International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2390640

Enhancing Wireless LAN Security : A Comprehensive Analysis on Threatsand Vulnerabilities

Bharath Ajay Gorli, Rithik Reddy Baddam, Geethika Chowdary Talasila

New Jersey Institute of Technology, Newark, New Jersey, USA

ARTICLEINFO

Article History:

Accepted: 10 Dec 2023

Published: 28 Dec 2023

Publication Issue

Volume 9, Issue 6

November-December-2023

Page Number

316-321

ABSTRACT

These days, wireless LANs are found everywhere—from large corporate networks to homes - because they are simple to set up, convenient for employees, don't require expensive wiring, and support continuous mobility. However, the greater availability of wireless LANs means increased danger from attacks and increased challenges to an organization, IT staff, and IT security professionals. We have implemented a time-based one-time password for wireless security lans to protect a network.

Keywords : Wireless LANs LANs, MFA

I. INTRODUCTION

Wireless LANs (WLANs) have become crucial in modern connectivity, offering flexibility and mobility. The increasing importance of Wireless LANs (WLANs) is evident in their ubiquitous presence in homes, businesses, and public areas. This widespread adoption is driven by the convenience and flexibility WLANs offer, allowing for easy Internet access without the need for physical cabling.

However, WLANs have inherent vulnerabilities, particularly in authentication and access control. These weaknesses expose them to security threats like eavesdropping and unauthorized access. Ensuring secure access is therefore a critical concern.

To enhance WLAN security, multi-factor authentication (MFA) is essential. MFA requires users to provide multiple forms of identification before gaining network access, significantly reducing the risk of unauthorized access. This approach addresses the vulnerabilities in WLANs by adding layers of security, making it more difficult for unauthorized users to gain access.

Traditional WLANs often rely on simple password-based authentication, which is susceptible to brute-force attacks and password breaches.

Weaknesses in access control mechanisms can lead to unauthorized users gaining access to the network. As WLANs transmit data wirelessly, they are susceptible to eavesdropping, where attackers can intercept and capture sensitive information.

With the increasing reliance on WLANs for internet access, ensuring secure access has become paramount to safeguarding sensitive data and maintaining user privacy.

The ubiquity of WLANs in various settings makes them attractive targets for malicious actors seeking to exploit vulnerabilities for unauthorized access. Striking a balance between providing users with convenient and flexible WLAN access and implementing robust security measures is a challenge.

II. Background

Introduction:
Evolution of WLAN Technology Trace the development of WLAN from its inception to its current advanced state. It includes the technological milestones and standardizations, like the progression from IEEE 802.11a/b/g to advanced protocols like 802.11n and 802.11ac. Exploration of the underlying principles of wireless networking, with a focus on how WLANs differ from traditional wired networks. Discusses the fundamental concepts of radio frequency (RF) technology, signal propagation, and WLAN network topology.
The Importance of WLANs in the Digital Era Discusses the growing importance of WLANs in the digital transformation era. Describes how wireless connectivity has become the foundation of many modern technologies and applications.

Usage:
Usage Applications in Various Settings: Describes how WLANs are used in various settings such as homes, businesses, educational institutions, and public hotspots. Explains how WLANs meet various needs in different settings, such as mobility in offices or convenience in homes. Facilitating Mobile

Computing and IoT : Describes how WLANs are critical in enabling mobile computing by allowing mobile devices to connect seamlessly. Also investigates the role of WLANs in the Internet of Things (IoT), which connects a plethora of devices and sensors.

Security Challenges and Risks: Discusses the security concerns that are inherent in WLANs. Discusses common flaws, such as weak encryption, and the risks they pose, such as data breaches and unauthorized network access. It emphasizes the importance of strong security measures.

III. Design Discussion

WLANs face several security challenges:

Unauthorized Access: This occurs when unauthorized users gain access to a network. Vulnerabilities in WLANs, such as weak passwords, can make networks susceptible to unauthorized access.

1. Man-in-the-Middle Attacks: In these attacks, a malicious actor intercepts communication between two parties, potentially altering or stealing data.
2. Limitations of Single-Factor Authentication: Traditional single-factor authentication, like passwords, is vulnerable to various attacks. It can be easily compromised through techniques like phishing, brute force, or social engineering.
These challenges necessitate robust security measures:
• Multi-Factor Authentication (MFA): MFA requires users to provide multiple forms of verification, vastly improving security. By combining something the user knows (like a password), something they have (like a smartphone), and something they are (like a fingerprint), MFA creates a layered defense, making unauthorized access much more difficult.

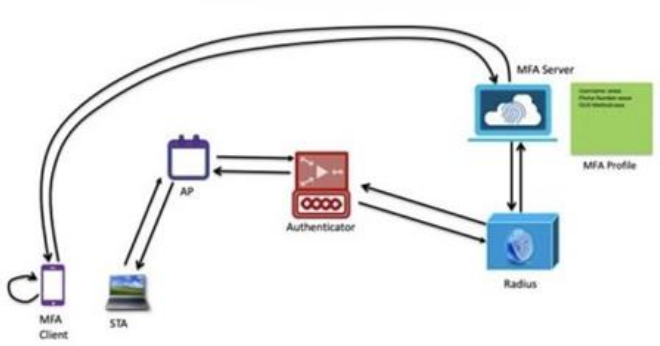

Fig 1 : WorkFlow of the MFA

User attempts to connect to the Wi-Fi network. The Wi-Fi access point sends a RADIUS authentication request to the FreeRADIUS server.

The FreeRADIUS server communicates with the Google Authenticator PAM module. The Google Authenticator PAM module prompts the user for a password and a Google Authenticator code.
User enters their password and the current Google Authenticator code from the app. The Google Authenticator PAM module validates the credentials with the user database.

If the credentials are valid, the FreeRADIUS server sends an authentication response to the Wi-Fi access point. The Wi-Fi access point grants or denies access based on the response.

IV. Architecture

The system's technical integration and architecture for implementing two-factor authentication (2FA) in Wireless LANs (WLANs). The following are the key architectural components and processes:

Technical integration entails configuring the WLAN infrastructure to support Google's 2FA, which is typically accomplished with Google Authenticator. The WLAN must be compatible with Google's authentication protocol to ensure seamless integration and function.

Configuring the Remote Authentication Dial-In User Service (RADIUS) server with user credentials and enabling a secondary authentication method, such as Time-based One-Time Passwords (TOTP) or SMS-based codes, is covered in this document. The RADIUS server is critical to the authentication process because it serves as the central point for verifying user credentials as well as the additional authentication factor.

WLAN Controller Integration: For authentication purposes, the wireless LAN controller is integrated with the RADIUS server. Configuring the wireless access points to use advanced security protocols such as WPA2-Enterprise or WPA3-Enterprise, with RADIUS serving as the authentication server, is required.

User Authentication: To gain network access, users must enter their regular credentials (such as username and password) as well as the secondary authentication factor (the OTP generated by Google Authenticator or another method). This dual-layer authentication significantly improves security.

RADIUS Client Configuration: It is critical for the system's integrity and security that RADIUS clients, such as access points, are correctly configured with RADIUS server details. Regular updates and

monitoring of the RADIUS server are also advised to ensure maximum security.

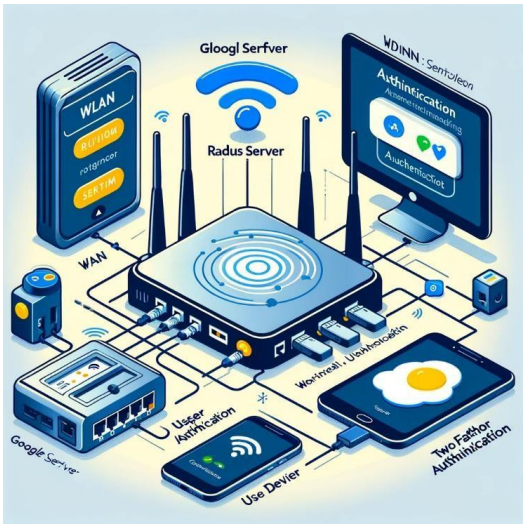

Fig 2 : WLAN -Enhanced Architecture

This architecture serves as the foundation of the WLAN-enhanced security system, focusing on robust authentication mechanisms to mitigate security risks and vulnerabilities inherent in wireless networks.

V. Methodology

Implementing two-factor authentication (2FA) using Google in WLANs involves:

1. Technical Integration: This includes setting up the network to support Google's 2FA, typically using Google Authenticator. The WLAN infrastructure must be compatible with the authentication protocol used by Google's system.
2. User Enrollment and Management: Users need to be enrolled in Google's 2FA system. This involves distributing setup instructions and potentially assisting users with the initial configuration.

When selecting authentication factors for different WLAN environments, it's crucial to balance security needs and usability. Factors like the sensitivity of the data being protected, the technical proficiency of users, and the physical security of the WLAN environment play a role in determining the most suitable authentication factors. The combination of a password and a TOTP from Google Authenticator is common, providing both security and ease of use. The effectiveness of multi-factor authentication (MFA) in enhancing WLAN security can be evaluated from both technical and practical standpoints.

We have to use the radius server for wireless LAN after implementing the 2-factor method. We have configured the RADIUS server with user credentials and enabled a secondary authentication method, such as Time-based One- Time Passwords (TOTP) or SMS-based codes. On the wireless LAN controller, we have integrated RADIUS for authentication. Configure the wireless access points to use WPA2-Enter-prise or WPA3-Enterprise security with RADIUS as the authentication server. Users must enter their regular credentials and the secondary factor for authentication. We should ensure that RADIUS clients, such as access points, are correctly configured with the RADIUS server details. Regularly update and monitor the RADIUS server for security.

WLAN Two-Factor Authentication Implementation:

Fig 3 : WLAN Two-Factor Authentication Implementation

The diagram below depicts the methodology for implementing two-factor authentication (2FA) in Wireless LANs (WLANs) to improve network security. Several key components and steps are involved in this process:

1. Wireless Router: A wireless router acts as a gateway for devices to connect to the WLAN. When a user attempts to connect, it is responsible for broadcasting the Wi-Fi signal and initiating the authentication process with the RADIUS server.

2. RADIUS Server: For user authentication, the RADIUS (Remote Authentication Dial-In User Service) server is essential. It validates the credentials of WLAN users and is set up to support two-factor authentication, in this case with Google Authenticator.
3. User Device with Google Authenticator: Users connect to the WLAN using devices that have Google Authenticator installed (such as smartphones or laptops).
4. Installing the RADIUS server software, configuring it to communicate with the wireless router, and preparing it for integration with Google Authenticator for 2FA are all part of this step.
5. Network Policies: Network policies define the rules and conditions for WLAN access. This includes defining authorized users, security protocols, and how the RADIUS server handles authentication requests.
6. Google Authenticator Integration: The final step is to integrate Google Authenticator with the RADIUS server.

VI. Evaluation

Technical Effectiveness

1. Reduction in Unauthorized Access: By requiring multiple forms of authentication, MFA significantly lowers the chances of unauthorized access. Traditional password- based systems are vulnerable to a variety of attacks, but with MFA, even if one factor (like a password) is compromised, unauthorized users still need to bypass additional layers of security.
2. Deterrence Against Common Attacks: MFA is particularly effective against common cyber attacks like phishing, credential stuffing, and brute force attacks. For instance, even if a phishing attempt retrieves a user's password, the attacker still lacks the second factor, thwarting unauthorized access.
3. Adaptability and Flexibility: MFA systems can be tailored to the specific security needs of a WLAN environment. For instance, a high-security network might use a combination of a password, a hardware token, and biometric authentication, while a less sensitive environment might only use a password and a mobile authenticator app.

VII. Related Work

Wireless LAN encryption standards such as WEP, and WPA/WPA2 are vulnerable to attack, according to Sheldon, Weber, Yoo, and Pan [1]. They showed some of the assaults on Encryption standards including the chop-chop attack, brute force, Beck-Tews, Halvorsen-Haugen, and hole 196 attacks, among others. Wang, Srinivasan, and Bhattacharjee
[2] proposed a 3-way handshake model for the 802.11i protocol instead of the traditional 4-way handshake method. They explained how their alternative method can effectively prevent DoS attacks such as de-authentication, disassociation, and memory/CPU DoS attacks. Souppaya and Scarfone [6] discussed the importance of security concerns in the WLAN configuration design, implementation, and evaluation stages, as well as the maintenance stage. They provided some general guidelines and recommendations to reduce the vulnerabilities and prevent the most common threats.
Deng Shiyang [7] and Li and Garuba [4] discuss various encryption standards related to 802.11 WLAN, as well as their vulnerabilities and security flaws. According to Stimpson et al. [9], war-driving techniques are a useful tool for assessing the security and vulnerabilities of home wireless networks.

Nevertheless, none of the researchers mentioned above have thoroughly discussed threats to WLAN security, vulnerabilities, and general recommendations for protecting them. The goal of this paper is to identify vulnerabilities, understand the most common threats, and provide general guidelines and recommendations for protecting WLAN networks and making them more secure for home users and enterprise networks.

VIII. Conclusion

MFA significantly enhances WLAN security by adding multiple layers of defense against unauthorized access and cyberattacks. Its effectiveness is evident in both theoretical analysis and real-world applications across various sectors. While the implementation of MFA does require careful planning and consideration of user experience, its benefits in securing network environments are well-documented and substantial. Wireless LANs (WLANs) play a vital role in modern connectivity, offering ubiquitous and convenient Internet access. The integration of Two-Factor Authentication (2FA) using Google Authenticator enhances WLAN security. The provided Python code demonstrates the generation and verification of Time-based One-Time Passwords (TOTPs) for user authentication, contributing to the overall security and adaptability of WLANs.

IX. Acknowledgment

"We would like to express our appreciation to the authors, Md. Waliullah and Diane Gan, for their insightful research presented in the paper 'Wireless LAN Security Threats & Vulnerabilities: A Literature Review.'" This work was critical in guiding our project and providing a fundamental understanding of WLAN security challenges. We also thank our team members and our academic mentors at the New Jersey Institute of Technology for their contributions. Their advice and expertise were invaluable in the successful completion of our WLAN security project."

X. REFERENCES

[1]. F. Sheldon, J. Weber, S. Yoo, W. Pan, 'The Insecurity of Wireless Networks." IEEE Computer Society, vol. 10, no. 4, July/August 2012, pp. 54-61.

[2]. L. Wang, B. Srinivasan, N. Bhattacharjee, 'Security Analysis and Improvements on WLANs", Journal of Networks, vol. 6, no. 3, March 2011, pp. 470-481

[3]. N. Sunday, 'Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures", Thesis (MSc), Blekinge Institute of Technology, 2008.

[4]. J. Li, M. Garuba, 'Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities", Fifth International Conference on Information Technology: New Generations, Las Vegas, Nevada, 7-9 April, 2008, pp. 557-562.

[5]. Wakudkar, Sachin D. and Campiglio, Ugo, "MULTI-FACTOR AUTHENTICATION IN WIRELESS NETWORKS"Technical Disclosure Commons, (April 20, 2022)

[6]. M. Souppaya, K. Scarfone, 'U.S Department of Commerce - Guidelines for Securing Wireless Local Area Networks (WLANs)", Gaithersburg, MD 20899-8930: National Institute of Standards and Technology, 2012, SP 800-153.

[7]. D. Shiyang," Compare of New Security Strategy With Several Others in WLAN", IEEE 2nd International Conference on Computer Engineering and Technology, Chengdu, China, 16-18 April 2010. pp. 24-28.

[8]. M. Mathews, R. Hunt, 'Evolution of wireless LAN security architecture to IEEE 802.11i (WPA2)", University of Canterbury, New Zealand.

[9]. T. Stimpson, L. Liu, J., Zhang, R. Hill, W. Liu, Y. Zhan, 'Assessment of Security and Vulnerability of Home Wireless Networks", IEEE 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, 29-31 May, 2012, pp. 2133-21

Cite this article as : Bharath Ajay Gorli, Rithik Reddy Baddam, Geethika Chowdary Talasila, "Enhancing Wireless LAN Security : A Comprehensive Analysis on Threatsand Vulnerabilities", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 6, pp.316-321, November-December-2023. Available at doi : https://doi.org/10.32628/CSEIT2390640
Journal URL : https://ijsrcseit.com/CSEIT2390640