Network Architecture Appendix

Ryan Coon

CYB-525

Dr. Emmett Ward

January 8, 2025

**Appendix A**

**Multi-Layered Software Architecture**

Defense in depth - a comprehensive cybersecurity strategy that employs multiple layers of security controls to protect an organization's data and systems. This approach integrates various defensive mechanisms—such as firewalls, intrusion detection systems, and encryption—across physical, technical, and administrative domains(Fortinet, 2024). By layering these defenses, organizations can create a robust security posture that mitigates risks and enhances resilience against potential attacks. The goal is to ensure that if one layer fails, additional layers continue to provide protection, thereby safeguarding valuable information and maintaining operational integrity.

Air gap - a crucial cybersecurity measure that involves physically isolating a secure computer network from unsecured networks, such as the public Internet. This isolation prevents unauthorized access and protects sensitive data from cyber threats(Fortinet, 2023). By creating a literal "gap" between networks, organizations can safeguard critical systems, especially in environments where data integrity is paramount. Air gaps are often used in high-security settings, such as military and financial institutions, to ensure that even if one network is compromised, the other remains secure.

DMZs - is a critical network architecture that creates a buffer between an organization’s internal network and external networks, such as the Internet. This subnetwork hosts external-facing services, like web servers and email servers, while protecting sensitive internal resources(Fortinet, n.d.). By isolating these services, a DMZ enhances security by limiting direct access to the internal network, thereby reducing the risk of attacks

Proxy servers - are like helpful middlemen for your internet connection. They can do a lot of things, like storing copies of web pages for faster access, acting as a translator between your browser and special services, or even speeding up your web communication. They can also be used to alter or monitor the information exchanged between your computer and the internet(What is a Proxy Server?, 2020).

Composition and security -  is essential for building and analyzing secure systems by ensuring that smaller components can be combined without introducing vulnerabilities. This approach allows developers to leverage existing software components while maintaining security integrity(Anupam Datta, n.d.). Key principles include the need for software composition analysis (SCA), which helps identify and manage open-source and third-party components, ensuring they do not expose systems to risks.

Cascading/Segmentation -  is a crucial cybersecurity strategy that involves dividing a network into smaller, isolated segments to enhance security and performance. This approach minimizes the risk of a cyber breach spreading across the entire network by creating barriers between segments(Cisco, 2019). Each segment can be monitored and controlled independently, allowing for tailored security measures. By effectively isolating critical infrastructure and sensitive data, organizations can significantly reduce the potential impact of attacks, ensuring that any breach is contained within a limited area.

**Appendix B**

**Understanding Network Dynamics**

Emergent properties - can be both beneficial and detrimental. For example, combining different security tools can create a stronger defense than the sum of its parts. However, unexpected vulnerabilities can also emerge when systems interact in unforeseen ways(Whitman & Mattord, 2022). Understanding emergent properties is crucial for building robust and adaptable security solutions.

Dependencies - refers to any external software component, library, or service that a system relies on to function properly. These dependencies create connections between various components, processes, and entities within a cybersecurity ecosystem(What is Dependency?, 2025). Understanding these relationships is crucial for effective risk management and decision-making. For instance, a cyber dependency can be defined as a connection between two assets, where the state of one relies on the other.

TCB subsets - refers to the collection of hardware, firmware, and software components critical for enforcing a system's security policies(Awati, n.d.). TCB subsets are specific architectures within the TCB that partition security responsibilities hierarchically among different components. This approach enhances security by isolating functions and minimizing the attack surface. Each subset is designed to ensure that only authorized components can access sensitive data, thereby maintaining the integrity and confidentiality of the system.

Transport layer security -  is like a digital padlock that protects your online conversations. It ensures that your data is encrypted and safe from snooping, and it verifies that you're actually talking to the person you think you are(Whitman & Mattord, 2022). Think of it as a secret code that only you and the person you're talking to know. However, even with TLS, there's still a risk of a "man-in-the-middle" attack, where someone could pretend to be you or the person you're talking to. That's where trusted third parties come in, like the Public Key Infrastructure, which helps to prevent these attacks.

BGP - is a crucial protocol used to exchange routing information between different autonomous systems on the internet. It enables the aggregation of specific routes into a single route, which helps conserve router resources and accelerates best path calculations by reducing the size of the routing table. BGP operates using a path vector mechanism, allowing it to maintain the path information that gets updated as the network topology changes. This ensures efficient and reliable data transmission across the internet(Cisco, 2024).

OSPF - Open Shortest Path First (OSPF) is a widely used link-state routing protocol that enables routers to determine the most efficient path for data transmission within an autonomous system. Utilizing the Shortest Path First (SPF) algorithm, OSPF calculates the best routes based on the cost associated with each path(GeeksforGeeks, 2018). It shares information about directly connected links with all routers in the network, ensuring that each router has a complete view of the network topology. This dynamic approach enhances routing efficiency and adaptability to network changes.

**Appendix C**

**Network Configuration and Management**

MPLS - Multiprotocol Label Switching (MPLS) is a high-performance networking technology that directs data from one node to another based on short path labels rather than long network addresses(Sturt, n.d.). This method enhances the speed and efficiency of data transmission across Wide Area Networks (WANs). MPLS supports multiple protocols, allowing for flexible traffic management and improved bandwidth utilization. By establishing predetermined paths for data packets, MPLS reduces latency and optimizes network performance, making it a popular choice for service providers and enterprises alike.

Configuration management - is a systematic process aimed at establishing and maintaining the consistency of a product's performance, functional, and physical attributes throughout its lifecycle. It involves tracking and controlling changes to software and hardware configurations, ensuring that systems remain in a desired state(Buchanan, 2024). Key aspects of CM include Change Control, Version Control, and Audit and Compliance.

DHCP - Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically assign IP addresses and other configuration settings to devices on a network(Microsoft, 2021). When a device connects, the DHCP server leases an IP address from a predefined pool, ensuring efficient use of IP addresses and reducing manual configuration efforts. Key functions of DHCP include IP address assignment, configuration information, and lease management.

VPN - A VPN, or Virtual Private Network, creates a secure, encrypted tunnel between your computer and a trusted network(GeeksforGeeks, 2017). This is like having a private, secure connection even when you're using public Wi-Fi or an untrusted internet service provider. It's a great way to protect your privacy and keep your online activity hidden from prying eyes. Think of it as a shield for your data, making it harder for others to see what you're doing online.

VLAN - A VLAN, or Virtual Local Area Network, is like creating smaller, separate domains within a network(GeeksforGeeks, 2023). Each room represents a VLAN, allowing you to group devices together based on their function or location. This helps keep traffic organized, improves security, and makes it easier to manage your network.

SIEM - Security Information and Event Management (SIEM) is a crucial component in cybersecurity that combines security information management (SIM) and security event management (SEM). SIEM systems collect and analyze logs from various sources across an organization, including servers, network devices, and security solutions(Fortinet, n.d.). This technology helps organizations detect potential security threats, manage compliance, and respond to incidents effectively. By aggregating and normalizing data, SIEM enables real-time monitoring and analysis, providing a comprehensive view of security activities and enhancing overall security posture.

References:

*Anupam Datta*. (n.d.). Www.andrew.cmu.edu. https://www.andrew.cmu.edu/user/danupam/compositional-security.html

Awati, R. (n.d.). *What is a trusted computing base (TCB)?* SearchSecurity. https://www.techtarget.com/searchsecurity/definition/trusted-computing-base

Buchanan, I. (2024). *Configuration management: definition and benefits*. Atlassian. https://www.atlassian.com/microservices/microservices-architecture/configuration-management

Cisco. (2019). *What Is Network Segmentation?* Cisco. https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

Cisco. (2024, August 15). *Understanding Route Aggregation in BGP*. Cisco. https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5441-aggregation.html

Fortinet. (n.d.-a). *What Is a DMZ and Why Would You Use It?* Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-dmz

Fortinet. (n.d.-b). *What is SIEM: A security information and event management primer*. Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-siem

Fortinet. (2023). *What is Air Gap? Essential Guide to Air Gap Security | Fortinet*. Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-air-gap

Fortinet. (2024). *What is Defense in Depth? Defined and Explained*. Fortinet. https://www.fortinet.com/resources/cyberglossary/defense-in-depth

GeeksforGeeks. (2018, April 20). *Open Shortest Path First (OSPF) protocol States - GeeksforGeeks*. GeeksforGeeks. https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-states/

GeeksforGeeks. (2023, March 24). *Virtual LAN (VLAN) - GeeksforGeeks*. GeeksforGeeks. https://www.geeksforgeeks.org/virtual-lan-vlan/

geeksforgeeks. (2017, October 5). *What is VPN & How It Works?* GeeksforGeeks. https://www.geeksforgeeks.org/what-is-vpn-and-how-it-works/

Microsoft. (2021, July 29). *Dynamic Host Configuration Protocol (DHCP)*. Learn.microsoft.com; Microsoft. https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

Sturt, R. (n.d.). *What is Multiprotocol Label Switching (MPLS)?* SearchNetworking. https://www.techtarget.com/searchnetworking/definition/Multiprotocol-Label-Switching-MPLS

*What is Dependency - Cybersecurity Terms and Definitions*. (2025). Vpnunlimited.com. https://www.vpnunlimited.com/help/cybersecurity/dependency?srsltid=AfmBOooQlddextjPAUrt-TayU-Ddg4ezsmbgws6OqPMBYJkRjp4MjV4o

*What is Proxy Server?* (2020, July 12). GeeksforGeeks. https://www.geeksforgeeks.org/what-is-proxy-server/

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage.