ISSN: 2832-790X
DOI: 10.33552/OJRAT.2025.04.000576
Online Journal of Robotics & Automation Technology
Iris Publishers

Mini-Review

Ensuring a Strong Security Architecture Using Security Engineering

Cheryl Ann Alexander[1]*, and Lidong Wang[2]

[1]*Institute for IT Innovation and Smart Health, Mississippi, USA*

[2]*Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA*

***Corresponding author:** Cheryl Ann Alexander, Institute for IT Innovation and Smart Health, Mississippi, USA

Received Date: April 22, 2024

Published Date: May 21, 2025

Abstract

Security engineering is the implementation of a security architecture for all members and processes in an enterprise to reduce the risk of cybercrimes. The security architect conducts a comprehensive risk assessment to ensure accurate provisions are covered. Security engineering is an iterative process. With the explosion of technology in recent years, it is important to identify risks and establish a threat-based system that meets the organization's security needs. Because data is the primary important asset and the most likely to be at risk for cybercrime, both a Virtual Private Network (VPN) and a Virtual Local Area Network (VLAN) are often used to protect against security risks and help with data protection. Another tool that security architects use is a firewall. A firewall is a common tool used in data protection and protecting hardware such as routers and servers. Other tools, such as switches and mitigation tools, are also being used for data protection and hardware protection. This paper introduces these concepts and discusses how these tools are used in protecting the enterprise and its systems.

Keywords: Firewall; Router; Switch; Virtual Private Network (VPN); Virtual Local Area Network (VLAN); Mitigation

Introduction

Security engineering is the implementation of the security architecture associated with all members and processes to reduce the risk of cybercrime. This is done to protect and secure all information within the business or enterprise [1]. To ensure that the security architecture meets the goals set by the security architect, a risk assessment must be conducted to get an accurate idea of the needs of the business or organization. In an iterative process, the identification of risks requires the security architect to design a security architecture that will encompass applicable security controls. For example, some of the risks to be identified are avoidance, transfer, reduction, and acceptance [1]. With technology exploding in the industry, enterprises are struggling to protect data and keep cybercriminals from controlling the industry. Organizations have realized that the informatization of production and operation is not perfect, and security architects have lagged behind the development of security engineering. The security architect should be able to establish a threat-based security system that protects the data [2].

Driving the technology behind enterprises is the cloud-based system. However, enterprises today must connect remote offices,

research sites, and other mobile or remote systems; thus, having a quality broadband system is critical. For a medical center, protecting data in remote and mobile systems is key to being a successful healthcare system. Medical providers, staff, nurses, etc., carry mobile phones and laptops to perform job duties [3]. A security engineer must consider what the facility's needs are and develop a security engineering plan. Subsequently, work mobility is essential for almost any enterprise, and as a result, the need to use a Virtual Private Network (VPN) becomes more obligatory for data protection because healthcare data has become one of the most precious commodities in networking. With the use of an established VPN, the two ends of a network become more securely connected [3].

A well-designed security architecture

With the rapid development of networking, science, and technology in modern society, enterprises are developing more open, standardized, and interconnected network designs. Therefore, there is a need for a more targeted network security mode that enhances security design and strength [3]. Security protects these interests and must be designed to accommodate the facility and the networking system. A well-designed security network is protected [1]. Some services, in their first stage and installation, are ready for all types of attacks, but others may have installation problems and need a careful evaluation to secure them from cyberattacks. Any unnecessary programs or designs should be avoided. Data must be transmitted across devices in the right format, at the right time, and at the correct location [4]. The smaller the system, the simpler the network security is, making complexity the enemy of a successful security system. When the system itself cannot be made sufficiently simple, breaking the system up into partitioned sections can be a solution. The parts with the most risk for attack should be broken down into simpler sections [1].

Migration to the cloud can bring cyberattacks

As technology advances, the design for migration to the cloud brings massive changes to the security architecture and security engineering. However, the cloud is highly susceptible to attacks. Blockchain can be used with the cloud to ensure data security. To assume the cloud service provider's ultimate authority over the data, a master hash value is provided for the data [5, 6]. Hash is a mathematical function used by blockchain to protect data integrity [6]. However, the network has become automated, and very advanced tools have become necessary to advance security design. Enterprises are currently facing new and advanced threats, and having software-implemented networks (SDNs) has the greatest potential for combating new threats. SDN is an architectural approach that uses central and intelligent control and shifts control from hardware to software. SDN architecture is made up of three layers: 1) the application layer; 2) the control layer; and 3) the infrastructure layer-switches and routers that receive instructions from the router on where the data packets go [7]. A centrally controlled security architecture has several benefits. Data is routed through a singular, centrally controlled node, making IDS and IPS data entry more efficient by pushing data packets through a singular node [7].

Smart healthcare and network slicing

Network slicing is widely being used in smart healthcare, mobile systems, Industry 4.0 drones, etc., and with a huge domain area, complicated intrinsic requirements, and large-scale applications, there are numerous areas suitable for future research and current open research areas [8]. At Charleston Medical Center, network slicing is used for machine learning of patient data to help predict outcomes, make recommendations for diagnosis and treatment, and protect mobile systems. Machine learning and artificial intelligence (AI) are used to improve network slicing. Network slicing saves energy and targets sustainability [8].

The Internet of Things (IoT) and the Internet of Medical Things (IoMT) have been considered in the medical field for quite some time. The question of how to secure reliable and accessible infrastructure becomes pertinent in the healthcare facility. Blockchain is one method of securing reliable and accessible IoT and MIoT. Because IoT has many privacy and security challenges, traditional security protocols leave much to be desired for IoT devices. However, blockchain is a distributed storage model where privacy and security are possible for the huge number of IoT and MIoT devices. Point-to-point transmission, a consensus mechanism, smart contracts, etc., are the foundation of blockchain. In Charleston Medical Center, blockchain is feasible not only to protect data but also to ensure that privacy standards such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 are met [9].

Network infrastructure in the Medical Center

Network infrastructure devices include routers, firewalls, switches, servers, etc. [10]. Figure 1 shows the main network infrastructure devices in Charleston Regional Medical Center in the US, where virtual local area networks (VLANs) are also used. For the network devices in the Medical Center, the vendor default settings are often not changed before they are used; the devices are often not hardened for operations, or regular patching is not performed. The network devices are often overlooked when intruders are investigated, and general-purpose hosts after cyber intrusions are restored. Attack surface minimization should be implemented. System hardening, removing/disabling unneeded components and services, is a kind of attack surface minimization [1]. Table 1 lists the security weaknesses in the Medical Center and recommended mitigations [10]. Virtual separation utilizes the same design principles as physical segmentation but requires no additional hardware. Unfiltered lateral communications allow an intruder to create backdoors that deter a defender's efforts to remove the intruder. Secure access procedures and policies should be implemented to stop unauthorized infrastructure access. Breaches in the supply chain provide opportunities for malicious hardware and software to be installed on devices. The integrity of the software should be checked regularly [10].

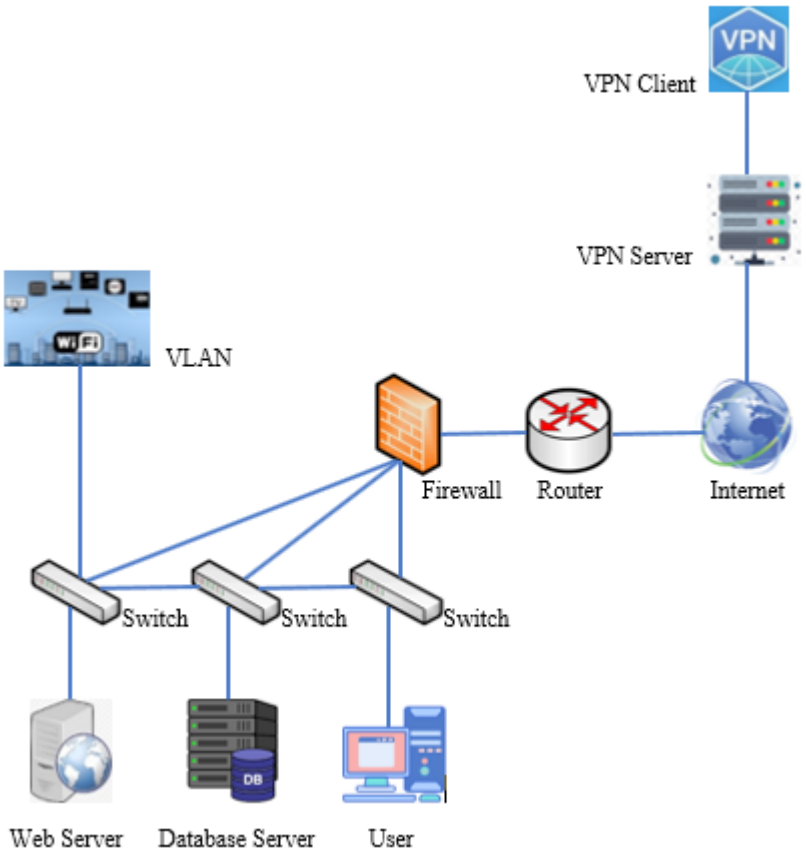

Figure 1: The Network Diagram of the Medical Center.

Table 1: Security Weaknesses in the Medical Center and Recommended Mitigations.

Weaknesses	Recommendations
Networks and functions are not well-segmented and well-segregated.	**Physical separation of sensitive information:** • Perform the least privilege when designing network segments. • Separate sensitive information and security **requirements into network segments.** Virtual separation of sensitive information: • Using VPNs to securely extend a host/network. • Using private VLANs to isolate a user from the rest of the broadcast domains.
Unfiltered lateral communications	**Limit unnecessary lateral communications:** • Restrict communication employing host-based firewall rules to deny the flow of packets from other hosts. • Ful fill a VLAN access control list that controls access to and from VLANs.

Networking devices with inadequately secure configurations	**Harden network devices:** • Disable unencrypted remote administration protocols used for managing network infrastructure. • Protect switches and routers by controlling access lists.
Administrative privileges are improperly authorized or not closely audited.	**Secure access to infrastructure devices:** • Perform multi-factor authentication using (password, fingerprint, token, etc.). • Manage privileged access according to the policy of least privilege.
Sometimes, primary communication services are interrupted due to network outages and disruptions.	**Implement Out-of-Band management:** • Segregate standard network traffic from management traffic. • Manage all administrative functions from a completely patched host over a secure channel, preferably on OoB.
Compromised hardware or software are possibly installed on devices.	**Validate integrity of hardware and software:** • Upon installation, check all devices for the signs of tampering. • Monitor and log devices to verify the network configuration of devices on a regular basis.

Conclusion

The security architect ensures that security architecture meets its goals, and it is crucial that a risk assessment is performed to get a precise idea of the needs of the business. In an iterative process, the security architect must design a security architecture that will incorporate applicable security controls. For example, some of the risks that can be threats to the security system are avoidance, transfer, reduction, and acceptance. The cloud has wide accessibility that makes it highly susceptible to attacks. Blockchain can be used with the cloud to ensure data security. A firmly segregated network can segregate malicious occurrences, reducing the impact of intruders. Virtual separation is the logical isolation of networks. To increase the awareness of security weaknesses in the Medical Center and follow the recommended mitigations help practice robust cybersecurity.

Acknowledgements

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

Declaration of the use of AI tools

The authors declare that they did not use AI tools in writing this paper.

Conflict of interest

The authors would like to announce that there is no conflict of interest.

Ethics

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

References

1. Warsinske J, Henry K, Graff M, Hoover C, Malisow B, et al. (2019) The Official (ISC) 2 Guide to the CISSP CBK Reference. John Wiley & Sons.
2. Wang Q (2020) The strategy of enterprise network security protection based on cloud computing. In IOP Conference Series: Materials Science and Engineering 750(1): 012234.
3. Gentile AF, Fazio P, Miceli G (2021) A Survey on the implementation and management of secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in static and mobile scenarios. In Telecom 2(4): 430-445.
4. Kamalov F, Gheisari M, Liu Y, Feylizadeh MR, Moussa S (2023) Critical controlling for network security and privacy based on blockchain technology: A Fuzzy DEMATEL approach. Sustainability 15(13): 10068.
5. Awadallah R, Samsudin A, Teh JS, Almazrooie M (2021) An integrated architecture for maintaining security in cloud computing based on blockchain. IEEE Access 9: 69513-69526.
6. Bhutta MNM, Khwaja AA, Nadeem A, Ahmad HF, Khan MK, et al. (2021) A survey on blockchain technology: Evolution, architecture, and security. IEEE Access 9: 61048-61073.
7. Alaoui RM, Claver NP, Aissata C, Samake M, Bahnasse A (2021) Use cases of SDN for network security. Turkish Online Journal of Qualitative Inquiry 12(7).
8. Martins JS, Carvalho TC, Moreira R, Both C, Donatti A, et al. (2023) Enhancing network slicing architectures with machine learning, security, sustainability, and experimental network integration.
9. Kharatyan A, Günther M, Anacker H, Japs S, Dumitrescu R (2022) Security-and Safety-Driven functional architecture development exemplified by automotive systems engineering. Procedia CIRP 109: 586-591.
10. Cybersecurity & Infrastructure Agency (CISA). (2020) Securing network infrastructure devices. CISA.