WiFi Security

Petri Riihikallio, CWNE#307
Metis Oy

Broadcast media

- Anyone can intercept
- Encryption is vital
- Wired Equivalent Protection (WEP)
  - 56 bit static key
  - Hampered by U.S. export restrictions
  - Easily broken

Wi-Fi Protected Access (WPA)

- Quick temporary patch
- RC4-based TKIP encryption
- Suitable for WEP-capable devices
- 64 or 128 bit key
- Limits bandwidth to 54 Mbps!
  - Disable WPA/WPA2 transitional or mixed mode!

802.11i or WPA2

- Ratified 2004, mandatory 2006
- 128-bit Advanced Encryption Standard (AES)
  - Also known as CCMP
  - Instructions in current processors
- Four-way handshake
- Pairwise master key & group master key
- Frame replay protection
- Management frames are not protected
  - Esp. deauthentication and disassociation frames
  - 802.11w a.k.a. MFP or PMF

Personal vs. Enterprise

- WPA2 Personal uses pre-shared key (PSK)
- WPA2 Enterprise uses per-user key in RADIUS
  - Same principle as in 802.1X (Ethernet port authentication)
  - Extensible authentication protocols (EAP)
    - Many require server certificates (X.509)
    - Some require client certificates
    - Certificate distribution requires MDM
    - Certificate renewals cause problems
    - See Mac Admins Slack channel #8021X
  - Enable 802.11r for Fast Roaming

EAP types

- Supported by Apple operating systems:
  - EAP-TLS
  - EAP-TTLS (MSCHAPv2)
  - EAP-FAST
  - EAP-SIM
  - EAP-AKA
  - PEAP-MSCHAPv2
  - PEAP-GTC
- RADIUS must support the same type!

WPA3

- Ratified 2018, mandatory 2020
- Either Personal or Enterprise
  - Personal uses Simultaneous Authentication of Equals (SAE)
  - Enterprise uses 128 or 192 bit AES
- Required for Wi-Fi 6E (6 GHz)
- Management frame protection is mandatory
- Don’t use WPA2/WPA3 transition mode
  - Create two SSIDs

WPA3 Extras

- Opportunistic Wireless Encryption (OWE)
  - Encryption for open SSIDs
- Wi-Fi Easy Connect
  - For devices without keyboard or display
  - Replaces Wi-Fi Protected Setup (WPS)
    - WPS should be disabled due to vulnerabilities!
  - Uses a device already authenticated on the Wi-Fi
    - Kind of like Apple devices do
  - Scan the QR code to enroll the device

WiFi 7

- 802.11be
- Extremely High Throughput (EHT)
- 2.4, 5 and 6 GHz multi-link option (MLO)
  - May be postponed to Wave2
- To be ratified in 2024 (estimate)
- Devices already available based on drafts

Thank you!