Wi-Fi Security

Josh Wilcox (jw14g24)

March 14, 2025

Table of Contents

Why do we need Wifi Security

- Wireless is inherently less secure than a wired connection
- Signal is not constrained by wires
- Anyone in the range of the connection can listen in or participate
- This causes a risk of unauthorised access with wireless networds

Wi-Fi Attacks

Eavesdropping

- Also known as network sniffing or packet sniffing
- Attacker secretly listens into the network
- They try to intercept data without the knowledge of the two parties trying to exchange the data
- This means they can capture sensitive information
- Especially damaging when there is no encryption
- Wireshark can be used to do this

Man in the Middle Attacks

- An **active** attack
- The attacker **modifies** the data being sent between the parties
- The attacker positions themself in the middle of the two parties
- Instead of just relaying messages they can change it
- This means they can inject malicious information
- They can also use DNS probing?

Types of Attack

- Deauthentication attack
  - Forces Wi-Fi devices to disconnect from a network
  - Attacker sends deauth messages to devices *pretending* to be the router
  - This kicks devices from networks
- Evil Twin Attack
  - Attacker sets up a fake Wi-Fi access point
  - The fake access point mimics a legitimate one
  - Users unknowingly connect to the fake access point
  - Attacker can intercept sensitive information
  - Often used in phishing attacks

Security Protocols

WEP

What is it

- First security protocol for 802.11 wireless networks
- Provides data confidentiality comparable to a wired network

How does it work

- Uses a Pre-Shared Key (PSK) that is manually set on both the router and the client device
  - This key is 40-bits long
- Also uses a 24-bit Initialization Vector (IV)
  - The IV is a randomly generated value that is attached to each packet
  - Ensures that identical plaintext blocks are encrypted into different ciphertext blocks
  - Adds randomness to the key stream to enhance security
- The PSK and IV are combined to create a key stream
  - The IV is concatenated with the PSK
  - This concatenated value is then input into the RC4 algorithm to generate the key stream
- Rivest Cipher 4 (RC4) is used to generate the key stream
- The key stream is XORed with the plaintext data to produce the ciphertext
- An Integrity Check Value (ICV) is calculated for the data and appended to the packet
  - The ICV ensures that the data has not been tampered with during transmission

WEP - Why is it insecure

- RC4 Encryption is **weak**
  - RC4 has known vulnerabilities that allow attackers to predict parts of the key stream.
  - This can lead to the recovery of plaintext data without needing to know the key.
- IV is too short and sent in plaintext
  - The 24-bit IV is too short, leading to IV collisions in busy networks.
  - Since the IV is sent in plaintext, attackers can capture it and use it to decrypt packets.
- Uses a **static** preshared key
  - The same key is used for all sessions, making it easier for attackers to perform brute-force attacks.
  - Once the key is compromised, all communications can be decrypted.
- The integrity check is weak
  - The Integrity Check Value (ICV) is based on CRC-32, which is not cryptographically secure.
  - Attackers can modify packets and recalculate the ICV, allowing them to inject malicious data.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) - **Properties**

- Uses a temporary key derived from the **Pre-Shared key**
  - Uses the *Temporal Key Integrity Protocol*
- Uses a new key for every packet of data
- RC4 Is kept for backwards compatibility
- Key Length - 128 bits
- IV extended to 48-bits

Wi-Fi Protected Access (WPA) - **Vulnerabilities**

- Still based on RC4 Encruption, which is weak
- WPA-PSK relies on a shared password - meaning it is vulnerable to:
  - **Brute Force** password guessing
  - Using **Dictionary Attacks** (common passwords lists)

WPA2

- Successor to WPA
- Uses **Authenticated Encryption** using AES
  - **Much** more secure than RC4
- More efficient than WPA and WEP - So improves performance

WPA Attacks

Key Reinstallation Attack

4. WPA Attacks
   - Key Reinstallation Attack (KRACK)
   - Kr00k

- Vulnerability found in **WPA** and **WPA2**
- Forces a device to reinstall an already used key
  - Leads to the decryption of data or injection of malicious traffic
- Fortunatley, manufacturers could release patches to address the KRACK vulnerabilities

Kr00k

4. WPA Attacks
   - Key Reinstallation Attack (KRACK)
   - Kr00k

- Allows an attacker to decrypt data packets
  - Found in devices like RPi 3, iPhone 8, Amazon Echo and some routers
- Sets the key to all zeros which is clearly easy to decrypt

Wi-Fi Protected Setup (WPS)

- Makes it easier to connect to a WPA-Protected network
- User enters an 8-digit pin or presses a button on the access point to connect
- This Pin can be **brute-forced** quickly
- Kinda stupid - **should disable!**

Summary Table

	WEP	**WPA**	**WPA2**	**WPA3**
Encryption Method	RC4	TKIP+RC4	AES	AES
Key Management	Static PSK	PSK	PSK	SAE
Encryption Key	64/128 bits	128 bits	128 bits	128/192 bits
Security	Very Low	Low	High (if patched), vulnerable to KRACK otherwise	High

Table: Summary of Wi-Fi Security Protocols