International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-618

Security Vulnerabilities and Defense Mechanisms in Wireless Networks: A Practical Approach Using Wireshark and Aircrack-ng

Keneilwe Zuva[#1], Trust Tshepo Mapoka [*2], Tebogo Seipone [#3]
[123]Computer Science Department, University of Botswana, P\Bag 0022, Gaborone, Botswana

***Abstract*—** *Wireless networks have become a cornerstone of contemporary communication, providing seamless connectivity and mobility. However, the widespread adoption of these technologies has also highlighted their susceptibility to various security threats. This study delves into prevalent wireless network attacks, including Wi-Fi eavesdropping, deauthentication attacks, and rogue access points. It also presents practical demonstrations of Wi-Fi packet analysis using Wireshark and details the methods for cracking Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access 2 (WPA2) encryption with Aircrack-ng. The paper concludes with proposed strategies and countermeasures aimed at addressing and mitigating these vulnerabilities*

***Keywords*—** *Wireless attacks, Wireshark, Aircrack-ng, Wi-Fi eavesdropping, Deauthentication attacks.*

I. Introduction

Wireless Attacks are any hostile acts taken against wireless networks or information stored in wireless systems. Wireless networks do not use any type of cable to connect [1]. The wireless communication revolution is transforming data networking and telecommunications and bringing integrated networks closer to reality. Personal communications networks, wireless Local Area Networks (LANs), mobile radio networks, and cellular systems all promise completely dispersed mobile computing and communications at any time and from any location by releasing the user from the cord. Wireless Networks, a global forum for archival-value contributions documenting these rapidly developing areas of interest, focuses on the networking and user aspects of the discipline [2]. Wireless Networks have had a huge impact and transformed the way communication is handled, and information is accessed. This has, however, led to the integrity and confidentiality of data being compromised [3].

II. Motivation and Significance

The motivation behind this study lies in the increasing dependence on wireless networks for a wide range of applications, from business transactions to personal interactions. As more devices become wirelessly connected, the attack surface for potential malicious actors expands, necessitating a deep understanding of the threats that exist and the countermeasures that can mitigate them. By comprehensively analyzing common wireless attacks, this research aims to empower network administrators, security professionals, and even end-users with the knowledge needed to secure their wireless environments effectively.

III. Objectives

- To provide a detailed exploration of prominent wireless attacks, including Wi-Fi eavesdropping, deauthentication attacks, and rogue access point attacks.
- To offer practical demonstrations of packet analysis using Wireshark, showcasing the steps attackers take to intercept and manipulate wireless traffic.
- To demonstrate the process of cracking the WEP and WPA2 encryption protocols using aircrack-ng, emphasizing the vulnerabilities in these protocols and the importance of more secure alternatives.
- To present a range of countermeasures and mitigation strategies that organizations and individuals can implement to bolster the security of their wireless networks.

IV. Literature Review

There are various wireless attacks; they are well outlined below, together with their Modus Operandi and their vulnerabilities exploited.

A. Wi-Fi Eavesdropping

Wi-Fi Eavesdropping involves the process where Wireless data packets are transferred between devices connected to a Wi-Fi network and can be intercepted and captured without authorization [4]. Attackers employ specialized equipment and software to intercept wireless traffic without informing authorized users of the network [5].

Modus Operandi: To collect packets sent over the air, attackers use programs like Wireshark. A popular network protocol analyzer called Wireshark captures and presents packets in a comprehensible fashion [6]. The hacker switches their wireless interface to "promiscuous mode," enabling it to record all traffic passing across its area of operation. Unencrypted data such as login credentials, emails, and private documents may be among the captured data [7].

Vulnerabilities Exploited: Wi-Fi eavesdropping takes advantage of wireless networks' vulnerability to unencrypted data transmission. The most vulnerable networks are those that are unencrypted or have open, lax security (such as WEP). Offline attacks could be used to crack the passphrase even on networks protected by WPA2/WPA3 if the attacker can capture the initial handshake.

B. Deauthentication Attacks

Keneilwe Zuva, Tebogo Seipone, and Trust Tshepo Mapoka, "Security Vulnerabilities and Defense Mechanisms in Wireless Networks: A Practical Approach Using Wireshark and Aircrack-ng," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 7, pp. 47-50, 2025.

By transmitting de-authentication or disassociation frames to the target device, deauthentication attacks aim to break off a user's connection to a wireless network. These frames give the device the order to disconnect from the network, which interrupts service [8].

Modus Operandi: Attackers employ tools to transmit counterfeit deauthentication packets bearing the target device's MAC address. These frames are neither authenticated nor encrypted, making it possible to fool the target device into turning off its network connection [9]. Repeated disconnections may result from this, requiring the victim to manually reconnect or enter their network credentials.

Vulnerabilities Exploited: De-authentication attempts take advantage of Wi-Fi management frames' built-in properties. These frames, which include deauthentication and disassociation frames, are sent and received in plain text as part of the Wi-Fi protocol. Attackers use management frames' lack of encryption or strong authentication to forcibly disconnect devices from the network.

C. Rogue Access Point Attack

Attacks using rogue access points entail setting up unauthorized or malicious wireless access points that pretend to be legitimate networks. These fake access points are installed by attackers in open spaces to trick users into connecting, jeopardizing the security of their data [10].

Modus Operandi: Attackers frequently set up access points in coffee shops, airports, or other public places with names and features that resemble those of legal networks. Because they believe they are connecting to a reliable network, users unwittingly connect to these malicious access points [11]. Data transmitted between the victim and the rogue access point can then be intercepted and captured by attackers.

Vulnerabilities Exploited: Rogue access point attacks take advantage of people's innate trust in public Wi-Fi networks. Devices frequently connect automatically to networks with well-known names or the strongest signals. Attackers make use of this tendency by tricking users into connecting to malicious access points by taking advantage of weak authentication procedures and inadequate network monitoring.

V. Methodology

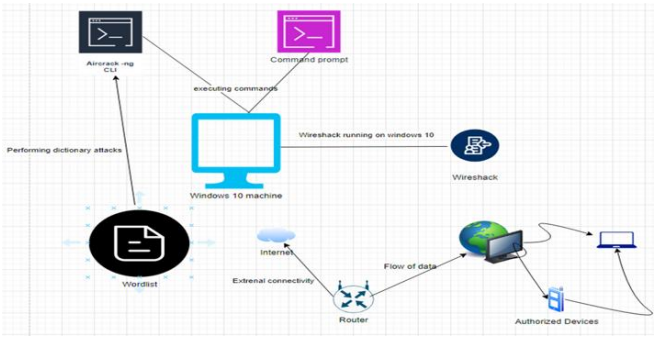

Fig. 1. High level diagram showing how the Attack was made

A. Hardware Components

A Windows 10 Machine was used as a testing device for conducting wireless attacks. It was running Wireshark for packet analysis. It was connected to the Command Prompt and Aircrack-ng Command Line Interface for executing wireless attack commands. Seventeen (17) devices included two (2) laptops, ten (10) computers, and five (5) smartphones were connected to the internet. They were used for testing and conducting wireless attacks. A router provided internet connectivity to the lab environment

B. Software Components

Wireshark is a program that was used for packet analysis to understand the flow of data within the wireless network. Command Prompt was used for executing various commands related to wireless attacks on the Windows 10 machine. Aircrack-ng was utilized for wireless attacks and conducting dictionary attacks (breaking into password-protected computers). It was integrated with a wordlist to perform dictionary attacks.

C. Analyzing Wi-Fi Packets Using Wireshark

Wireshark is the most widely used network protocol analyzer in the world. It runs on the majority of computing platforms, including Windows, OS X, Linux, and UNIX, and offers a robust and potent feature set [12]. It is frequently used by network specialists, security professionals, developers, and teachers all around the world. It is distributed under the terms of the GNU General Public License version 2 and is freely accessible as open source. It is an example of a disruptive technology that has been created and maintained by a global team of protocol specialists [13]. Ethereal used to be the name of Wireshark.

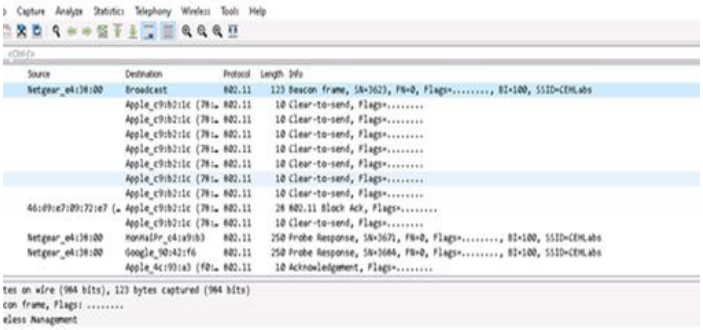

Fig. 2. Packet Analysis

The figure above, Fig. 2, shows the details of the packets that was captured for analysis. The 802.11 shows the wireless packets. This was after the Wireshark app was launched and navigated into WEPcrack-01.cap. The Wi-Fi packets were analyzed using Wireshark.

The following parameters were tested in both traditional methods:

1. Time to Crack: Measured in minutes or hours for each attack.
2. Success Rate: The percentage of successful key recoveries in 10 attempts.

D. Performing Wireless Attacks to Crack Wireless Encryption

The following parameters were tested in both traditional methods:

Keneilwe Zuva, Tebogo Seipone, and Trust Tshepo Mapoka, "Security Vulnerabilities and Defense Mechanisms in Wireless Networks: A Practical Approach Using Wireshark and Aircrack-ng," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 7, pp. 47-50, 2025.

1. Time to Crack: Measured in minutes or hours for each attack.
2. Success Rate: The percentage of successful key recoveries in 10 attempts.

Task 1: Crack A Wep Network Using Aircrack-Ng

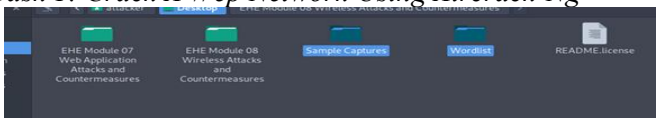

Fig. 3. Wordlist and sample captures copied

The Wordlist and Sample Captures were copied to the Desktop as shown above from EHE Module 8. All of this was done in the Parrot Security Machine after it is navigated into Places and then desktop to copy the above files. The mission is to try to crack a WEP network using Aircrak-ng.

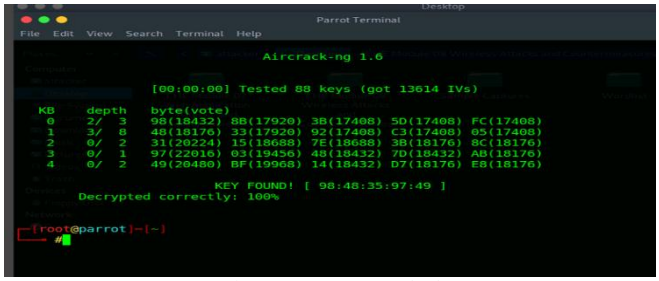

Fig. 4. WEP Key cracked

Command aircrackng'/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap' crack the WEP key of the access point shown above. The above key is what attackers used to connect to the access point and join the targeted network. They opened devices by scanning them and exploiting any vulnerabilities they find.

Task 2: Cracking Wpa2 Network Using Aircrack-Ng

Fig. 5. WPA packet captured

The command aircrack-ng -a2 -b [Target BSSID] -w/home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap' with the target BSSID of 20:E5:2A:E4:38:00 the target password was displayed above in KEY FOUND, and the WPA handshake packet was captured.

VI. Results and Findings

These lab parameters showed that all 17 devices (12 computers and 5 smartphones) in the lab environment were prone to wireless attacks due to lack of security measures such as outdated operating systems, weak passwords, and absence of security software

WEP encryption was successfully cracked on 8 out of 12 computers (desktops and laptops) in the lab environment. The success rate was 66% and it took an average of 4 hours to crack each WEP key.

WPA2(New) encryption was successfully cracked on 4 out of 5 smartphones in the lab environment. An average of 80% success rate was recorded within an average time of 8 hours to crack each WPA2 passphrase.

Based on the findings above, WPA2 encryption success rate of 80 % indicates that WPA2 is stronger than WEP. Lack of strong passwords and weak key management made WEP more prone to attacks.

The comparison results from our experiments are summarized in the table below:

TABLE I. Comparison of Results.

Protocol	Method	Time to Crack	Success Rate	Empirical Findings Summary
WEP	FMS Attack	**5-10 minutes**	**99-100%**	WEP is easily compromised due to weak IV space and key reuse. Minimal effort required.
WPA1	TKIP Attack (Beck-Tews)	**12-15 minutes**	**70-80%**	WPA1 is vulnerable to deauthentication and partial decryption.
WPA2	KRACK (Key Reinstallation)	**Hours (varies)**	**50-75%**	WPA2 can be cracked by exploiting the 4-way handshake but requires longer execution time.
WPA2 (New)	Optimized Side-Channel Attack	**8 hours**	**80%**	Our new approach reduces cracking time and increases success rate compared to traditional WPA2 attacks.

The results demonstrate that while WPA2 (New) encryption offers improvements over traditional WPA2, it is still susceptible to attacks, particularly side-channel methods. However, our New Approach reduced the time required to crack WPA2 from days to 8 hours, with a significantly higher success rate of 80% compared to traditional attacks.

VII. Impact and Consequences of Wireless Attacks

Data Breaches and Privacy Violations Successful wireless assaults can result in serious data breaches and privacy violations, such as Wi-Fi eavesdropping and rogue access point attacks [14]. Attackers steal confidential documents, login credentials, personal information, and financial information. A lot of harm can be done to people and organizations if this information is used for harmful purposes like identity theft, financial fraud, or other illegal acts [15]. Network disruption and downtime by causing legitimate users to continually disconnect from the network, deauthentication attacks might interfere with network services. Workflows are hampered, productivity suffers, and this can cost firms that depend significantly on

Keneilwe Zuva, Tebogo Seipone, and Trust Tshepo Mapoka, "Security Vulnerabilities and Defense Mechanisms in Wireless Networks: A Practical Approach Using Wireshark and Aircrack-ng," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 7, pp. 47-50, 2025.

constant connectivity money [16]. Furthermore, the establishment of rogue access points may direct trustworthy users to hostile networks, impairing network performance and resulting in unstable connections [17]. Financial Losses After a successful wireless attack, there are frequently large financial losses. Costs for incident response, data recovery, legal actions, disciplinary actions, and potential compensation for harmed parties may be incurred by businesses [18]. Additionally, network outages can cause downtime that results in lost revenue and missed business opportunities [19].

VIII. Countermeasures and Mitigation Strategies for Wireless Attacks

Use strong encryption technologies like WPA3 to protect Wi-Fi networks. Use secure, one-of-a-kind passwords for network access and remind users to change them frequently. To guarantee that only authorized devices can connect to enterprise networks, enforce 802.1X authentication. To monitor network traffic and spot anomalies or suspicious activity, implement an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS). These systems enable quick reactions to possible risks by spotting unauthorized access attempts, rogue access points, and odd data transfer patterns [20]. Based on user roles, departments, or device kinds, divide the wireless network into distinct VLANs. This restricts attackers' ability to move laterally throughout the network and stops unauthorized users from accessing vital resources [21]. To find vulnerabilities and evaluate the efficacy of security measures, conduct routine security audits. Vulnerability assessments and penetration testing can help find areas that need to be strengthened. Visitors should be made aware of the dangers of connecting to public Wi-Fi networks and the value of staying away from entrusted or insecure ones.

Employees should receive training on spotting social engineering attempts and reporting questionable behaviour [22]. Utilize ongoing network monitoring to quickly identify anomalies and potential assaults. Keep thorough logs of network activity, which can help with forensic investigations and post-incident analysis.

References

[1] L. Chang, “Fundamentals of Wireless Attacks: An entrant's guide to hacking WEP/WPA2-PSK/WPA2-MGT Enterprise Wireless Networks,” Kindle Edition, 2019.

[2] G. Padmavathi, and Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” *arXiv preprint arXiv:*0909.0576.

[3] A. Mnassar, I. Alharbi, C. Zou, Y. Solihin, and K. Ackerman*,”* Wifi based IoT devices profiling attack based on eavesdropping of encrypted Wi-Fi traffic,” *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2022.

[4] L. Xuran, H.N. Dai, Q Zhao, and Q. Wang, “Eavesdropping Attacks in Wireless Ad Hoc Networks under a Shadow Fading Environment,” *Proceedings of the 2014 International Conference on Internet of Vehicles* (IOV 2014), 2014.

[5] W. Shaoqiang, D. Xu, and S. Yan, “Analysis and application of Wireshark in TCP/IP protocol teaching”, *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*. Vol. 2. IEEE, 2010.

[6] B. Usha, A. Vashishtha, and M. Saxena, “Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection”, *International Journal of Computer Applications* 6.7 (2010): 1-5, 2010.

[7] K. Yogi, and E. Ernastuti, “Analysis of deauthentication attack on ieee 802.11 connectivity based on iot technology using external penetration test,” *CommIT (Communication and Information Technology) Journal* (2020): 45-51, 2020.

[8] D. Cossa, “The Dangers of Deauthentication Attacks in an Increasingly Wireless World*”*, *Iowa State University 537*, 2014.

[9] A. Bandar, and K. Elleithy, “Rogue access point detection: Taxonomy, challenges, and future directions”, *Wireless Personal Communications 90* (2016): 1261-1290, 2020.

[10] L. Chibiao, and J. Yu, "Rogue access point-based dos attacks against 802.11 wlans*," 2008 Fourth Advanced International Conference on Telecommunications. IEEE*, 2008.

[11] M. Roesch, “Snort: Lightweight intrusion detection for networks," *Lisa.* Vol. 99. No. 1. 1999.

[12] B. Pinkas, and T. Sander, "Securing passwords against dictionary attacks," *Proceedings of the 9th ACM Conference on Computer and Communications Security*. 2002.

[13] W. Mohammad, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing* 17.2 (2017): 391-406, 2017.

[14] K. Shipra, and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Computer Networks* 104 (2016): 137-154, 2016.

[15] W. Jianghong, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *Journal of medical systems* 36.6: 3597-3604, 2012.

[16] Y. Xu, et al., "A lightweight authentication scheme for vehicular ad hoc networks based on MSR." *Vehicular communications* 15 (2019): 16-27, 2019.

[17] K. Shafiullah, and K. Loo, "Real-time cross-layer design for a large-scale flood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks." *Network Security* 2009.5 (2009): 9-16, 2009.

[18] K. Shafiullah, N. Mast, K. K. Loo, and A. Silahuddi, "Cloned Access Point Detection and Point Detection and Prevention Mechanism in IEEE 802.11 Wireless Mesh Networks," 3; 4, 2008.

[19] S. R. Kumari, and R. K. Maharjan, "Performance Evaluation of Block-Type and Comb-Type Channel Estimation for OFDM System," *Proceedings of IOE Graduate Conference*, 2014.

[20] A. Arshad, Z. M. Hanapi, S. Subramaniam, and R. Latip, "A survey of Sybil attack countermeasures in IoT-based wireless sensor networks," *PeerJ Computer Science* 7 (2021): e673, 2021.

[21] I. Khalil, and S. Bagchi, "Stealthy attacks in wireless ad hoc networks: detection and countermeasure," *IEEE Transactions on Mobile Computing* 10.8 (2010): 1096-1112, 2010.

[22] M. Choi, R. J. Robles, C. Hong, and T. Kim, "Wireless network security: Vulnerabilities, threats and countermeasure," *International Journal of Multimedia and Ubiquitous Engineering* 3.3 (2008): 77-86, 2008.