Wireless system security

Wi-Fi security and the ease of password hacking

Ante Čavar, 10.10.2025

Lecture overview

- Motivation
- What is Wi-Fi and how does it protect traffic?
- WPA2 vs WPA3
- Demonstration
- How to protect yourself?
- Conclusion
- Literature

Motivation

- ***Wi-Fi rules everything around me***
  - More and more devices require Wi-Fi connection
    - security cameras, IoT devices, NAS, (phones especially for updates)
  - Wi-Fi has many uses other than acting as a wireless switch
    - Room mapping, human sensing, reconstructing photorealistic images from signal
  - It is unavoidable yet mystery to many
- **Why care?**
  - As it is omnipresent we should focus on information it leaks
  - A single compromised AP or reused passphrase = big exposure
  - Not many people are invested in its security
  - Once ‘in’ attacker can pivot and access anything

What is Wi-Fi and how does it protect traffic?

- family of wireless protocols based on IEEE 802.11 (same as Ethernet)
- AP + Switch + Router/NAT
- 3 pillars of security
  - Authentication
  - Key exchange
  - Encryption

WPA2 vs. WPA3

Mode	Authentication	Key exchange	Encryption
WPA2-Personal	**PSK** (Pre-Shared Key)	PSK converted directly to **PMK** (Pairwise Master Key) → 4-way handshake	AES-**CCMP**-128 (Counter mode cipher block Chaining Message Protocol - aka CBC-MAC)
WPA3-Personal	PSK authenticated with **SAE** (Simultaneous Authentication of Equals)	SAE performs passwd.-authenticated **KEX** output used as PMK → 4-way handshake (Key EXchange)	AES-**GCMP**-128 (Galois/Counter Chaning message Protocol)
WPA2-Enterprise	Individual user/device auth. through 802.1X / EAP (PEAP, EAP-TLS, EAP-FAST…)	PMK derived from successful **EAP** negotiation (client and RADIUS server; Extensible Authentication Protocol)	AES-CCMP-128
WPA3-Enterprise	EAP-TLS	PMK from EAP exchange	AES-GCMP-256

PSK, SAE and PMK

- PSK (WPA2-Personal)
  - PMK = PBKDF2(HMAC-SHA1, passphrase, SSID, 4096 iterations, 256-bit output)
- SAE (WPA3-Personal)
  - KEX produces shared secret → PMK
- EAPOL
  - Contains ANonce and SNonce and EAPOL key frames → PMK → PTK/GTK (Pairwise/Group Transient Key)
  - WPA2 - EAPOL exchange + SSID → offline password cracking
  - WPA3 - SAE prevents offline password cracking

Demonstration

DISCLAIMER: Test only on AP’s that you have permission to test on or on those that you own. This is purely educational and is not to be used outside of this class.

Failure to comply to this can lead to legal issues from which are FER (Faculty of Electrical Engineering and Computing) and myself (Ante Čavar) excluded.

Conclusion

- Wi-Fi is easy to misuse and easy to break if passwords are weak
- WPA3 improves security, but adoption matters
- Defenses are practical: use strong passphrases, firmware updates, network segmentation (walled-garden)
- Continue to educate yourself on latest practices and vulnerabilities

Sources

- https://www.aircrack-ng.org/documentation.html
- https://www.wifi-professionals.com/2019/01/4-way-handshake
- https://en.wikipedia.org/wiki/IEEE_802.11i-2004
- https://www.portnox.com/cybersecurity-101/wpa3/
- https://www.youtube.com/watch?v=hg_yR1UsBdI

Thank you for attending and cooperation!