

Enhancement of Security in Wireless Network

Mrs.C.Radha, Mr.R.Midunkumar, Mr.S.Muralibabu, Mr.V.Partheeban, Mr.C.Mani

Department of MCA,
Muthayammal Engineering College Namakkal, Tamilnadu, India

Abstract- Wireless networks have become ubiquitous in our modern digital landscape, facilitating connectivity and enabling seamless access to information. However, the inherent vulnerabilities of wireless communication pose significant security challenges. This paper provides a comprehensive overview of wireless network security, examining various aspects such as encryption, authentication mechanisms, access control, intrusion detection, and physical security measures. The discussion begins by highlighting the importance of encryption protocols, such as WPA2 and WPA3, in safeguarding data transmitted over wireless networks. Strong encryption mechanisms are essential for ensuring the confidentiality and integrity of sensitive information, protecting against eavesdropping and data tampering. The aim of this study was to review some literatures on wireless security in the areas of attacks, threats, vulnerabilities and some solutions to deal with those problems. It was found that attackers (hackers) have different mechanisms to attack the networks through bypassing the security trap developed by organizations and they may use one weak pint to attack the whole network of an organization. Overall, this paper provides valuable insights into the various techniques and strategies for enhancing security in wireless networks.

Index Terms- Wireless security, Connectivity, Security Challenges, Encryption Protocols, WPA2, WPA3, Authentication, Security Strategies.

I. INTRODUCTION

Wireless security refers to the technology and practices used to safeguard networks from unauthorized access, theft and other hostile actions. Wireless networks broadcast data using radio waves, which can be intercepted by anybody within the network range. As a result, wireless networks are prone to eavesdropping, illegal access and theft. A wireless network can be a cellular network, wireless LAN or other sensor or communications network, but Wi-Fi is the wireless network protocol people are generally most familiar with. Wireless security protocols such as WEP, WPA, WPA2, and WPA are commonly used to secure wireless networks. The oldest protocol, WEP, is no longer considered secure because of its vulnerability to attack. WPA and WPA2, on the other hand, were released as improved versions of WEP.

II. WIRELESS NETWORK SECURITY ARCHITECTURE

Wireless network security architecture involves a structured approach to safeguarding wireless communications and data against various threats and vulnerabilities. This architecture typically includes several layers of protection, beginning with secure device configuration and network design. At the foundation, encryption protocols such as WPA2 (Wi-Fi Protected Access 2) or the newer WPA3 play a critical role in

protecting data transmitted over the air. These protocols encrypt the data packets, making it difficult for unauthorized users to intercept and decipher the information.

Authentication mechanisms are also essential in wireless security. Implementing robust authentication methods, like 802.1X with RADIUS servers, helps verify user identities before granting access to the network. This layer ensures that only authorized users and devices can connect, reducing the risk of rogue access points and unauthorized access.



Fig.1. Wireless Network Security Architecture

Monitoring and intrusion detection systems (IDS) are also vital components. These systems analyze traffic patterns for anomalies and alert administrators to suspicious activities, allowing for real-time responses to potential threats. Regular

security audits and vulnerability assessments help identify weaknesses in the network architecture, ensuring that security measures remain effective against evolving threats.

Network segmentation is a key strategy, where the wireless network is isolated from critical internal systems. This minimizes exposure and limits the potential damage from any security breaches. For instance, guest networks can be established with restricted access to internal resources, ensuring that visitors cannot compromise the main network.

III. WORKING OF WIRELESS SECURITY

Wireless security establishes multiple layers of defense by integrating encryption, authentication, access control, device security, and intrusion detection to protect against unauthorized access and maintain network integrity. The process starts with activating encryption methods such as WPA2 or WPA3, which scramble data transfers. This ensures that even if data is intercepted, it remains unreadable to unauthorized individuals.

The next step involves securing network devices by keeping antivirus software up to date, regularly updating operating systems, and limiting the use of administrator credentials to prevent unauthorized access. Integrated intrusion detection and prevention systems (IDPS), along with other monitoring tools, track the network for any suspicious activities or security breaches. These systems are designed to detect and respond to unauthorized access attempts, malware infections, and other threats in real time.

IV. WIRELESS PROTOCOLS

Wireless network security relies on several key protocols to ensure the confidentiality, integrity, and availability of data transmitted over wireless connections. WPA2 (Wi-Fi Protected Access 2) is one of the most widely used protocols, employing the Advanced Encryption Standard (AES) to encrypt data and provide robust security against unauthorized access. Its successor, WPA3, offers enhanced security features, including improved password-based authentication and protection against offline dictionary attacks. Another important protocol is 802.1X, which facilitates port-based network access control, enabling the implementation of authentication mechanisms like RADIUS for verifying user identities before granting network access. Additionally, WEP (Wired Equivalent Privacy), an older protocol, is largely considered insecure due to its vulnerabilities, and its use is discouraged. EAP (Extensible Authentication Protocol) is also essential, supporting various authentication methods, including certificates and token-based systems. Together, these protocols form a critical framework for securing

wireless networks, addressing threats and ensuring that only authorized users can access sensitive data and resources.

1. WEP

Wired Equivalent Privacy (WEP) was introduced in 1997 to secure wireless networks through encryption and access controls. However, its reliance on the insecure RC4 encryption and shared key authentication left networks vulnerable to attacks. While WEP initially provided encryption comparable to that of wired networks, its significant flaws were quickly exploited by hackers, rendering it obsolete.

2. WPA

Wi-Fi Protected Access (WPA), introduced in 2003, was designed as a robust successor to WEP, effectively addressing its vulnerabilities. WPA employs the Temporal Key Integrity Protocol (TKIP) for improved key management and integrity checks. It operates in two modes: WPA-Personal, intended for home networks, and WPA-Enterprise, which is suited for businesses using RADIUS servers. WPA's 128-bit encryption offers significantly better protection than WEP's weaker standards, though it still pales in comparison to WPA2, leaving some potential vulnerabilities and compatibility challenges. Additionally, implementing WPA may require hardware upgrades, posing a challenge for users with older devices.

3. WPA2

WPA2 (Wi-Fi Protected Access 2) is a security protocol designed to protect wireless networks by ensuring data privacy and integrity.

It uses Advanced Encryption Standard (AES) for strong encryption, making it difficult for unauthorized users to intercept or access network data. WPA2 also employs a more secure authentication method through the use of a pre-shared key (PSK) or an enterprise model with a RADIUS server. This protocol is essential for safeguarding personal and sensitive information transmitted over Wi-Fi, making it a widely adopted standard in both home and enterprise networks.

4. WPA3

WPA3 (Wi-Fi Protected Access 3) is the latest security protocol designed to enhance wireless network security. Introduced by the Wi-Fi Alliance, WPA3 addresses vulnerabilities found in its predecessor, WPA2. It offers several key improvements, including stronger encryption with a 192-bit security suite, which helps protect against brute-force attacks. WPA3 also introduces a feature called Simultaneous Authentication of Equals (SAE), enhancing password security by making it harder for attackers to capture and crack passwords.

V. WAYS TO SECURE WI-FI NETWORKS

1. Encryption Methods

Utilize encryption methods to safeguard your network data, making it more difficult for unauthorized users to access sensitive information. Secure your Wi-Fi network with WPA2 or WPA3 standards to ensure data protection. Regularly update to the latest encryption protocols to enhance network security and defend against potential threats and data breaches.

2. Protect Your Service Set Identifier

Enable your router's firewall to enhance protection against viruses, malware, and hackers. Review its status in your router settings to strengthen your network's defenses. For added security, segment sensitive areas of your network and consider installing firewalls on all connected devices to ensure comprehensive protection.

3. Utilize Virtual Private Networks

A VPN safeguards your Wi-Fi network by encrypting your data, rendering it unreadable to potential eavesdroppers on public Wi-Fi. Opt for VPNs that utilize industry-standard AES-256 encryption and enhance security by implementing reliable open-source protocols. Many VPN applications also offer additional privacy features, such as ad blocking, split tunneling, and double VPN capability, which further enhance overall network security and privacy.

4. Deploy a Wireless Security Software

Wireless security software enhances Wi-Fi network security by integrating various features, including performance analysis, network scanning, site surveys, spectrum analysis, heat mapping, security audits, traffic analysis, packet sniffing, penetration testing, monitoring, and management. These tools enable users to identify vulnerabilities, detect unauthorized access, and implement effective security measures. Additionally, features like real-time alerts, automated reporting, and compliance checks help users maintain robust protection against potential threats and breaches, ensuring a safer Wi-Fi environment.

VI. AUTHENTICATION MECHANISMS FOR SECURING WIRELESS NETWORKS

1. Multi-factor Authentication

MFA (Multi-Factor Authentication) is a robust security measure that requires two or more forms of identity verification, such as a password combined with a physical token or biometric data like fingerprints or facial recognition. By adding extra layers of verification beyond just passwords, MFA significantly enhances security, reducing the risk of unauthorized access and defending against cyber threats like phishing and credential theft. Additional MFA options include

authenticator apps, one-time passcodes (OTPs), email confirmations, and SMS codes. Some systems also support push notifications and security questions for further authentication. Implementing MFA is a crucial step in securing sensitive information and maintaining overall cybersecurity.

2. Single Sign-On

Single Sign-On (SSO) enables users to log into one application and gain access to multiple applications across various platforms and domains seamlessly. This streamlined approach reduces the need for multiple logins, enhancing user experience and operational efficiency. A central authentication domain manages the login process and shares the session with other applications, although specific protocols may vary in their session-sharing methods. SSO often integrates features like user provisioning, federated identity management, and enhanced security measures such as MFA to bolster protection.

3. Password-Based Authentication

Password-based authentication verifies a user's identity by requiring a username and password combination. When users enter their credentials, the system compares them against stored data in its database, granting access if they match. Although this method is straightforward for users, it necessitates additional technical measures to ensure security and effective access control. To enhance protection, systems can implement features such as password complexity requirements, expiration policies, and account lockout mechanisms after multiple failed attempts. Additionally, integrating password hashing and salting techniques can help safeguard stored credentials. To further bolster security, organizations can adopt multi-factor authentication (MFA), enabling an extra layer of verification beyond just passwords.

4. Password-less Authentication

Password-less authentication replaces traditional password entry with more secure alternatives, enhancing user convenience and security. This approach utilizes various methods, such as biometrics that analyze unique physical traits like facial recognition or fingerprints. Other techniques involve possession factors, such as one-time passcodes (OTPs) sent via SMS or authenticator apps.

Additionally, passwordless authentication can employ magic links sent through email, allowing users to log in with a single click. By eliminating the need for passwords, this method reduces the risk of phishing and credential theft. Many implementations also incorporate multi-factor authentication (MFA) for added security, combining biometrics or possession factors with contextual information like device recognition or geolocation.

VII. WI-FI NETWORK SECURITY DEVICES

1. Active Device

Active device monitoring in wireless network security involves continuously tracking and managing devices connected to the network to ensure safety and compliance. This process helps identify unauthorized or suspicious devices, enabling prompt action to mitigate potential threats. By maintaining an updated inventory of connected devices, administrators can enforce security policies, manage access controls, and conduct regular audits. Additionally, active monitoring can alert users to unusual activity, such as unexpected connections or data usage spikes, allowing for swift responses to potential security breaches.

2. Passive Device

Passive device monitoring in wireless network security involves observing and analyzing network traffic without actively interfering with it. This approach enables administrators to detect unauthorized devices, analyze usage patterns, and identify potential security threats by examining data packets and communications. By collecting information on network behavior, passive monitoring can reveal vulnerabilities and anomalies, allowing for informed security assessments and strategic responses, overall security posture and ensure compliance with security policies.

3. Preventive Device

Preventive device measures in wireless network security focus on proactively safeguarding the network from potential threats before they occur. This includes implementing security protocols such as WPA3 encryption, configuring firewalls, and using intrusion prevention systems (IPS) to block unauthorized access attempts. Regular software updates and patch management are also essential to fix vulnerabilities and strengthen defenses. Additionally, conducting risk assessments and user training can enhance awareness of security practices, helping to prevent security breaches.

VIII. SECURITY THREATS

1. DNS Cache Poisoning

DNS cache poisoning is a cyberattack where a malicious actor corrupts the cache of a DNS resolver, causing it to return incorrect IP addresses for domain names. When users attempt to access a legitimate website, the poisoned DNS resolver directs them to a fraudulent site instead, potentially leading to phishing, data theft, or malware installation. This attack exploits vulnerabilities in the DNS system, emphasizing the need for security measures like DNSSEC (Domain Name System Security Extensions) to verify the authenticity of DNS responses and mitigate such risks.

2. Evil Twin Attack

An evil twin attack is a type of cyber attack where a malicious actor sets up a fake Wi-Fi hotspot that mimics a legitimate one, often in public places like cafes or airports. Unsuspecting users may connect to this rogue network, thinking it's safe. Once connected, the attacker can intercept sensitive information such as passwords, emails, and personal data. This method exploits the trust users have in familiar network names, making it crucial for individuals to verify network authenticity before connecting.

3. IP Spoofing

IP spoofing is a technique used by attackers to send IP packets from a false (or "spoofed") source address, disguising their true identity. This can be employed to bypass security measures, launch denial-of-service attacks, or impersonate another system in a network. By masquerading as a trusted source, attackers can trick systems into accepting malicious traffic or gaining unauthorized access. IP spoofing exploits the trust inherent in the Internet's design, emphasizing the importance of robust security protocols to verify the authenticity of incoming traffic.

4. Piggybacking

Piggybacking is a security breach that occurs when an unauthorized person gains access to a secure area or system by following an authorized user. This often happens in physical spaces, like offices, where someone tailgates behind an employee using a keycard or code to enter restricted areas. In digital contexts, it can involve unauthorized access to networks by exploiting a legitimate user's session. Piggybacking highlights the need for vigilance and security measures, such as access control systems and awareness training, to prevent unauthorized entry and protect sensitive information.

5. Shoulder Surfing

Shoulder surfing is a form of visual hacking where an individual observes someone else's private information, such as passwords or personal data, by looking over their shoulder. This often occurs in public places like cafes, airports, or public transportation, where screens are visible to passersby. Attackers can exploit this technique with minimal effort, making it essential for users to be aware of their surroundings and employ privacy screens or shielding techniques to protect sensitive information from prying eyes.

IX. WIRELESS NETWORK SECURITY MONITORING TOOL

1. Wireshark

A widely used network protocol analyzer that captures and inspects packets traveling through a network. It helps identify security issues by providing detailed insights into traffic and

enabling deep analysis of protocols, making it essential for diagnosing network problems and monitoring suspicious activities.

2. Airmagnet

A comprehensive wireless network performance and security solution that provides real-time monitoring, troubleshooting, and threat detection. It offers features like rogue access point detection, network visualization, and compliance reporting, making it suitable for enterprise environments.

3. Kismet

An open-source wireless network detector, sniffer, and intrusion detection system. Kismet can monitor multiple types of networks (Wi-Fi, Bluetooth, etc.) and is capable of detecting hidden networks and unauthorized devices, providing robust monitoring capabilities for security professionals.

4. NetSpot

A Wi-Fi analysis and survey tool that helps visualize wireless networks and identify coverage issues. While primarily focused on optimizing network performance, it also aids in detecting unauthorized access points and assessing overall network security.

5. Nessus

While primarily a vulnerability scanner, Nessus includes capabilities for assessing wireless network security. It scans for weaknesses in the network and can help identify rogue devices and potential security risks.

6. Cisco Wireless Security Solutions

Cisco offers a range of integrated wireless security tools that include intrusion prevention, rogue access point detection, and client profiling, providing a comprehensive approach to securing enterprise wireless networks.

X. CONCLUSION

In conclusion, the journey toward securing wireless networks is both critical and ongoing, propelled by our growing reliance on mobile connectivity and the ever-evolving threat landscape. As we have discussed, an effective wireless security strategy encompasses several key elements: the implementation of robust encryption protocols like WPA3, strong authentication mechanisms including multi-factor authentication, and continuous monitoring to detect anomalies in real time. Regular vulnerability assessments and penetration testing are essential to uncover potential weaknesses, while user education fosters a culture of security awareness. By embracing best practices and staying informed about emerging threats, organizations can significantly reduce risks. Ultimately, cultivating a proactive and vigilant approach empowers both individuals and organizations to navigate the

complexities of wireless networks safely, ensuring the integrity and confidentiality of sensitive information in our increasingly interconnected world.

REFERENCES

1. Allen-Ware MS, Bloom J, Chou JHH, Cochran M, Hughes KA, Iannicelli AT, Pearce JG, Ross A (2019) Preparing computer nodes to boot in a multidimensional torus fabric network. U.S. Patent 10,169,048, issued January 1, 2019.
2. Poonam KK, Laghari A, Laghari R (2019) A Step towards the Efficiency of Collisions in the Wireless Sensor Networks. EAI Endorsed Transactions on Scalable Information Systems,6, no. 23.
3. Wang Z, Ruan Q (2020) Research on network security subsystem based on digital signal. J Intell Fuzzy Syst 38(1):97–103.
4. Nguyen G, Nguyen BM, Tran D, Hluchy L (2018) A heuristics approach to mine behavioural data logs in mobile malware detection system. Data Knowl Eng 115:129–151.
5. Catania V, Mineo A, Monteleone S, Palesi M, Patti D (2017) Improving energy efficiency in wireless network-on-chip architectures. ACM J Emerg Technol Comput Syst (JETC) 14(1):1–24.
6. Liu Y, Chen H-H, Wang L (2016) Physical layer security for next generation wireless networks: theories, technologies, and challenges. IEEE Commun Surv Tutor 19(1):347–376.
7. Karp B, Kung HT (2000) GPSR: Greedy perimeter stateless routing for wireless networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, pp 243–254.
8. Pärilä K, Riihonen T, Wichman R, Korpi D (2018) Transfer-ring the full-duplex radio technology from wireless networking to defense and security. In 2018 52nd Asilomar Conference on Signals, Systems, and Computers. IEEE, pp 2196–2201.
9. Aneja N, Gambhir S (2018) Profile-based ad hoc social net-working using Wi-Fi direct on the top of android. Mob Inf Syst 2018:1–7.
10. Gwebu KL, Wang J, Wang Li (2018) The role of corporate reputation and crisis response strategies in data breach management. J Manag Inf Syst 35(2):683–714.
11. Palanisamy R, Norman AA, Kiah MLM (2020) Compliance with bring your own device security policies in organizations: a systematic literature review. Comput Secur 2020:101998.
12. Jouini M, Rabai LBA (2019) A security framework for secure cloud computing environments. Cloud security: concepts, methodologies, tools, and applications. IGI Global, Pennsylvania, pp 249–263.