WiFi Security

Luca Campa

University of Klagenfurt – Introduction to Cybersecurity

Introduction

Wireless Networks

- Most important standard for wireless networks: IEEE 802.11 (released 1997)
- Engineered to function similarly to a wired network
- Uses the same type of MAC addresses as Ethernet
- Communication is physically separated by using different channels (frequencies)
- Two different modes of operation:
  - Ad-hoc mode: peer-to-peer communication between nodes
  - Infrastructure mode: communication through access point (AP)

IEEE 802.11

- IEEE 802.11 Wireless LAN: a set of specifications (at Physical layer and MAC sublayer) for implementing Wireless LAN (WLAN) networks
- A WLAN network is identified by its SSID (Service Set IDentifier), the network's name.

IEEE 802.11 Wireless LAN vs OSI Model

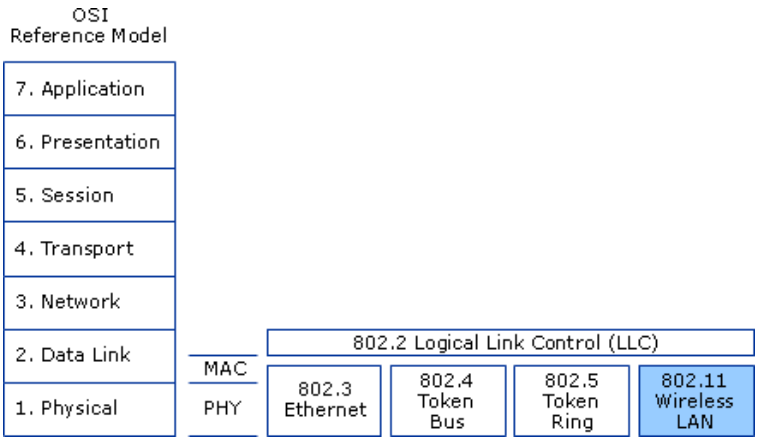


Image taken from
https://learn.microsoft.com/pt-pt/previous-versions/windows/server/cc757419(v=ws.10)?redirectedfrom=MSDN

Connecting to a Wireless Network

- APs send beacon frames containing: Timestamp, Beacon interval, SSID, etc.
- Connecting to a network:
  1. Client scans for available networks (passive or active)
  2. Client sends authentication request with its identification (MAC), the network's SSID, etc.
  3. If AP decides to accept the client, sends authentication OK.
  4. Client sends association request.
  5. AP sends association OK.

WiFi Security

802.11 Security Timeline

	Protocol	**Security status**
1999	WEP (RC4 + CRC-32)	Broken in practice; deprecated
2003	WPA (TKIP/RC4)	Transitional; legacy only
2004	WPA2 (AES-CCMP)	Long-standing baseline, still common
2018+	WPA3 (SAE, GCMP/CCMP)	Stronger authentication and forward secrecy

WiFi Threat Model

- Adversary can passively monitor radio traffic from nearby locations.
- Adversary can actively inject/deauthenticate frames (unless protected).
- Human factors: weak passphrases and rogue AP trust decisions.

WEP and RC4

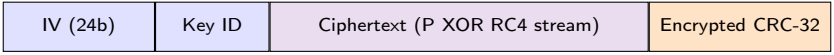
WEP (Wired Equivalent Privacy) Encryption

- Stream cipher: *RC4 key stream* XOR *plaintext* to produce *ciphertext*.
- Per-packet RC4 key material built from:
  - 24-bit IV (sent in clear)
  - long-term shared secret key (40 or 104 bits)
- Integrity (checksum): CRC-32 (linear, not cryptographic MAC).

WEP packet logic:

$$C = P \oplus \mathrm{RC4}(\mathrm{IV} \| K) \quad \text{and} \quad \mathrm{ICV} = \mathrm{CRC32}(P)$$

WEP Packet Format and Weaknesses



- Small IV space causes frequent IV reuse on busy networks.
- RC4 key scheduling biases leak key information when many packets observed.
- CRC-32 allows bit-flipping style manipulation without strong authentication.

RC4 Algorithm Specification: KSA

Key Scheduling Algorithm (KSA)

The KSA takes the secret key K (length L) and initializes a state array S of 256 bytes (0 to 255). It scrambles the array based on the key bytes.

1. **Initialization:** For $i = 0$ to 255, set $S[i] = i$.
2. **Scrambling Loop:** Set $j = 0$.
3. For $i = 0$ to 255:

$$j = (j + S[i] + K[i \bmod L]) \bmod 256$$

   Swap $S[i]$ and $S[j]$.

In WEP, the key K is formed by prepending the 3-byte public IV to the secret root key.

RC4 Algorithm Specification: PRGA

Pseudo-Random Generation Algorithm (PRGA)

After the KSA finishes, the PRGA produces the keystream bytes Z that will be XORed with the plaintext.

1. **Initialization:** Set $i = 0$, $j = 0$.
2. **Generation Loop** (run once per required keystream byte):

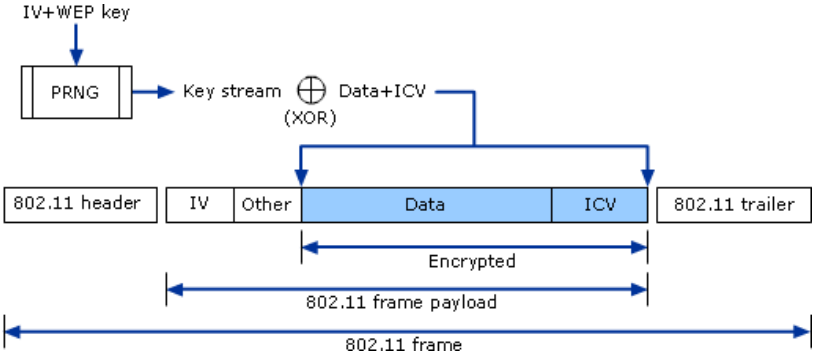
$$i = (i + 1) \bmod 256$$

$$j = (j + S[i]) \bmod 256$$

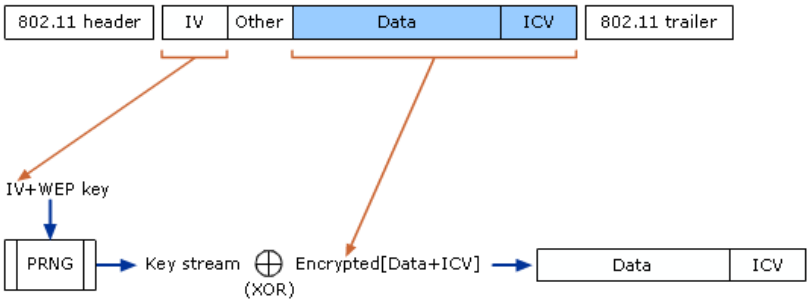
Swap $S[i]$ and $S[j]$.

$$Z = S[(S[i] + S[j]) \bmod 256]$$

WEP Encryption



WEP Decryption



WEP Encryption Weaknesses

- Small IV space (24 bits) leads to frequent IV reuse on busy networks.
- After many packets, the same IV will be used with the same secret key, allowing statistical attacks: e.g. after 5000 frames there is a 50% chance of at least one IV collision.
- RC4 key scheduling biases leak information about the secret key when many packets are observed.

Keystream reuse

If the same IV is reused, the same RC4 keystream is generated. This allows an attacker to recover plaintexts by XORing two ciphertexts with the same IV:

$$C_1 \oplus C_2 = (P_1 \oplus Z) \oplus (P_2 \oplus Z) = P_1 \oplus P_2$$

where Z is the keystream generated by RC4 for that IV and key. If one of the plaintexts is known or can be guessed, the other can be recovered.

- This is a classic example of a *two-time pad* problem, where reusing a keystream compromises confidentiality.
- In practice, many WEP networks had predictable traffic (e.g., ARP requests), which made it easier to exploit this weakness.

The FMS Attack: Overview

- The FMS attack (Fluhrer, Mantin, Shamir) is a statistical attack that exploits specific weaknesses in the RC4 KSA when certain "weak IVs" are used.
- In a perfectly secure cryptographic function, the first keystream byte (Z_1) should be completely random. The chance of Z_1 happening to mathematically equal any specific internal variable (like j_{A+3}) should be exactly 1 over 256 (about 0.39%).
- The FMS attack proves that when a Weak IV is used, this probability jumps from 0.39% to roughly 5%.
- This bias can be exploited by an attacker to recover key bytes with high confidence after observing enough packets with weak IVs.

The FMS Attack: Weak IVs

What is a Weak IV? An IV is "weak" if it takes the specific form $(A + 3, 255, X)$, where:

- A is the index of the secret root key byte we want to guess ($A \geq 0$).
- X is any value (acts as a variation to collect multiple packets).

Because WEP transmits the IV in plaintext, an attacker simply observes traffic and filters for packets where the first two bytes of the IV match this pattern.

The FMS Attack: The Mathematical Leak

For a weak IV $(A+3, 255, X)$, consider the KSA loop at step $A+3$. By this step, the attacker knows all key bytes up to $K[A+2]$ (because they know the IV and have recursively guessed prior root key bytes). They can simulate the KSA locally to find S and j at step $A+2$. At step $A+3$, the KSA update is:

$$j_{A+3} = (j_{A+2} + S[A+3] + K[A+3]) \bmod 256$$

The Bias: Due to the specific 255 value in the IV, there is a $\approx 5\%$ probability that the first keystream byte Z_1 directly equals j_{A+3}. By rearranging the equation, we isolate the unknown key byte:

$$K[A+3] = (Z_1 - j_{A+2} - S[A+3]) \bmod 256$$

Attackers collect many packets with varying X, calculate this formula for each, and the most frequent result is likely to be the correct key byte.

WEP Attack Preconditions and Inputs

- Attacker is within radio range and can passively capture 802.11 traffic.
- WEP IV is transmitted in clear, so each packet reveals IV.
- Many packets are needed because the attack is *statistical*, not single-shot.
- Repeated packet structures (e.g., ARP/LLC patterns) allow deduction of the first keystream byte (Z_1).

Detailed WEP Break: Phase 1 (Traffic Collection)

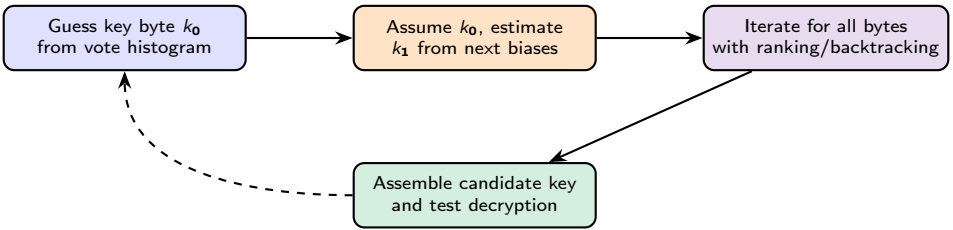
- Collect frames and index by IV, ciphertext first bytes, and packet type.
- Wait for natural traffic or trigger additional traffic in authorized lab scenarios.
- Keep only packets useful for RC4-bias analysis (weak-IV classes and known structures).

Typical intuition on data needs:

- 40-bit WEP keys: often recoverable with relatively fewer packets.
- 104-bit WEP keys: generally require larger captures but remain practical.

Exact counts depend on IV distribution, and attack variant (FMS/KoreK/PTW).

Detailed WEP Break: Phase 2 (Byte-by-Byte Key Recovery)



KoreK/PTW refine the vote model and reduce required traffic compared to original FMS.

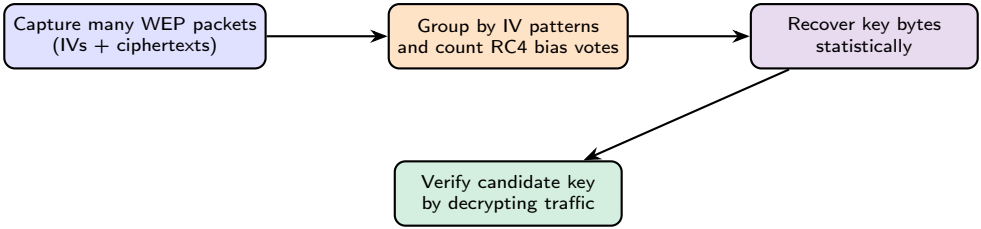
Detailed WEP Break: Phase 3 (Validation and Exploitation)

- Validate candidate key by decrypting captured packets and checking CRC consistency.
- Once key is confirmed, attacker can decrypt, inject, and impersonate on that WLAN.
- Shared-key usage: one recovered key compromises all users on that SSID.

Solution:

- Migration to WPA2/WPA3 removes the structural cryptographic weakness.

WEP Key Recovery Flow (High Level)



WPA and WPA2

WPA (TKIP) as Transitional Fix

- Retained RC4 but added TKIP key mixing and per-packet keying.
- Added MIC (Michael) to improve integrity over WEP.
- Introduced replay protection with sequence counters.

Limitations:

- Legacy constraints kept weak primitives (RC4) and high complexity.
- Practical attacks and deprecation make WPA/TKIP unsuitable today.

TKIP Architecture and Key Mixing

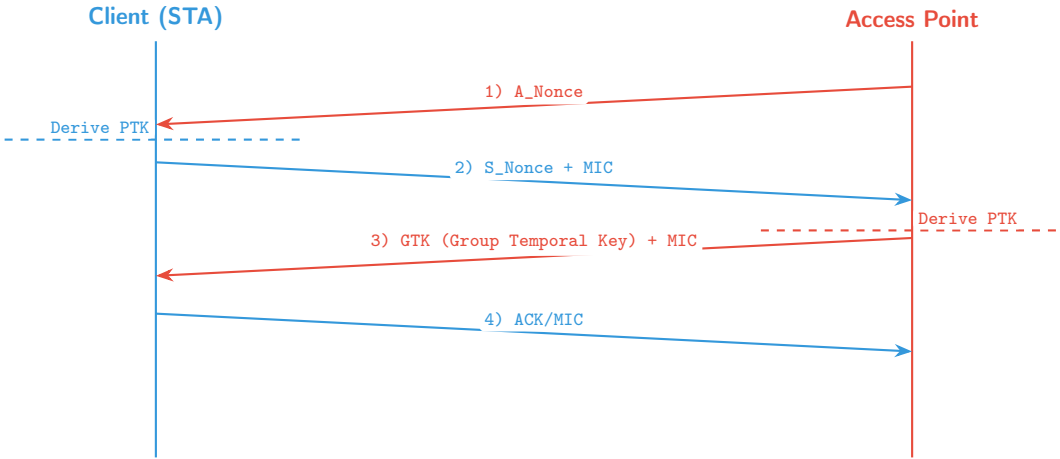
- **Sequence Counter (TSC):** Extends the IV to 48 bits to reduce IV reuse and prevent replay attacks.
- **Michael MIC:** A 64-bit Message Integrity Code added to prevent the bit-flipping forgeries common in WEP.
- **Key Mixing:** Destroys the weak IV correlation that enabled the FMS attack by mathematically isolating the base key from the RC4 engine.

$$\text{Ciphertext} = (\text{Data} \parallel \text{MIC} \parallel \text{ICV}) \oplus \text{RC4}(\text{Per-Packet Key})$$

WPA2 Core Model

- Encryption/authentication with AES-CCMP (counter mode + CBC-MAC).
- Two major modes:
  - Personal (PSK): shared passphrase-derived key
  - Enterprise (802.1X/EAP): per-user authentication and dynamic keys
- Four-way handshake derives fresh session keys from PMK (Pre-Master Key) and nonces.
- PMK is either derived from PSK or obtained via 802.1X authentication.

WPA2 Four-Way Handshake (Simplified)



Both sides derive PTK (Pairwise Transient Key) from PMK, nonces, and MAC addresses.

WPA2 Attack Surface

- Offline dictionary attack after capturing handshake (weak PSK risk).
- KRACK-style key reinstall issues from protocol/implementation behavior.
- PMKID capture attacks against poorly configured deployments.
- Evil twin APs to harvest credentials or force downgrade behavior.

Defenses: strong passphrases, updates, enterprise auth, rogue-AP monitoring.

WPA3

What WPA3 Improves

- Replaces PSK authentication with SAE (Simultaneous Authentication of Equals) in personal mode.
- Better resistance to offline dictionary attacks.
- Forward secrecy properties for session establishment.
- Mandatory Protected Management Frames (PMF) in standard profiles:
  - Prevents deauthentication/disassociation frame spoofing.
  - Mitigates rogue AP and deauthentication-based attacks.

Note: PMF (Protected Management Frames) is a feature that encrypts and authenticates management frames, such as deauthentication and disassociation frames, to prevent spoofing and other attacks that rely on unauthenticated management traffic.

SAE Authentication Idea

- Both parties contribute to a shared secret using a password element and random nonces.
- The protocol ensures that an eavesdropper cannot verify guesses without active interaction. Captured traffic does not directly enable classic WPA2-style offline handshake guessing.
- Even if the password is weak, the attacker must perform an active attack for each guess, which can be rate-limited and monitored.

WPA3 Real-World Caveats

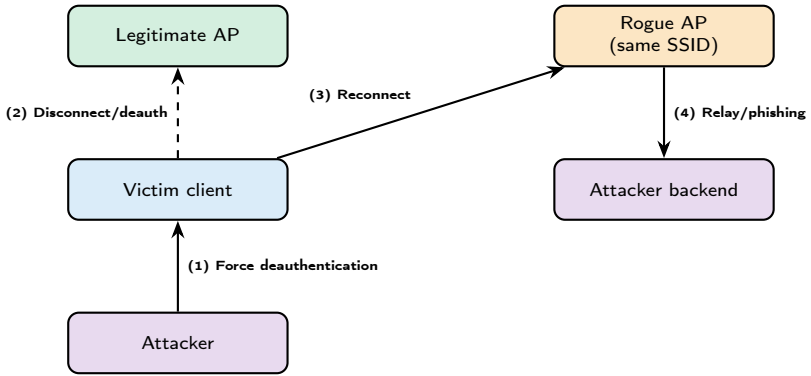
- Transition mode (WPA2/WPA3 mixed) can reintroduce weaker paths.
- Side-channel and implementation flaws still require patch discipline.
- Weak passwords still matter, even with stronger protocol design.

Attack patterns

Common WiFi Attack Patterns

Attack	Mechanism	Common impact
Handshake capture	Passive sniffing during association	Password cracking attempt
Evil twin	Rogue AP imitates SSID	Credential theft/MITM
Deauthentication abuse	Force reconnect to capture handshakes	Availability loss, capture packets
Downgrade	Push clients to weaker mode	Reduced security baseline

Example: Evil Twin Attack Flow



WiFi Hardening Checklist

- Prefer WPA3-SAE; avoid transition mode where possible.
- For WPA2, use long random passphrases and rotate on compromise events.
- Enable PMF (802.11w) and disable legacy ciphers/TKIP/WEP.
- Use separate VLANs/SSIDs for guests and IoT devices.
- Monitor for rogue APs, anomalous deauthentication floods, and unusual associations.
- In enterprise: use WPA2/3-Enterprise with EAP-TLS and certificate lifecycle controls.

References (Selected)

- IEEE 802.11 family (security amendments and revisions).
- Fluhrer, Mantin, Shamir: Weaknesses in the Key Scheduling Algorithm of RC4.
- NIST SP 800-153: Guidelines for Securing Wireless LANs.
- Wi-Fi Alliance: WPA2/WPA3 security guidance.
- Images are taken from `https://learn.microsoft.com/pt-pt/previous-versions/windows/server/cc757419(v=ws.10)?redirectedfrom=MSDN`.

Questions?