**Mitigation Plans for Rogue Access Point Attack**

Group 12: Brianna Deaubler, Madelyn Speers, Angelin Benny, Daut Hadzijusufovic

CIS4219: Human Aspects of Cybersecurity

*November 18, 2024*

**Introduction**

Our company, a mid-sized organization in a secure, multi-floor building, recently faced a serious cybersecurity breach caused by a rogue access point (AP) attack. Although we have strong physical security measures in place, like ID card scanners and a guard desk at the entrance, our network lacks a Network Access Control (NAC) system. This decision was made by a previous administrator, who determined that the cost of implementing a NAC wasn’t justified given the building’s physical security. Additionally, our organization does not have the budget to deploy a full Ethernet-based NAC system. Unfortunately, this attack revealed a critical gap in our defenses, resulting in the theft of corporate trade secrets and highlighting the urgent need for stronger network security measures. To address this vulnerability, we explored multiple mitigation techniques to protect against future rogue AP attacks. Each proposed solution was evaluated based on its cost and effectiveness, leading to the selection of an approach that balances affordability with enhanced security.

A rogue access point is an unauthorized device that connects to a network, allowing attackers to bypass traditional security controls [1]. It can be physically installed on the premises or remotely configured to intercept data or steal sensitive information. In our case, we assume the rogue AP was either physically placed in our building or connected through a company-provided device, as our network is primarily Ethernet-based. This incident highlights the importance of addressing network vulnerabilities to prevent similar attacks in the future.

To mitigate this threat, we considered three solutions: intrusion prevention systems (IPS), MAC address filtering, and employee cybersecurity training. An IPS monitors network traffic in real time to identify and block suspicious activity, providing a proactive layer of defense. MAC address filtering restricts access to approved devices only, preventing unauthorized connections like rogue APs. Employee training focuses on raising awareness about security best practices, such as using strong passwords and recognizing phishing attempts, to minimize human error. After evaluating the cost and effectiveness of these options, we selected MAC address filtering as our primary solution because it offers the best balance between affordability and security. This paper will analyze the rogue AP attack, evaluate the proposed mitigation techniques, and explain why MAC address filtering is the most effective approach to strengthening our network security.

**Mitigation Technique: Intrusion Prevention System**

An Intrusion Prevention System (IPS) is a proactive security measure designed to monitor network traffic, detect potential threats, and prevent unauthorized access to a network [2]. In the context of an Ethernet-based network within a mid-sized company, implementing an IPS can significantly mitigate the risks associated with rogue Access Point (AP) attacks. Given that the organization operates primarily on Ethernet connections and cannot afford an Ethernet-based Network Access Control (NAC) system, an IPS serves as an effective alternative.

Implementing an IPS involves integrating software or hardware solutions into the existing network infrastructure to continuously monitor and analyze network traffic for signs of malicious activity [3]. The IPS can be configured to recognize patterns indicative of a rogue AP or other unauthorized devices connected to the Ethernet network. For example, the IPS would monitor for unusual traffic patterns, such as unexpected MAC addresses, abnormal data flows, or unauthorized DHCP servers. When such anomalies are detected, the IPS can automatically block the suspicious activity and alert the network administrators for further investigation.

Consider a scenario where an attacker, Alex, gains unauthorized physical access to the building—perhaps by slipping past the guard desk or using a stolen ID card. Alex then connects a rogue AP to an unused Ethernet port in a conference room. This rogue AP creates a backdoor into the network, allowing external devices to connect wirelessly and access sensitive information.

With an IPS in place, the system would detect the new device on the network by identifying an unfamiliar MAC address and unusual traffic patterns associated with the rogue AP. The IPS would then take immediate action to block network communication with the rogue device and notify the security team, effectively neutralizing the threat before any data could be compromised.

Going back to Implementing an IPS, the actual process for doing so is comprehensive and can be broadly divided into seven steps. The first is the assessment and planning stage, where professionals would conduct a thorough network assessment to identify critical points where an IPS can be most effective. This includes mapping out all network segments and identifying potential vulnerabilities where unauthorized devices could be connected. The second step is the selection of an IPS solution where the organization would then choose an IPS that is compatible with the existing network infrastructure. An open-source option like Snort can be a cost-effective solution [4]. The third step is the configuration and deployment of the IPS, where it is installed on strategic points within the network, such as on core switches or network gateways. This can be taken a step further and the system can be configured to monitor for specific indicators of compromise related to rogue APs and unauthorized devices. The fourth step relates to policy development, where security policies and rules within the IPS are established in order to define what constitutes normal network behavior versus suspicious activity. The fifth step relates to integrating existing security measures, like firewalls and security information and event management (SIEM) systems, to create a unified defense strategy. The sixth and seventh step focus on testing, validation, and employee training related to managing and responding to alerts from the IPS.

Implementing an IPS would be considered a moderate cost [5]. While it does not require the extensive financial resources of a full Ethernet-based NAC system, there are costs associated with purchasing or licensing the IPS software, integrating it into the network, and training staff. Open-source solutions can mitigate software costs, but the organization should budget for potential hardware upgrades, maintenance, and ongoing support [6].

An IPS is effective in enhancing network security for several reasons such as real-time monitoring, automated threat responses and enhanced visibility. However, the effectiveness of an IPS depends on proper configuration and maintenance. It requires regular updates to recognize new threats and must be carefully managed to prevent false positives.

In conclusion, implementing an Intrusion Prevention System provides a practical and effective solution to mitigate rogue AP attacks in an Ethernet-based network. It addresses the vulnerabilities that physical security measures alone cannot, particularly in scenarios where an attacker gains physical access to network ports. By proactively monitoring and controlling network traffic, the IPS enhances the organization's ability to protect its assets and maintain the integrity of its operations. When combined with cybersecurity awareness training and MAC address filtering, an IPS helps form a strong network security posture against future threats.

**Mitigation Technique: MAC Address Filtering**

MAC Address Filtering is a network security approach that governs which devices are allowed to connect to an organization’s network [7]. This technique can improve overall security by restricting the number of devices that can automatically connect to the network. The devices are allowed or denied access based on their Media Access Control, or MAC address. Each distinctive address is found on the device’s Network Interface Card or NIC [8]. Devices that have pre-approved MAC addresses are the only ones allowed to connect to the private network. Administrators have full jurisdiction over which devices are permitted to connect, and which get booted from the network [9].

When looking at the implementation of MAC addressing, there are numerous aspects to examine, including design, functionality, and effectiveness in mitigating unauthorized access. The first step to ensure MAC address filtering is implemented is device registration. This process begins with assembling a list of all the MAC addresses of the authorized devices. This ensures that the devices that were successful in connecting are registered [10]. This compiled list will then be utilized by the network’s security infrastructure to authenticate each connection request. Another aspect of MAC address filtering is the configuration of network devices to administer and enforce access control policies effectively. Administrators need to configure the control settings to allow connections from only registered MAC addresses, specifically on routers and switches. Wireless networks can be configured on access points, which prevent unsanctioned devices from initiating a wireless connection [8].

Policy enforcement is also crucial because it establishes the policies for regular updating of address lists. As devices are added or removed, the list is updated to remain constantly current [9]. Configure alerts are also present which alert against unauthorized connection attempts. These alerts can signal any rogue access points or a possible attack attempting to access the network. Regular audits and maintenance are also key to implementing MAC address filtering. This can be executed by performing periodic audits to inspect for any addresses that may be duplicates or outdated [7]. It is pivotal to update the list of any instances in which new company-owned devices are issued or replaced. This ensured that employees could not connect to any unauthorized devices [10].

When examining the estimated cost of deploying MAC address filtering, it is usually a moderately cost-effective method to enhance network security. The cost of implementing the process mainly depends on the device management policy of the organization and network size [11]. If an organization is mid-sized with its own company-owned devices, the cost is moderate and balances both security and affordability. In an environment in which devices are changed frequently and policies are enforced casually, the cost can surge too high. To maximize the effectiveness of MAC Address Filtering, it is essential to balance expenses with scalability [9]. Some of the main cost factors are the initial setup, ongoing maintenance, and tool costs. Some other costs that need to be taken into consideration are training, tools and automation, and compliance audits [12]. The overall cost of implementing and maintaining MAC Address Filtering within a company's system is a spectrum.

MAC address filtering is effective at preventing any unauthorized devices from connecting to the internal network. This makes it a very reliable hindrance against rogue access points. Two limiting factors, however, are MAC spoofing and maintenance and scalability. In MAC spoofing, attackers can spoof a legitimate MAC address and bypass the filter [7]. When looking at maintenance and scalability, the MAC address list must be constantly updated to accommodate new devices and remove outdated ones [12]. By combining MAC addressing filtering, it can be justified that overall security can be strengthened. This can be seen in a single building environment, in which access is already heavily monitored and tightly controlled [11].

**Mitigation Technique: Employee Cybersecurity Training**

A low-cost effective way for the mid-size organization to reduce the risk of a rogue access point (AP) attack is through employee cybersecurity awareness training. This training is key to helping employees understand the importance of protecting both themselves and the organization's assets. Even though physical security measures like ID card scanners and guard desks are already set in place, the biggest vulnerability often lies in human factors. With the right training, employees can serve as the first line of defense against rogue AP attacks, helping to protect the organization’s data and trade secrets from potential threats.

As stated above in the introduction, rogue AP attacks typically occur when someone physically plugs into the network by ethernet, in order to get employees to login to a “fake” network to access company data. They can do it wirelessly as well but since the office is mainly on ethernet, this is most likely a physical security breach. In this scenario, the absence of an ethernet-based NAC system 802.1X protocol, combined with physical security measures, created a false sense of security for the organization. Employees may unknowingly connect their devices to these rogue networks, thinking they are legitimate. By investing in comprehensive cybersecurity awareness training such as KnowBe4 or CISA’s training programs, the organization can prepare its employees with the knowledge to recognize the signs of such threats. These training programs can also prevent future security breaches. The cybersecurity training programs should focus on educating employees about the risks associated with connecting to unknown networks, as well as the importance of verifying network authenticity before accessing corporate resources and data. For example, employees should be trained to check for unusual network names, request identification from IT for new access points, and report any suspicious behavior. These measures make all employees active participants in protecting important corporate assets and themselves.

Furthermore, the awareness training should include best practices for device security, such as maintaining updated antivirus software on corporate devices, continually changing passwords, and enabling multi-factor authentication (MFA) wherever possible. By drilling these practices in employees’ brains, the organization can create a more secure environment that complements the physical security measures already set in place. Employees must understand that their behavior directly impacts the organization, a single negligent action can lead to significant data breaches and financial losses. It is also important to highlight the social engineering tactics attackers commonly use. Employees need to understand the unusual ways cybercriminals try to manipulate people into giving away access or sensitive information. For instance, phishing emails or pretexting calls are often used to build trust and take advantage of human vulnerabilities. Awareness training that includes verifying SSID names, recognizing rogue APs, phishing, pretexting and safe connectivity practices can help employees recognize and respond to these threats effectively.

According to Verizon’s 2024 Data Breach Investigations Report, the graph illustrates how as the years go on, employees are improving on not clicking phishing email links shown below:

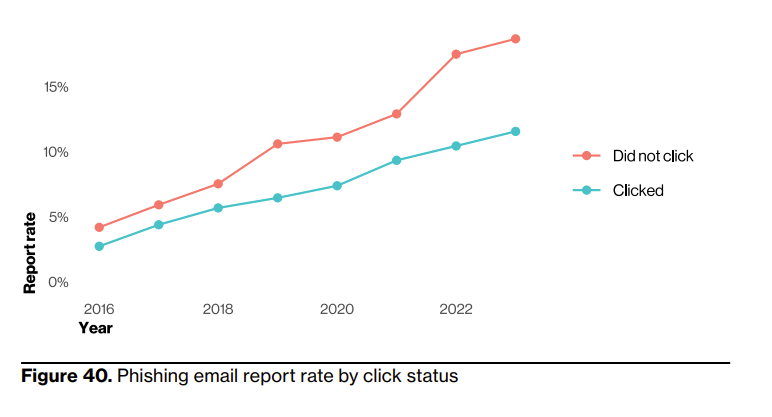


Figure 1**:** Phishing email report rate by click status

*Source: Adapted from [17]*

This figure clearly shows that employee cybersecurity awareness training is effective, but it is important to remember that cybersecurity is not a one-time task—it is an ongoing effort. The threat landscape is always changing, with new types of attacks and vulnerabilities emerging regularly. To keep up, awareness training programs need to be updated often to cover the latest cyber threats and defense techniques. Regular refresher courses every few months can help reinforce key concepts and ensure employees are aware of new risks, such as evolving social engineering tactics or advanced persistent threats (APTs). Employees should also be encouraged to report any suspicious access requests or unusual behavior right away, as quick reporting can help prevent attackers from exploiting vulnerabilities.

Incorporating feedback mechanisms into the training program can further enhance effectiveness. The organization should seek input from employees about the training materials and formats, allowing them to voice what works and what could be improved. This feedback can lead to more engaging training sessions, ensuring that they meet the learning preferences of employees. The organization should also think about introducing a rewards system to encourage participation in training programs. Recognizing employees who demonstrate a strong understanding of cybersecurity can motivate them to get more involved in the training. This not only raises cybersecurity awareness but also fosters a sense of shared responsibility in safeguarding the organization’s assets. By offering low-cost effective training programs, the organization can create a workforce that is informed and ready to tackle any potential threats. Investing in cybersecurity awareness training not only helps reduce the risk of cyberattacks but also strengthens the overall security framework. It is an important way for the organization to protect its trade secrets and encourage a proactive approach to adapting to new cybersecurity challenges.

**Conclusion**

In conclusion, the rogue access point (AP) attack revealed critical vulnerabilities in our network security, emphasizing the need for effective and feasible mitigation strategies. After analyzing multiple options, including Intrusion Prevention Systems (IPS), MAC address filtering, and employee cybersecurity training, we selected MAC address filtering as the preferred mitigation technique. This approach strikes the optimal balance between cost and effectiveness, directly addressing the risks posed by rogue APs without requiring significant financial or operational overhead.

MAC address filtering offers a practical solution by restricting network access to authorized devices. Its moderate cost makes it accessible for organizations like ours, which cannot afford the expense of implementing an ethernet-based Network Access Control (NAC) system. While it does require ongoing management to maintain an accurate list of approved devices, its straightforward implementation on existing infrastructure ensures minimal disruption to current operations. Moreover, MAC address filtering serves as an immediate barrier to unauthorized devices, preventing rogue APs from exploiting network vulnerabilities.

Though it has some limitations, such as vulnerability to MAC spoofing, MAC address filtering complements other security measures like employee training and intrusion prevention systems to create a layered defense. By focusing on this technique, we address the root cause of the attack while maintaining financial and operational feasibility. Implementing MAC address filtering positions our organization to better protect sensitive data and mitigate future threats, providing a strong and cost-effective foundation for enhanced network security.

**References**

[1] "What is a rogue access point & how to protect against them," Nilesecure. [Online]. Available: <https://nilesecure.com/network-security/what-is-a-rogue-access-point-how-to-protect-against-them#:~:text=A%20rogue%20access%20point%20is,restrictions%20or%20improve%20connectivity%20results>.

[2] "What is an intrusion prevention system (IPS)," Palo Alto Networks Cyberpedia. [Online]. Available: <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips#:~:text=What%20is%20an%20IPS%3F,potential%20threats%20and%20unauthorized%20access>.

[3] "Intrusion prevention system (IPS)," VMware. [Online]. Available: <https://www.vmware.com/topics/intrusion-prevention-system>.

[4] "Snort," Fortinet Cyberglossary. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/snort>.

[5] "Intrusion prevention system (IPS)," GeeksforGeeks. [Online]. Available: <https://www.geeksforgeeks.org/intrusion-prevention-system-ips/>.

[6] "Integrated product support (IPS) elements overview," DAU Acquipedia. [Online]. Available: <https://www.dau.edu/acquipedia-article/integrated-product-support-ips-elements-overview>.

[7] R. S. Ross, M. McEvilley, and J. C. Oren, “Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems,” *NIST Special Publication 800-160, vol. 1*, National Institute of Standards and Technology, Gaithersburg, MD, USA, Nov. 2016. Available: <https://doi.org/10.6028/NIST.SP.800-160v1>.

[8] S. R. Tate and K. S. Trivedi, "MAC address filtering: Practical implications and limitations," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Honolulu, HI, USA, Apr. 2018, pp. 1–6. doi: 10.1109/INFCOMW.2018.8407012.

[9] T. A. Fulford, "Security considerations and challenges in MAC-based filtering techniques for modern networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 3, pp. 764-774, Sept. 2019. doi: 10.1109/TNSM.2019.2921918.

[10] L. Xie, K. Kang, and J. H. Park, "Security and privacy in IEEE 802.11 wireless local area networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2876-2924, 4th Quart., 2017. doi: 10.1109/COMST.2017.2732991.

[11] A. Salah, H. D. Chen, and Y. Lin, “Assessment of MAC address filtering effectiveness in small enterprise networks,” in *Proc. 15th Int. Conf. Netw. Security (ICNS)*, Tokyo, Japan, Oct. 2017, pp. 90–95. Available: <https://doi.org/10.1109/ICNS.2017.8046812>.

[12] F. Wang and Z. Li, "Evaluation of physical and logical access control in secure environments: Lessons for modern organizations," *IEEE Access*, vol. 8, pp. 204032-204041, 2020. doi: 10.1109/ACCESS.2020.3038064.

[13] "AI-powered, new-school security awareness training," KnowBe4, 2024. [Online]. Available: [https://www.knowbe4.com](https://www.knowbe4.com/).

[14] Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity training and exercises," 2024. [Online]. Available: <https://www.cisa.gov/cybersecurity-training-exercises>.

[15] U.S. Department of Health & Human Services (HHS), "Security awareness training," 2024. [Online]. Available: <https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html>.

[16] Center for Internet Security (CIS), "Why employee cybersecurity awareness training is important," 2024. [Online]. Available: <https://www.cisecurity.org/insights/blog/why-employee-cybersecurity-awareness-training-is-important>.

[17] Verizon, "2024 Data Breach Investigations Report," 2024. [Online]. Available: <https://www.verizon.com/business/resources/Taf9/reports/2024-dbir-data-breach-investigations-report.pdf>.