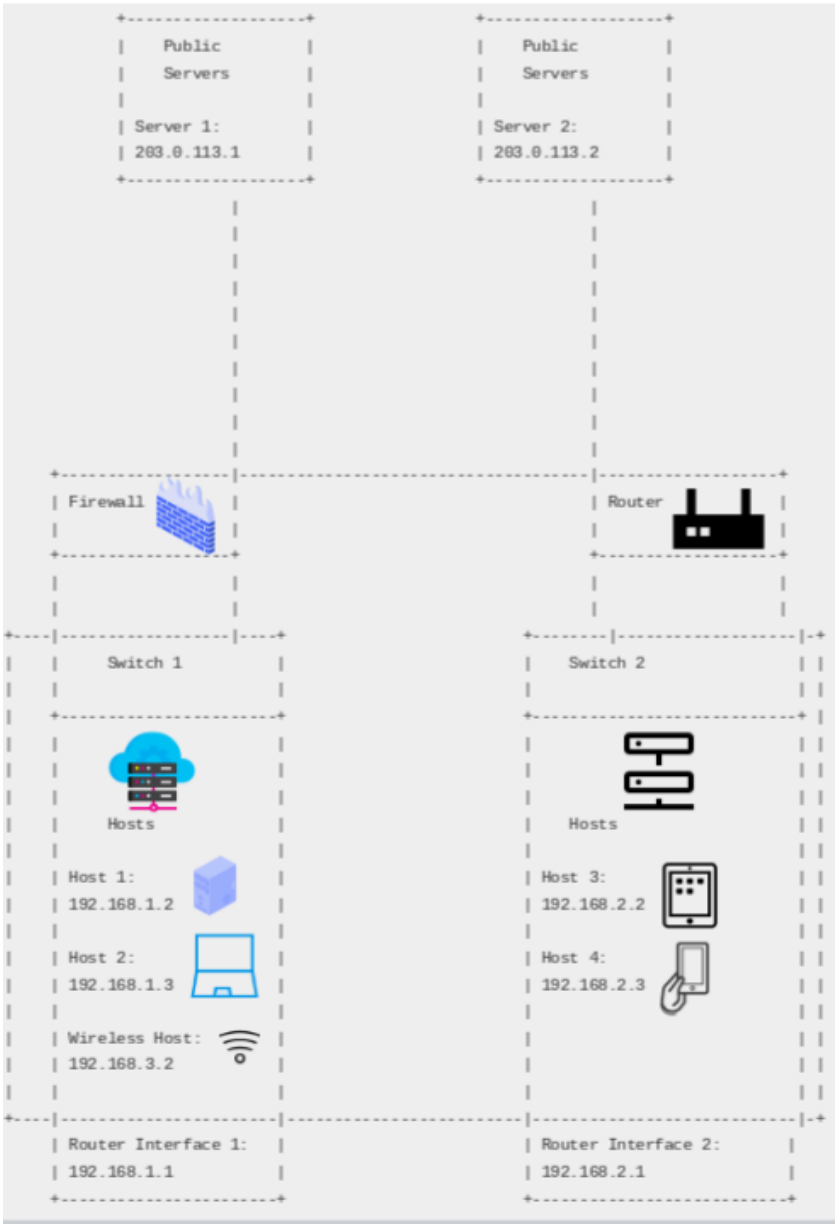
Wireless Network Analysis

Adam H Guled

University Of Arizona

Network Architecture



This network diagram provides a clear and concise overview of how Faye delivered an email to Spike via a TCP/IP network. A firewall is positioned strategically to guard the network boundary from threats and unauthorized access. Other essential components include hosts connected by switches, which represent the local network configuration; a router, which is essential for controlling traffic across various subnets and guaranteeing that emails find the

correct route; and public servers, which include email and DNS servers and are in charge of processing emails, routing them, and converting domain names into IP addresses. Each component in the diagram is identified and shown with care, not just to represent its physical existence but also to highlight its specialized function in aiding an email's trip through the tiered architecture of network communication.

Resource Request

Application Layer - User Interface and Protocols

Faye connects with her network services through the Application Layer. She composes and sends an email using her email client on Host 1 (192.168.1.2). MIME handles email formatting and structuring messages for network compatibility. The email is submitted to the mail server via SMTP, which runs on TCP port 25 (Server 1: 203.0.113.1). Using UDP port 53, a DNS Lookup is done to resolve Spike's email domain to an IP address. The email is retrieved at Spike's end (Host 3: 192.168.2.2) via IMAP or POP3 protocols, demonstrating the Application Layer's involvement in initiating and receiving network connections.

Transport Layer - Segmentation and Secure Transmission

TCP segments the email for delivery in the Transport Layer, guaranteeing that each segment is properly sent and correctly arranged when it reaches Spike. UDP is a quicker communication technique for DNS lookups (Kurose & Ross, 2020). The SSL/TLS protocols encrypt email data, which is critical for network security. TCP checksums provide Data Integrity, ensuring that the email's content is not altered. TCP's Flow Control controls the data transfer rate, improving network efficiency.

Internet Layer: Routing and Addressing

The Internet Layer's principal function is to assign specific addresses to direct email through the network to its destination (Kurose & Ross, 2020). ARP resolves IP addresses to MAC addresses within the local network. Routing, made possible by the router interfaces (192.168.1.1 and 192.168.2.1), determines the optimum path for email using protocols such as BGP or OSPF. Gateways allow email to move between network types, and NAT (Network Address Translation) converts Faye's private IP address for communication over the public internet.

Network Access Layer - Foundations of Physical Data Transmission

The Network Access Layer, which deals with the physical transport of data, is critical in Faye's journey of sending an email. The Ethernet Protocols, which control the framing and physical transfer of data across network cables, serve as the core notion here (Kurose & Ross, 2020). Another critical idea is switching; network switches within Faye's local network (Switch 1 for Network 1 and Switch 2 for Network 2) direct the email's journey, ensuring it correctly navigates within and between networks. Firewalls serve as network security guardians, inspecting email for compliance with security regulations. The vast Internet Infrastructure is the collection of networks, routers, and paths that carry Faye's email to Spike. Finally, MAC Addressing is essential at this layer because it offers unique IDs for devices on the local network, guaranteeing that email is delivered to the correct physical device on that network.

Network Attacks

Application Layer - Phishing

The Application layer, which acts as a conduit between end users and network applications, is the target of phishing assaults. These attacks employ deceptive strategies, mainly via phony websites or emails that mimic reputable companies. The intention is to deceive others into disclosing private information, like financial or login credentials, so jeopardizing the confidentiality of user data (Abroshan, Devos, Poels, & Laermans, 2018).

Phishing attacks are carried out by creating convincing emails or websites that look and sound like authentic sources. These assaults play on user ignorance or lack of knowledge, taking advantage of the human element of security (Abroshan, Devos, Poels, & Laermans, 2018). The primary goal is to violate the CIA triad's 'Confidentiality' aspect by gaining unauthorized access to sensitive material.

Organizations should install strong, multi-factor authentication systems, run regular user education and awareness programs, and deploy email filtering solutions that can detect and block phishing emails to prevent phishing attacks.

Transport Layer - Buffer Overflow Attacks

Buffer overflow attacks at the Transport layer are a serious danger. These occur when too much data is transmitted to a network buffer, causing it to overflow and overwrite adjacent memory space (Tian, Xiong, Hu, & Liu, 2014). This can result in system crashes or allow attackers to run arbitrary code.

Buffer overflow attacks work primarily by flooding a buffer with more data than it is intended to contain. Adjacent memory locations may get corrupted by this overflow, giving attackers access to modify the system (Tian, Xiong, Hu, LIU, 2014). Attackers frequently try to

compromise the system's "Availability," but they can also jeopardize "Confidentiality" and "Integrity" by running unauthorized code or gaining access to private data.

Numerous well-known buffer overflow attacks throughout the years have brought attention to the Transport Layer systems' susceptibility. These incidents highlight the necessity of strong security protocols and show how attackers can take advantage of buffer overflow flaws (Tian, Xiong, Hu, LIU, 2014).

It is recommended that bounds checking be implemented in software applications, memory-safe programming languages be used, and regular system and application updates be performed to address known vulnerabilities.

Network Layer - Routing Table Poisoning

Routing Table Poisoning is a complex attack carried out at the Network layer of the TCP/IP stack that involves spreading fake routing information to routers via protocols such as RIP or BGP. The mechanism of the attack involves modifying routing tables, which are critical for finding the best channels for data transfer throughout the network (Ismail, Germanus, & Suri, 2017). Attackers fool routers into rerouting network traffic down less efficient or attacker-controlled channels by submitting inaccurate routing information.

The goals of this assault are multifaceted: first and foremost, it seeks to compromise the network's 'availability' by producing disruptions or denial of service. Furthermore, by redirecting traffic, it can violate 'Confidentiality' and 'Integrity' if the data is redirected through the attacker's servers. This type of attack takes use of flaws in routing protocols as well as the inherent trust that routers place in incoming routing changes (Ismail, Germanus, & Suri, 2017).

To reduce the risk of Routing Table Poisoning, network administrators must use secure routing protocols that authenticate routing information, closely monitor network traffic for unusual patterns, and update and patch network devices on a regular basis to address known vulnerabilities.

Physical Layer Security - NAT Attacks

Network security is crucial in today's linked world, and one of the primary areas of vulnerability is in the Physical Layer, specifically in the form of NAT (Network Address Translation) exploits. NAT is critical in handling IP address mappings, notably in translating private IP addresses to public IP addresses. However, this critical process also opens the door to potential vulnerabilities. Attackers can exploit the NAT process to gain unwanted access or intercept sensitive data, posing a substantial danger to network security (Meidan, Sachidananda, Peng, Sagron, Elovici, & Shabtai, 2020).

NAT attacks are carried out by exploiting flaws in the NAT setup or implementation. Attackers look for flaws in session tracking or IP address mapping. They can obtain access to secured internal networks or secret information by exploiting these flaws and rerouting or intercepting network traffic (Meidan, Sachidananda, Peng, Sagron, Elovici, & Shabtai, 2020). This type of assault typically targets the 'Confidentiality' and 'Integrity' of network communication, but it can also have an effect on 'Availability' if it causes network disruptions.

Establishments must prioritize secure configuration and regular auditing of their NAT configurations to protect against these vulnerabilities. Implementing strong, multi-layered security measures, including modern network monitoring tools, can lower the danger of such vulnerabilities dramatically. Regular network device updates and patches, as well as rigorous security audits, are critical in discovering and mitigating potential NAT-related vulnerabilities

(Meidan, Sachidananda, Peng, Sagron, Elovici, & Shabtai, 2020). Organizations can strengthen their network's defenses and secure their sensitive data from illegal access and manipulation by adopting these proactive steps.

Conclusion

The thorough examination of the network architecture, which is based on the fundamentals of TCP/IP, demonstrates a comprehensive and successful strategy for network security and communication. By investigating the TCP/IP stack from several levels, providing information about possible weaknesses and the corresponding security controls at each stage.

In conclusion, the network architecture created efficiently incorporates fundamental TCP/IP concepts, exhibiting a practical understanding of network communication and security. We demonstrate the necessity of robust security measures in ensuring network integrity by studying various threats at each tier of the TCP/IP stack. This comprehensive method not only improves practical network administration but also adheres to the basic cybersecurity principles of confidentiality, integrity, and availability.

References

Abroshan, Devos, J., Poels, G., & Laermans, E. (n.d.). Phishing Attacks Root Causes. In Risks and Security of Internet and Systems (pp. 187–202). Springer International Publishing. https://doi.org/10.1007/978-3-319-76687-4_13

Ismail, Germanus, D., & Suri, N. (2017). P2P routing table poisoning: A quorum-based sanitizing approach. *Computers & Security*, *65*, 283–299. https:// doi.org/10.1016/j .cose.2016.12. 007

Kurose, J. F., & Ross, K. (2020). Computer Networking (8th ed.). Pearson Education (US). https://online.vitalsource.com/books/9780135928523

Meidan, Sachidananda, V., Peng, H., Sagron, R., Elovici, Y., & Shabtai, A. (2020). A novel approach for detecting vulnerable IoT devices connected behind a home NAT. *Computers & Security*, *97*, 101968–23. https://doi.org/10.1016/j.cose.2020.101968

Tian, Xiong, X., Hu, C., & Liu, P. (2014). Defeating buffer overflow attacks via virtualization. Computers & Electrical Engineering, 40(6), 1940–1950. https://doi.org/ 10.1016/ j . compeleceng.2013.11.032