Wi-Fi Network Security

Attacking WEP and WPA/WPA2 Protocols

Mohammad Asim, Mohammad Zubair

Presented To: Dr. Bechir Hamdaoui

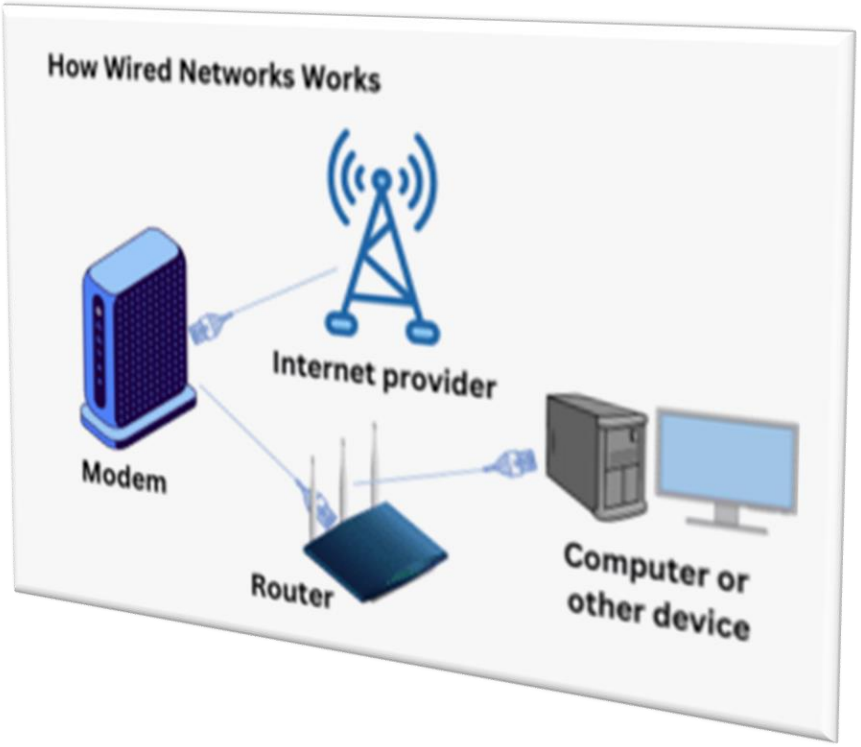
Outline

- Introduction to Wi-Fi Security
- Background & Fundamentals
- Research & Technical Challenges
- State-of-the-Art Solution Approaches
- Open & Unsolved Challenges
- Implementation

Introduction

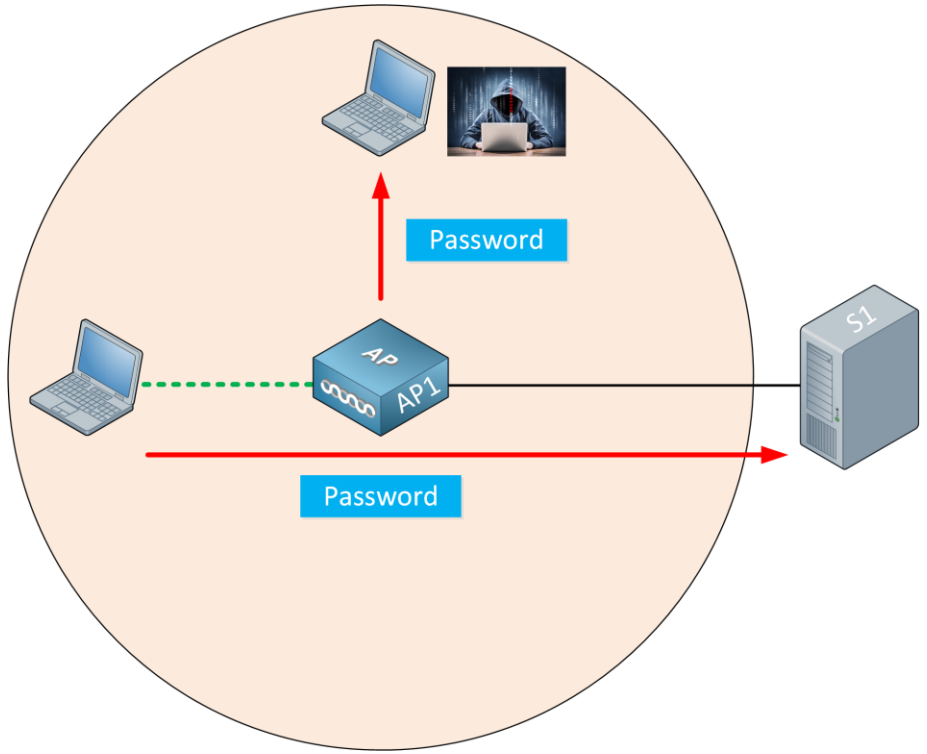
Introduction to Wi-Fi Security

- Wi-Fi enables wireless internet and device communication.
- It is used in homes, businesses, and public spaces.
- Vulnerable to threats like data interception, unauthorized access, and DoS attacks without security.
- Wi-Fi security protects data, prevents unauthorized access, and defends against cyber threats.



Importance of Wi-Fi Security

- Billions of devices connected worldwide.
- Common attack vectors:
  - Eavesdropping
  - Man-in-the-Middle attacks
  - Denial of Service
  - Credential theft
- Consequences of breaches:
  - Data theft
  - Identity theft
  - Network compromise

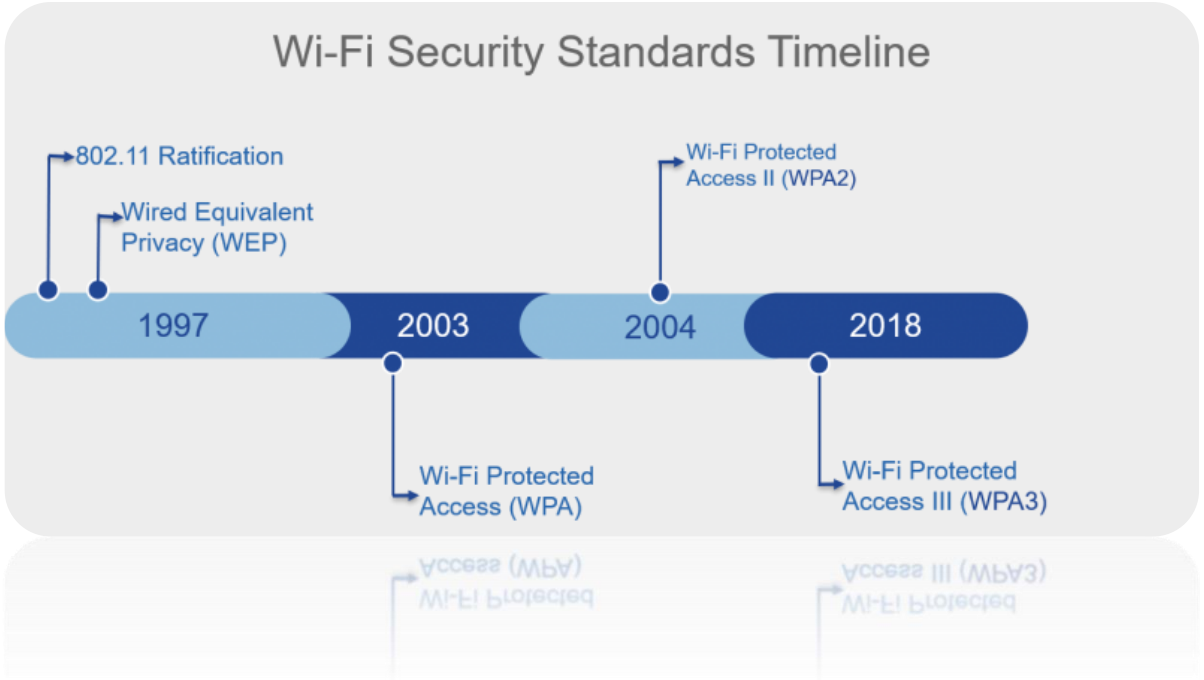


Wireless Communication Security Requirements

- Confidentiality
  - Messages sent over the wireless links must be encrypted
- Authentication
  - Origin of messages received over wireless links must be verified
- Replay Detection
  - Freshness of messages received over the wireless links must be checked
- Integrity
  - Modifying messages on the fly is not so easy, but possible.
- Access Control
  - Access to the network should be provided only to legitimate entities

Type of Wi-Fi Security Protocols

- Wireless networks have become ubiquitous in modern computing
- Security is paramount due to sensitive data transmission
- Evolution of protocols:
  - WEP (1999) - First attempt at security
  - WPA (2003) - Interim solution
  - WPA2 (2004) - Stronger encryption
  - WPA3 (2018) - Latest standard



WEP

WEP Protocol Overview

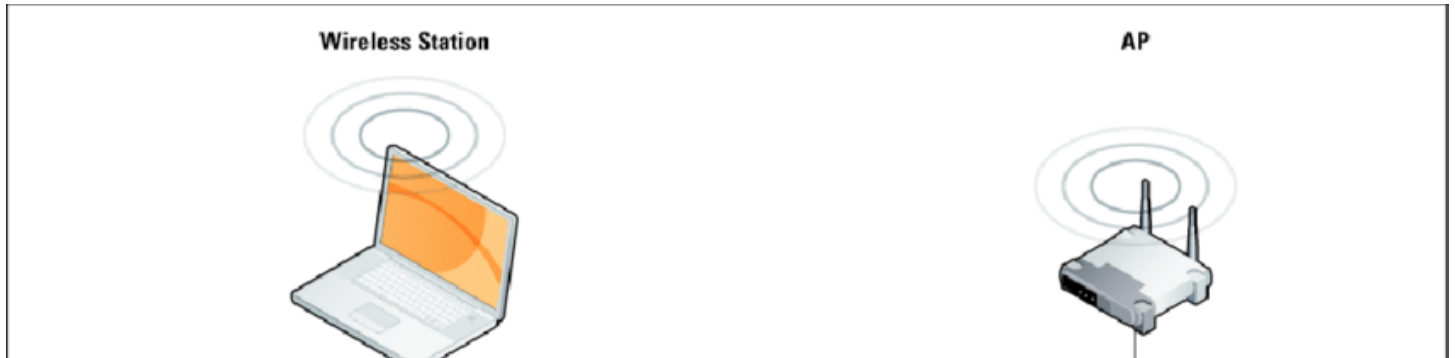
- WEP was the first security protocol for Wi-Fi, introduced in the IEEE 802.11 standard in 1999.
- To provide security equivalent to wired networks by encrypting data transmitted over the air.
- Components
  - RC4 Stream Cipher: Used for encryption.
  - Initialization Vector (IV): 24-bit value used to ensure different encryption keys for each packet.
  - Shared Key Authentication
  - Integrity Check Value (ICV): CRC-32 checksum to verify data integrity.

Confidentiality/Privacy in WEP

- Encryption Mechanism
  - WEP uses RC4, a stream cipher.
  - IV (24-bit) + Secret key (40/104-bit) forms the seed.
  - Keystream is XORed with plaintext to generate ciphertext.
- Example
  - Plaintext: HELLO
  - Keystream: XMCKL
  - Ciphertext: EIGDF (via XOR)
- Small IV space (2^24 = 16.7 million) causes frequent reuse, leading to keystream collisions.

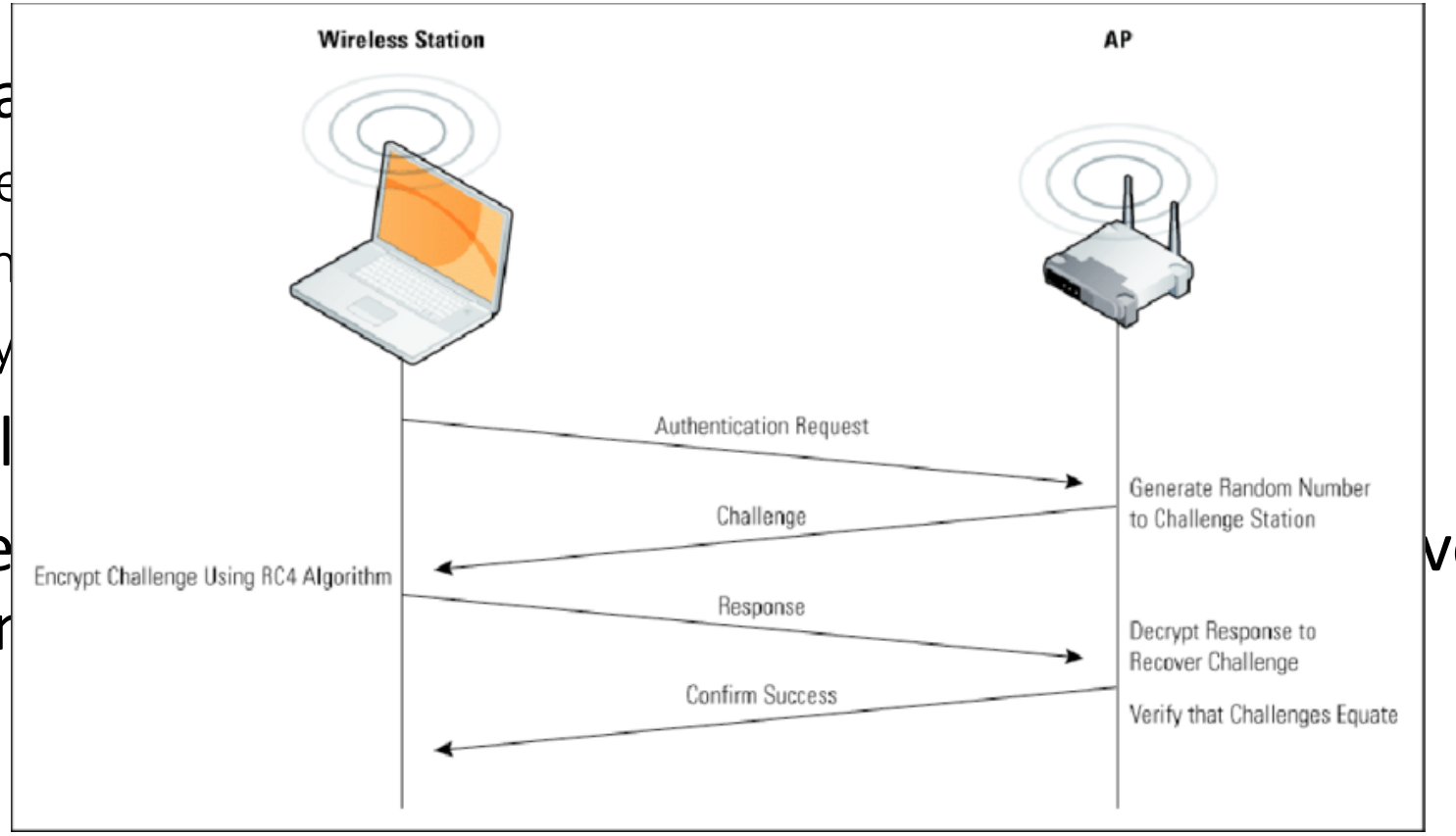
User/Message Authentication in WEP

- Authentication Process
  - The Access Point (AP) sends a random challenge to the client.
  - Client encrypts it using the shared WEP key.
  - AP decrypts the response and compares it.
- Ensure only users with the key can authenticate.
- An attacker can capture challenge-response pairs and derive the key through analysis.



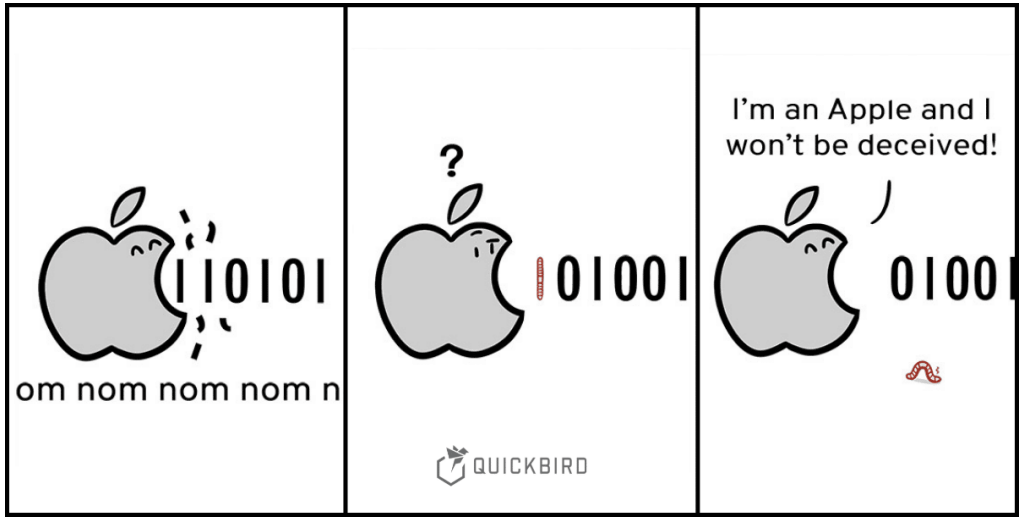
User/Message Authentication in WEP

- Authentica
  - The Acce
  - Client en
  - AP decry
- Ensure onl
- An attacke ve the key through ar

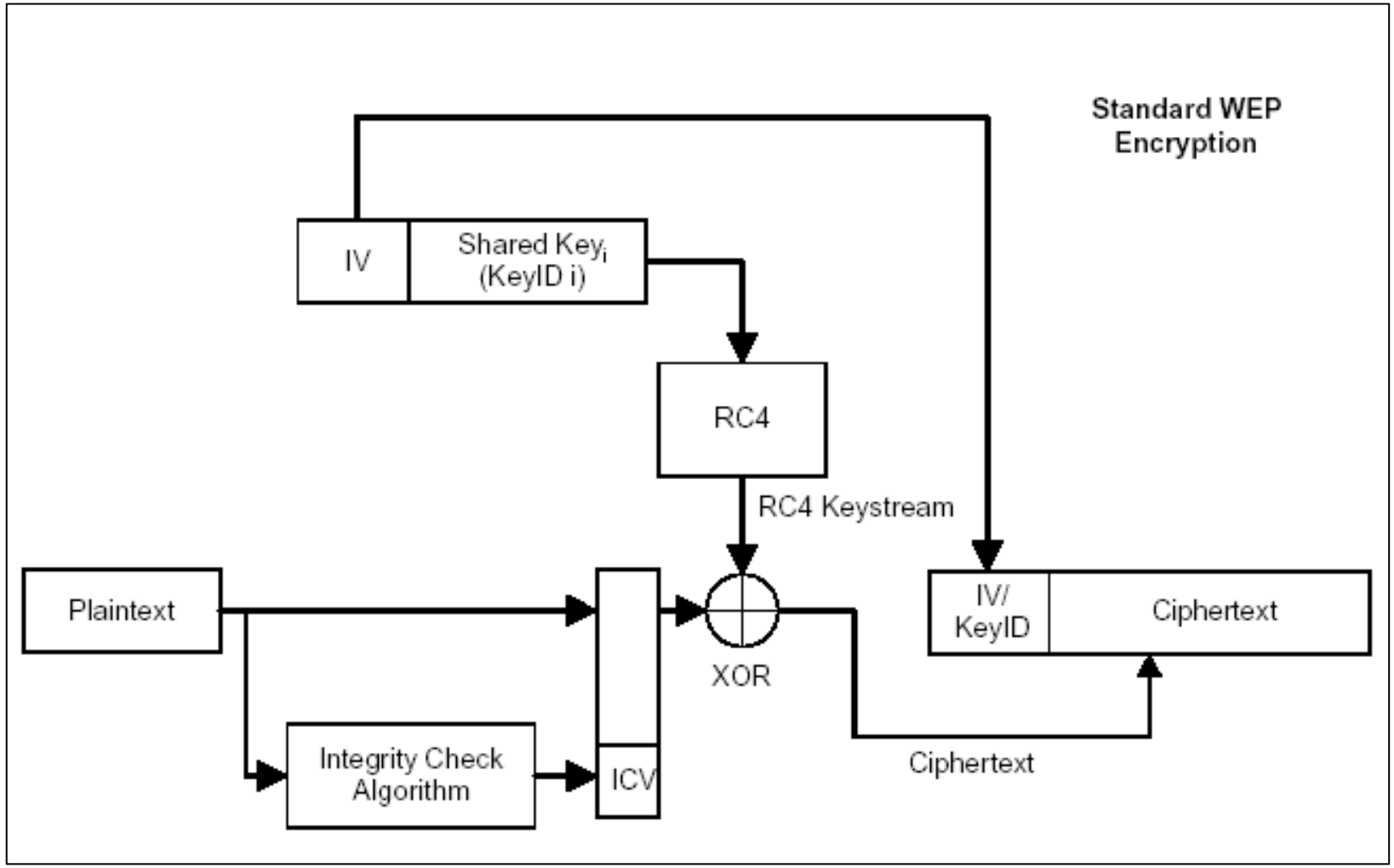


Message Integrity in WEP

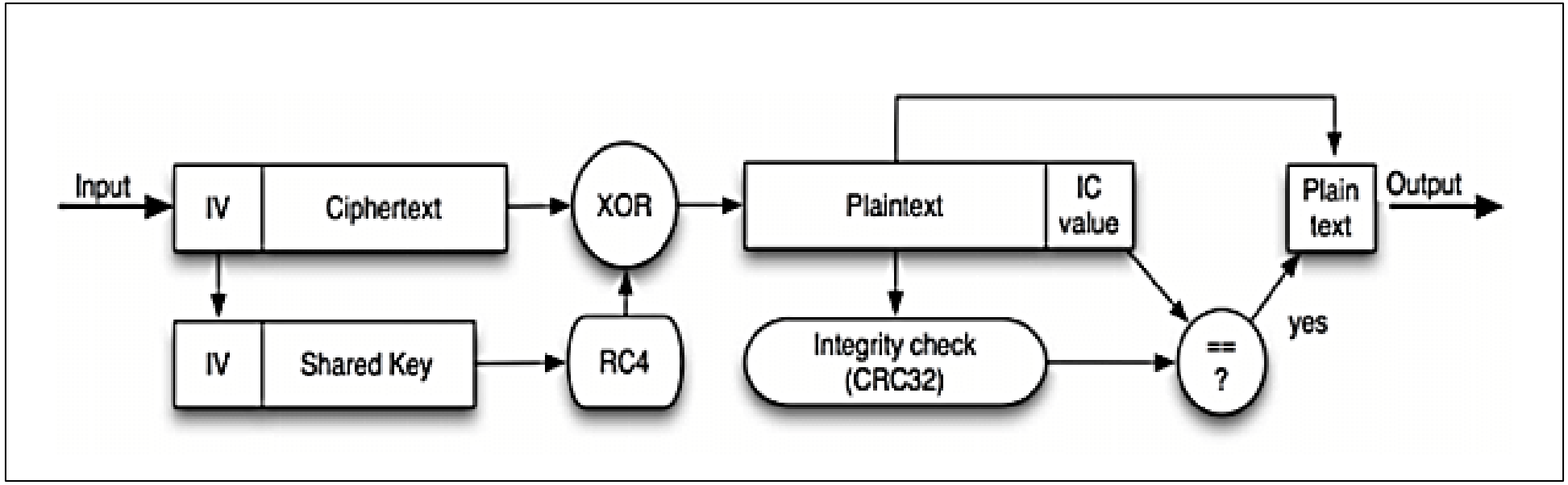
- ICV (Integrity Check Value)
  - Computed using CRC-32 and appended to plaintext.
  - Entire message + ICV is then encrypted.
- Detect accidental changes.
- Security Issue
  - CRC-32 is linear and can be forged.
  - Attackers can modify messages and recompute ICV accordingly.



WEP Encryption Process

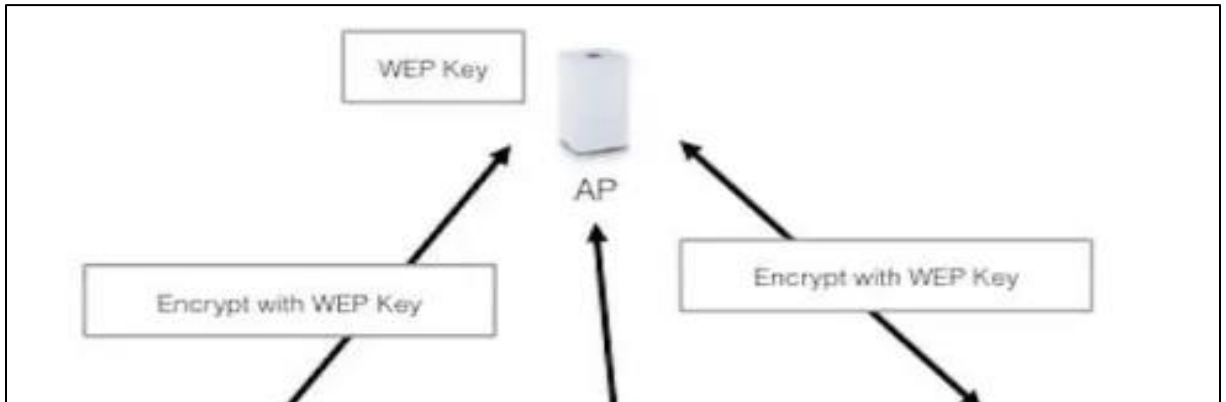


WEP Decryption Process



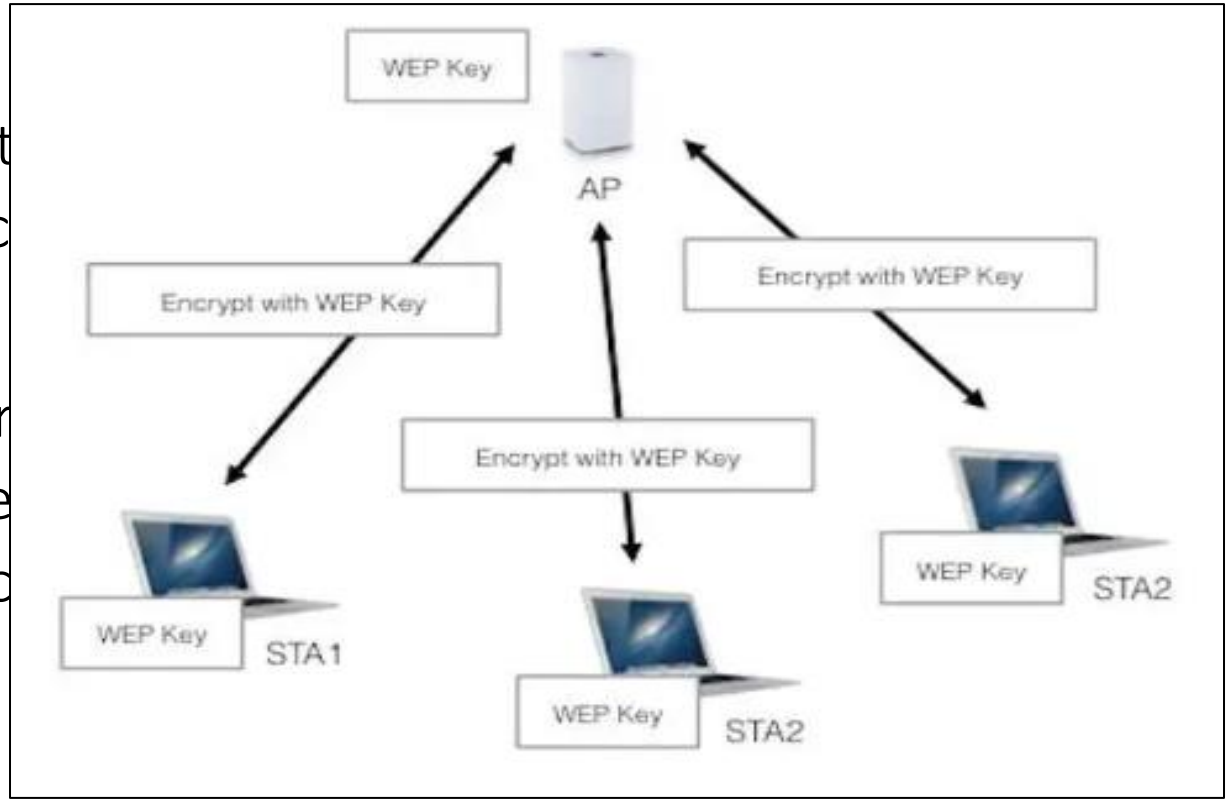
Access Control in WEP

- Mechanism
  - Devices must know the shared WEP key to join the network.
  - Once connected, no distinction among users.
- Problems
  - All users share the same key.
  - Keys must be manually distributed.
  - No user-specific access control or revocation.

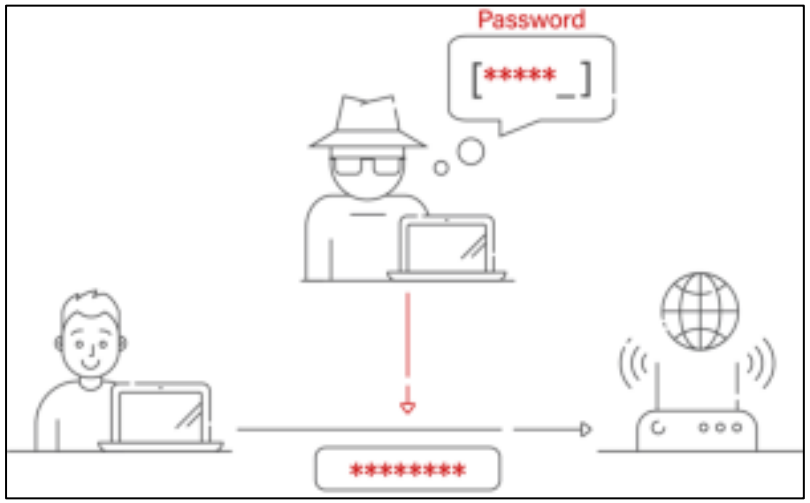


Access Control in WEP

- Mechanism
  - Devices must
  - Once connec
- Problems
  - All users shar
  - Keys must be
  - No user-spec



Key Vulnerabilities in WEP



1. Short Initialization Vector (IV)
   - 24-bit IV is too small (only ~16 million combinations)
   - Leads to repetition and keystream reuse
   - Example: In busy networks, IV collisions occur in minutes
2. Weak Encryption (RC4 misuse)
   - RC4 keystreams are reused due to repeated IVs
   - Attackers can recover plaintext from XOR patterns
3. Linear Integrity Check (CRC-32)
   - Not cryptographically secure
   - Allows bit-flipping attacks

Key Vulnerabilities in WEP (Cont’d)

4. Shared Key Authentication Weaknesses

- Challenge-response can be captured and reused
- Attacks: Replay, dictionary, man-in-the-middle (MITM)

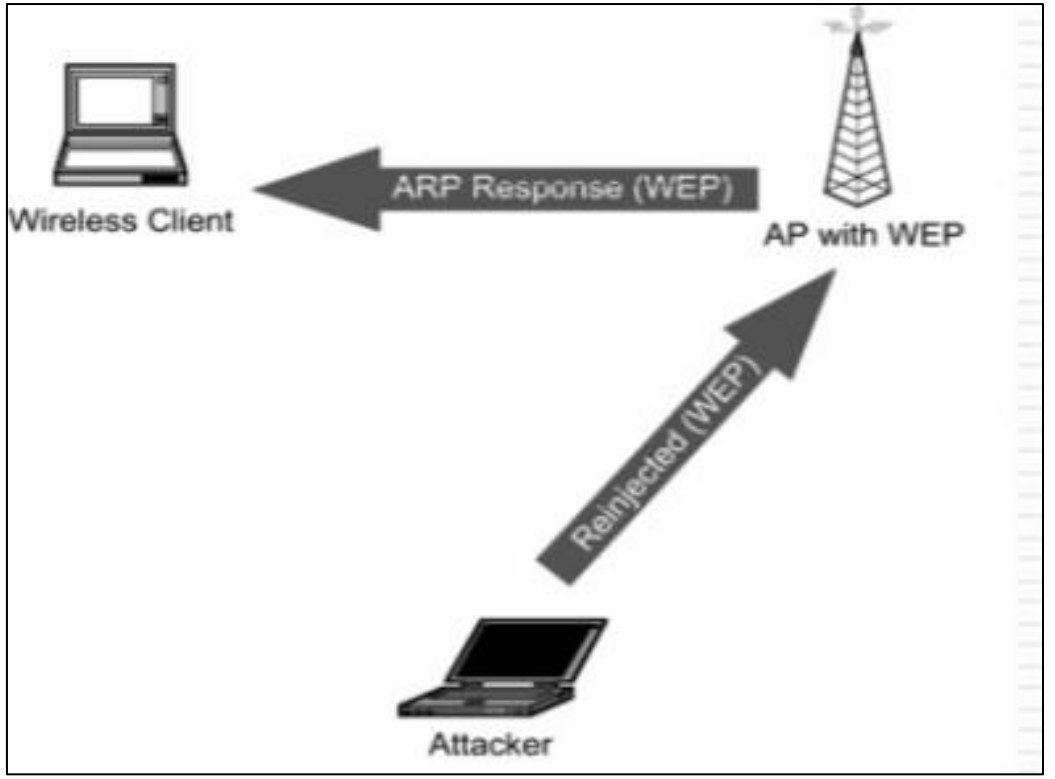
Example of WEP Attacks

- FMS Attack (Fluhrer, Mantin, Shamir)
  - Weaknesses in WEP
    - Short Initialization Vector (IV): 24 bits, leading to IV collisions.
    - Key Reuse: Same key used over long periods, allowing for easier cracking.
  - Attack Process
    - Collects large amounts of ciphertext (encrypted packets).
    - Analyzes the IVs, looking for patterns and weaknesses in the RC4 key stream.
    - Uses statistical analysis to recover the secret WEP key.

Fluhrer, S., Mantin, I., and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Selected Areas of Cryptography: SAC 2001, Lecture Notes in Computer Science Vol. 2259, pp 1-24, 2001.

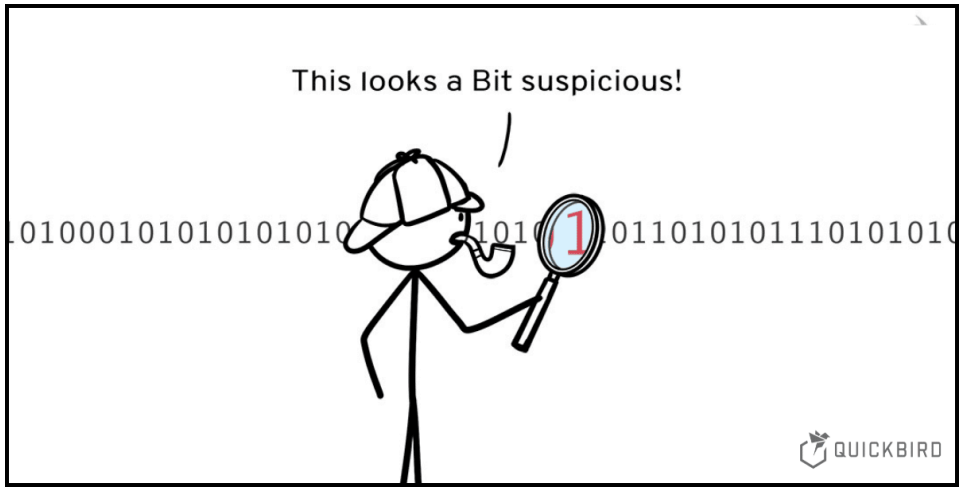
Example of WEP Attacks (Cont'd)

- ARP Replay Attack
  - Attacker injects spoofed ARP requests to generate predictable encrypted responses
  - Speeds up packet collection for FMS



Example of WEP Attacks (Cont'd)

- Bit-Flipping Attack
  - Due to linear CRC and XOR, attacker modifies encrypted messages without knowing key



Example of WEP Attacks (Cont'd)

- KoreK attack
  - Utilizes correlations between the first few bytes of the RC4 key, the generated keystream, and the next key byte.
  - Employs 16 additional correlations beyond the initial FMS attack.
  - Reduces the number of packets required for a successful attack compared to earlier methods like FMS.
- How KoreK Attack Works
  - Capture encrypted packets from the WEP-protected network.
  - Recover the first few bytes of the keystream for each packet.
  - Use predefined correlations to vote for possible values of the root key bytes
  - Construct a decision tree to determine the root key byte by byte.
  - Validate the recovered key by attempting to decrypt packets.

Tews, Erik, and Martin Beck. "Practical attacks against WEP and WPA." Proceedings of the second ACM conference on Wireless network security. 2009.

Example of WEP Attacks (Cont'd)

- PTW Attack
  - Introduces new correlations that do not require specific conditions on the RC4 state.
  - Votes for the sum of multiple key bytes simultaneously, reducing the number of packets needed.
  - Dramatically reduces the number of packets required (~35,000-40,000) and attack time.
- How PTW Attack Works
  - Capture encrypted packets from the WEP-protected network.
  - Recover the first few bytes of the keystream for each packet.
  - Use modified correlations to vote for the sum of multiple key bytes.
  - Calculate individual key bytes from the sums.
  - Validate the recovered key by attempting to decrypt packets.

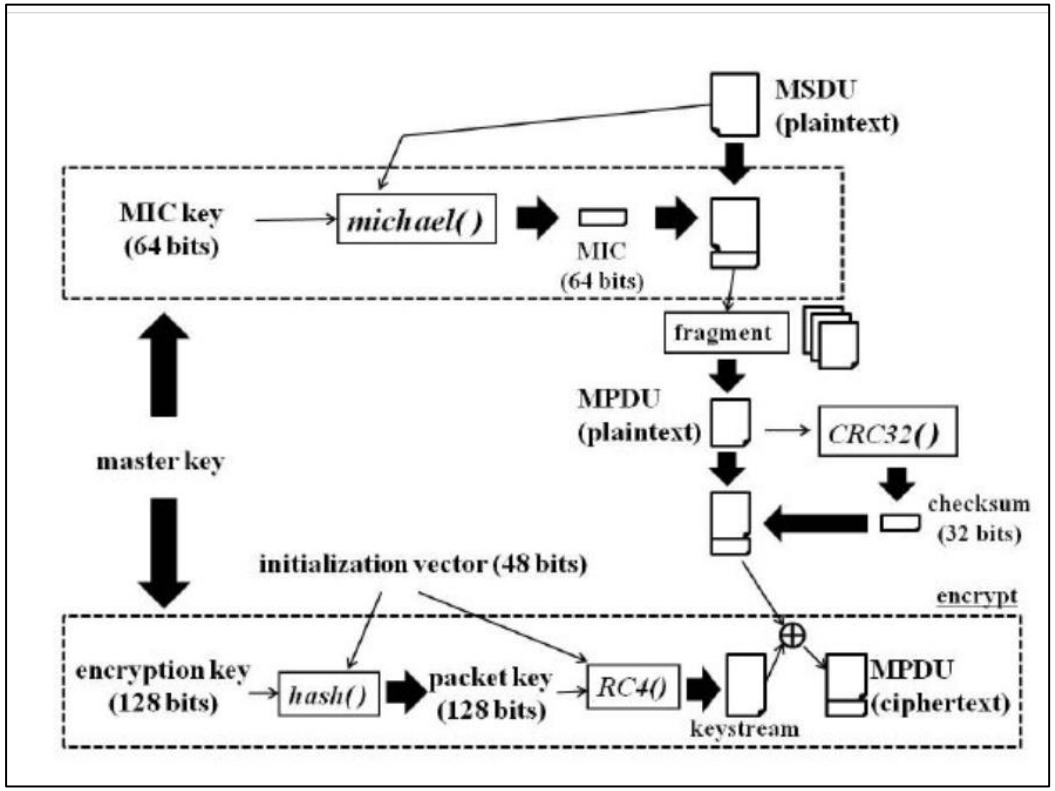
Tews, Erik, and Martin Beck. "Practical attacks against WEP and WPA." Proceedings of the second ACM conference on Wireless network security. 2009.

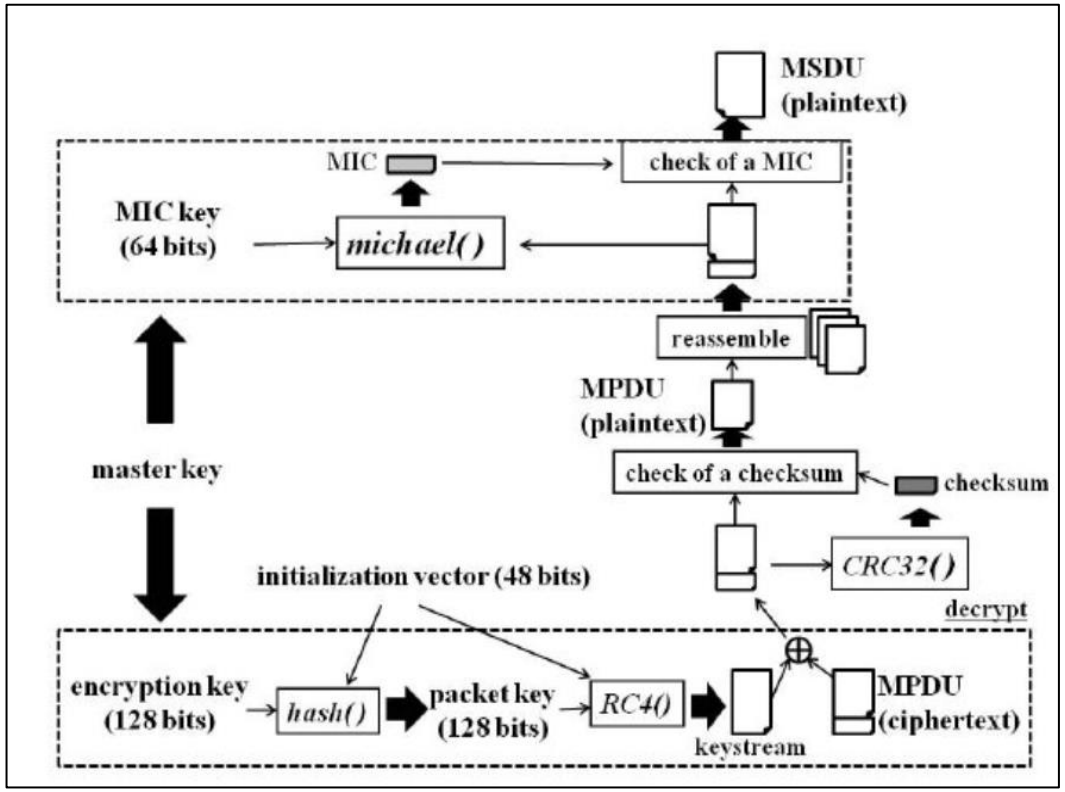
WPA

WPA – Protocol Overview

- WPA (Wi-Fi Protected Access) Introduced in 2003 by the Wi-Fi Alliance as a response to WEP vulnerabilities.
- Built on the draft IEEE 802.11i standard before the finalization of WPA2.
- Designed as a software/firmware upgrade for WEP-compatible hardware.
- Implements Temporal Key Integrity Protocol (TKIP) to enhance encryption.
- Two Modes:
  - WPA-Personal (PSK): For home/small office use.
  - WPA-Enterprise (802.1X): For larger organizations with RADIUS (Remote Authentication Dial-In User Service) servers.

WPA – Encryption and Decryption





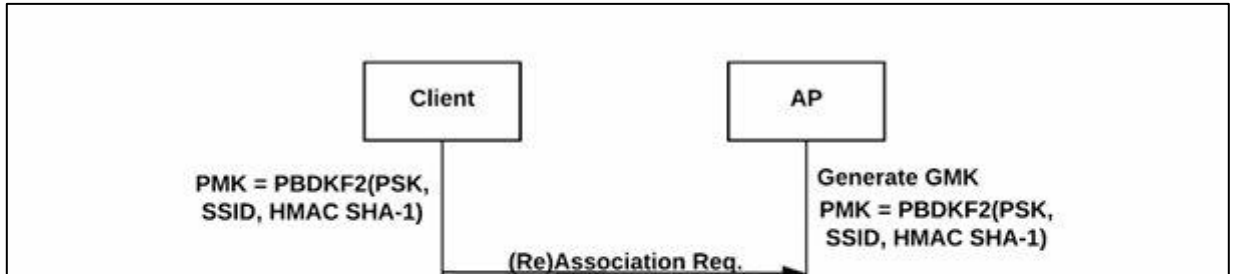
Confidentiality/Privacy in WPA

- Uses RC4 stream cipher with TKIP to encrypt user data.
- TKIP features:
  - Per-packet key mixing: Each packet has a unique encryption key.
  - 48-bit Initialization Vectors (IVs) to avoid reuse.
  - Sequence counter prevents replay attacks.
- Provides forward secrecy: Compromising one key doesn’t expose others.

User/Message Authentication in WPA

Authentication Methods

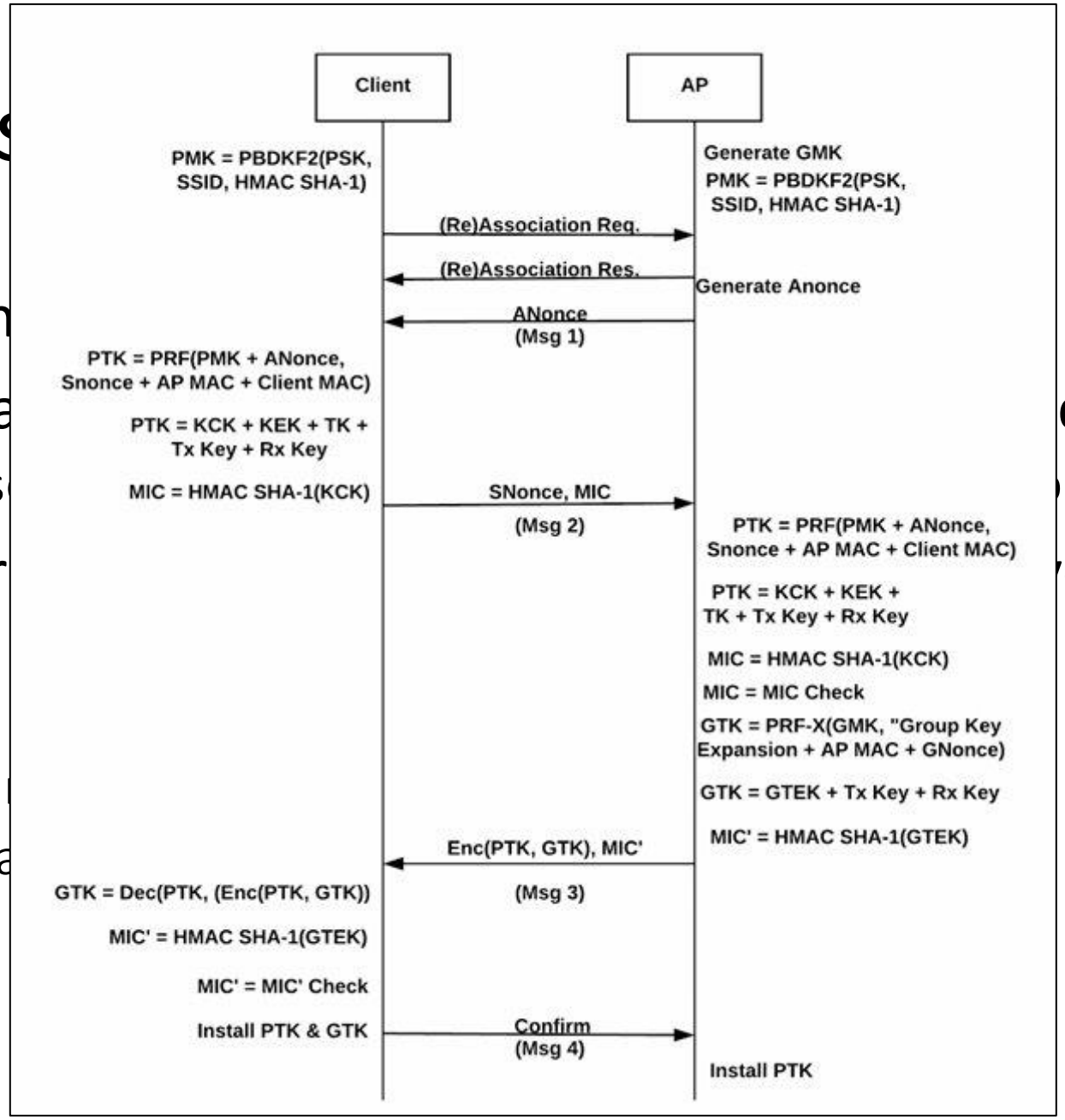
- WPA-Personal (PSK): Users authenticate using a shared passphrase.
    - Simpler setup but vulnerable to brute-force if weak passphrase is used.
- WPA-Enterprise (802.1X): Uses an authentication server (e.g., RADIUS).
    - Supports EAP-Extensible Authentication Protocol (e.g., EAP-TLS, EAP-TTLS).
    - Provides mutual authentication (user and network).
    - Dynamically generates session keys per user.



User/Mes PA

Authentication

- WPA-Persona d passphrase.
  - Simpler s hrase is used.
- WPA-Enterpr er (e.g., RADIUS).
  - Supports
  - Provides
  - Dynamica



Message Integrity in WPA

- Protecting Data from Tampering
- TKIP includes the Michael Message Integrity Code (MIC):
  - Detects packet tampering or injection attacks.
  - Adds an 8-byte MIC to each data frame.
- Replay protection:
  - Uses packet sequence numbers.
  - Discards packets with duplicate or old sequence numbers.
- Ensures data authenticity and integrity, not just confidentiality.

Access Control in WPA

Who Gets In and Who Doesn’t

- Access is granted only after successful authentication and key exchange.
- In WPA-Enterprise:
  - 802.1X controls access via centralized authentication (e.g., RADIUS).
  - VLAN assignment and ACLs for user-specific access control.
- In WPA-Personal:
  - All clients share the same key; access control is binary (all-or-nothing).
- No inherent role-based access control in WPA itself — depends on the network backend.

Key Vulnerabilities in WPA

1. Weaknesses in TKIP (Temporal Key Integrity Protocol)

- Legacy RC4 cipher: RC4, already known to have biases, was reused in WPA. While TKIP tried to mitigate this with per-packet key mixing, RC4's foundational flaws remained.
- MIC (Michael) algorithm is weak:
  - Designed to work on legacy hardware, it sacrifices cryptographic strength for speed.
  - Can be brute-forced with enough captured packets (~2^20 computations).
  - Allows packet injection if MIC keys are recovered.
- Limited number of replays allowed: If 2 MIC failures occur within 60 seconds, the client disconnects, which can be exploited for DoS attacks.

Key Vulnerabilities in WPA (Cont’d)

2. Vulnerabilities in WPA-Personal (PSK Mode)

- Shared key model: One compromised device can compromise the entire network.
- Offline dictionary attacks:
  - Attackers capture the 4-way handshake and try password guesses offline.
  - No rate-limiting during guessing.
  - If the PSK is weak (e.g., “12345678” or “iloveyou”), it's easily cracked.

Key Vulnerabilities in WPA (Cont’d)

3. Session Hijacking / Evil Twin

- No server authentication in WPA-Personal:
  - Attackers can set up a rogue access point mimicking the SSID (Evil Twin).
  - Clients auto-connect to the strongest signal — often the attackers.
  - Used for man-in-the-middle (MitM) attacks or credential harvesting.

4. Key Reuse & Replay

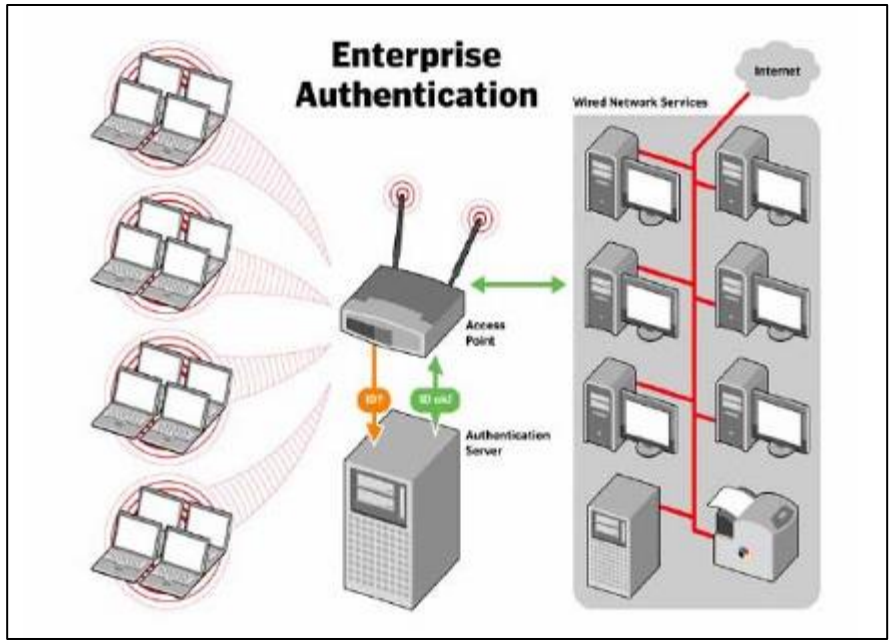
- Although TKIP includes replay protection via sequence counters, poor implementation or key reinstallation bugs can still allow replay or rekeying attacks.

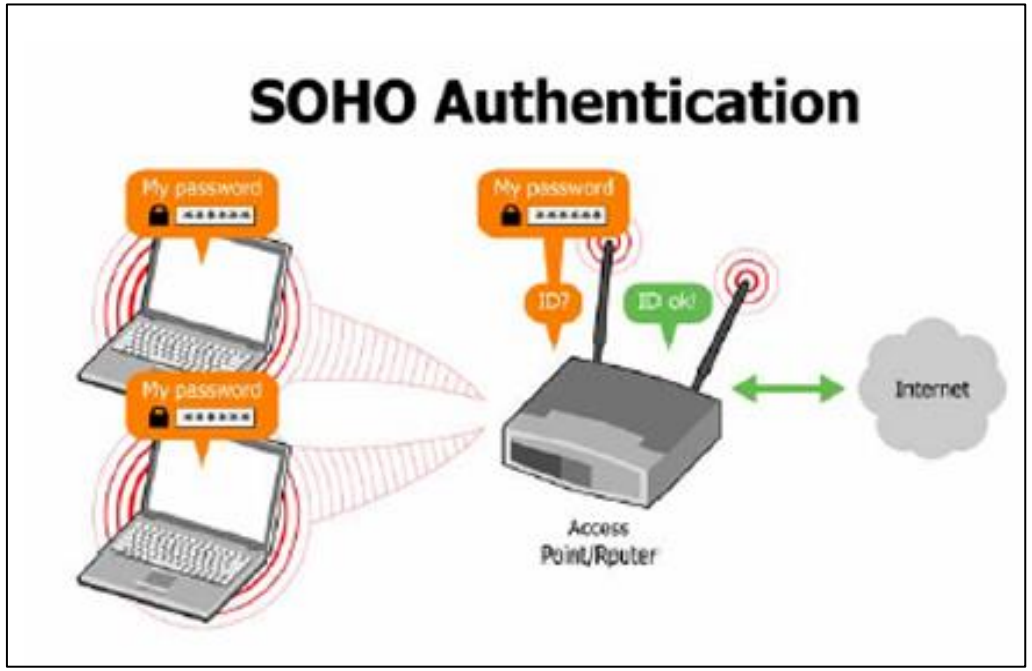
WPA2

WPA2 – Protocol Overview

- Introduced in 2004 by the Wi-Fi Alliance to fully implement the IEEE 802.11i security standard.
- Designed to replace WPA and WEP with stronger encryption and integrity mechanisms.
- Supports two modes:
  - WPA2-Personal (PSK): Uses a shared passphrase.
  - WPA2-Enterprise (802.1X): Uses RADIUS and EAP for centralized authentication.
- Mandatory support for AES-CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

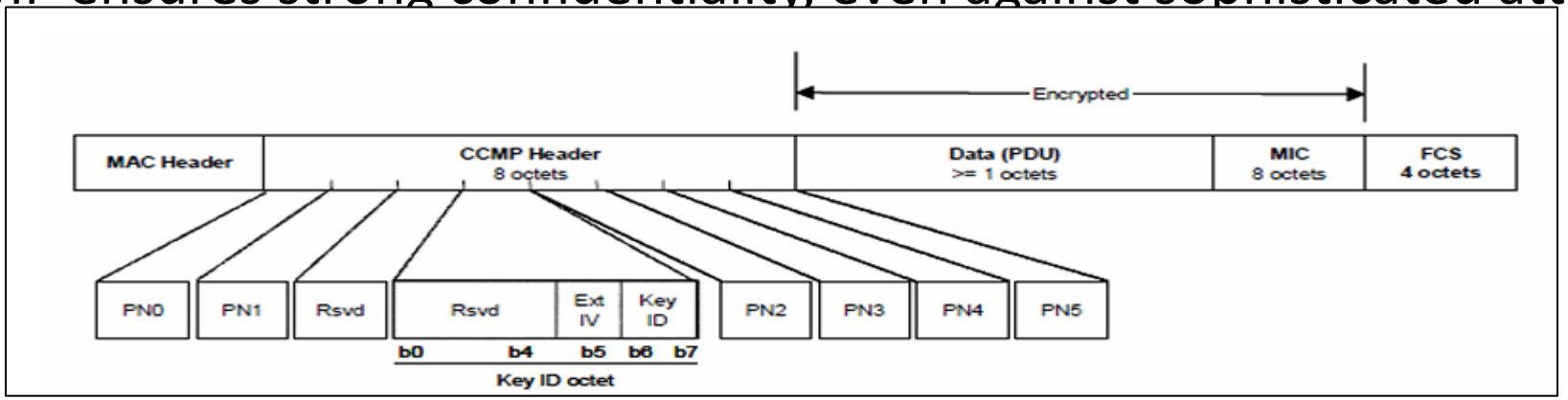
WPA2 – Protocol Overview (Cont'd)





Confidentiality/Privacy in WPA2

- Data Encryption & Privacy
- AES (Advanced Encryption Standard) used instead of RC4.
- CCMP provides:
  - 128-bit AES encryption in CTR mode (for confidentiality).
  - CBC-MAC (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for message authentication.
- Each packet uses a unique nonce to prevent replay and key reuse.
- AES-CCMP ensures strong confidentiality, even against sophisticated attacks.



WPA2 – Encryption and Decryption

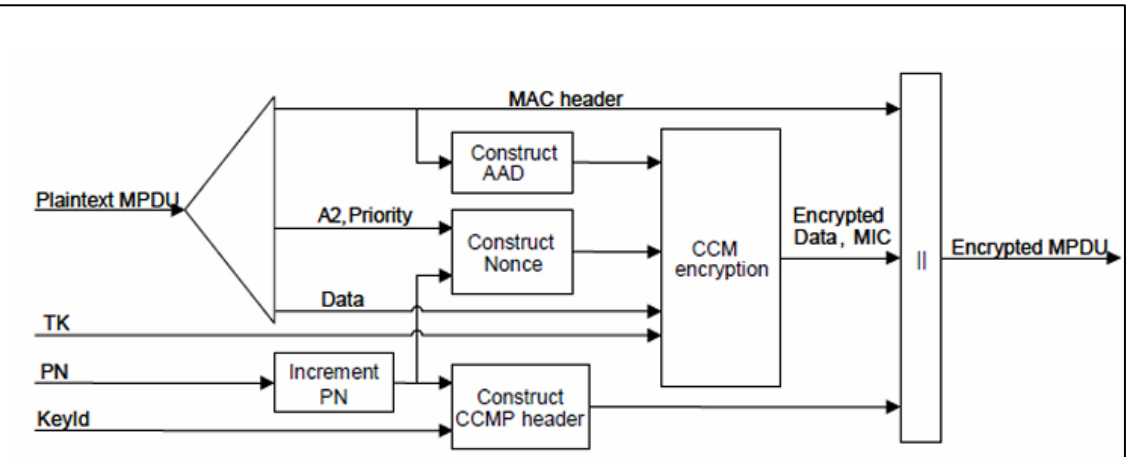


Figure 2.12. CCMP Encapsulation process [34]

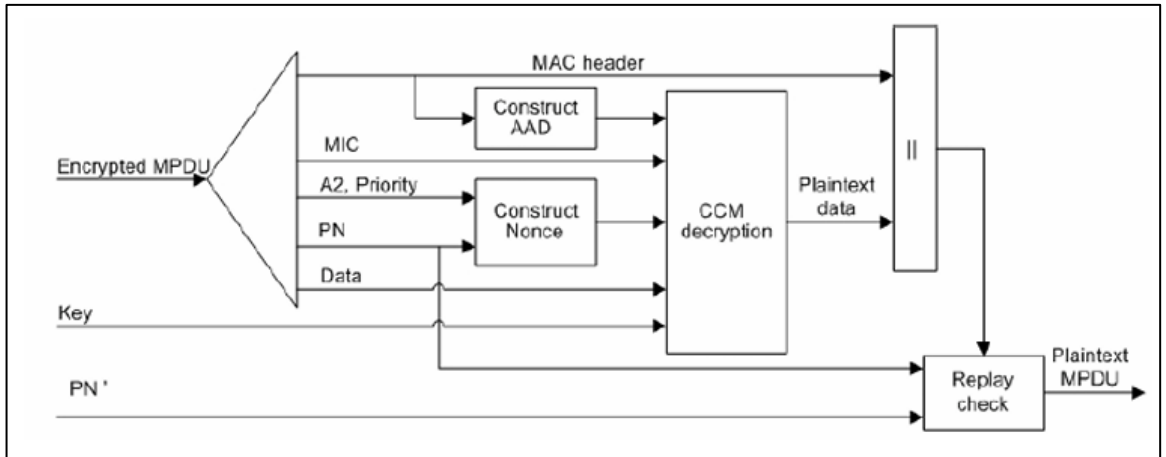
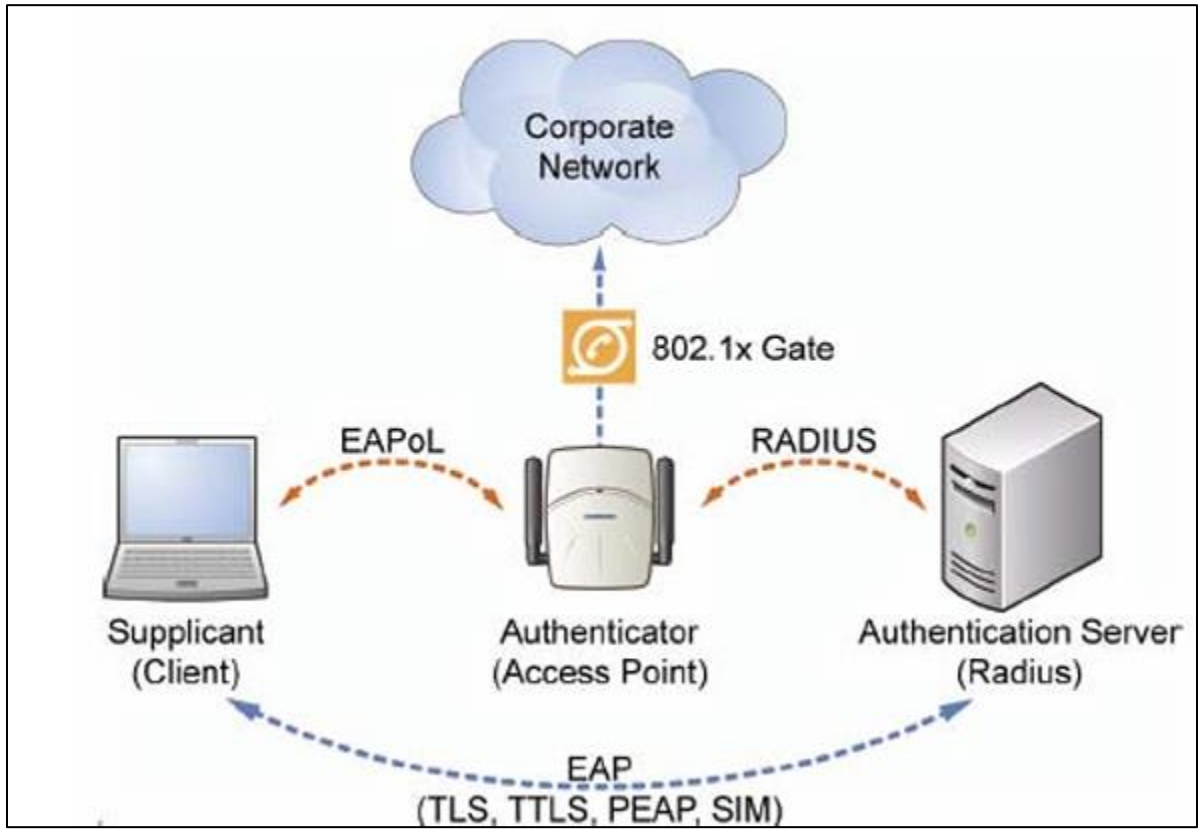


Figure 2.13. CCMP Decapsulation process [34]

User/Message Authentication in WPA2

- Authentication Approaches
- WPA2-Personal (PSK):
  - Shared key used across all clients.
  - Simpler but vulnerable to dictionary attacks if passphrase is weak.
- WPA2-Enterprise (802.1X):
  - Uses EAP protocols (e.g., EAP-TLS, PEAP).
  - Involves a RADIUS server for mutual authentication.
  - Supports per-user credentials and dynamic session keys.

User/Message Authentication in WPA2 (Cont'd)



Message Integrity in WPA2

- Ensuring Data is Untampered
- CBC-MAC in CCMP provides strong message integrity.
- Uses a Message Integrity Code (MIC) for each packet.
- Protects against:
  - Packet forgery
  - Tampering
  - Replay attacks
- Nonces are used per packet, ensuring unique encryption/integrity contexts.

Access Control in WPA2

Managing Who Gets In

- WPA2 uses EAP and 802.1X in Enterprise mode for dynamic and role-based access control.
- Authentication server assigns VLANs, ACLs, and session timeouts.
- PSK mode allows access if the user knows the shared passphrase.
- Once authenticated, a Pairwise Transient Key (PTK) is derived per session.

Key Vulnerabilities in WPA2

KRACK Attack

- Found in 2017 by Mathy Vanhoef.
- Exploits flaws in the WPA2 4-Way Handshake.
- Forces clients to reinstall an already-used key by manipulating handshake messages.
- Effects:
    - Decrypt network traffic
    - Hijack TCP connections
    - Inject malware or ransomware
- Impact: All WPA2 devices (before patches) were vulnerable.

Key Vulnerabilities in WPA2 (Cont’d)

PMKID Attack

- Discovered in 2018.
- Captures the PMKID directly from the Access Point — no need for full 4-way handshake.
- Enables offline brute-force cracking of passwords.
- Impact:
  - Makes capturing handshakes easier.
  - Very dangerous for weak passwords.
- Only possible due to WPA2's PMK caching.

Key Vulnerabilities in WPA2 (Cont’d)

Nonce Reuse Issues

- AES-CCMP encryption in WPA2 expects unique nonces for every frame.
- Poor device implementations sometimes reuse nonces accidentally.
- Effects:
  - Compromises encryption integrity.
  - Allows attackers to decrypt or replay packets.
- Unique to WPA2 because WPA (TKIP) had a different frame protection mechanism.

Key Vulnerabilities in WPA2 (Cont’d)

Group Key Rekeying Flaws

- WPA2 networks periodically rekey group traffic encryption keys.
- Some systems fail to correctly invalidate old keys.
- Effects:
    - Attackers can continue decrypting group broadcast/multicast traffic even after a "new" key is installed.
- Specific to WPA2's group keying mechanisms.

Key Vulnerabilities in WPA2 (Cont’d)

Enterprise (EAP) Vulnerabilities

- WPA2-Enterprise uses EAP (Extensible Authentication Protocol) with 802.1X.
- Common issues:
  - Using weak EAP types like EAP-MD5.
  - Clients failing to validate server certificates.
- Effects:
  - Man-in-the-Middle (MitM) attacks.
  - Credential theft even without cracking encryption.

Examples of WPA/WPA2 Attacks

1. Beck-Tews Attack (2008)

- **Target:** WPA-TKIP, WPA2 with TKIP mode is also theoretically vulnerable.
- **Mechanism:** Reuses parts of the WEP chopchop attack.
- Details:
    - Exploits TKIP's limited replay protection and weak MIC.
    - Attacker injects arbitrary packets by carefully crafting MICs.
    - Works only on small packets (like ARP).
- Impact: Packet injection into WPA-TKIP networks within ~15 minutes.

Examples of WPA/WPA2 Attacks (Cont’d)

2. Hole196 Attack

- **Target:** WPA2 but conceptually possible in WPA too.
- **Mechanism:**
  - Relies on misuse of the Group Temporal Key (GTK).
  - GTK is shared among all clients for broadcast/multicast — but malicious clients can forge packets to others on the same network.
- Impact:
  - An attacker connected to the network can spoof DHCP, DNS, or ARP responses, leading to MitM or DoS.

Examples of WPA/WPA2 Attacks (Cont’d)

3. Dictionary and Brute-force Attacks

- **Target:** WPA-Personal (PSK), WPA2-Personal (PSK)
- **Mechanism:**
  - Capture the 4-way handshake between a client and access point.
  - Use wordlists or brute-force to guess the PSK offline.
  - Popular tools: aircrack-ng, hashcat, pyrit.
- **Impact:** Easy to break networks using weak or default passwords.

Examples of WPA/WPA2 Attacks (Cont’d)

4. TKIP MIC DoS Attack

- **Target**: WPA-TKIP, WPA2-TKIP
- **Mechanism**:
  - Sends forged packets that fail MIC validation.
  - After two MIC failures in 60 seconds, the access point **kicks the client** off the network.
- **Impact**: Denial of service — especially disruptive in enterprise environments.

Examples of WPA/WPA2 Attacks (Cont’d)

5. Evil Twin Attack

- **Target**: WPA-Personal/WPA2-Personal users
- **Mechanism**:
    - Attacker sets up a rogue AP with the same SSID as the target network.
    - Devices connect automatically if the rogue AP signal is stronger.
    - Attacker can launch MitM, SSL stripping, or phishing attacks.
- **Impact**: Credential theft, malware injection, traffic manipulation.

Examples of WPA/WPA2 Attacks (Cont'd)

6. KRACK Attack (2017) – *Key Reinstallation Attack*

- **Target**: WPA2, but shows WPA design flaws.
- **Mechanism**:
  - Exploits reinstallation of cryptographic keys during the 4-way handshake.
  - Causes nonce reuse, breaking encryption guarantees.
- **Impact**:
  - Allows attackers to decrypt data, hijack connections, or inject packets.
  - Affects nearly all devices before patches were released.

WPA3

WPA3

- WPA3 (Wi-Fi Protected Access 3) is the latest Wi-Fi security protocol, introduced by the Wi-Fi Alliance in 2018, and became mandatory for all Wi-Fi Certified devices from July 2020.
- Addresses vulnerabilities found in WPA2, offering enhanced security for both personal and enterprise networks.
- Comparison with Previous Versions:
  - WPA1: Introduced TKIP; vulnerable to various attacks.
  - WPA2: Adopted AES-based CCMP; susceptible to KRACK attacks.
  - WPA3: Implements Simultaneous Authentication of Equals (SAE), forward secrecy, and mandatory Protected Management Frames (PMF).

How WPA3 Works

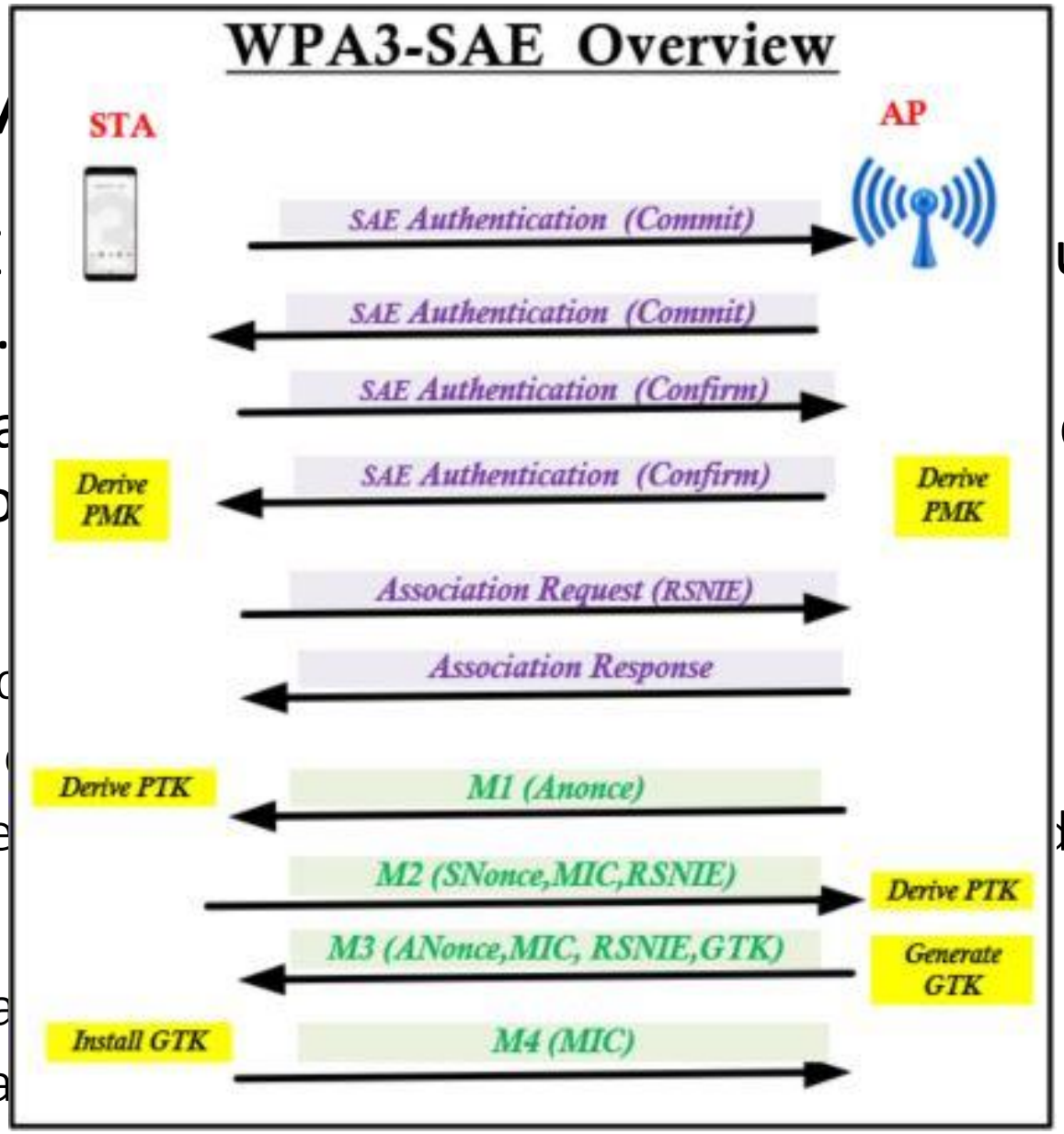
- WPA3 uses advanced cryptographic techniques to secure wireless communications.
- It enhances security through features like Simultaneous Authentication of Equals (SAE), forward secrecy, and stronger encryption algorithms.
- Key Features
  - SAE: Provides secure key exchange, making it resistant to offline dictionary attacks.
  - Forward Secrecy: Ensures that even if a key is compromised, past communications remain secure.
  - Stronger Encryption: Uses AES-CCMP-256 for encryption, providing a higher level of security.

User and Message Authentication

- WPA3 uses SAE to authenticate users, replacing the vulnerable WPA2 Personal mode.
- SAE ensures that even if an attacker captures the handshake, they cannot brute-force the password offline.
- Process
  - Both client and access point exchange cryptographic elements.
  - Derive a shared secret independently.
  - Authenticate each other without transmitting the password.
- Advantages
  - Provides forward secrecy.
  - Resistant to passive eavesdropping and active attacks.

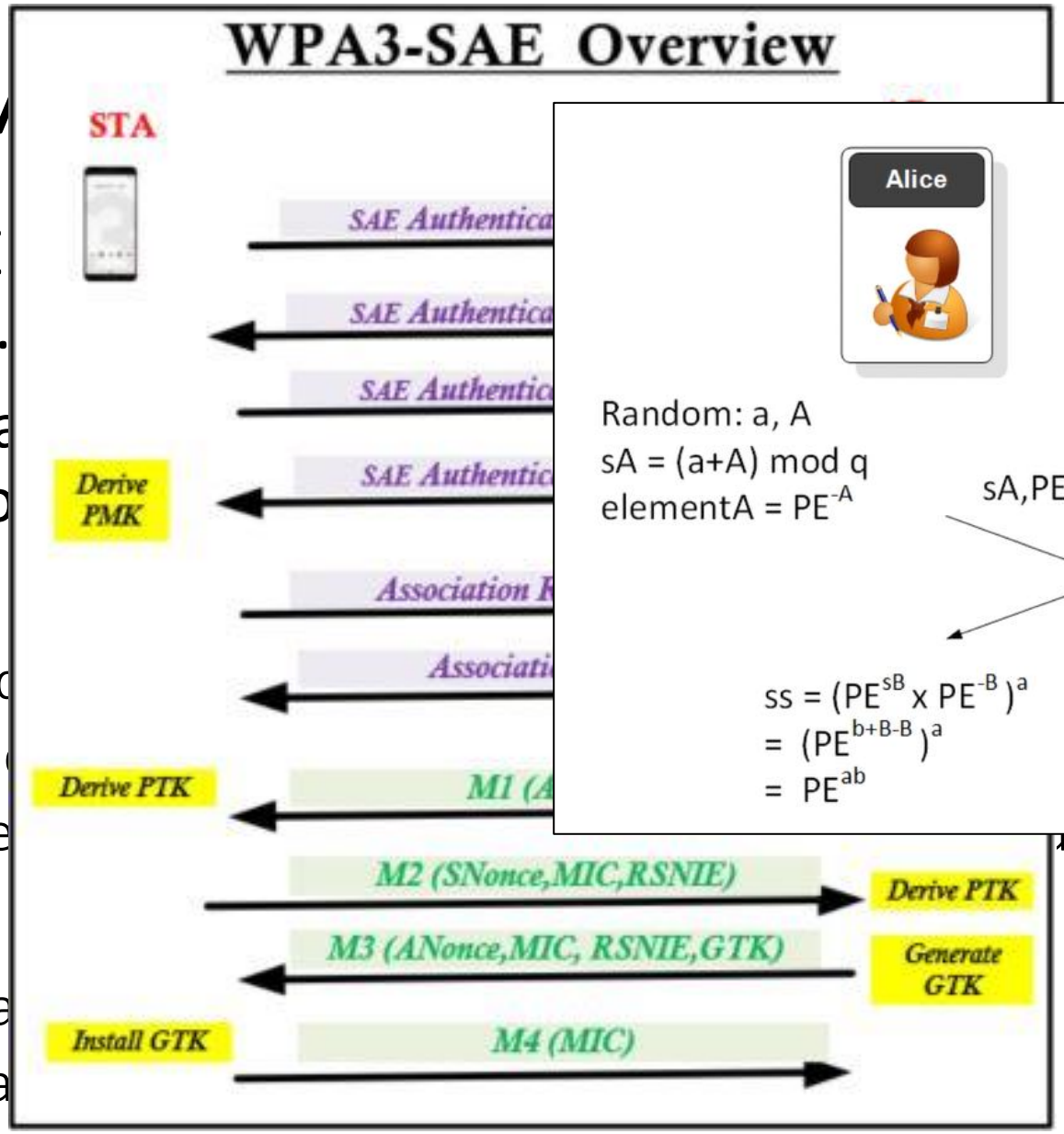
User and M

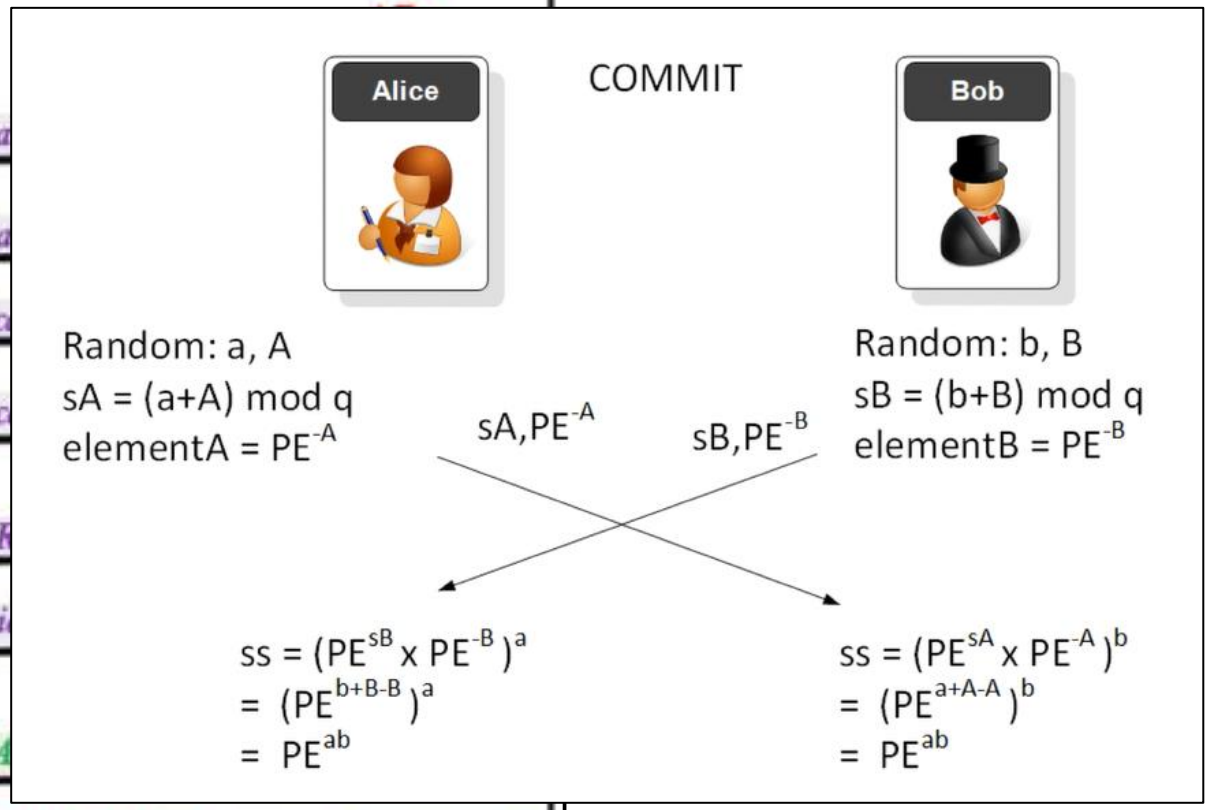
- WPA3 uses SAE ulnerable WPA2 Personal mode.
- SAE ensures tha dshake, they cannot brute-fo
- Process
  - Both client and nts.
  - Derive a share
  - Authenticate e d.
- Advantages
  - Provides forwa
  - Resistant to pa



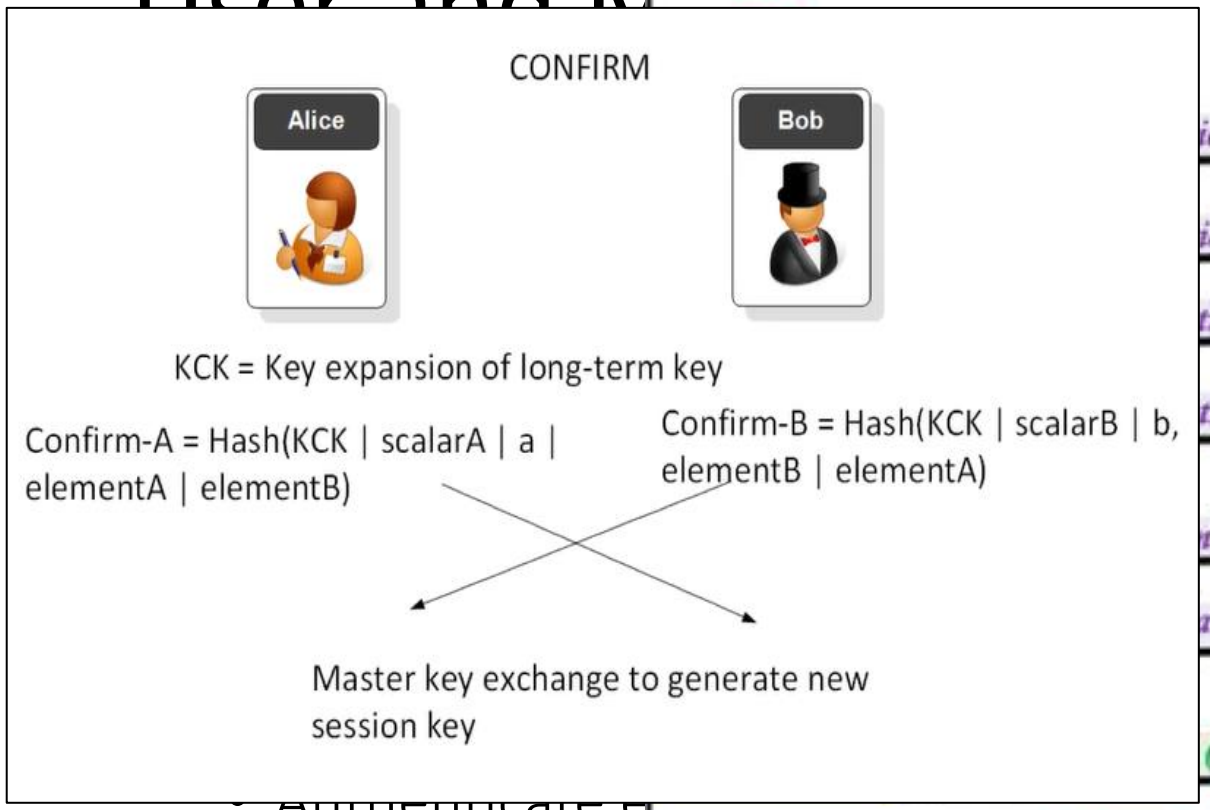
User and M

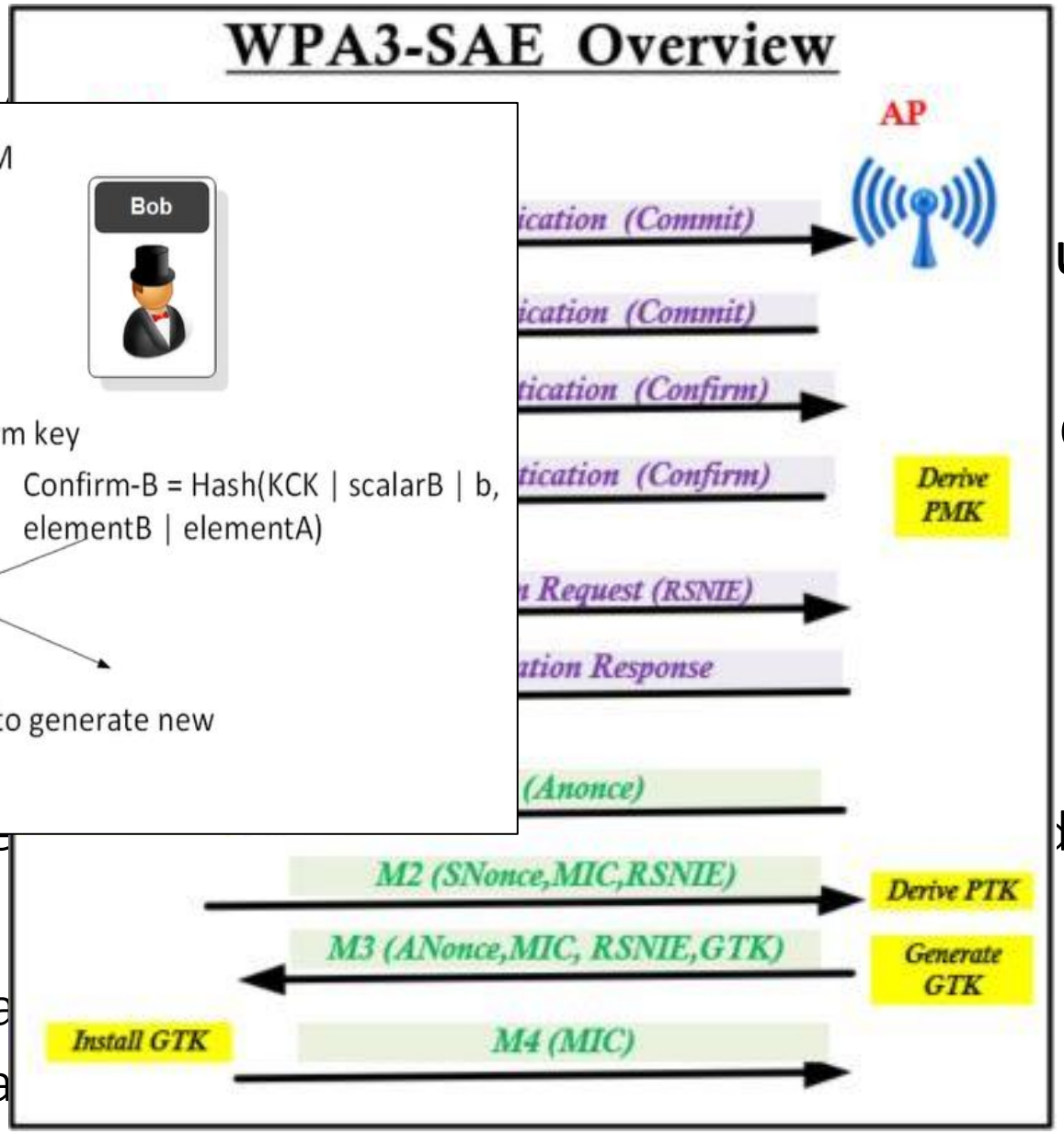
- WPA3 uses SAE
  Personal mode.
- SAE ensures tha
  cannot brute-fo
- Process
  - Both client and
  - Derive a share
  - Authenticate e
- Advantages
  - Provides forwa
  - Resistant to pa





User and M





ulnerable WPA2

dshake, they

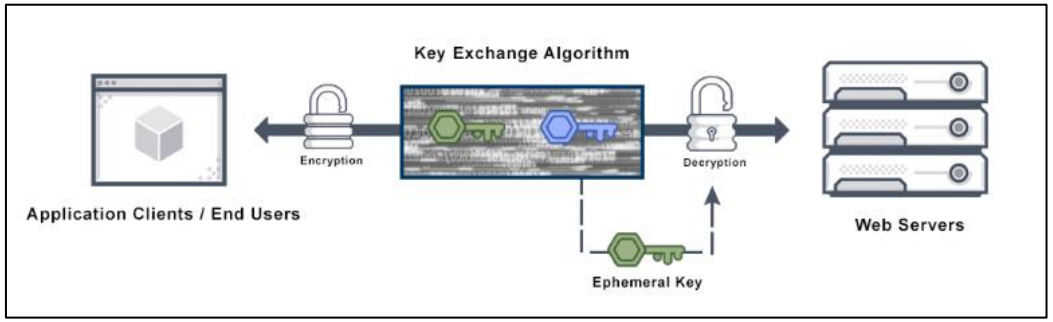
nts.

d.

- Authenticate e

- Advantages
  - Provides forwa
  - Resistant to pa

Confidentiality and Privacy



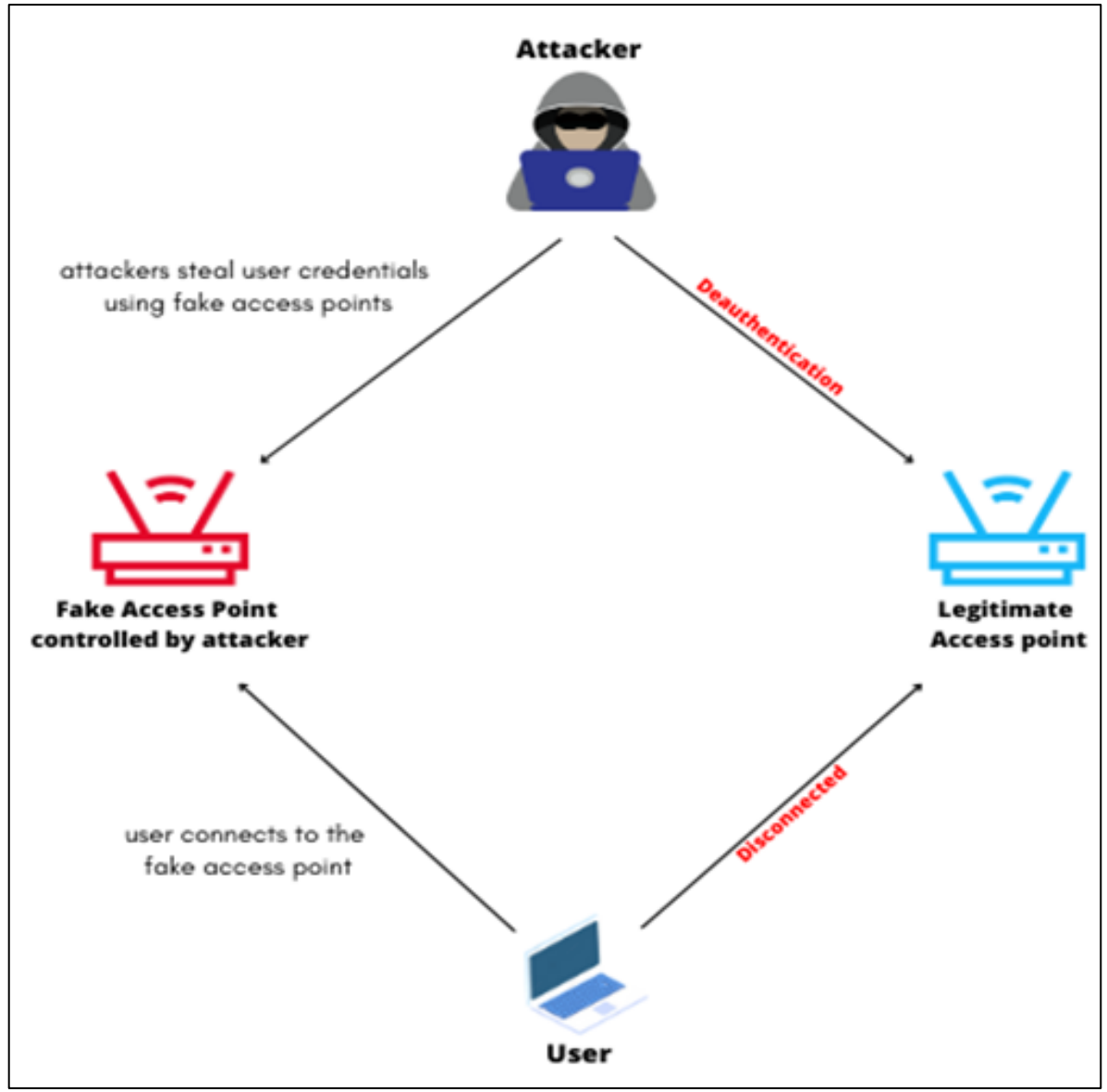
- Encryption Mechanisms
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
    - Utilizes AES-128 in WPA3-Personal.
    - Ensures data confidentiality and integrity.
  - GCM (Galois/Counter Mode):
    - Employs AES-256 in WPA3-Enterprise.
    - Provides higher security for sensitive enterprise environments.
  - Forward Secrecy
    - Ensures that the compromise of one session key does not affect past or future sessions.
    - Even if an attacker obtains the current session key, they cannot decrypt previously captured traffic.

Message Integrity

- WPA3 uses cryptographic hash functions to ensure that data has not been tampered with during transmission.
- It employs Message Integrity Code (MIC) to detect any modifications to the data.
- Cryptographic Hash Functions
  - WPA3 uses strong hash functions like SHA-384 to ensure data integrity.
  - These functions provide a unique fingerprint for the data, making it easy to detect any changes.
- Examples
  - An attacker tries to modify a message in transit. WPA3’s integrity checks detect the tampering and discard the message.

Access Control Mechanisms

- WPA3 introduces several enhancements to control access to the network.
- One key feature is Management Frame Protection (MFP), which protects against certain types of attacks.
- Role of MFP
  - MFP ensures that management frames (used for network control) are authenticated and protected.
  - It prevents attacks like rogue access points and denial-of-service attacks.
- **Scenario**: A company implements WPA3 with MFP. An attacker tries to set up a rogue access point, but MFP detects and prevents the attack.


Attacker
attackers steal user credentials
using fake access points
Deauthentication
Fake Access Point
controlled by attacker
Legitimate
Access point
user connects to the
fake access point
Disconnected
User

Key Components of WPA3

- TKIP (Temporal Key Integrity Protocol)
  - Limitations: TKIP was used in WPA1 and had several vulnerabilities, including weak encryption and susceptibility to replay attacks.
  - Deprecation: TKIP is no longer used in WPA3 due to its weaknesses.
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
  - CCMP is used in WPA3 for encryption and integrity. It provides strong encryption using AES-CCMP-256.
  - CCMP is resistant to attacks like replay attacks and provides robust data integrity.

Key Components of WPA3 (Cont’d)

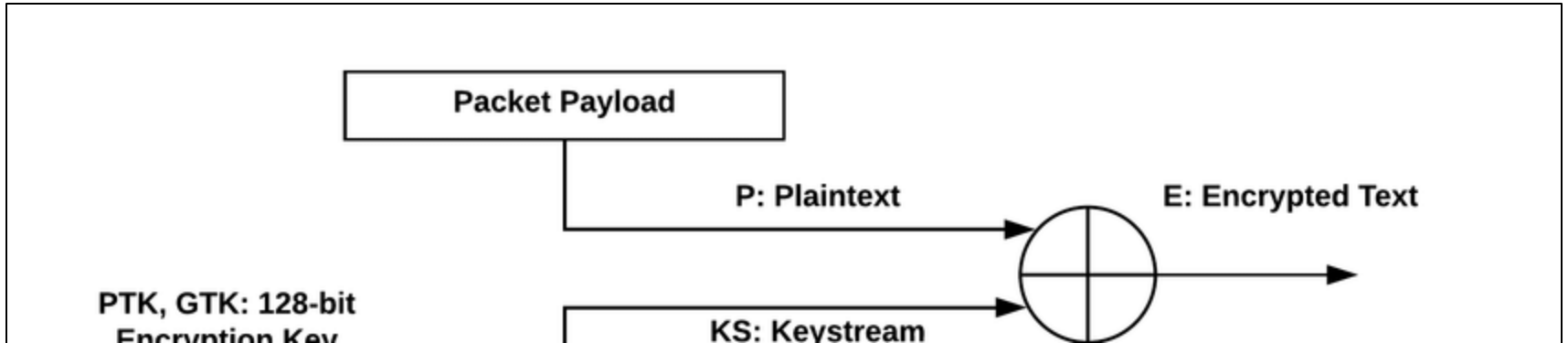
- PSK (Pre-Shared Key)
  - PSK is used in WPA3 for secure access. It is combined with SAE to provide secure key exchange.
  - PSK ensures that only authorized users can access the network.
- 802.1X/EAP (Extensible Authentication Protocol)
  - 802.1X/EAP is crucial in enterprise environments for secure authentication.
  - It allows for strong authentication mechanisms like certificates and multi-factor authentication.

Role of TKIP and RC4

- Historical Context
  - TKIP: Used in WPA1, it provided temporary security improvements over WEP but had significant vulnerabilities.
  - RC4: Used in WEP and early WPA, it was a stream cipher that was found to be insecure.
- Insecurity
  - TKIP: Vulnerable to replay attacks and weak encryption.
  - RC4: Known vulnerabilities like weak keys and susceptibility to statistical attacks.
- Exclusion in WPA3
  - WPA3 does not use TKIP or RC4 due to their weaknesses. It relies on stronger encryption algorithms like AES-CCMP-256.

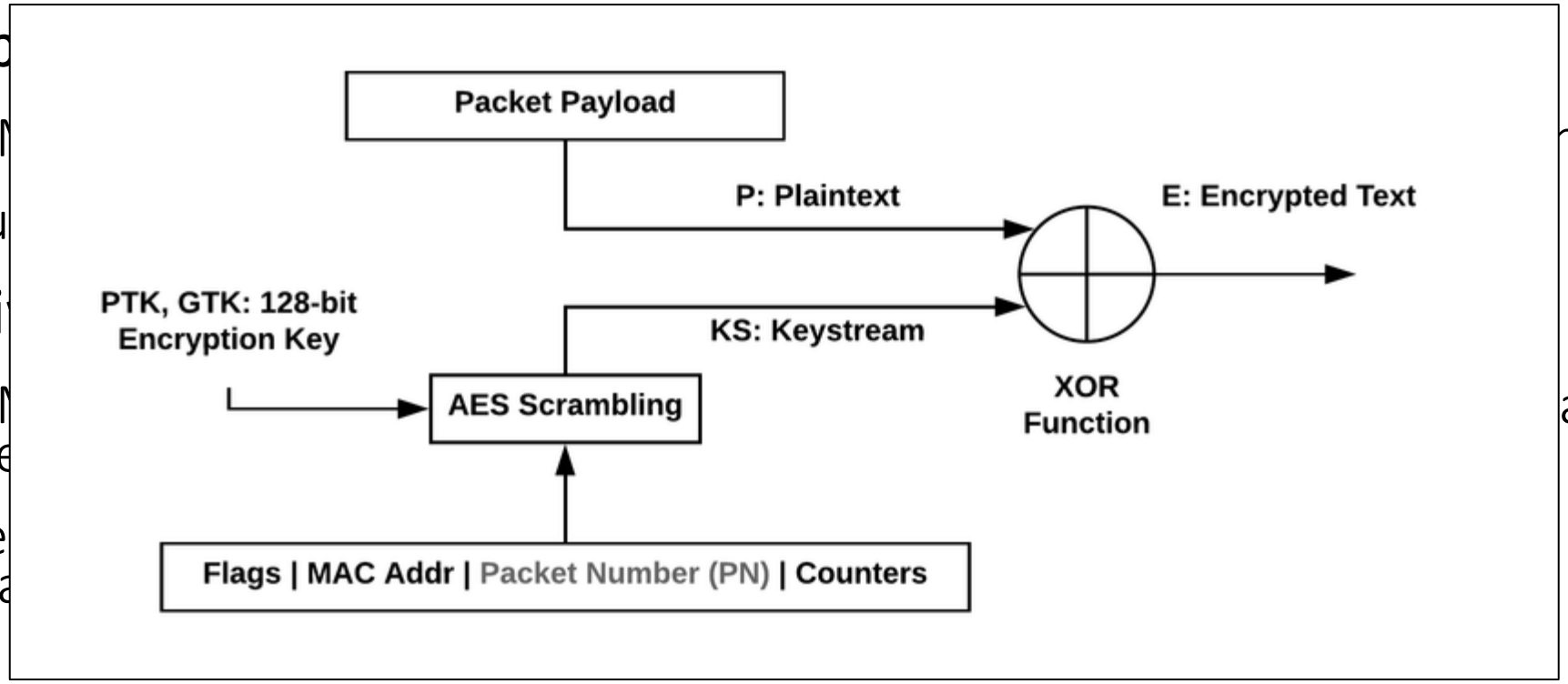
CCMP and Its Importance

- In-Depth Look at CCMP
  - CCMP is a key component of WPA3, providing robust encryption and integrity.
  - It uses AES-CCMP-256, which is a strong encryption algorithm.
- Effectiveness Against Attacks
  - CCMP is resistant to attacks like replay attacks and provides strong data integrity.
  - It ensures that data is encrypted and authenticated, making it difficult for attackers to intercept or modify.



CCMP and Its Importance

- In-Dep
  - CCM
  - It u
- Effecti
  - CCM
    inte
  - It e
    atta



ntegrity.

a

for

Real-World Application Scenarios

- Home Networks
  - WPA3 provides strong security for home networks, protecting against common threats like password cracking and data interception.
  - Example: A family uses WPA3 to secure their home Wi-Fi, ensuring that their personal data remains confidential.
- Corporate Networks
  - WPA3 is crucial in corporate environments, where sensitive data is transmitted over the network.
  - Example: A company uses WPA3 with 802.1X/EAP to ensure that only authorized employees can access the network.
- Potential Vulnerabilities
  - Without WPA3, networks are vulnerable to attacks like KRACK, which can compromise data integrity and confidentiality

Side-Channel Attacks

- Exploits physical implementations of cryptographic algorithms to extract secret information.
- The Dragonfly handshake in WPA3 is susceptible to cache-based and timing side-channel attacks, allowing attackers to recover passwords.
- Example: An attacker monitors the timing of operations during the handshake to infer password information.

Vanhoef, M., & Ronen, E. (2019). "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd

Downgrade Attacks

- Forces a system to revert to a less secure protocol version.
- Attackers can coerce WPA3-capable devices to fall back to WPA2, reintroducing previously mitigated vulnerabilities.
- A rogue access point tricks a client into connecting using WPA2 instead of WPA3.

Vanhoef, M., & Ronen, E. (2019). "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd

Denial-of-Service (DoS) Attacks

- Overwhelms a system to disrupt normal operation.
- Attackers can exploit the authentication process to cause excessive resource consumption, leading to service disruption.
- Repeatedly initiating handshake processes to exhaust the access point's resources.

Vanhoef, M., & Ronen, E. (2019). "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd

Authentication Bypass Vulnerabilities

- Allows unauthorized access by circumventing authentication mechanisms.
- Flaws in implementations like wpa_supplicant can be exploited to bypass authentication, leading to unauthorized network access.
- An attacker sets up a malicious access point that deceives clients into connecting without proper authentication.

Cybersecurity News. (2023). "New Wi-Fi Auth Bypass Flaw Exposes Home & Enterprise Attacks"

Formal Verification Challenges

- Ensuring the correctness of protocols through mathematical methods.
- The complexity of the Dragonfly handshake makes formal verification difficult, potentially leaving undiscovered vulnerabilities.
- Inadequate formal analysis leads to overlooked flaws in the handshake process.

Liu, C., et al. (2023). "Modeling and Verification of WPA3 Security Protocol Based on SPIN"

WPA3-PK Specific Vulnerabilities

- WPA3-PK uses public keys for authentication in open networks.
- Implementation flaws can lead to precomputation attacks, allowing attackers to recover passwords.
- An attacker precomputes possible password hashes to expedite brute-force attacks.

Vanhoef, M., & Robben, J. (2023). "A Security Analysis of WPA3-PK: Implementation and Precomputation Attacks"

Summary

Vulnerability Type	Description	Impact
Side-Channel Attacks	Exploits physical implementation leaks	Password recovery
Downgrade Attacks	Forces use of less secure protocols	Reintroduction of old vulnerabilities
Denial-of-Service Attacks	Overwhelms system resources	Service disruption
Authentication Bypass	Circumvents authentication mechanisms	Unauthorized network access
Formal Verification Gaps	Incomplete protocol analysis	Potential undiscovered vulnerabilities
WPA3-PK Implementation Flaws	Precomputation attacks due to flawed implementations	Password recovery in open networks

Mitigating Side-Channel Attacks

- Dragonshield
  - Enhances the Dragonfly handshake to resist side-channel attacks by introducing randomized elements and fixed iteration counts [1]
- Autoencoder-Based Noise Injection
  - Utilizes autoencoders to preprocess and inject noise into signal traces, mitigating correlation power analysis attacks. [2]
- Hamming-Distance Redistribution
  - Applies machine learning to redistribute Hamming distances, obscuring power consumption patterns. [3]

[1] Barai, Suvendu. (2022). An Approach to Reduce Side-Channel Timing Attack in Dragonfly Handshake of WPA3 for MODP Group. 10.5281/zenodo.7002349.
[2] "Implementation and Analysis of Side-Channel Attack Mitigation Based on Autoencoder“
[3] "Machine learning based side-channel-attack countermeasure with hamming-distance redistribution and its application on advanced encryption standard"

Comparison

Technique	Advantages	Limitations	Assumptions	Performance Metrics
Dragonshield	Low overhead; protocol-level solution	Requires protocol modification	Assumes compliant devices	Not specified
Autoencoder-Based Noise	Effective against power analysis	Computationally intensive	Assumes hardware support	Not specified
Hamming-Distance Redistribution	Obscures power patterns effectively	Requires machine learning training	Assumes stable environment	Not specified

Preventing Downgrade Attacks

1. Transition Disable
   - Prevents devices from falling back to WPA2 by disabling transition mode once WPA3 support is confirmed. *
2. SSID Inclusion in Handshake
   - Incorporates SSID into the 4-way handshake to prevent SSID confusion attacks.**
3. Adaptive Feature Selection and Thresholding (AFST-DA)
   - Employs machine learning to detect and prevent downgrade attacks in real-time.***

** Wi-Fi CERTIFIED WPA3™ December 2020 update brings new protections against active attacks: SAE Public Key and Transition Disable*

*** New Wi-Fi Vulnerability Enables Network Eavesdropping via Downgrade Attacks*

**** Tareef, Aya & Alabadleh, Ahmad & Alkasasbeh, Anas & Alghamdi, Mansoor. (2024). Enhancing Wi-Fi Security by Preventing Backward Compatibility Attacks on WPA3 Protocols. 10.21203/rs.3.rs-4830716/v1.*

Comparison

Technique	Advantages	Limitations	Assumptions	Performance Metrics
Transition Disable	Simple implementation; protocol-level	Requires updated firmware	Assumes updated devices	Not specified
SSID Inclusion in Handshake	Prevents SSID confusion	Requires standard modification	Assumes standard adoption	Not specified
AFST-DA	Real-time detection; adaptive	Requires training data	Assumes availability of labeled data	~99.8% accuracy

Addressing Denial-of-Service (DoS) Attacks

- Bad-Token Detection
  - Identifies and mitigates DoS attacks exploiting token validation mechanisms. *
- Intrusion Detection Systems (IDS)
  - Deploys IDS to monitor and respond to anomalous traffic patterns indicative of DoS attacks. **

* *Zulkernine, Mohammad. (2019). Bad-token: denial of service attacks on WPA3. SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks. 1-8. 10.1145/3357613.3357629.*

** *Halbouni, Asmaa & Ong, Lee-Yeng & Chew, Leow. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access. PP. 1-1. 10.1109/ACCESS.2023.3322931.*

Comparison

Technique	Advantages	Limitations	Assumptions	Performance Metrics
Bad-Token Detection	Targets specific DoS vectors	May not cover all attack types	Assumes known attack patterns	Not specified
IDS	Broad detection capabilities	Potential for false positives	Assumes well-configured IDS	Not specified

Enhancing Authentication Mechanisms

- SAE Public Key (SAE-PK)
  - Introduces public key cryptography to the SAE handshake, mitigating evil twin attacks.*
- ComPass Protocol
  - Replaces user-selected passphrases with automatically generated ones to prevent guessing attacks. **

* *Wi-Fi CERTIFIED WPA3™ December 2020 update brings new protections against active attacks: SAE Public Key and Transition Disable“*

** *Halbouni, Asmaa & Ong, Lee-Yeng & Chew, Leow. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access. PP. 1-1. 10.1109/ACCESS.2023.3322931.*

Formal Verification and Protocol Analysis

- SPIN Model Checking
  - Applies formal verification to model and analyze WPA3 protocols for potential vulnerabilities.
- Comparison

Technique	Advantages	Limitations	Assumptions	Performance Metrics
SPIN Model Checking	Systematic protocol analysis	May not capture all real-world scenarios	Assumes accurate modeling	Not specified

Halbouni, Asmaa & Ong, Lee-Yeng & Chew, Leow. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access. PP. 1-1. 10.1109/ACCESS.2023.3322931.

Summary of Techniques

Category	Techniques	Key Advantages	Notable Limitations
Side-Channel Mitigation	Dragonshield, Autoencoder, Hamming-Distance Redistribution	Enhanced resistance to side-channel attacks	Implementation complexity
Downgrade Attack Prevention	Transition Disable, SSID Inclusion, AFST-DA	Prevents fallback to insecure protocols	Requires standard updates
DoS Attack Mitigation	Bad-Token Detection, IDS	Detects and mitigates DoS attacks	Potential false positives
Authentication Enhancement	SAE-PK, ComPass Protocol	Strengthens authentication mechanisms	User adoption challenges
Formal Verification	SPIN Model Checking	Identifies protocol vulnerabilities	Modeling limitations

Open Challenges in WPA3

Persistent Side-Channel Vulnerabilities

- Despite mitigations, WPA3's Simultaneous Authentication of Equals (SAE) handshake remains susceptible to side-channel attacks.
  - The Dragonblood vulnerabilities exploit timing and cache-based side channels in the SAE handshake, enabling password partitioning attacks.
  - Recent studies, such as "Dragonblood is Still Leaking," demonstrate that these vulnerabilities persist in implementations like iwd and FreeRADIUS. *
- Implications
  - Attackers can recover passwords with fewer measurements, reducing the effort required for successful attacks.
  - The continued presence of these vulnerabilities indicates that current mitigations are insufficient.

* *de Almeida Braga, Daniel, Pierre-Alain Fouque, and Mohamed Sabt. "Dragonblood is still leaking: Practical cache-based side-channel in the wild." Proceedings of the 36th Annual Computer Security Applications Conference. 2020.*

User-Centric Threats and Social Engineering

- Human factors remain a critical vulnerability, with attackers leveraging social engineering to bypass WPA3 protections. *
- Researchers demonstrated that users could be tricked into connecting to rogue WPA3 networks with captive portals, capturing their credentials
- Implications
  - Technical safeguards are insufficient if users can be deceived into compromising actions.
  - There's a need for enhanced user education and interface designs that minimize the risk of social engineering attacks.

* *Chadee, Kyle, Wayne Goodridge, and Koffka 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).*

Implementation Inconsistencies Across Devices

- Variations in WPA3 implementations lead to inconsistent security levels and potential vulnerabilities.
  - Studies have found that some devices do not properly implement PMF, leaving them open to attacks.
  - Others fail to adhere strictly to the SAE handshake specifications, introducing exploitable flaws.
- Implications
  - The lack of uniformity in implementations undermines the overall security promised by WPA3.
  - There's a pressing need for rigorous certification processes and compliance testing

Gaps in Formal Verification

- The complexity of WPA3's protocols poses challenges for formal verification, leaving potential vulnerabilities undiscovered.
  - While efforts like the "Dragonstar" project aim to formally verify the Dragonfly handshake, the process is intricate and not yet comprehensive. *
  - Without complete formal verification, subtle flaws may persist unnoticed.
- Implications
  - Incomplete verification can lead to a false sense of security.
  - Investing in formal methods is essential to uncover and address deep-seated protocol issues.

* *Braga, Daniel De Almeida, et al. "From dragondoom to dragonstar: Side-channel attacks and formally verified implementation of WPA3 dragonfly handshake." 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P). IEEE, 2023.*

Summary of Open Challenges

Challenge	Description	Implications
Side-Channel Vulnerabilities	Persistent flaws in SAE handshake exploitable via timing and cache attacks	Risk of password compromise despite mitigations
Downgrade Attacks	Exploitation of transition mode to force WPA2 connections	Exposure to known WPA2 vulnerabilities
Social Engineering Threats	Users deceived into connecting to rogue networks	Credential theft bypassing technical safeguards
Implementation Inconsistencies	Variations in device adherence to WPA3 standards	Uneven security landscape across devices
Formal Verification Gaps	Incomplete analysis of complex protocols	Potential undiscovered vulnerabilities

Implementation

Attack 1 - Evil Portal (Captive Portal Phishing)

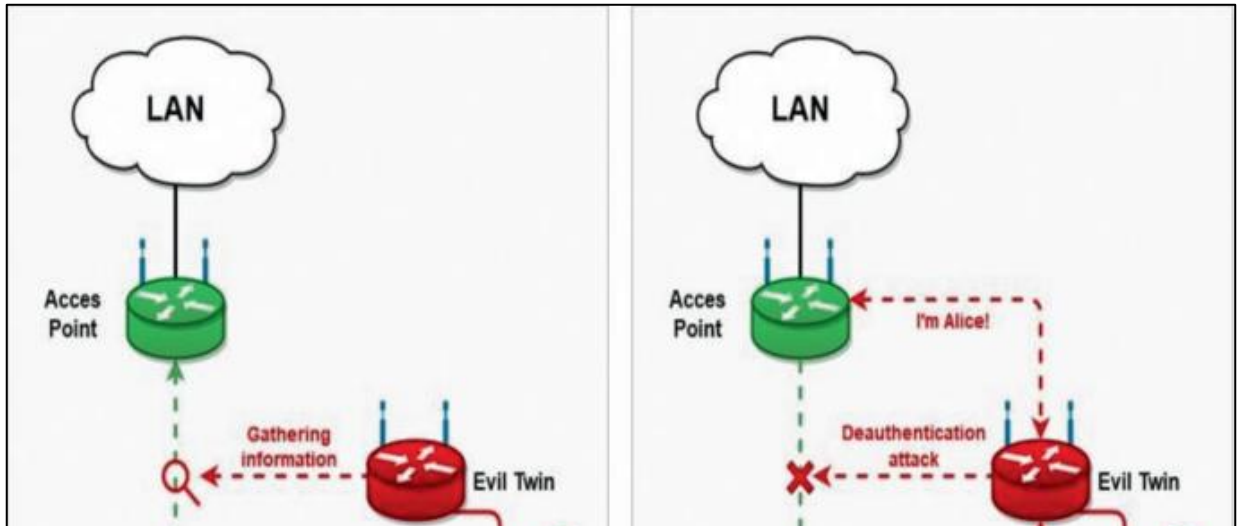
Tools and Environment Setup

- **Hardware:** Flipper Zero with Wi-Fi Development Board.
- **Software:** Hashcat for password cracking.
- **Network:** Personal Wi-Fi router configured for testing.

Note: *Ensure compliance with ethical guidelines; unauthorized access to networks is illegal.*

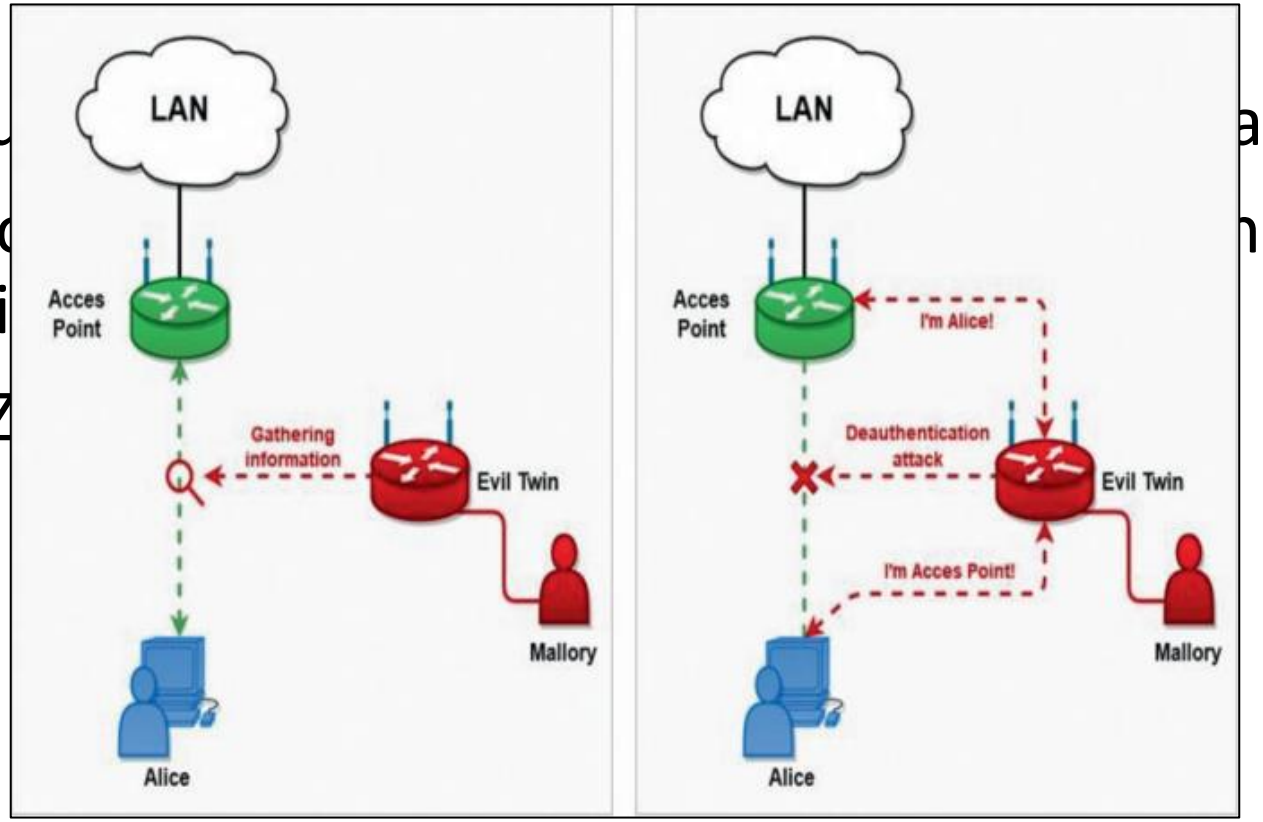
Attack 1 – Evil Portal (Captive Portal Phishing)

- Creates a rogue Wi-Fi access point mimicking a legitimate network.
- When users connect, they are redirected to a fake login page, capturing their credentials.
- **Tool:** Flipper Zero's Evil Portal application.



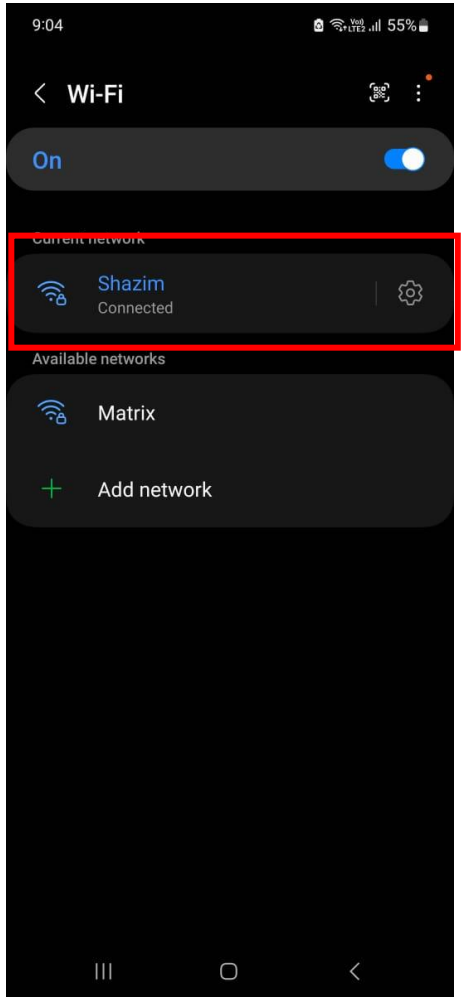
Attack 1 – Evil Portal (Captive Portal Phishing)

- Creates a rogu ate network.
- When users co n page, capturing thei
- **Tool:** Flipper Z

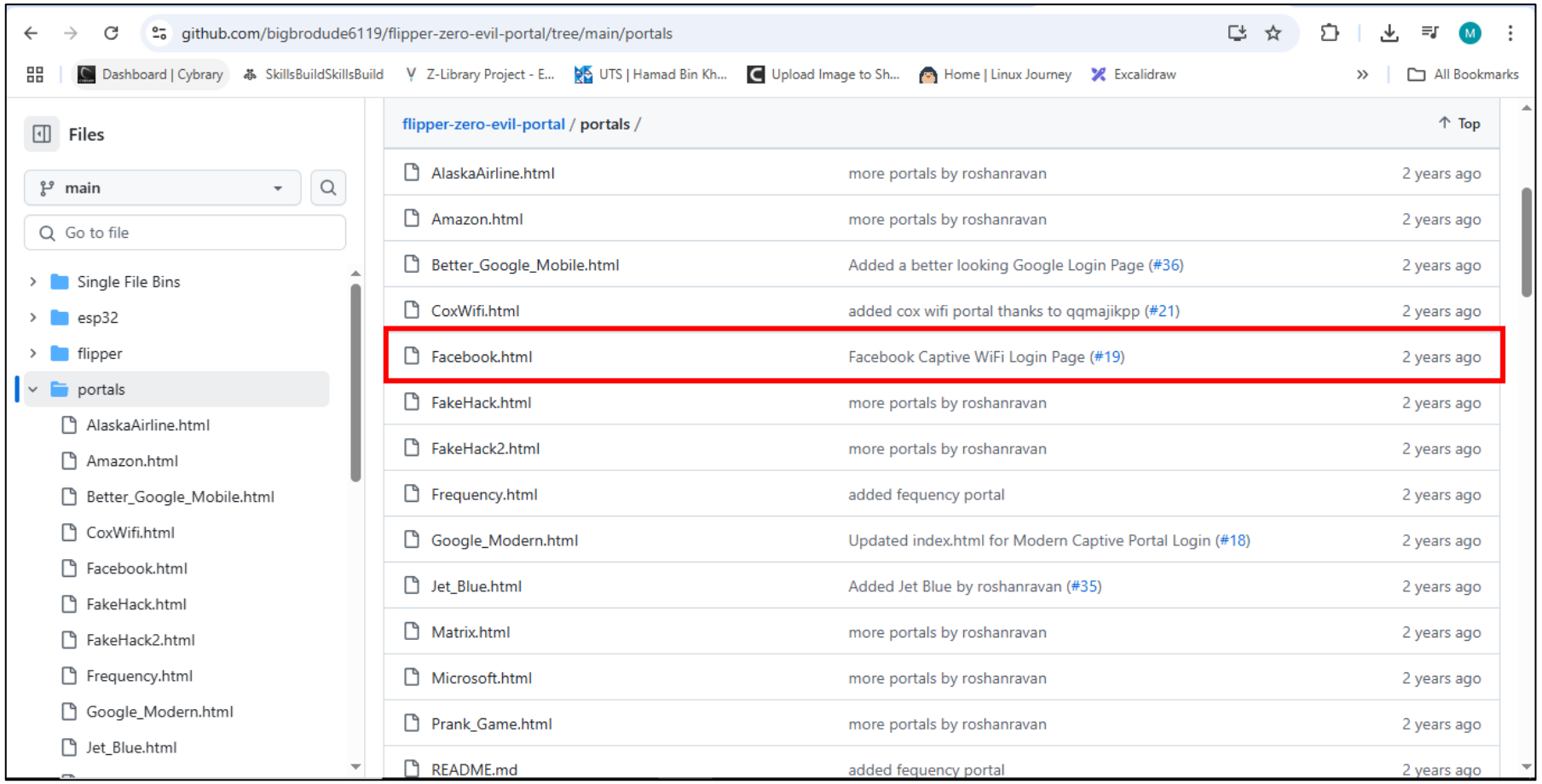


Demonstration

1) Mobile Device Connected to **Legitimate** Wi-Fi Network



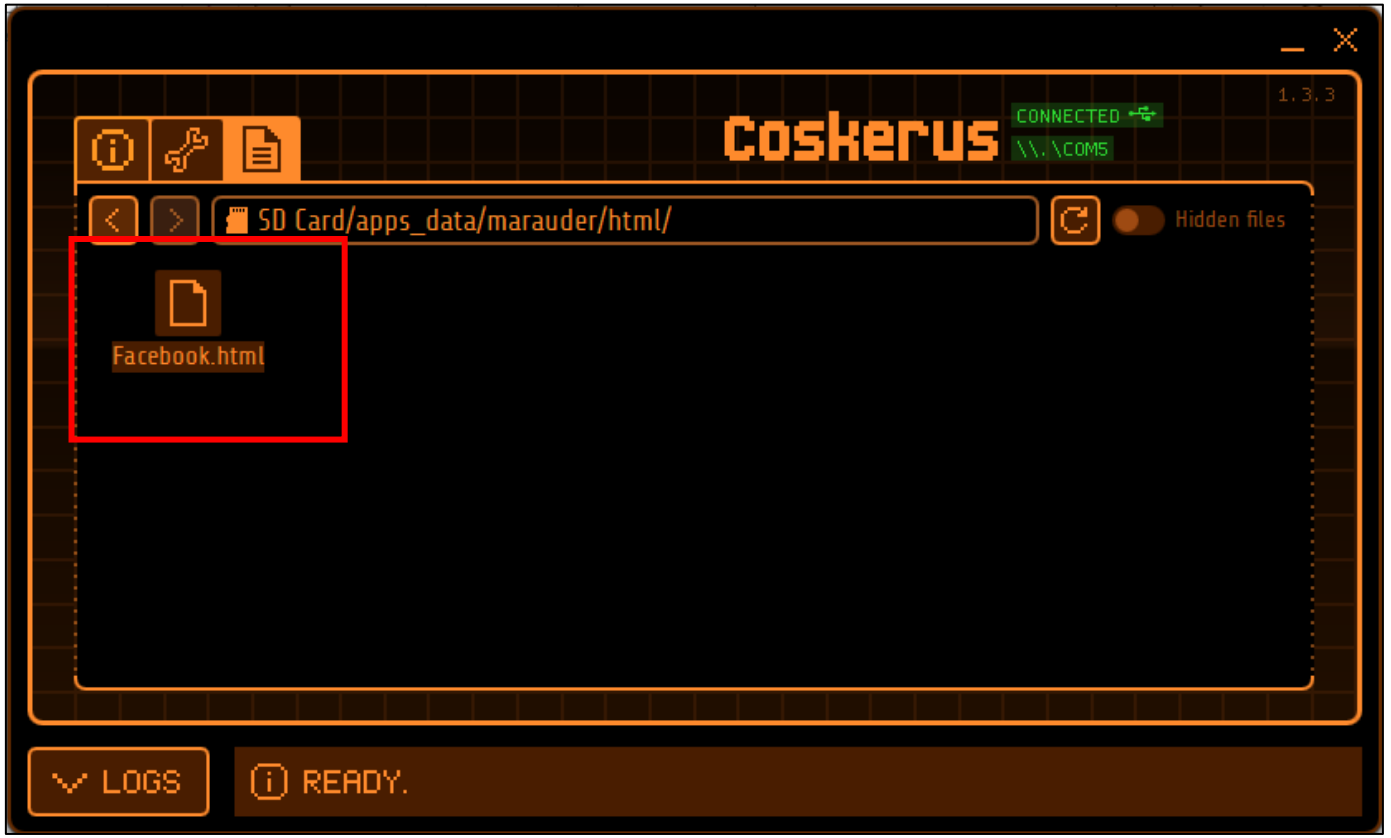
2) Downloading Fake Facebook page from GitHub



Demonstration

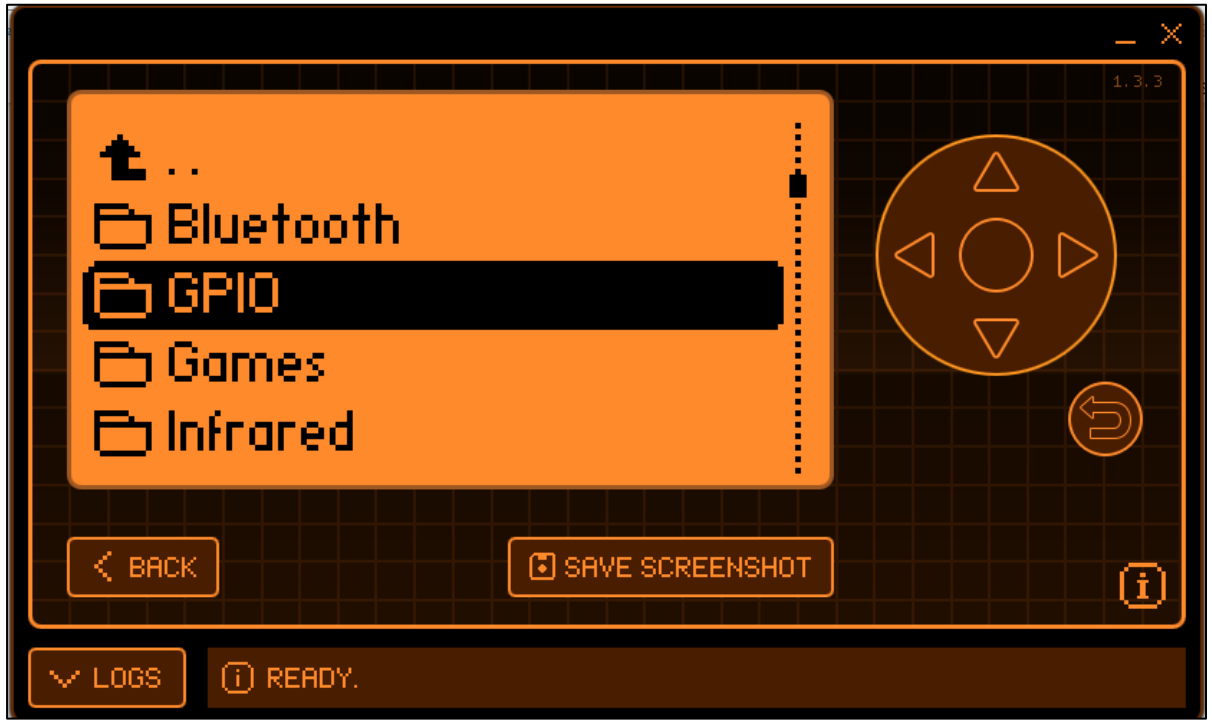
3) Device connected to Laptop for easier Display

4) Uploading the fake page to flipper zero



Demonstration

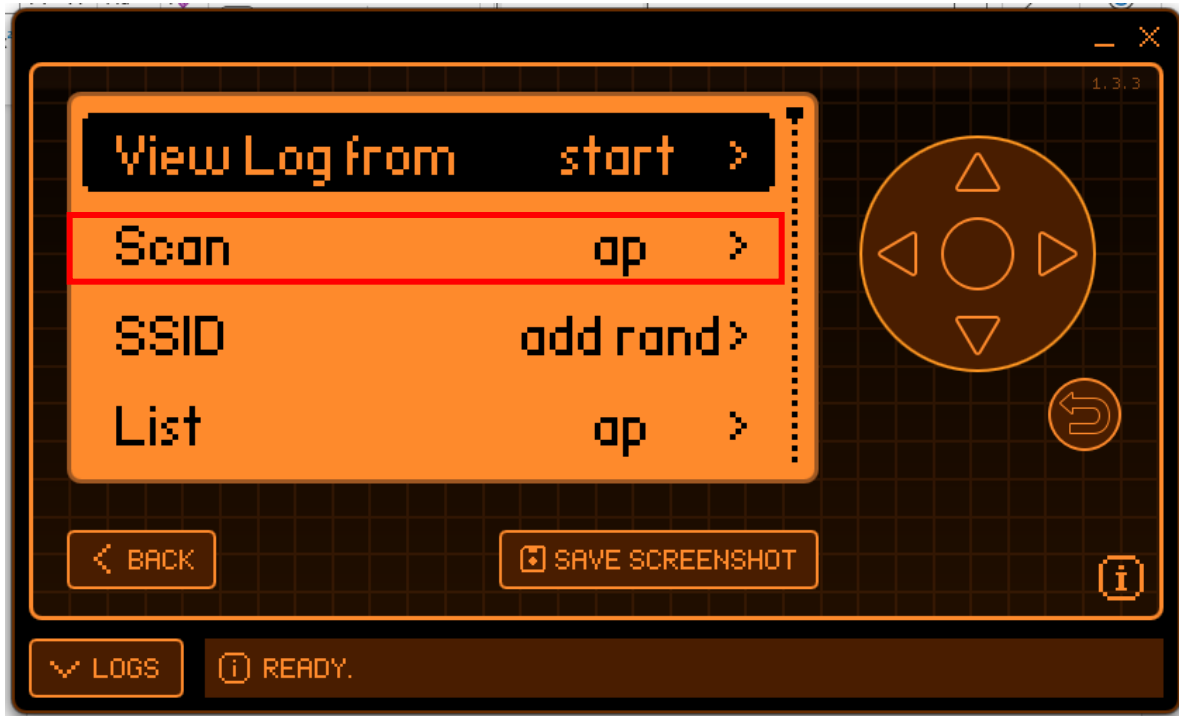
5) Flipper Zero Navigation

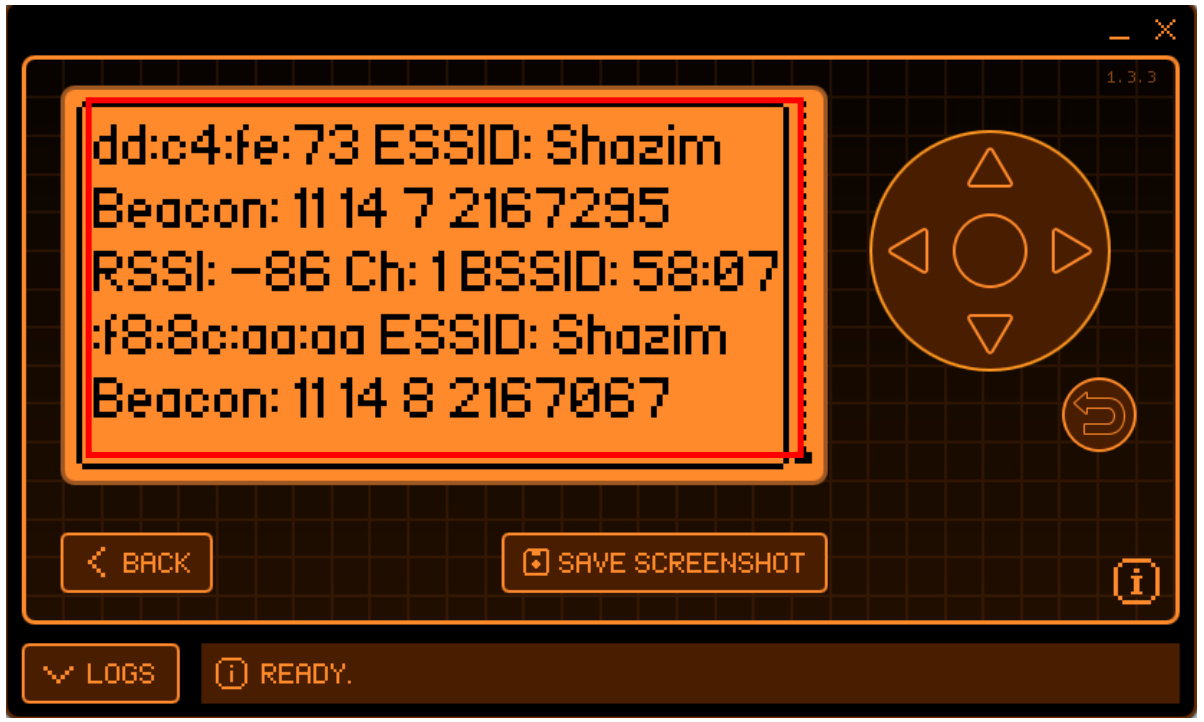


6) [ESP-32] Wi-Fi Maruder

Demonstration

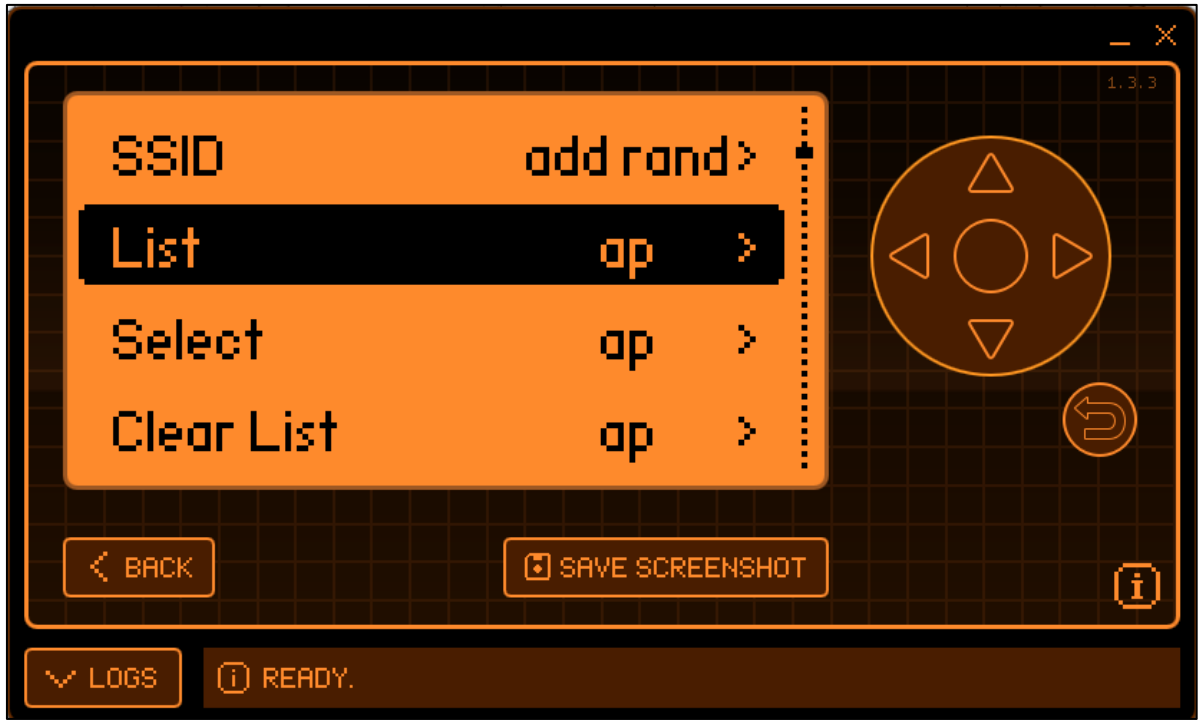
7) Scanning Access Points

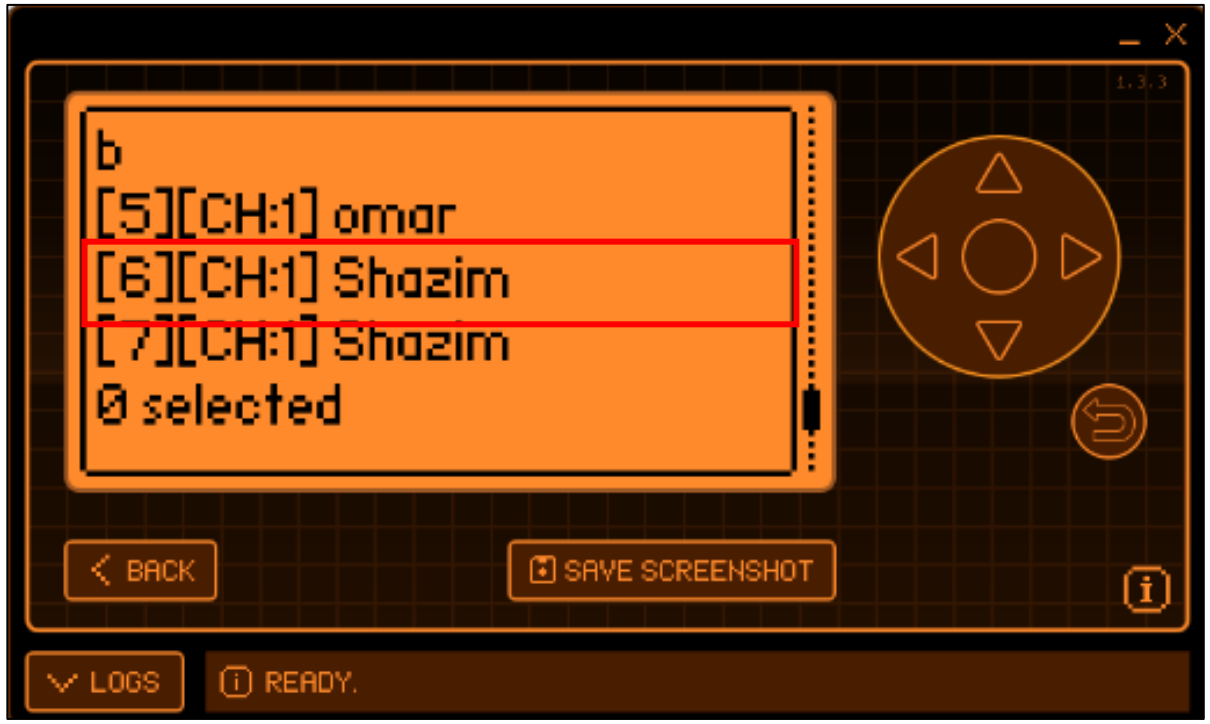




Demonstration

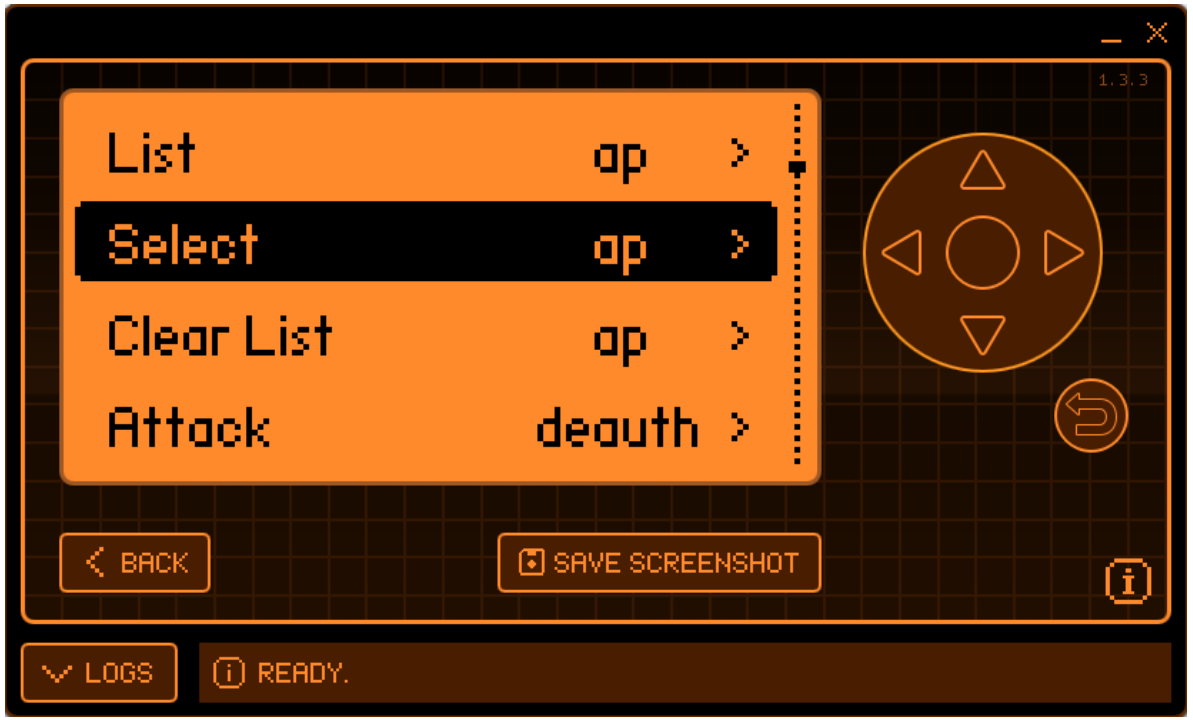
7) Selecting the right Access Point





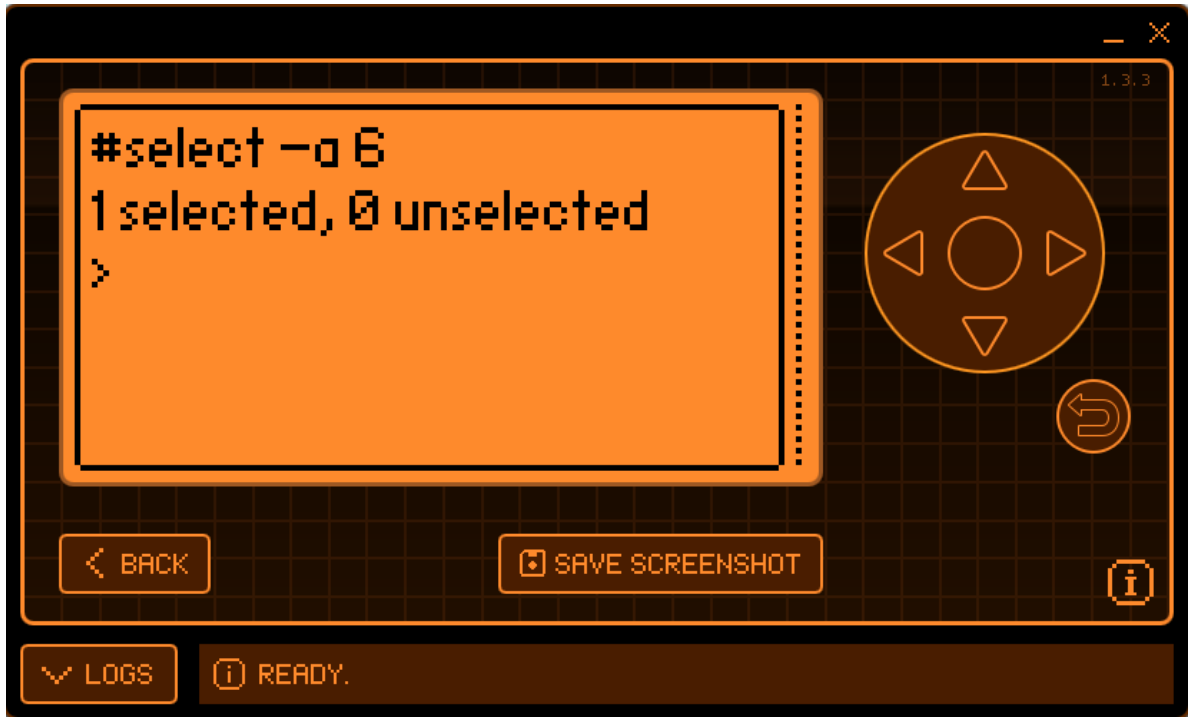
Demonstration

7) Selecting the right Access Point

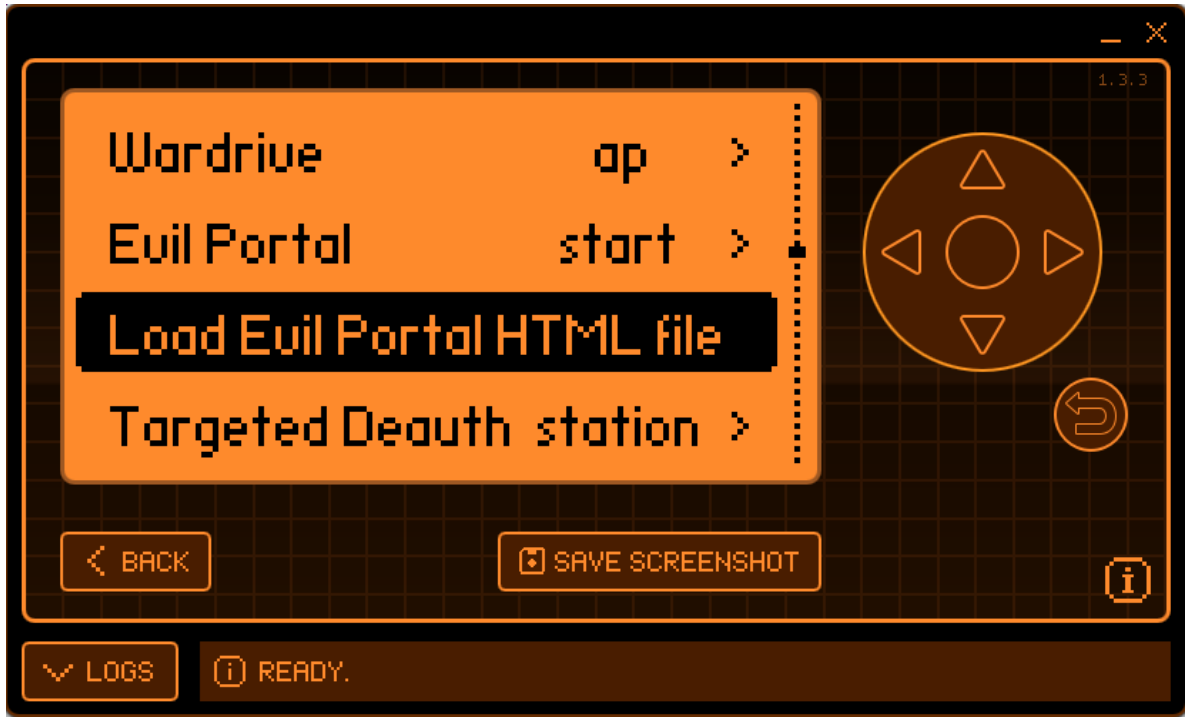


Demonstration

7) Selecting the right Access Point

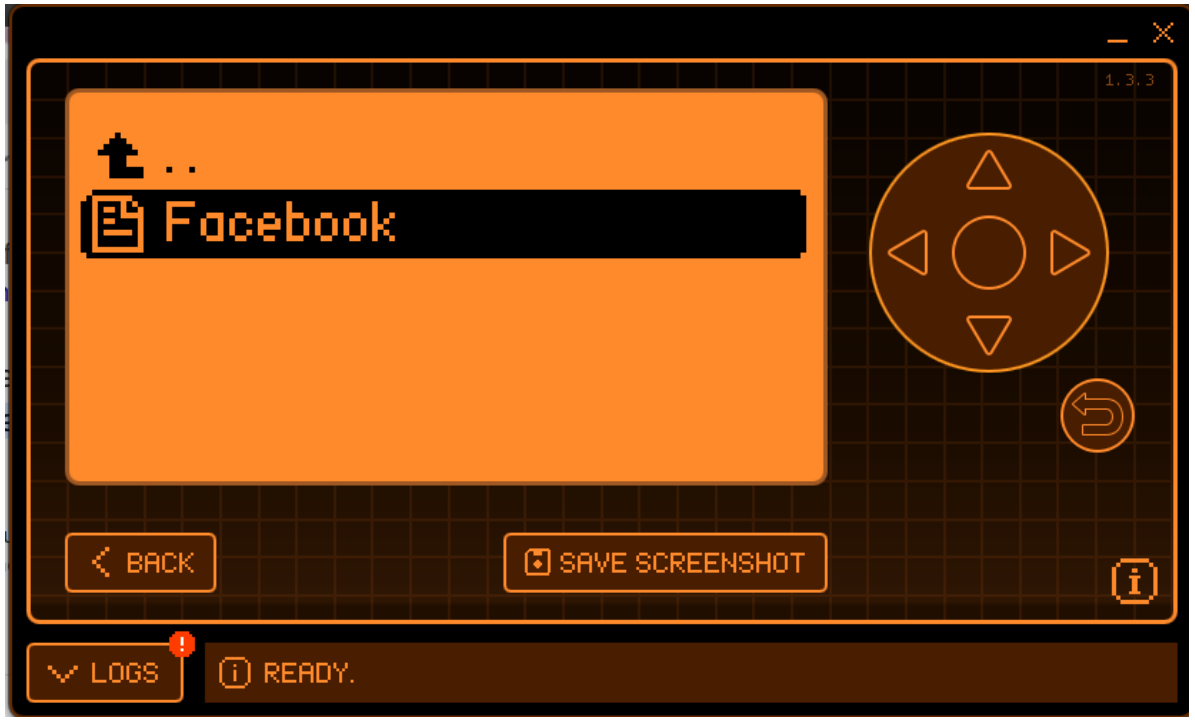


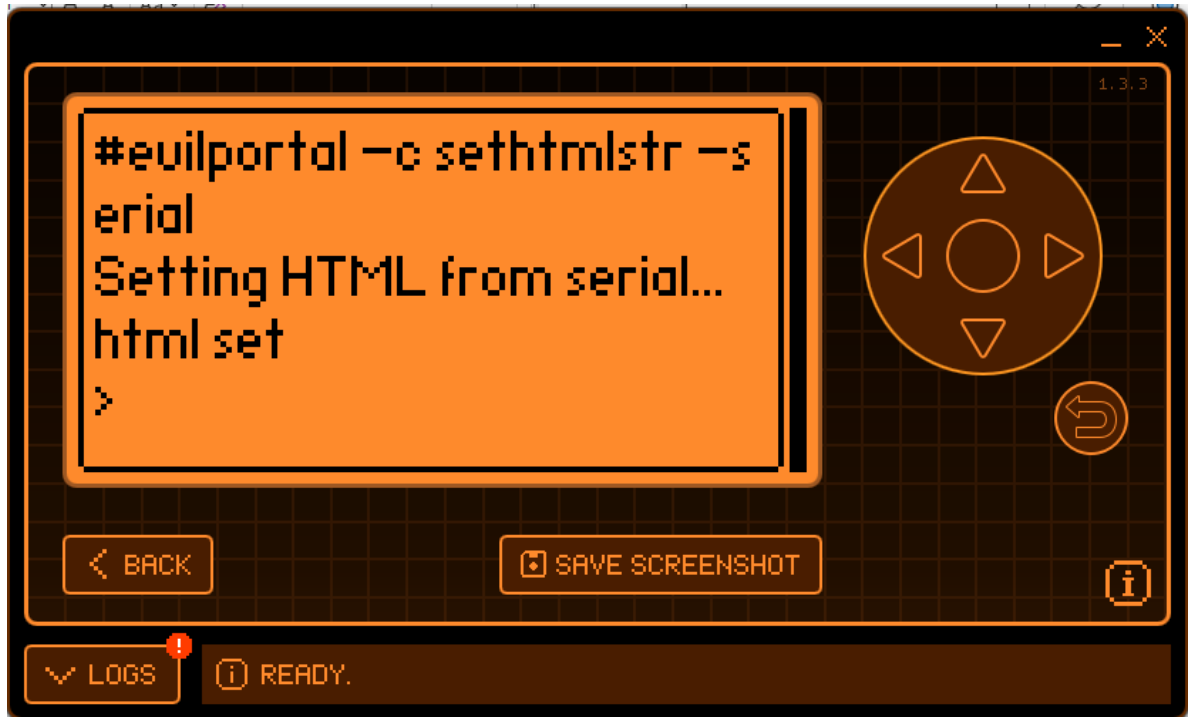
8) Loading Evil Portal HTML file we Just downloaded



Demonstration

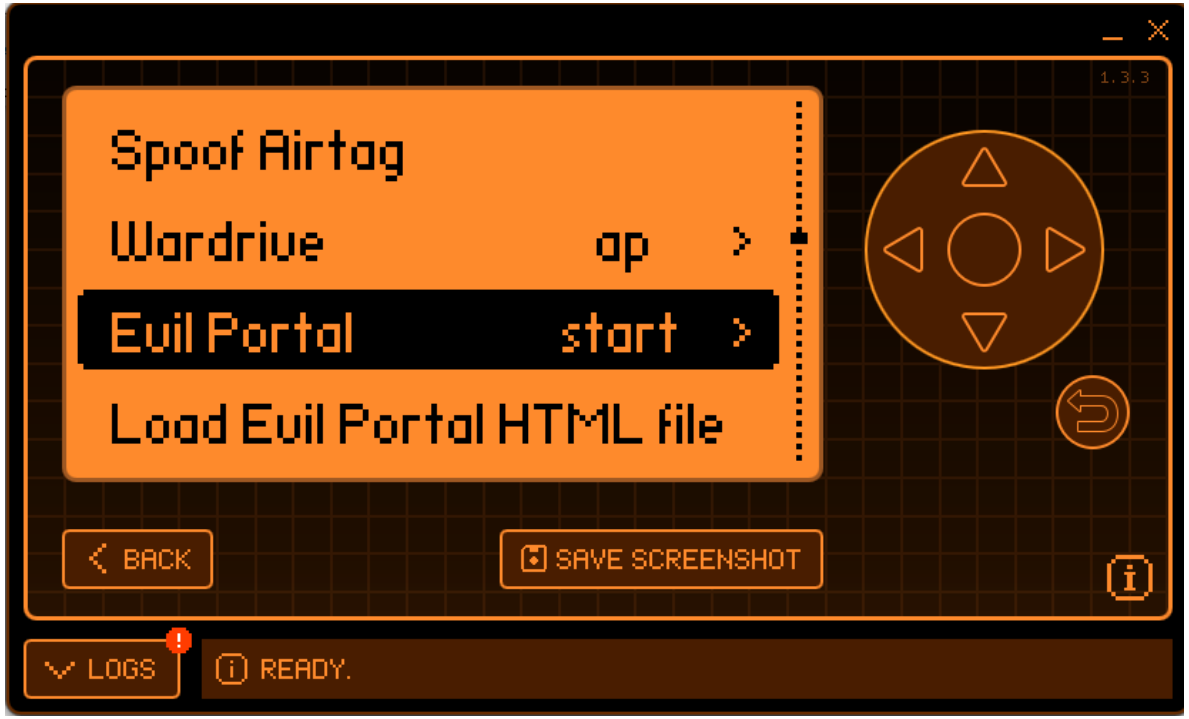
8) Loading Evil Portal HTML file we Just downloaded



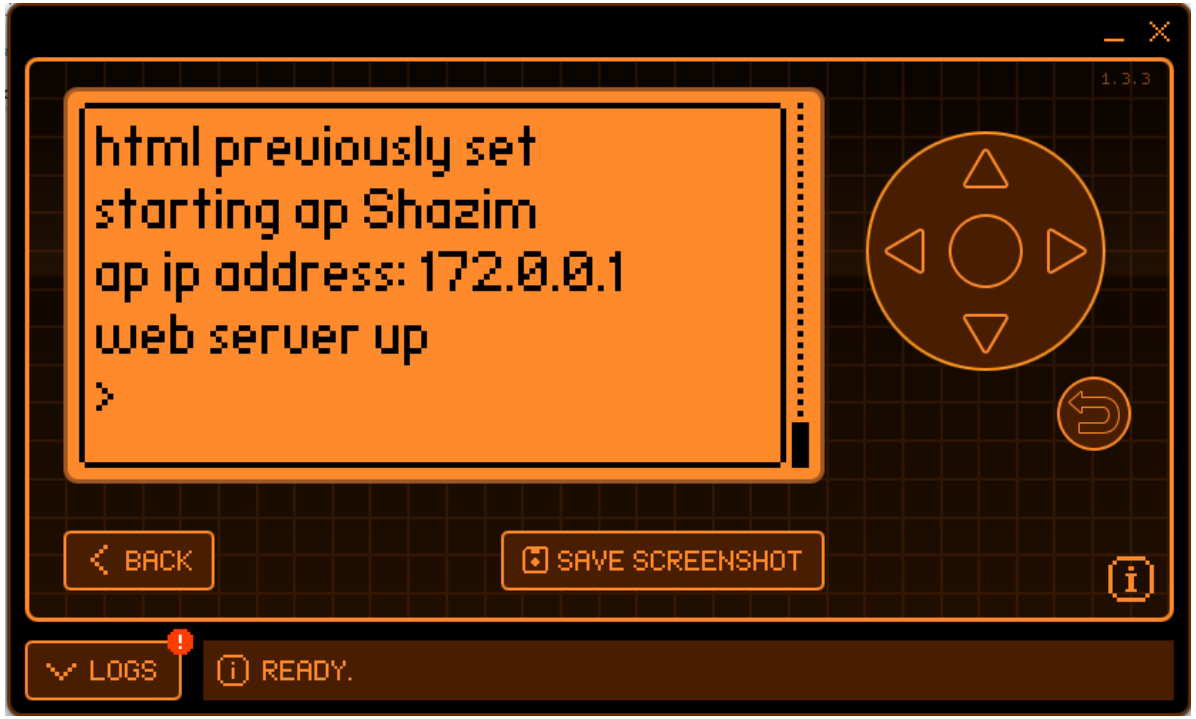


Demonstration

9) Loading Evil Portal

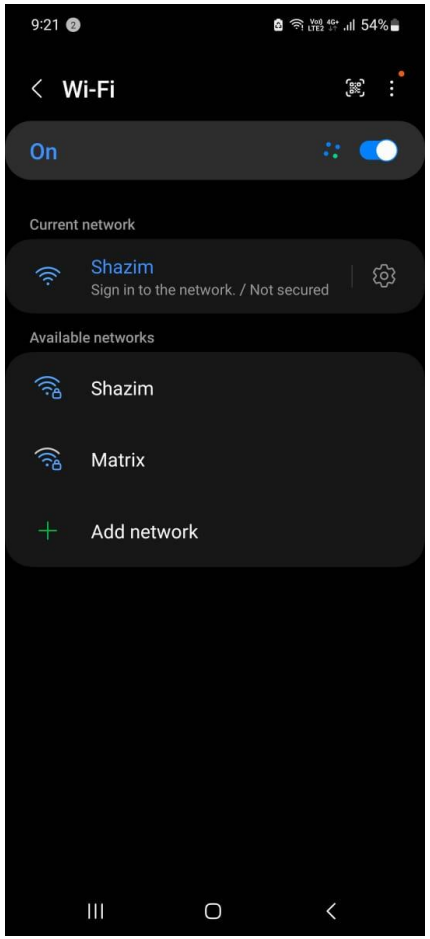


10) Evil Portal Set-up

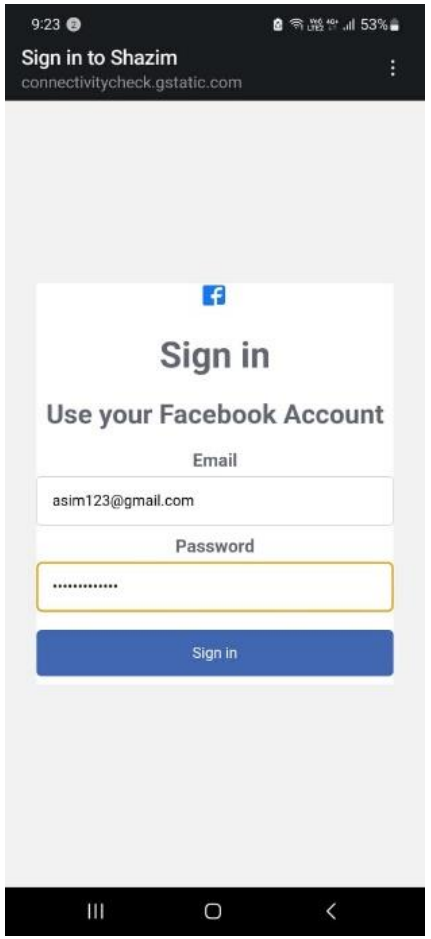


Demonstration

11) Fake Network



12) Fake Facebook Page – User enters his credentials



13) Credential captured by adversary

Evil Portal – Analysis

- Lack of authentication for Wi-Fi access points; users cannot distinguish between legitimate and rogue Aps
- Affected Protocols: WEP, WPA, WPA2.
- Potential for widespread credential theft through social engineering.
- User education, implementation of HTTPS, and network authentication mechanisms.

Implementation

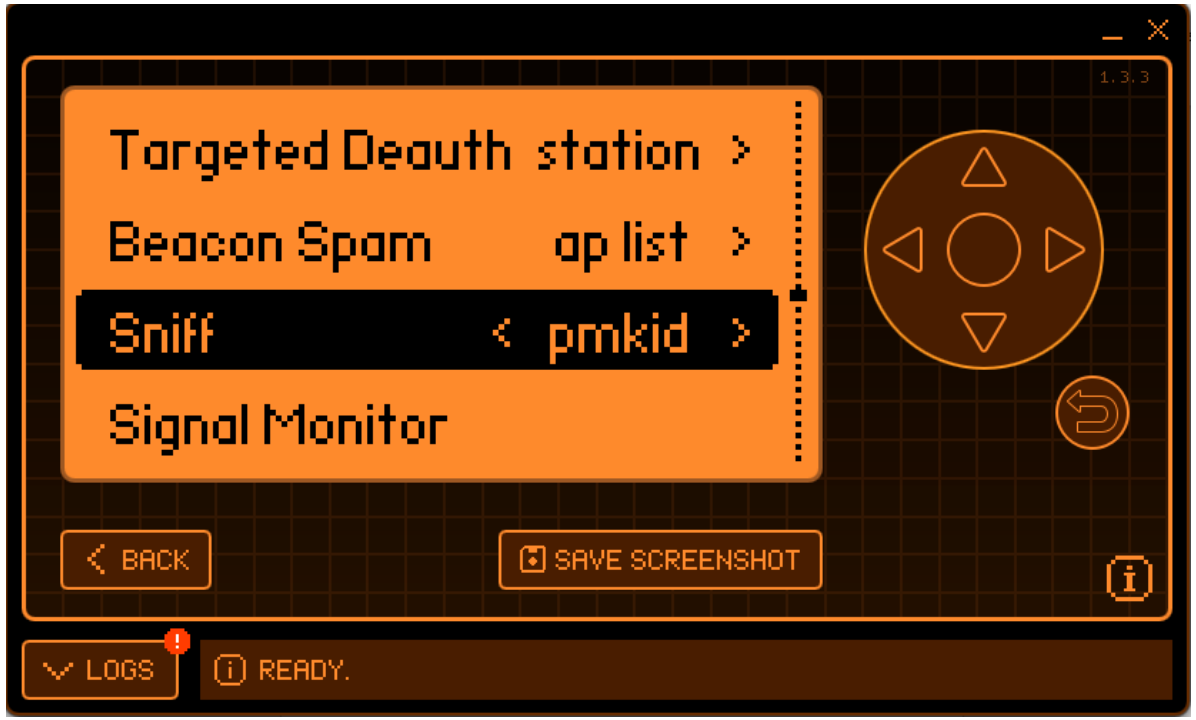
Attack 2 – PMKID Based WPA2 Password Cracking

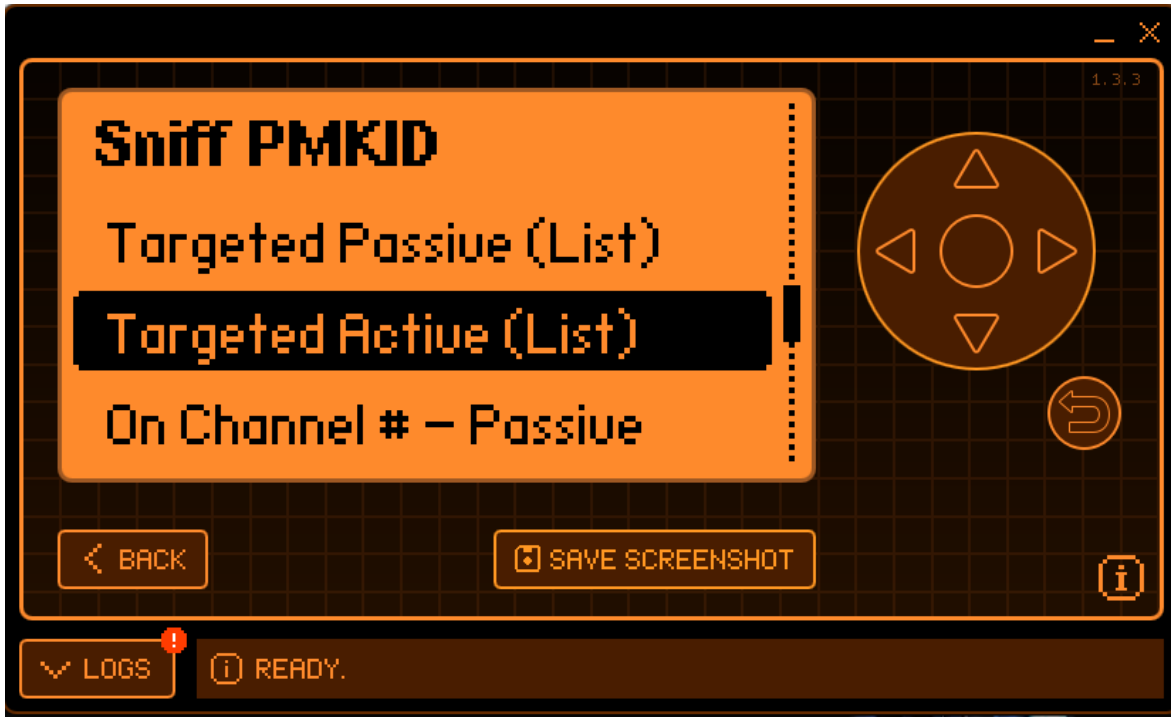
Attack 2 – PMKID-Based WPA2 Password Cracking

- Extracts the PMKID from a WPA2 handshake to perform offline password cracking.
- Captures PMKID without requiring client deauthentication.
- Flipper Zero for PMKID capture, Hashcat for password cracking.

PMKID Attack – Demonstration

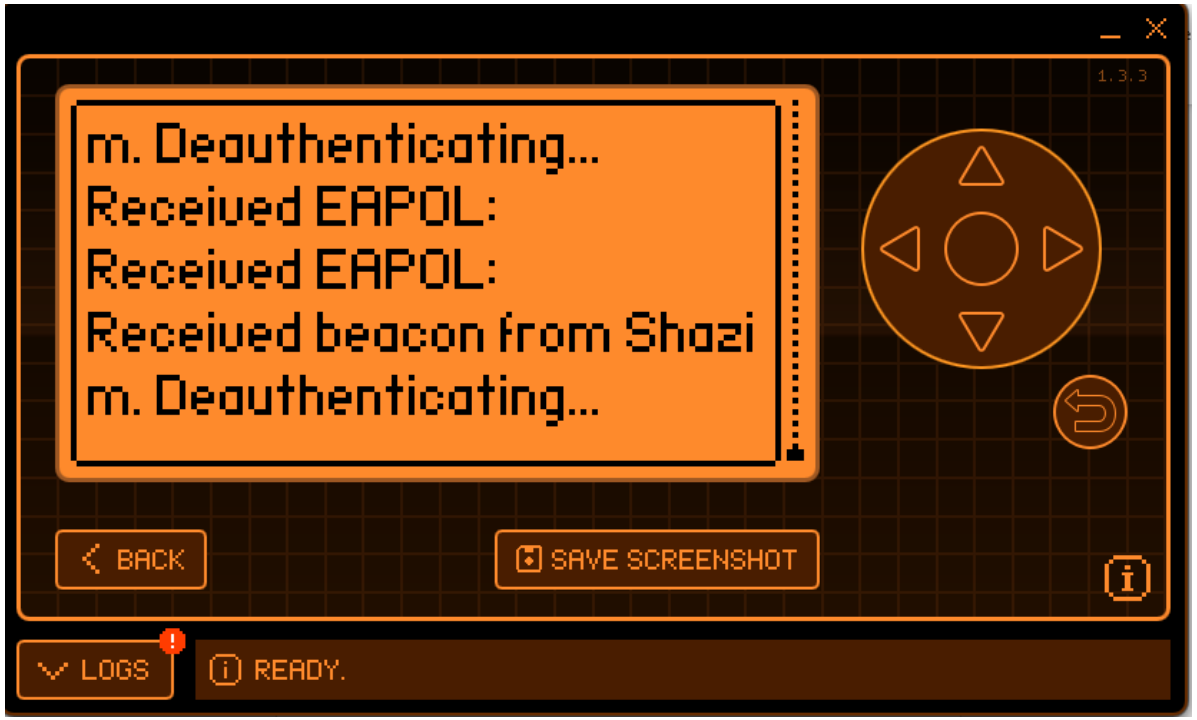
1) Sniffing PMKID



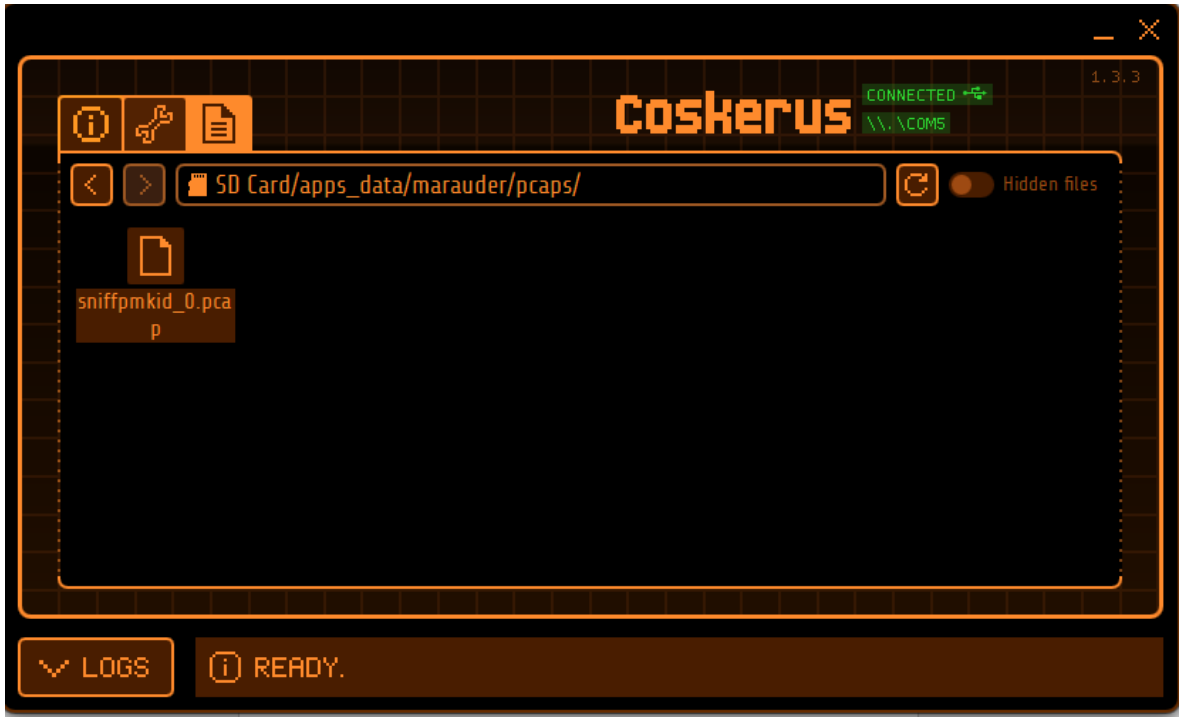


PMKID Attack – Demonstration

2) Capturing 4-way handshake

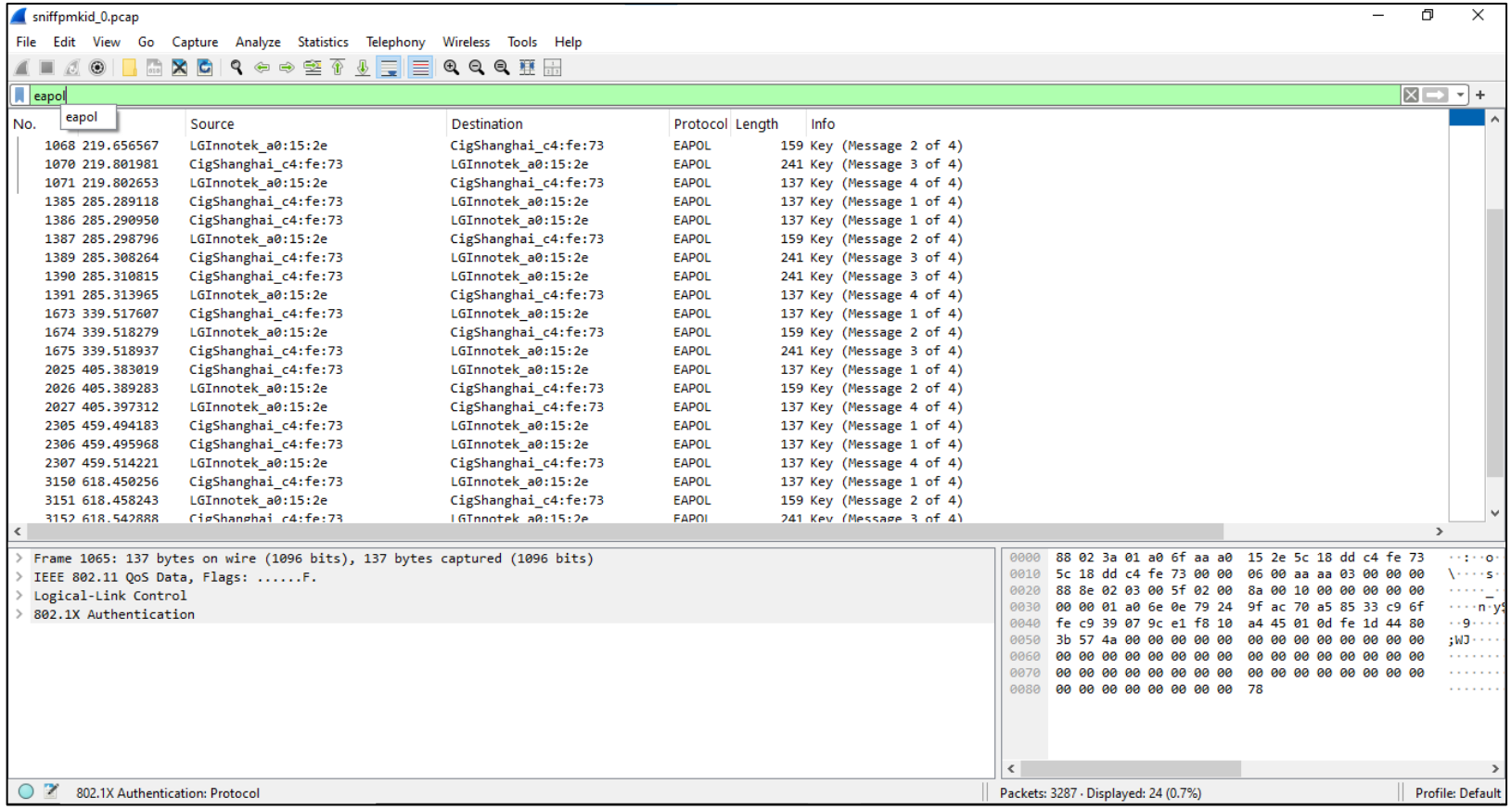


3) Handshake saved as pcap

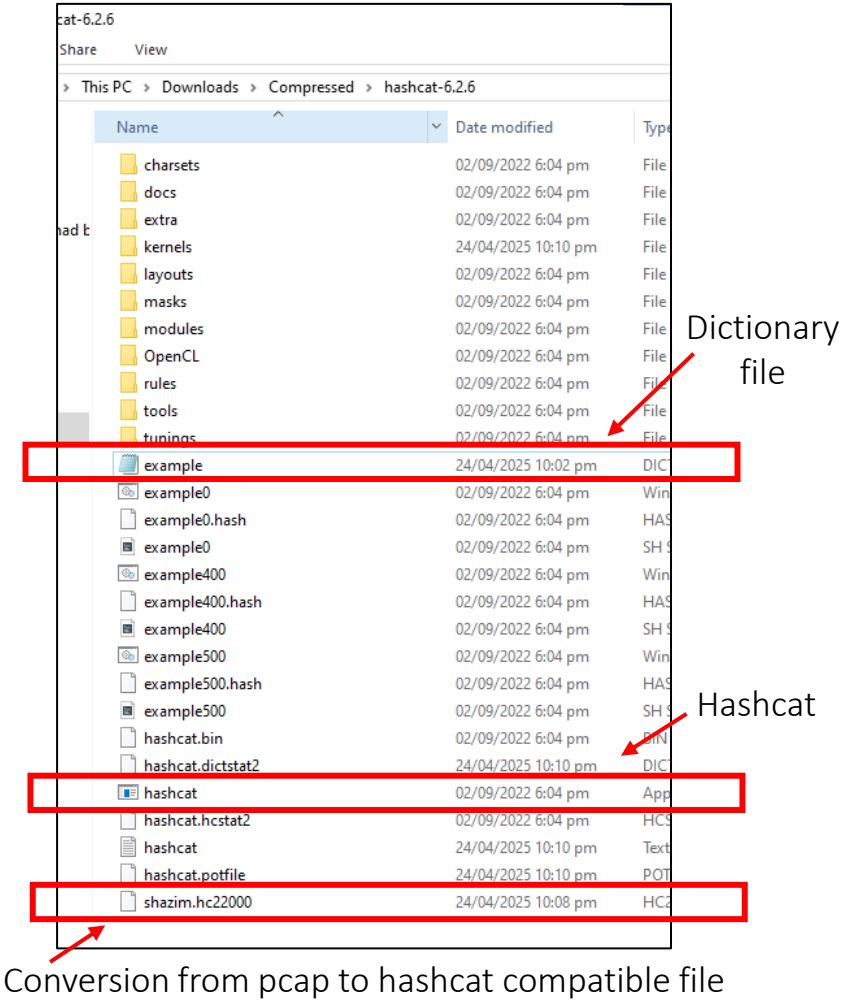


PMKID Attack – Demonstration

4) Analysing pcap file in WireShark

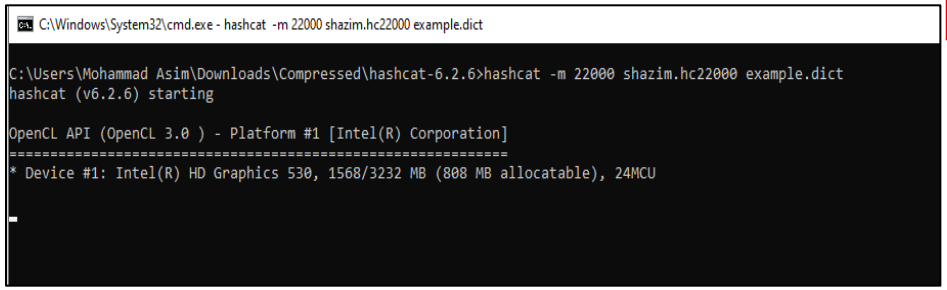


5) Launching Hashcat



PMKID Attack – Demonstration

6) Running Hashcat




```
222fcce22aa5e393ae794d5c27016667:5c18ddc4fe73:a06faaa0152e:Shazim:50471688

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: shazim.hc22000
Time.Started.....: Thu Apr 24 22:10:27 2025 (5 secs)
Time.Estimated...: Thu Apr 24 22:10:32 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (example.dict)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     5482 H/s (7.16ms) @ Accel:128 Loops:8 Thr:8 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 47444/128417 (36.95%)
Rejected.........: 22868/47444 (48.20%)
Restore.Point....: 0/128417 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 00000000 -> black1707

Started: Thu Apr 24 22:09:52 2025
Stopped: Thu Apr 24 22:10:33 2025

C:\Users\Mohammad Asim\Downloads\Compressed\hashcat-6.2.6>
```

PMKID Attack – Analysis

- Use of weak or common passwords in WPA2-PSK networks.
- Affected Protocols: WPA2.
- Allows attackers to gain unauthorized access to Wi-Fi networks.
- Use of strong, complex passwords; implementation of WPA3 where possible.

Comparative Analysis of Attacks

Aspect	Evil Portal Attack	PMKID Attack
Attack Type	Social Engineering (Phishing)	Cryptographic (Offline Cracking)
User Interaction	Required	Not Required
Target Protocols	WEP, WPA, WPA2	WPA2
Tools Used	Flipper Zero (Evil Portal App)	Flipper Zero, Hashcat
Mitigation Strategies	User Education, HTTPS Enforcement	Strong Passwords, WPA3 Implementation

Thank You

Any Questions?