Wi-Fi Network Security

Mohammad Asim*
College of Science & Engineering
Hamad Bin Khalifa University
Doha, Qatar
moas88849@hbku.edu.qa

Mohammad Zubair
College of Science & Engineering
Hamad Bin Khalifa University
Doha, Qatar
mozu11431@hbku.edu.qa

***Abstract*—Wireless network security has become an increasingly pressing concern. As Wi-Fi becomes the go-to access medium for internet connectivity in homes, businesses, and public spaces alike, the primary access point for attackers is also becoming more accessible. Despite the progress made from WEP to WPA3, vulnerabilities persist at both the protocol and implementation levels. This project aims to closely examine the evolution of IEEE 802.11 security protocols – WEP, WPA, WPA2, and WPA3. It explores the improvements, their known weaknesses, and the ongoing challenges arising from backward compatibility, poor configuration, and user-centered attack vectors.**

Through a detailed literature analysis and the open and unsolved challenges across all those protocol generations, this project also includes a practical case study of two contemporary wireless attack techniques. We used tools like Flipper Zero, Wireshark and Hashcat in a controlled test environment to demonstrate just how easily unsuspecting users can be tricked into handing over their sensitive credentials via a rogue access point (in the case of Captive Portal Phishing, via the *Evil Portal*) and how poor password policies can lead to complete key compromise through passive monitoring and offline brute-force cracking.

Our findings show that wireless security remains fundamentally vulnerable despite the advances in cryptography due to a mix of technical and human factors. We believe that robust encryption, secure implementation practices, real-time monitoring systems, and user education are the keys to maintaining the integrity of wireless networks and we think that's where future research should focus: on formally verified cryptographic implementations, enhanced intrusion detection systems, and moving toward passwordless authentication models to reduce our reliance on shared credentials.

***Index Terms*—Wi-Fi Security, WPA2, WPA3, Wireless Attacks, PMKID Cracking, Captive Portal, Evil Twin, Key Reinstallation Attack, Social Engineering, Wireless Protocol Vulnerabilities, IEEE 802.11, Flipper Zero, Hashcat**

I. Introduction: Motivation and Objectives

Wireless networking has become essential for modern digital life, with Internet access available in homes, businesses, and public spaces. The IEEE 802.11 standard, also known as Wi-Fi, makes this possible. However, the openness of wireless channels exposes networks to many security threats, requiring a need for more robust security protocols.

A. Evolution of Wi-Fi Security Protocols

Over the years, several security protocols have been developed to protect Wi-Fi. The first, Wired Equivalent Privacy (WEP), was found to be fundamentally broken. The Fluhrer, Mantin, and Shamir (FMS) attack showed that WEP's RC4 encryption could be broken by analyzing statistical biases in the key scheduling algorithm, so an attacker could recover the encryption key with minimal effort [1].

To fix WEP's problems, Wi-Fi Protected Access (WPA) and WPA2 with stronger encryption were introduced. But they also had vulnerabilities. The Key Reinstallation Attack (KRACK) exploited a flaw in the WPA2 four-way handshake, so an attacker could decrypt the data by manipulating and replaying the cryptographic handshakes [2].

WPA3 was developed to enhance Wi-Fi security further. It introduced the Simultaneous Authentication of Equals (SAE) handshake to provide forward secrecy and resistance to offline dictionary attacks. But the Dragonblood suite of attacks showed that WPA3 implementations could still be vulnerable to side channel attacks and downgrade vulnerabilities, so security improvements were broken [3].

B. Practical Implications and Challenges

The vulnerabilities in Wi-Fi security protocols have real-world implications. Attackers can exploit these to intercept sensitive information, inject malicious data or gain unauthorized access to the network. For example, the KRACK attack showed that even WPA2 secured networks could be broken, affecting millions of devices worldwide [2].

The Dragonblood attacks showed that WPA3, despite its improvements, is not immune to attacks. They used side-channel vulnerabilities and implementation flaws to break the security of the protocol [3]. Therefore developing secure protocols and finding new attack vectors were essential.

C. Objectives and Goals

This project aims to conduct a comprehensive analysis of Wi-Fi security protocols, focusing on their vulnerabilities and the effectiveness of corresponding mitigation strategies. The specific objectives include:

- Examine the cryptographic weaknesses in WEP, WPA, WPA2 and WPA3.
- Study different attack methods and their impact.
- Evaluate the security enhancements in WPA3 and find the remaining vulnerabilities.
- Implement and demonstrate some attack scenarios in a controlled environment to test their feasibility and impact.
- Compare the attacks and defense mechanisms based on complexity, resources and success rate.

The outcome of this project will help us understand the evolution of Wi-Fi security and guide the development of

*Corresponding author

better protection.

D. Paper Structure

The remainder of this paper is organized as follows:

- **Section II** - Background on Wi-Fi security and what is needed for secure wireless
- **Section III** - Research and technical challenges with current Wi-Fi security
- **Section IV** - State of the art solutions and mitigation techniques, comparison
- **Section V** - Open and unsolved problems in Wi-Fi security
- **Section VI** - Case study of selected attacks
- **Section VII** - Conclusion, challenges and future work
- **Section VIII** - Individual contributions

II. Background and Fundamentals

Wireless Local Area Networks (WLANs) are everywhere and seamless across domains, but the broadcast nature of wireless communication introduces a lot of security challenges. Over the years, several security protocols have been developed to secure Wi-Fi, each fixing the flaws of the previous one. This section will give an overview of these protocols so their evolution and vulnerabilities could be understood.

A. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) was the original security protocol introduced with the IEEE 802.11 standard in 1997. Its goal was to provide a security level similar to wired Ethernet networks by providing data confidentiality and limited access control over wireless transmissions. WEP uses the RC4 stream cipher with a 24-bit IV and a secret key (typically 40 or 104 bits) to generate the keystream used to encrypt data [1].

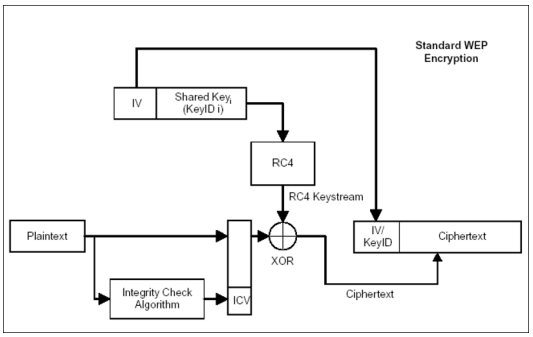

Fig. 1: WEP Encryption Process

The WEP encryption process works as follows: for each packet, the 24-bit IV is concatenated with the shared secret key to produce the RC4 seed. This seed initializes the RC4 key scheduling algorithm (KSA) which in turn generates a pseudo-random keystream. The plaintext data is XORed with this keystream to produce the ciphertext. A CRC-32 checksum is appended to the plaintext before encryption to provide a form of integrity verification.

Despite its widespread use in early Wi-Fi networks, WEP was found to be fundamentally broken due to multiple cryptographic and design level weaknesses:

- **Short IV Length and Reuse**: The 24-bit IV space results in only 2^{24} (approximately 16 million) possible IVs. In a busy network, IVs are quickly reused, enabling attackers to collect multiple packets encrypted with the same keystreamâa critical vulnerability that enables key recovery via statistical attacks.
- **RC4 Key Scheduling Weaknesses**: The combination of IV and key is input into RC4 without sufficient mixing. Fluhrer, Mantin, and Shamir (FMS) discovered that certain IV-key combinations produce observable biases in the RC4 output, which can be exploited to recover the key from captured packets [1]. This weakness is the basis of the popular Aircrack-ng and WepCrack tools.
- **Lack of Strong Integrity Checks**: WEP uses a CRC-32 checksum to verify message integrity. However, CRC-32 is linear and not cryptographically secure. An attacker can modify encrypted packets and recompute a valid checksum, allowing for undetectable tampering or packet injection [4].
- **Static Key Management**: WEP does not support any key distribution protocol. Most deployments used manually configured, static keys shared across all users. This increases the risk of compromise and makes periodic key updates cumbersome or infeasible.

These weaknesses made WEP vulnerable to both passive and active attacks. Tools like AirSnort and Aircrack-ng could crack WEP in a matter of minutes by capturing traffic. Due to these vulnerabilities, the Wi-Fi Alliance deprecated WEP in 2004 in favor of WPA and later WPA2.

WEP is now obsolete, but its shortcomings were a lesson in wireless security protocol design – especially key management, nonce/IV size, cryptographic integrity verification, and secure cipher initialization.

B. Wi-Fi Protected Access (WPA)

In response to the WEP vulnerabilities, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA) in 2003 as a transitional security solution while waiting for the full IEEE 802.11i standard. WPA was designed to be deployable on existing WEP-capable hardware via firmware upgrades, which meant its design was constrained by legacy compatibility requirements. WPA improved over WEP but still used RC4 and therefore inherited some of the weaknesses.

The main innovation in WPA is the introduction of the *Temporal Key Integrity Protocol* (TKIP), a wrapper that enhances RC4 based encryption by improving key management and integrity checking. The main components of TKIP are:

- **Per-Packet Key Mixing**: WPA generates a new, unique key for every packet by mixing the temporal session key with the packet's 48-bit Initialization Vector (IV) and the sender's MAC address. This mechanism increases resistance to key reuse attacks and significantly expands the effective key space compared to WEP.
- **Message Integrity Code (MIC)**: Often referred to as *"Michael"* the MIC provides integrity checking and helps detect tampering with packets in transit. Unlike WEP's weak CRC-32, the MIC is designed to be more tamper-resistant. However, due to performance limita-

tions on older hardware, it offers only a minimal level of cryptographic protection.

- **Extended IV and Replay Protection**: WPA uses a 48-bit IV instead of the 24-bit IV used in WEP, drastically reducing the likelihood of IV collisions. It also implements sequence counters to defend against replay attacks.

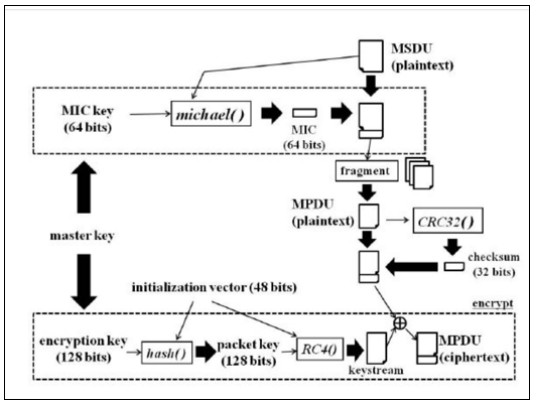

Fig. 2: WPA Encryption Process

WPA was available in two modes: **WPA-Personal** which uses a pre-shared key (PSK) and **WPA-Enterprise** which uses an 802.1X authentication server and EAP methods for dynamic key exchange. WPA-Personal is easier to deploy but vulnerable to offline dictionary attacks if weak passwords are used.

Despite fixing many of WEP's problems, WPA's use of RC4 and the limitations of the MIC (Michael) algorithm eventually made it obsolete. The Michael algorithm was found to be vulnerable to forgery attacks that could only be mitigated by temporary disconnection penalties, making strong defenses impractical [5]. Moreover, researchers showed that packet injection was possible under certain conditions due to weaknesses in the MIC's protection mechanism.

WPA was a large step forward in wireless security, especially with key rotation and packet specific encryption, but its dependency on legacy ciphers and backward-compatible design limited its life. It was eventually replaced by WPA2, which introduced a stronger cryptographic foundation with AES-based encryption under the CCMP mode

C. Wi-Fi Protected Access II (WPA2)

Wi-Fi Protected Access II (WPA2), standardized as IEEE 802.11i in 2004, succeeded WPA as the dominant security protocol for wireless networks for over a decade. Unlike WPA, which used RC4 and TKIP for encryption, WPA2 introduced support for the Advanced Encryption Standard (AES) in Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). This was a big upgrade in both data confidentiality and integrity mechanisms.

The core components that distinguish WPA2 from its predecessors are:

- **AES-CCMP**: WPA2 uses AES in CCM (Counter with CBC-MAC) mode to provide both encryption and authentication. This construction not only ensures confidentiality through AES encryption in counter mode but also guarantees integrity and authenticity via CBC-MAC. AES-CCMP supports 128-bit keys and significantly increases resistance to known plaintext attacks and message forgery.
- **Four-Way Handshake**: WPA2 introduces a robust handshake mechanism that occurs between the client (supplicant) and the access point (authenticator) after successful authentication. The four-way handshake derives a Pairwise Transient Key (PTK) from the Pairwise Master Key (PMK), along with nonces exchanged during the handshake. This PTK is then used to encrypt data frames securely.

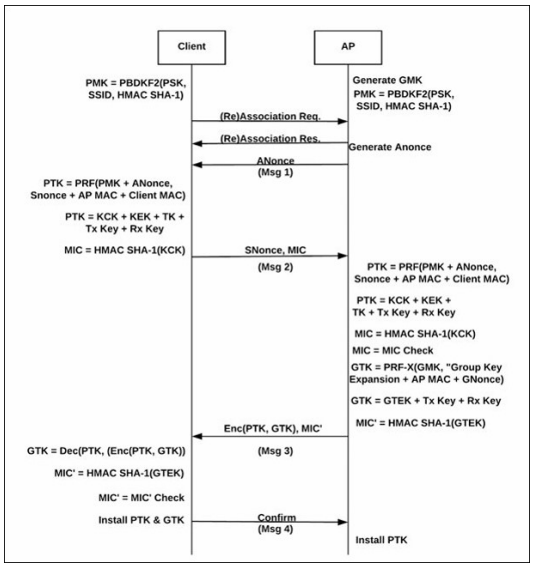

Fig. 3: WPA2 Four-Way Handshake Process

WPA2 operates in two deployment modes: **WPA2-Personal**, which uses a pre-shared key (PSK), and **WPA2-Enterprise**, which uses 802.1X with a RADIUS server to authenticate users and dynamically assign session keys. WPA2-Enterprise offers stronger user-level control and is more suitable for corporate environments, while WPA2-PSK is used in home networks

WPA2 has been a solid security protocol but not without flaws. The most notable is the *Key Reinstallation Attack* (KRACK) discovered by Vanhoef and Piessens in 2017 [2]. KRACK targets the four-way handshake and exploits the fact that retransmitted handshake messages can cause the client to reinstall the same session key multiple times. When this happens, associated counters such as the nonce and replay counter are reset, allowing an attacker to reuse keystreams to decrypt packets, inject forged data, and hijack connections. Note that this flaw is not in the cryptographic primitives of WPA2 but in its implementation logic, which made nearly all WPA2-compliant devices vulnerable at the time of discovery.

Besides KRACK, other practical issues have plagued WPA2 over time. For example, weak or predictable passwords in WPA2-PSK configurations are still vulnerable to

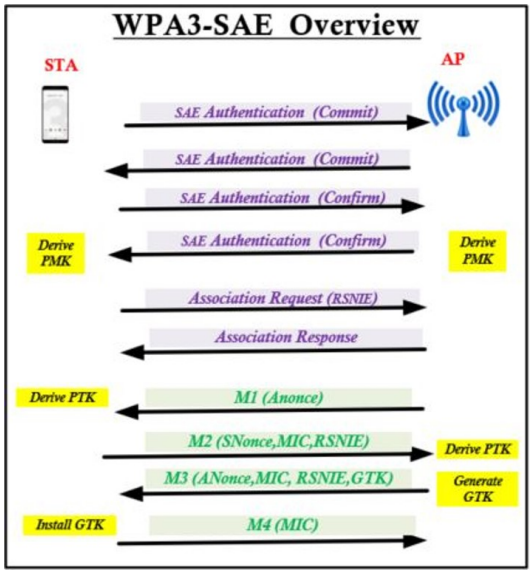

Fig. 4: WPA3 SAE Handshake

offline dictionary and brute-force attacks. WPA2 also lacks forward secrecy, if the PSK or PMK is compromised, all previous communications encrypted with that key can be decrypted retroactively.

Despite its strengths, the combination of long-term key reuse, weak password practices, and flawed retransmission handling has shown that WPA2, while secure in theory, is only as strong as its implementation and configuration in practice. These limitations led to the development and adoption of WPA3, which introduces new mechanisms to address many of WPA2's weaknesses.

D. Wi-Fi Protected Access III (WPA3)

WPA3 was introduced in 2018 to fix the issues with WPA2 and improve Wi-Fi security. Key features include:

- **Simultaneous Authentication of Equals (SAE)**: A password-based authentication protocol that provides forward secrecy and resistance to offline dictionary attacks.
- **Protected Management Frames (PMF)**: Enhances protection against eavesdropping and forging of management frames.
- **192-bit Security Suite**: Offers higher security for enterprise networks.

However, WPA3 is not without its challenges. The Dragonblood attacks show that some WPA3 implementations are vulnerable to side-channel and downgrade attacks [3].

E. Comparative Analysis

TABLE I
Comparison of Wi-Fi Security Protocols

Feature	WEP	WPA	WPA2	WPA3
Encryption Algorithm	RC4	RC4	AES-CCMP	AES-GCMP
Integrity Protection	CRC-32	MIC	CCMP	GCMP
Key Management Method	Static Key	TKIP	4-Way Handshake	SAE
Known Vulnerabilities	High	Moderate	Low (KRACK)	Low (Dragonblood)

Table I summarizes the key features and vulnerabilities of the discussed protocols. As evident, each successive protocol addresses the shortcomings of its predecessor, enhancing the security of wireless networks.

Understanding the evolution of Wi-Fi security protocols is crucial for comprehending the current state of wireless network security. While significant advancements have been made from WEP to WPA3, each protocol has its own set of vulnerabilities and challenges. Continuous research and development are essential to address emerging threats and ensure the robustness of wireless communications.

III. Research and Technical Challenges

The evolution of Wi-Fi security protocols from WEP to WPA3 has been marked by a continuous battle against emerging threats and vulnerabilities. Despite significant advancements, each protocol has presented unique challenges that have been the focus of extensive research. This section delves into these challenges, highlighting the technical complexities and research efforts aimed at fortifying wireless network security.

A. Challenges in WEP Security

Wired Equivalent Privacy (WEP), introduced as part of the original IEEE 802.11 standard in 1997, was designed to provide confidentiality comparable to that of wired networks. However, over time, numerous vulnerabilities have been identified, rendering WEP insufficient for securing wireless communications. This section explores the critical challenges inherent in WEP's design and implementation.

1) Short Initialization Vectors (IVs) and Key Reuse

WEP uses a 24-bit IV combined with a secret key to form the RC4 encryption key. The small size of the IV leads to repetition especially in high traffic networks. This repetition allows an attacker to collect enough packets with the same IV to perform statistical analysis and recover the encryption key [1].

2) Weaknesses in RC4 Key Scheduling Algorithm

The RC4 stream cipher used in WEP has a weakness in its Key Scheduling Algorithm (KSA). Fluhrer, Mantin and Shamir showed that certain IVs, called weak IVs, can leak key information. By capturing enough packets with these weak IVs, an attacker can recover the secret key [1].

3) Lack of Robust Integrity Checks

WEP uses CRC-32 for data integrity verification. But CRC-32 is not cryptographically secure and is linear, so it can be attacked by bit-flipping. An attacker can modify the encrypted message and adjust the checksum accordingly without being detected, and compromise data integrity [4].

4) Authentication Vulnerabilities

WEP's authentication mechanism is flawed. In shared key authentication, the challenge-response process can be exploited by an attacker to derive the keystream used for encryption. By capturing the plaintext challenge and the corresponding encrypted response, an attacker can compute the keystream and then decrypt other packets encrypted with the same key [6].

5) Susceptibility to Replay Attacks

Since WEP doesn't have sequence numbers or timestamps, it's vulnerable to replay attacks. An attacker can capture legitimate packets and retransmit them and potentially gain unauthorized access or disrupt network operations [4].

6) Advanced Key Recovery Attacks

Beyond the FMS attack, more efficient key recovery methods have been developed. The PTW attack by Pyshkin, Tews and Weinmann reduces the number of packets required to recover a WEP key. This attack doesn't rely on weak IVs and can recover a 104-bit key with high success rate using fewer packets [7].

7) Fragmentation and Packet Injection Attacks

WEP doesn't have protection against packet fragmentation and an attacker can use this to inject arbitrary packets into the network by manipulating packet fragments. Also tools like Chopchop and fragmentation attacks can decrypt packets without needing the encryption key [8].

8) Implementation Flaws and Misconfigurations

Many WEP implementations have poor key management practices such as using default keys and infrequent key changes. These practices exacerbate WEP's inherent vulnerabilities and makes the network more vulnerable to attacks [6].

9) Rapid Evolution of Attack Tools

The development and dissemination of tools like AirSnort and Aircrack-ng have made WEP exploitation more accessible to everyone. These tools automate the process of capturing packets and key recovery attacks, so the barrier to entry for attackers is much lower [7].

B. Challenges in WPA Security

Wi-Fi Protected Access (WPA) was introduced in 2003 as a stopgap to fix the WEP problems. WPA had some improvements over WEP, like TKIP and MIC, but was not immune to vulnerabilities. This section will cover the design and implementation flaws of WPA.

1) Temporal Key Integrity Protocol (TKIP) Limitations

TKIP was designed to provide per-packet key mixing, message integrity check and re-keying. But it still used the RC4 stream cipher which was already known to be broken. Since WPA used RC4, it inherited some of the WEP weaknesses [9].

2) Beck-Tews Attack on TKIP

In 2008, Martin Beck and Erik Tews showed an attack on WPA-TKIP that allowed to inject arbitrary packets into a WPA-protected network. The attack exploited the MIC and the predictability of the TKIP sequence counter to decrypt short packets and inject malicious packets in a short time [9].

3) Dictionary Attacks on Pre-Shared Keys

WPA networks with pre-shared keys (PSK) are vulnerable to dictionary attacks especially when users choose weak or common passphrases. Attackers can capture the four-way handshake between a client and an access point and then perform offline dictionary attacks to guess the passphrase [10].

4) Vulnerabilities in Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) was introduced to simplify the process of connecting devices to a wireless network. But a big flaw in the WPS PIN authentication was found, allowing attackers to brute-force the PIN and get the WPA/WPA2 passphrase. This vulnerability breaks the security of networks that use WPS [11].

5) Lack of Forward Secrecy

WPA does not provide forward secrecy, so if an attacker gets the pre-shared key, they can decrypt previously captured traffic. This causes a large risk especially in environments where sensitive data is transmitted over the wireless network [5].

6) Implementation Flaws and Misconfigurations

Many WPA implementations have poor key management and misconfigurations. For example, some access points do not enforce strong passphrase requirements and users choose weak passwords. Firmware vulnerabilities and outdated software can also expose WPA networks to attacks [10].

7) Susceptibility to Denial-of-Service (DoS) Attacks

WPA networks are vulnerable to DoS attacks through the exploitation of management frames. Attackers can send deauthentication or disassociation frames to clients, causing them to disconnect from the network. Since these management frames are not encrypted or authenticated in WPA, they can be easily spoofed. [12]

C. Challenges in WPA2 Security

Wi-Fi Protected Access II (WPA2), standardized in IEEE 802.11i, has been the wireless security standard since 2004. While it has fixed many of the issues with WPA, research has since found several critical flaws in WPA2's design and implementation. This section covers the main WPA2 challenges.

1) Key Reinstallation Attacks (KRACK)

In 2017, Vanhoef and Piessens discovered a major vulnerability in WPA2's four way handshake, called Key Reinstallation Attack (KRACK). This attack exploits the handshake's design, allowing an attacker to manipulate and replay the cryptographic handshake messages. By forcing the victim to reinstall an already in use key, an attacker can reset the nonce and replay counter, resulting in nonce reuse. This allows for packet decryption, packet replay, TCP connection hijacking and HTTP content injection. [2]

2) Dictionary Attacks

WPA2-PSK (Pre-Shared Key) networks are vulnerable to offline dictionary attacks when users choose weak or common passphrases. An attacker can capture the four way handshake between a client and an access point and then perform offline dictionary attacks to guess the passphrase. The feasibility of such attacks is increased by the use of weak passwords and lack of complexity requirements. [10]

3) Implementation Flaws and Misconfigurations

Beyond protocol level vulnerabilities, WPA2's security is often broken by poor implementation and misconfigurations. Many users and administrators don't update firmware or apply patches, leaving devices open to known vulnerabilities. Many also use default configurations and inadequate security settings. [13]

4) No Forward Secrecy

WPA2 doesn't have forward secrecy. If an attacker gets the pre-shared key, they can decrypt previously captured traffic. The lack of forward secrecy is a large risk, especially in

environments where sensitive data is transmitted over the wireless network. [5]

5) WPA2-Enterprise Configurations

WPA2-Enterprise, which uses 802.1X authentication, is designed for enterprise security. However, research has shown that improper configuration of supplicants (client devices) can lead to credential leakage. For example, if a supplicant is not configured to validate server certificates, it becomes vulnerable to man-in-the-middle attacks and an attacker can capture authentication credentials. [13]

6) Side-Channel Attacks

Recent research has shown that WPA2 is vulnerable to side-channel attacks. For example, an attacker can infer information from the size of the frames. By analyzing the pattern of packet sizes and timing, an attacker can deduce sensitive information without decrypting the content. [14]

D. Challenges in WPA3 Security

Wi-Fi Protected Access III (WPA3), introduced by the Wi-Fi Alliance in 2018, was supposed to fix the security issues of WPA and WPA2. While WPA3 has many improvements, including the Simultaneous Authentication of Equals (SAE) handshake and better encryption, subsequent research has found several vulnerabilities and implementation problems. This section covers the problems in WPA3 design and deployment.

1) Dragonblood Vulnerabilities

The Dragonblood attacks, found by Vanhoef and Ronen, expose multiple vulnerabilities in WPA3's SAE handshake. These include:

- **Downgrade Attacks**: Attackers can force WPA3-capable devices to fall back to WPA2, reintroducing known vulnerabilities. [3]
- **Side-Channel Attacks**: Timing-based side-channel attacks can leak information about the password, enabling offline dictionary attacks. [3]

These vulnerabilities show the problems in implementing the SAE handshake across different hardware and software platforms.

2) Implementation Flaws and Misconfigurations

Despite WPA3's robust design, improper implementations can introduce vulnerabilities. For example, some devices don't validate cryptographic parameters during the SAE handshake properly, which can lead to security breaches [3]. And misconfigurations like weak password policies can undermine WPA3's security benefits.

3) Denial-of-Service (DoS) Attacks

WPA3's anti-clogging mechanism, intended to prevent DoS attacks, can be exploited. Attackers can flood a device with authentication requests and trigger the anti-clogging mechanism and prevent legitimate users from connecting [3]. And the computational intensity of the SAE handshake can be used to exhaust device resources and cause service disruption.

4) Transition Mode Vulnerabilities

WPA3's transition mode, designed to support both WPA2 and WPA3 clients, can be used by attackers to downgrade connections to WPA2 and reintroduce WPA3 vulnerabilities [3]. This feature is good for user experience but poses significant security risks if not managed properly.

5) Challenges in IoT and Resource-Constrained Devices

Implementing WPA3 in Internet of Things (IoT) and other resource-constrained devices has its own challenges. The SAE handshake and other WPA3 features may exceed the capabilities of these devices, leading to security compromises or continued use of less secure protocols [3].

IV. State-of-the Art Solution Approaches

A. State-of-the-Art Solution Approaches for Enhancing WEP Security

Wired Equivalent Privacy (WEP) was introduced as part of the IEEE 802.11 standard to provide confidentiality like wired networks. However many vulnerabilities have been found and researchers have proposed various fixes. This section categorizes and analyzes these solutions based on the problem they solve.

1) Enhancements in Key Management and Distribution

a) Dynamic WEP

Dynamic WEP integrates EAP with 802.1X authentication to change keys periodically thus reducing the window of opportunity for key compromise [15].

b) WEP2

WEP2 extends the IV and key sizes to 128 bits to address the weak IV problem in WEP. While it provides better resistance to some attacks it is still vulnerable to others due to protocol flaws [16].

2) Encryption Algorithm Improvements

a) Modified RC4 Implementations

Several studies have proposed modifications to the RC4 algorithm used in WEP to make it more secure. These include changing the key scheduling algorithm to prevent known attacks and per-packet key mixing [17].

b) Transition to AES-Based Encryption

Recognizing the fundamental flaws of RC4 some approaches suggest replacing it with AES. While this is more secure it often requires hardware upgrades which limits its applicability in existing WEP deployments [16].

3) Authentication Mechanism Enhancements

a) Integration of 802.1X Authentication

Adding 802.1X authentication frameworks to WEP deployments introduces mutual authentication between clients and access points. This makes the authentication process stronger and reduces the risk of unauthorized access [16].

b) Use of Biometric Authentication

Some researchers have explored the integration of biometric authentication methods like fingerprint or facial recognition to enhance user verification in wireless networks. While promising these approaches raise concerns on user privacy and system complexity [18].

4) Comparative Analysis of Proposed Solutions

B. State-of-the-Art Solution Approaches for Enhancing WPA Security

Wi-Fi Protected Access (WPA) was introduced as a stopgap solution to address the many security flaws in WEP. While WPA had several improvements over WEP including TKIP and MIC it was not immune to vulnerabilities. This section

TABLE II
Comparison of WEP Enhancement Techniques

Technique	Advantages	Limitations	Implementation Considerations
Dynamic WEP	Periodic key changes enhance security	Requires 802.1X infrastructure	Suitable for enterprise environments
WEP2	Extended IV and key sizes mitigate weak IV attacks	Does not address all WEP vulnerabilities	Limited adoption due to partial improvements
Modified RC4	Enhances resistance to known attacks	May introduce compatibility issues	Requires careful algorithm tuning
AES-Based Encryption	Provides robust security	Necessitates hardware upgrades	Not feasible for legacy systems
802.1X Integration	Strengthens authentication mechanisms	Increases system complexity	Demands additional infrastructure
Biometric Authentication	Enhances user verification	Raises privacy concerns	Requires specialized hardware

TABLE III
Comparison of WPA Security Enhancement Techniques

Technique	Advantages	Limitations
Dynamic Key Management	Reduces key reuse; enhances security	Requires infrastructure support
802.1X with EAP Integration	Provides robust authentication; dynamic key distribution	Complex configuration; requires RADIUS server
Transition to CCMP	Stronger encryption and integrity protection	May not be compatible with older devices
Strong Passphrase Policies	Mitigates dictionary attacks	Relies on user compliance
Two-Factor Authentication	Adds additional security layer	Requires additional hardware or software
Management Frame Protection	Prevents unauthorized management frame attacks	Not supported by all devices

will discuss the problems in WPA's design and implementation and the various solutions proposed to fix them.

1) Enhancements in Key Management and Distribution

a) Dynamic Key Management

To address the problem of static key usage dynamic key management schemes have been proposed. These involve frequent rekeying and unique session keys for each client to reduce the window of opportunity for an attacker to exploit a compromised key [5].

b) Integration with 802.1X and EAP

WPA with IEEE 802.1X and EAP provides a framework for robust authentication and dynamic key distribution. This makes keys not statically configured and unique per session [10].

2) Improvements in Encryption and Integrity Mechanisms

a) Transition from TKIP to CCMP

Since TKIP has vulnerabilities researchers have suggested to transition to Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which uses AES. CCMP provides stronger encryption and integrity protection than TKIP [12].

3) Mitigation of Dictionary Attacks

a) Strong Passphrase Policies

Implementing policies that require strong, complex passphrases can reduce the risk of dictionary attacks. This includes minimum length, multiple character types and regular password changes [11].

b) Use of Two-Factor Authentication

Adding two-factor authentication (2FA) adds an extra layer of security so even if an attacker gets the passphrase [11].

4) Protection Against Denial-of-Service (DoS) Attacks

a) Management Frame Protection

To counter DoS attacks that exploit unprotected management frames, implement Management Frame Protection (MFP) to ensure the authenticity and integrity of those frames so deauthentication and disassociation attacks are not possible [12].

5) Comparative Analysis of Proposed Solutions

While WPA was a big improvement over WEP, it still has its vulnerabilities. Dynamic key management, 802.1X and EAP integration, transition to stronger encryption protocols like CCMP, strong passphrase policies, 2FA and management frame protection all contribute to a more secure wireless network

C. State-of-the-Art Solution Approaches for Enhancing WPA2 Security

Wi-Fi Protected Access 2 (WPA2) has been the foundation of wireless security. Despite its improvements over its predecessors, WPA2 has its own vulnerabilities that need to be addressed. This section will look into modern solutions to fortify WPA2 security, focusing on key management, encryption mechanisms, dictionary attacks and management frame exploits.

1) Enhancements in Key Management and Distribution

a) Dynamic Key Management

Dynamic key management schemes have been proposed to address the limitations of static key usage in WPA2. These schemes involve frequent rekeying and unique session keys per client to reduce the window of opportunity for attackers to exploit compromised keys [19].

b) Integration with IEEE 802.1X and EAP

WPA2 with 802.1X and EAP frameworks allows for robust authentication and dynamic key distribution. This means keys are not statically configured and are unique per session so overall security is enhanced [20].

2) Improvements in Encryption and Integrity Mechanisms

a) Adoption of AES-CCMP

WPA2 requires the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) with the Advanced Encryption Standard (AES). This transition from the weaker TKIP protocol provides stronger encryption and integrity protection [21]

b) Mitigation of KRACK Vulnerabilities

The Key Reinstallation Attack (KRACK) exposed vulnerabilities in the four-way handshake of WPA2. To counter such threats, researchers have proposed protocol-level fixes and implementation patches to prevent nonce reuse and strict key management [22].

3) Mitigation of Dictionary Attacks

a) Enforcement of Strong Passphrase Policies

Implementing policies that require complex passphrases can reduce the risk of dictionary attacks. This includes minimum length, multiple character types and regular password changes [23].

b) Deployment of Two-Factor Authentication

Adding two-factor authentication (2FA) adds an extra layer of security so even if an attacker gets the passphrase [23].

4) Protection Against Management Frame Exploits

a) Implementation of Protected Management Frames (PMF)

To counter attacks that exploit unprotected management frames, implement Protected Management Frames (PMF) as specified in IEEE 802.11w to ensure the authenticity and integrity of those frames so deauthentication and disassociation attacks are not possible [24].

5) Comparative Analysis of Proposed Solutions

TABLE IV
Comparison of WPA2 Security Enhancement Techniques

Technique	Advantages	Limitations
Dynamic Key Management	Reduces key reuse; enhances security	Requires infrastructure support
802.1X with EAP Integration	Provides robust authentication; dynamic key distribution	Complex configuration; requires RADIUS server
Adoption of AES-CCMP	Stronger encryption and integrity protection	May not be compatible with older devices
Strong Passphrase Policies	Mitigates dictionary attacks	Relies on user compliance
Two-Factor Authentication	Adds additional security layer	Requires additional hardware or software
Protected Management Frames	Prevents unauthorized management frame attacks	Not supported by all devices

WPA2 has improved wireless network security but is not bulletproof. Dynamic key management, 802.1X and EAP integration, AES-CCMP encryption, strong passphrase policies, two-factor authentication and management frame protection all contribute to a more secure wireless network.

D. State-of-the-Art Solution Approaches for Enhancing WPA3 Security

Wi-Fi Protected Access 3 (WPA3) is a large step forward in wireless security protocols, it addresses many of the vulnerabilities of its predecessors. Despite the improvements WPA3 has been attacked and implemented with challenges. This section highlights current solutions to fortify WPA3 security, protocol enhancements, mitigation of known vulnerabilities and advanced authentication mechanisms.

1) Protocol Enhancements and Mitigations

a) Formally Verified Implementations

The complexity of WPA3 SAE handshake has led to implementation specific vulnerabilities. To address this researchers have proposed formally verified implementations, like Dragonstar, which uses cryptographic libraries like HACL* to resist side-channel attacks and other vulnerabilities [25].

b) Mitigation of Dragonblood Attacks

The Dragonblood attacks exploits the SAE handshake weaknesses, allowing offline dictionary attacks and side-channel exploits. Mitigation strategies are to disable support for weak elliptic curves, enforce constant-time cryptographic operations and stricter validation checks during the handshake [3].

2) Advanced Authentication Mechanisms

a) Opportunistic Wireless Encryption (OWE)

OWE makes open Wi-Fi networks more secure by providing encrypted communication without user authentication. This mechanism protects users from passive eavesdropping attacks, data confidentiality even in public networks [26].

b) Wi-Fi Easy Connect

To simplify the secure onboarding of IoT devices WPA3 introduces Wi-Fi Easy Connect which uses QR codes or NFC tags for device provisioning. This reduces the reliance on pre-shared keys and makes it more secure by minimizing human error during device configuration [27].

3) Intrusion Detection and Monitoring

a) Wireless Intrusion Detection Systems (WIDS)

Since some attacks like deauthentication and beacon flooding are still possible under WPA3 the deployment of WIDS has been proposed. These systems monitor wireless traffic for anomalies and can detect and mitigate threats in real-time [28].WPA3 is a big step forward but not bulletproof. Formally verified implementations, Dragonblood mitigation, advanced authentication and intrusion detection systems all contribute to a more secure wireless.

4) Comparative Analysis of Proposed Solutions

TABLE V
Comparison of WPA3 Security Enhancement Techniques

Technique	Advantages	Limitations
Formally Verified Implementations	Ensures resistance against side-channel attacks; enhances protocol robustness	Requires significant development effort; potential performance overhead
Mitigation of Dragonblood Attacks	Addresses known vulnerabilities in SAE handshake	May reduce compatibility with legacy devices; necessitates firmware updates
Opportunistic Wireless Encryption	Provides encryption in open networks without user intervention	Does not authenticate users; limited protection against active attacks
Wi-Fi Easy Connect	Simplifies secure device onboarding; reduces human error	Relies on device support for QR codes or NFC; potential privacy concerns
Wireless Intrusion Detection Systems	Enables real-time threat detection; enhances network monitoring	May generate false positives; requires continuous maintenance

While WPA3 introduces substantial improvements over previous wireless security protocols, it is not impervious to threats. The adoption of formally verified implementations, mitigation of known vulnerabilities like Dragonblood, integration of advanced authentication mechanisms, and deployment of intrusion detection systems collectively contribute to a more secure wireless networking environment.

V. Open/Unsolved Challenges

Wired Equivalent Privacy (WEP) was the first security protocol for IEEE 802.11 wireless networks to provide confidentiality like wired networks. Although it's old. WEP is no longer secure due to many vulnerabilities. But understanding the unresolved issues is important to understanding the evolution of wireless security protocols.

1) Weaknesses in Encryption Mechanism

WEP uses the RC4 stream cipher for encryption, combining a secret key with a 24-bit IV. The small size of the IV leads to repetition, making the cipher vulnerable to statistical attacks. Fluhrer, Mantin, and Shamir showed that these repetitions can be used to recover the encryption key [1].

2) Lack of Robust Key Management
WEP has no standard key management protocol, so most people use static, manually configured keys. This increases the risk of key compromise and makes key updates a pain [29].
3) Ineffective Integrity Check Mechanism
The protocol uses CRC-32 for data integrity check, which is linear and not cryptographic. Attackers can manipulate packets and recalculate the checksum without being detected, compromising data integrity [4].
4) Susceptibility to Replay Attacks
Due to the predictability of IVs and lack of sequence numbering, WEP is vulnerable to replay attacks. Attackers can capture and retransmit valid data packets, gain unauthorized access, or disrupt network operations [4].
5) Challenges in Legacy Systems
Although deprecated some legacy systems still use WEP due to hardware limitations or no firmware updates. This continued use is a security risk as these systems are vulnerable to known attacks with available tools [29].

WEP has been replaced by more secure protocols like WPA and WPA2, but its vulnerabilities highlight the importance of robust encryption, key management, and integrity checks. The issues in WEP's design and implementation have informed the development of subsequent wireless security protocols; we need to continue to evaluate and enhance security measures.

A. Open and Unsolved Challenges in WPA Security

Wi-Fi Protected Access (WPA) was introduced as an improvement over the flawed WEP protocol to provide data confidentiality and integrity for wireless networks. Although it's better than WEP and WPA, especially with TKIP, which has many vulnerabilities that have been around for a long time. Understanding these issues is important for the continued evolution of wireless security protocols.

1) Vulnerabilities in the Temporal Key Integrity Protocol (TKIP)
TKIP was designed to fix WEP's issues by introducing per-packet key mixing, message integrity check and rekeying. But it still uses the RC4 stream cipher, which is weak. Researchers have shown that TKIP can be attacked to inject arbitrary packets and decrypt short packets without the encryption key. These vulnerabilities are due to the Michael message integrity code and the predictability of the packet sequence numbers, allowing attackers to do replay attacks and compromise data integrity [30].
2) Susceptibility to Key Reinstallation Attacks (KRACK)
The KRACK attack, discovered by Vanhoef and Piessens, exposes a fundamental flaw in the WPA2 four way handshake. By manipulating and replaying handshake messages, an attacker can get a victim to reinstall an already in-use key and reset associated parameters like the nonce and replay counter. This reinstallation allows the reuse of cryptographic nonces, violating the protocol's assumptions and allowing an attacker to decrypt data, hijack connections or inject malicious content [2].
3) Implementation Flaws and Inconsistent Patch Deployment
Even after the disclosure of vulnerabilities like KRACK many devices are still vulnerable due to inconsistent or absent patching. Some vendors have not released updates, and some legacy devices can't receive updates at all. Moreover, different WPA implementations on different platforms can introduce unique vulnerabilities, making the security landscape even more complicated [2].
4) Challenges in Legacy System Support and Transition to WPA3
The transition from WPA to more secure protocols like WPA3 is hindered by the presence of legacy systems that don't support the new standards. These old devices are still using vulnerable protocols and pose a big security risk. The coexistence of multiple protocol versions in the same network can lead to downgrade attacks where an attacker forces a connection to use a less secure protocol version [2].

While WPA was a big improvement over WEP, the use of outdated crypto and the discovery of KRACK shows we need to stay vigilant in wireless security. The challenges of TKIP's weaknesses, protocol flaws, inconsistent patching and legacy systems highlight the need to move to more robust security standards and make sure it's implemented on all devices.

B. Open and Unsolved Challenges in WPA2 Security

Wi-Fi Protected Access II (WPA2) has been the foundation of wireless security since 2004. Despite being widely deployed and improved over WPA, several vulnerabilities and challenges have emerged over time. This section will cover the open and unresolved issues with WPA2, the areas that need more research and mitigation.

1) Key Reinstallation Attacks (KRACK)
One of the biggest vulnerabilities in WPA2 is the Key Reinstallation Attack (KRACK). This attack exploits a flaw in the four way handshake, allowing an attacker to manipulate and replay cryptographic handshake messages. By forcing nonce reuse an attacker can decrypt data, hijack connections and inject malicious content. The vulnerability is in the WPA2 protocol itself, all implementations are affected [2].
2) Implementation Flaws and Patch Deployment Challenges
While protocol level vulnerabilities like KRACK are serious, implementation specific flaws are also a big risk. Devices from different manufacturers have not followed the WPA2 specification correctly, introducing exploitable weaknesses. Moreover patching of known vulnerabilities is often delayed or not done at all, especially in legacy systems and IoT devices. The delay in patching of known vulnerabilities makes the known vulnerabilities even more risky [31].
3) Enterprise Network Misconfigurations
In WPA2-Enterprise deployments, EAP methods introduce complexity that can lead to misconfigurations. Studies have shown that many enterprise networks are vulnerable to credential theft due to misconfigured supplicants and authentication servers. These misconfigurations undermine the security of WPA2-Enterprise and leave networks open to man-in-the-middle attacks [13].
4) Hardware-Specific Vulnerabilities: The Case of Kr00k
Beyond protocol and implementation issues, hardware-specific vulnerabilities have surfaced. The Kr00k vulnerability, identified in Wi-Fi chips by Broadcom and Cypress, causes devices to transmit encrypted data frames with all-zero

encryption keys under certain conditions. This flaw allows attackers to decrypt portions of wireless traffic, emphasizing the need for rigorous hardware-level security assessments [32].

5) Challenges in Transitioning to WPA3

Although WPA3 has been introduced to fix many of WPA2's issues, the transition is hindered by compatibility issues and legacy devices. Many devices do not support WPA3, and mixed mode networks that support both WPA2 and WPA3 clients can inadvertently expose vulnerabilities. The slow adoption of WPA3 prolongs the period during which WPA2âs problems are relevant [31].

Although WPA2 has significantly advanced wireless security, its vulnerabilities - ranging from protocol-level flaws like KRACK to hardware-specific issues like Kr00k - highlight the need for continuous scrutiny and improvement. Addressing these challenges requires a multifaceted approach, encompassing protocol enhancements, rigorous implementation standards, timely patch deployments, and a concerted effort to transition to more secure protocols like WPA3.

C. Open and Unsolved Challenges in WPA3 Security

WPA3 was designed to address the issues with WPA2. While it brings many improvements in wireless security (e.g. better protection against offline dictionary attacks and improved encryption) there are still open and unsolved issues. This section will go over these issues and areas that need more research and mitigation.

1) Side-Channel Attacks on the Dragonfly Handshake

WPA3 uses the Simultaneous Authentication of Equals (SAE) protocol, also known as the Dragonfly handshake, for authentication. However research has found vulnerabilities where side-channel attacks (e.g. cache-timing attacks) can leak information about the password. For example the "Dragondoom" attack shows how microarchitectural mechanisms can be used to recover passwords in widely deployed Wi-Fi daemons like `hostapd` in its default settings [25].

2) Denial-of-Service (DoS) Attacks

Despite the improvements WPA3 is still vulnerable to some DoS attacks. For example an attacker can exploit the computational intensity of the Dragonfly handshake by sending a flood of authentication requests and overwhelm the access point and cause service disruption. Also vulnerabilities in the SAE protocol can be used to exhaust resources and prevent legitimate users from connecting to the network [33].

3) Transition Mode Vulnerabilities

To be compatible with WPA2 devices WPA3 has a transition mode that supports both WPA2 and WPA3 connections. However this mode can be used by an attacker to downgrade a connection from WPA3 to WPA2 and reintroduce the vulnerabilities that WPA3 is trying to fix. This downgrade attack undermines the security benefits of WPA3, especially when users are not aware of the fallback to WPA2 [34].

4) Implementation Flaws in WPA3-PK

WPA3-PK, an extension to enhance hotspot security using public key authentication, has been found to have implementation flaws. Specifically vulnerabilities in random number generation can leak private keys. Also an attacker can perform precomputation attacks using rainbow tables to crack passwords across multiple networks especially when weak passwords are used [35].

5) Social Engineering Exploits

WPA3 strengthens technical defenses but does not protect against social engineering attacks. An attacker can set up a rogue access point that mimics a legitimate network and trick users into connecting and giving away sensitive information. These attacks bypass the cryptographic protections of WPA3 by exploiting human factors, so user awareness and additional security measures are needed [36].

6) Challenges with IoT Devices and Legacy Systems

WPA3 in IoT devices and legacy systems has its own challenges due to hardware limitations and compatibility issues. Many IoT devices don't have the computational resources to support WPA3's advanced encryption so they will continue to use older and less secure protocols. This gap in adoption creates vulnerabilities in networks that have a mix of devices [34].

WPA3 is a large step forward in wireless security but not invulnerable. Side-channel attacks, DoS exploits, transition mode downgrades, implementation flaws, social engineering, and compatibility issues with IoT and legacy devices mean we need to be vigilant, research, and user education to fully realize the security benefits of WPA3.

VI. Case Study: Implementation and Evaluation

A. The Studied Techniques

To examine the real-world impact of wireless security vulnerabilities, this project focuses on two well-established attack techniques: **Captive Portal Phishing (Evil Portal)** and **PMKID-based WPA2 Password Cracking**. These methods were selected because they illustrate two distinct threat vectors – one that exploits human factors through social engineering, and another that targets cryptographic weaknesses in the WPA2 key exchange process.

1) Captive Portal Phishing (Evil Portal Attack)

Captive portal phishing exploits the lack of mutual authentication in public and semi-open wireless networks. The attacker sets up a rogue access point (AP) that mimics a legitimate Wi-Fi network. When a user connects to this fake AP, they are redirected to a fake login page often a clone of a popular service (e.g. Facebook or a company intranet). Unaware users may enter their credentials and the attacker captures them.

This attack uses social engineering and DNS spoofing rather than breaking cryptographic mechanisms. It's especially dangerous in environments where users are used to captive portals (e.g. cafes, airports, universities). Despite modern browser safeguards, this attack still works because users are unaware and there's poor UI feedback during network transitions.

Open Challenges:

- Exploits the lack of authentication in open network discovery.
- Highlights user-centric vulnerabilities that are difficult to address via protocol-level fixes.

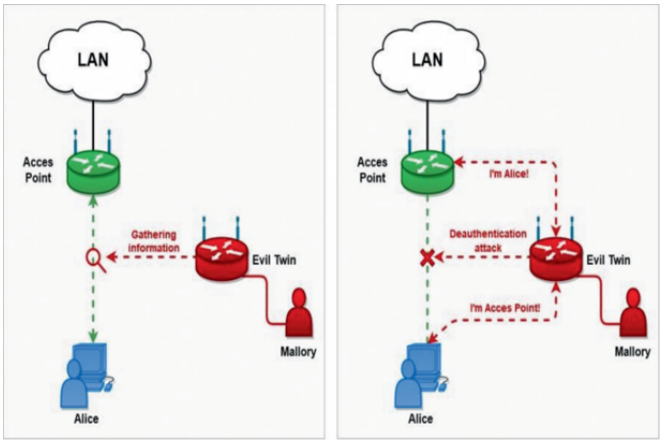

Fig. 5: Evil Portal

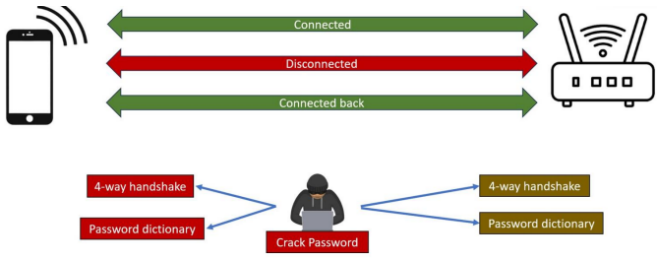

Fig. 6: WPA2 Password Cracking

- Demonstrates the importance of educating users and enforcing HTTPS.

2) PMKID-Based WPA2 Password Cracking

This attack targets the cryptographic weaknesses in WPA2-Personal networks. During the initial handshake, the Pairwise Master Key Identifier (PMKID) is sometimes sent by the access point without requiring client-side deauthentication. An attacker can capture this PMKID and use tools like `Hashcat` to perform offline dictionary or brute-force attacks on the pre-shared key (PSK).

This attack is dangerous because it doesn't require user interaction and leaves no trace. It's a direct result of the design decisions in WPA2 where backward compatibility and performance were prioritized over brute-force resistance.

Open Challenges:

- Demonstrates the vulnerability of static PSKs and poor password hygiene.
- Highlights how even well-implemented cryptographic protocols can be subverted with weak inputs.
- Motivates the shift to protocols like WPA3-SAE and passwordless authentication.

Both of these methods are real world attacks that work and show that we need to address both technical and human-centric vulnerabilities in wireless networks. These were implemented and tested in this project, as described in Section VI.B.

B. Evaluation and Analysis

To test the real world feasibility and effectiveness of the techniques, both attacks – Captive Portal Phishing and PMKID-based WPA2 Cracking – were implemented and tested in a lab. The evaluation focused on impact, stealth, user interaction and practicality using common hardware and tools.

Fig. 7: Flipper Zero with Wi-Fi Dev Board

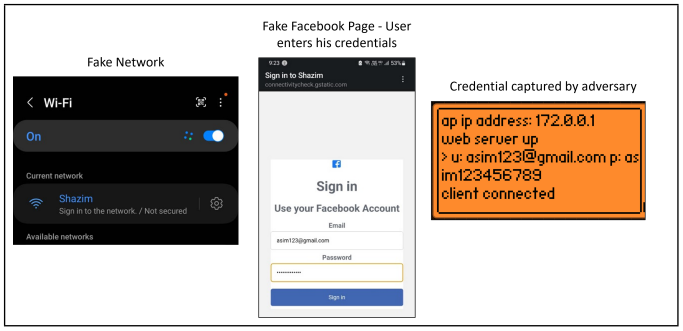

Fig. 8: Captive Portal Phishing

1) Experiment Setup and Tools

The following tools and hardware were used:

- **Flipper Zero (with Wi-Fi Dev Board)** – Used to simulate a rogue access point and deploy the phishing portal.
- **Hashcat** – Employed for offline brute-force cracking of the WPA2 PSK using captured PMKID.
- **Wireshark** – Utilized to monitor and confirm handshake packet capture.
- **Windows OS** – Served as the host system for attack orchestration and password cracking.
- **Dictionary File** – Included common and weak passwords for brute-force testing in the PMKID attack.

2) Implementation Summary

a) Captive Portal Phishing (Evil Portal).

A rogue AP was set up using Flipper Zero's Evil Portal application. A cloned Facebook login page was uploaded to mimic a legit service. When a target device connected to the fake SSID, it was redirected to the spoofed login page. When credentials were entered, the input was captured and displayed on the attacker's terminal in real time.

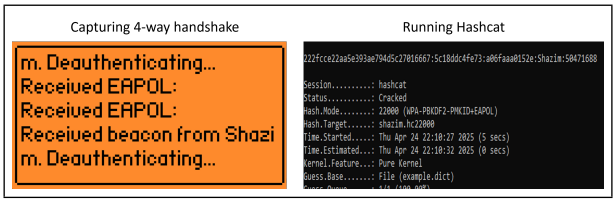

Fig. 9: WPA2 Password Cracking

b) PMKID-Based WPA2 Password Cracking.

A WPA2-Personal network was created with a known weak password. Flipper Zero and Wireshark were used to extract the PMKID without disconnecting any connected clients. The hash was then converted and fed into Hashcat with a dictionary list to brute force the PSK.

3) Evaluation Metrics

Both techniques were evaluated based on the following criteria:

- **User Interaction Requirement** – Whether the attack requires the target to take explicit action.
- **Attack Stealth** – How easily the attack could be detected by the user or network administrator.
- **Time to Success** – Approximate time taken to retrieve credentials or crack a password.

TABLE VI
Comparison of Implemented Techniques

Metric	Evil Portal Phishing	PMKID WPA2 Attack
User Interaction Required	Yes (credential input)	No
Stealth	Medium (visible rogue SSID)	High (passive capture)
Time to Success	Instant (upon user input)	Depends on password strength
Dependency on Password Strength	No	High
Protocol Targeted	WEP/WPA/WPA2	WPA2-PSK
Tools Used	Flipper Zero, HTML clone	Flipper Zero, Hashcat

4) Observations and Insights

The Evil Portal attack worked in scenarios where the user was unaware – credentials were harvested when the user thought they were authenticating to a legit network. However, it required manual user interaction and could be noticed by observant users due to suspicious network names or browser warnings.

In contrast, the PMKID attack was fully passive, required no user interaction and left almost no trace. Its success was heavily dependent on the target's password. Weak passwords were cracked in seconds with dictionary attacks, strong passwords made the attack computationally impractical.

Both attacks show different aspects of wireless security vulnerabilities. Evil Portal shows the social engineering threat in open or semi-protected environments. PMKID-based cracking shows the cryptographic weakness of WPA2 with poor password hygiene. Both attacks prove that wireless network security is only as strong as its weakest layer – be it human behavior or cryptographic design.

VII. Conclusion

This project looked at Wi-Fi network security, covering both the theoretical underpinnings of wireless encryption protocols and the practical vulnerabilities that affect real world deployments. We started by looking at the evolution from WEP to WPA3 and how each protocol tried to fix the issues of the previous one. But our research showed that despite the advancements in cryptography and protocol complexity, wireless network security is still vulnerable due to design flaws, implementation errors and user centric weaknesses.

In the theoretical part we looked at fundamental weaknesses like WEP's short IVs and weak key scheduling, WPA's reliance on RC4 and WPA2's key reinstallation and dictionary attacks. Even WPA3, with its forward-looking SAE handshake and 192-bit cryptography, has been shown to be vulnerable to attacks like Dragonblood and Dragondoom, mainly due to side channel vulnerabilities and insecure default implementations and the requirement for backward compatibility (e.g. WPA3 transition mode) still introduces downgrade vectors that allow attackers to bypass newer protections.

To test these vulnerabilities we implemented two attacks: Captive Portal Phishing and PMKID based WPA2 Cracking. The Evil Portal attack showed how easily users can be tricked into submitting credentials through fake login pages served by rogue APs. This attack was very effective in scenarios where users are used to captive portals and don't know how to distinguish legitimate network behavior from malicious spoofing. The PMKID attack showed how WPA2 networks with weak passwords are still vulnerable to silent, offline cracking without user interaction. This attack used passive packet capture and dictionary based brute force to recover the pre-shared key, highlighting the importance of strong credential policies even in secure looking environments.

During the project we encountered several challenges. First, configuring and calibrating hardware tools like Flipper Zero took a lot of time and firmware knowledge to get it working reliably. Second, simulating real world wireless network behavior in a lab setup required careful isolation to not affect other networks or violate ethical guidelines. Third, making sure the experiments mirrored the attack methods described in academic papers meant a lot of cross referencing between documentation, tool limitations and expected behavior. These constraints while hard, helped to gain a deeper technical understanding of wireless protocol mechanics and attacker strategies.The results of this project show that Wi-Fi network security is not just about cryptographic strength but about the whole ecosystem: secure implementations, regular patching, user awareness and resilient system architecture. WPA3 brings many security improvements but is only as good as its weakest link – whether that be legacy hardware, misconfigured APs or untrained end users. The coexistence of WPA2 and WPA3 in mixed environments makes things even more complicated especially in networks with resource constrained IoT devices that can't upgrade to newer standards.

VIII. Group Member Contributions

This project was done by Mohammad Asim and Mohammad Zubair. Below is the breakdown of work done by each team member across all phases of the project:

Reading and Research: Both Asim and Zubair read relevant academic papers, technical documentation and protocol specifications to understand WEP, WPA, WPA2 and WPA3 security protocols, their vulnerabilities and countermeasures.

Writing: Asim wrote the Abstract, Introduction, all WEP and WPA3 content (background, challenges, mitigation techniques) and full Implementation and Evaluation sections. He also handled the formatting and structuring of the whole report. Zubair wrote all WPA and WPA2 content (vulnerabilities, open challenges, security improvements).

Implementation: Asim implemented the attack techniques – Captive Portal Phishing using Evil Portal and PMKID-based WPA2 cracking – alone. This included tool configuration, environment setup, attack execution and data capture.

Presentation: In the final presentation, Zubair presented WPA and WPA2 sections and Asim presented WEP and WPA3 sections along with implementation walkthrough and demo explanation.

This distribution of work is balanced and reflects the strengths of each team member and their contributions to the final deliverables.

REFERENCES

[1] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of rc4," in *Selected Areas in Cryptography*. Springer, 2001, pp. 1–24.

[2] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1313–1328.

[3] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd," in *Proceedings of the 2019 IEEE Symposium on Security and Privacy*. IEEE, 2019, pp. 517–533.

[4] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proceedings of the 7th annual international conference on Mobile computing and networking*. ACM, 2001, pp. 180–189.

[5] C. He and J. C. Mitchell, "Security analysis and improvements for ieee 802.11i," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2005.

[6] W. A. Arbaugh, N. Shankar, and Y. C. J. Wan, "Your 802.11 wireless network has no clothes," in *Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*. IEEE, 2001, pp. 131–144.

[7] E. Tews, "Attacks on the wep protocol," Cryptology ePrint Archive, Report 2007/471, 2007. [Online]. Available: https://eprint.iacr.org/2007/471

[8] A. Bittau, M. Handley, and J. Lackey, "The final nail in wep's coffin," in *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, 2006, pp. 386–400.

[9] E. Tews and M. Beck, "Breaking 104 bit wep in less than 60 seconds," in *International Workshop on Information Security Applications*. Springer, 2008, pp. 188–202.

[10] X. Li, X. Wang, and D. Wang, "Analysis of wpa protocol and its vulnerability to dictionary attacks," *Journal of Computer Science and Technology*, vol. 20, no. 5, pp. 702–707, 2005.

[11] S. Viehböck, "Brute forcing wi-fi protected setup," Technical Report, 2011, https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

[12] T. D. Nguyen, D. H. Nguyen, B. N. Tran, H. Vu, and N. Mittal, "A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks," in *Proceedings of the 17th IEEE International Conference on Computer Communications and Networks*. IEEE, 2008, pp. 1–6.

[13] A. Bartoli, E. Medvet, A. De Lorenzo, and F. Tarlao, "(in)secure configuration practices of wpa2 enterprise supplicants," *arXiv preprint arXiv:1806.03215*, 2018.

[14] Z. Wang, X. Feng, Q. Li, K. Sun, Y. Yang, M. Li, G. Du, K. Xu, and J. Wu, "Off-path tcp hijacking in wi-fi networks: A packet-size side channel attack," *arXiv preprint arXiv:2402.12716*, 2024.

[15] A. Name, "Security enhancement of wep protocol ieee802.11b with dynamic key management," in *Proceedings of the World Congress on Engineering and Computer Science*, 2011, pp. 172–176.

[16] ——, "Wired equivalent privacy," *Journal Name*, Year, https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy.

[17] ——, "Wep and wpa improvement," in *Conference Name*. Organization, Year.

[18] I. A. Ajah, "Evaluation of enhanced security solutions in 802.11-based networks," *arXiv preprint arXiv:1409.2261*, 2014.

[19] S. Xiao, W. Gong, and D. Towsley, "Secure wireless communication with dynamic secrets," in *Proceedings of the IEEE INFOCOM*, 2010, pp. 1–9.

[20] SecureW2, "A security analysis of wpa-personal for wi-fi networks," https://www.securew2.com/blog/a-security-analysis-of-wpa-personal, accessed: 2025-04-30.

[21] D. Nguyen *et al.*, "Improving wireless security with enhancement in wpa2 protocol," *International Journal of Computer Science and Network Security*, vol. 8, no. 6, pp. 276–284, 2008.

[22] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1313–1328.

[23] S. ViehbÃ¶ck, "Brute forcing wi-fi protected setup," https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf, accessed: 2025-04-30.

[24] M. Malekzadeh, A. A. A. Ghani, Z. A. Zulkarnain, and Z. Muda, "Security improvement for management frames in ieee 802.11 wireless networks," *International Journal of Computer Science and Network Security*, vol. 7, no. 6, pp. 276–284, 2007.

[25] D. D. A. Braga, N. Kulatova, M. Sabt, P.-A. Fouque, and K. Bhargavan, "From dragondoom to dragonstar: Side-channel attacks and formally verified implementation of wpa3 dragonfly handshake," *arXiv preprint arXiv:2307.09243*, 2023.

[26] W.-F. Alliance, "Wi-fi certified enhanced open: Owe specification," 2018, https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-enhanced-open.

[27] ——, "Wi-fi certified easy connect: Simplifying device provisioning," 2018, https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect.

[28] N. Dalal, N. Akhtar, A. Gupta, N. Karamchandani, G. S. Kasbekar, and J. Parekh, "A wireless intrusion detection system for 802.11 wpa3 networks," *arXiv preprint arXiv:2110.04259*, 2021.

[29] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security flaws in 802.11 data link protocols," *Communications of the ACM*, vol. 46, no. 5, pp. 35–39, 2003.

[30] M. Vanhoef and F. Piessens, "Practical verification of wpa-tkip vulnerabilities," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. ACM, 2013, pp. 427–436.

[31] C. Cremers, B. Kiesl, and N. Medinger, "A formal analysis of ieee 802.11's wpa2: Countering the kracks caused by cracking the counters," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 2020, pp. 1–17.

[32] M. ÄermÃ¡k, R. LipovskÃœ, and Å. SvorenÄÃk, "Kr00kâserious vulnerability deep inside wi-fi encryption," https://www.eset.com/int/kr00k/, 2020.

[33] S. Alshahrani, W. Alasmary, F. Alhaidari, F. Alhaidari, and F. Alhaidari, "Wpa3 connection deprivation attacks," in *Risks and Security of Internet and Systems*. Springer, 2020, pp. 135–150.

[34] G. S. Guaki, "Wpa3; an analysis of its flaws and limitations: A literature review," *ResearchGate Preprint*, 2024.

[35] M. Vanhoef and E. Ronen, "A security analysis of wpa3-pk: Implementation and precomputation attacks," in *Applied Cryptography and Network Security*. Springer, 2023, pp. 123–143.

[36] K. Chadee, W. Goodridge, and K. Khan, "Recovering wpa-3 network password by bypassing the simultaneous authentication of equals handshake using social engineering captive portal," *arXiv preprint arXiv:2412.15381*, 2024.