WLAN Encryption and Authentication

Topics

- Wi-Fi encryption standards
- The RADIUS authentication process
- Guest user policies

Wi-Fi Authentication and Encryption Options

- None - OSA
- Wired Equivalent Privacy
- Wi-Fi Protected Access (WPA)
- WPA2
- WPA3
- Wi-Fi Advanced Open
- RADIUS
- https://ui.linksys.com/LAPAC2600/V1.0.00.004/Menu_Conf.htm#
  - Wireless Security and Connection Control options

Authentication and Association

- Standard mechanisms under 802.11:
  - **Open System Authentication (OSA):** As long as the SSID is known, client can access the network and receive non-encrypted information
  - **Shared Key Authentication (SKA):** Is part of WEP encryption; client can access wireless network and send and receive encrypted data by matching encryption key on the access point
    - Deprecated; not recommended

Authentication and Association (Cont.)

- **OSA**
- Requires minimal exchange between client stations and authenticating access points
- Devices exchange probe request -response, confirming that both parties are 802.11 devices and can use and understand 802.11 frames
- An access point using OSA will authenticate any 802.11 client

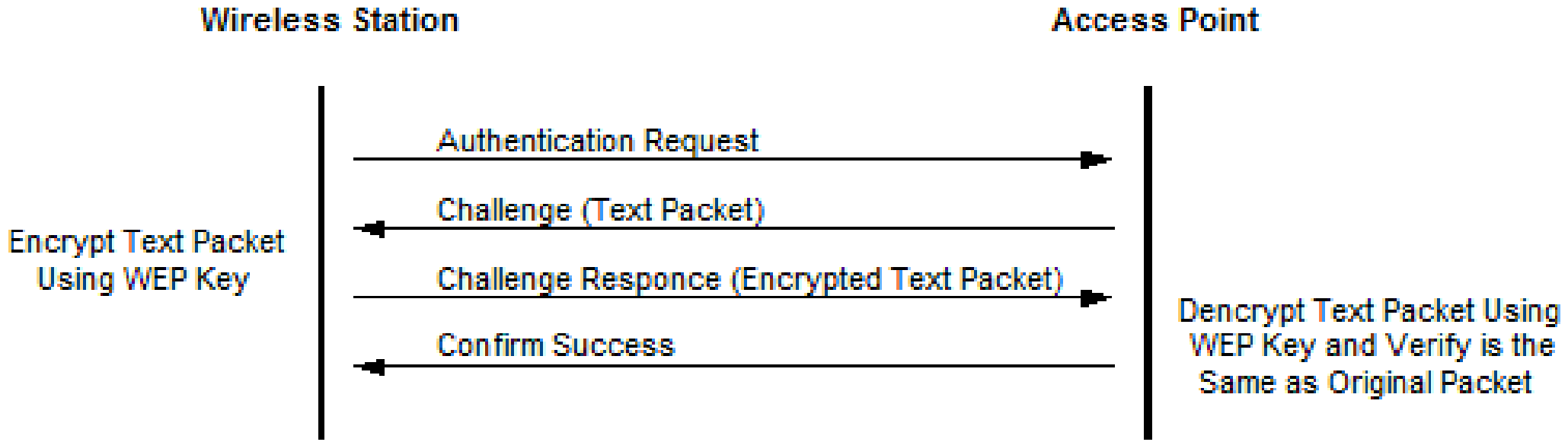
Wired Equivalent Privacy (WEP)

- Goal of WEP protocol was to provide confidentiality, integrity, and access control for wireless networks
- Provides data privacy through encryption, access control via a static-key form of authentication, and data integrity through a checksum to ensure that data had not been modified
- Layer 2 protocol 64-bit WEP uses a secret static key of 40 bits
- 128-bit WEP supports a 104-bit static key

WEP Issues

- Can enter a static WEP key into device configuration using hexadecimal or ASCII characters; many people did not understand base-16 numbers and did not turn on security
- Confusion regarding choice of static WEP keys
  - Access point might permit four static keys to be entered, only one can be the transmission key used to encrypt traffic
- WEP is prone to Initialization Vector (IV) collision attacks
- WEP is no longer considered a viable method for authentication

WEP Authentication Process



WEP Packet Exchanges

simplewepauth.pcapng

wepauthfail.pcapng

Wi-Fi Protected Access

- Wi-Fi Alliance introduced **Wi-Fi Protected Access (WPA)** certification in 2003
- Supports Temporal Key Integrity Protocol (TKIP)/Rivest Cipher 4 (RC4) dynamic encryption key generation
  - TKIP is now deprecated
- Viewed as intermediate solution to address WEP weaknesses
- Uses passphrase-based authentication in SOHO environments
- Supports 802.1X/Extensible Authentication Protocol (EAP) authentication in the enterprise

Wi-Fi Protected Access 2

- Use at least WPA2 whenever available
- Built on AES algorithm in CCMP
- Supports 802.1X/EAP authentication with preshared keys (PSK)
- In SOHO environments, WPA2 uses 64 byte -hexadecimal PSKs
  - Called WPA2-PSK or WPA2-Personal
- PSK is a plaintext English passphrase containing up to 63 characters
- Passphrase used to generate unique encryption keys for each wireless client

WPA2 with Advanced Encryption Standard

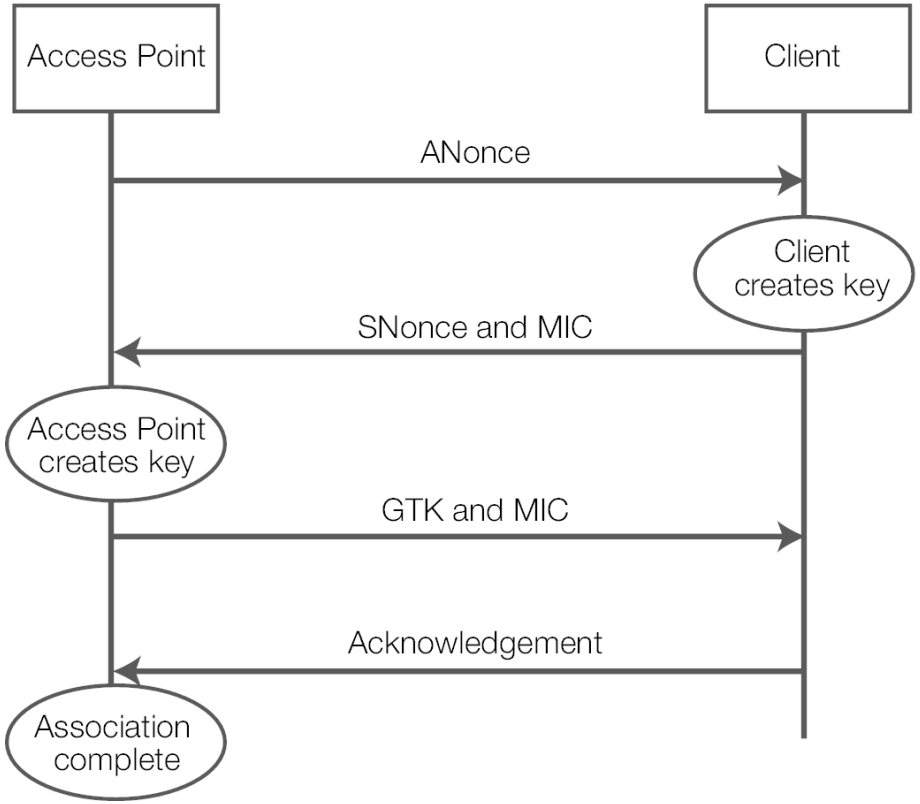
- **Advanced Encryption Standard (AES)** is block cipher algorithm
- AES encryption:
  - Is standard adopted by U.S. government
  - Is used as encryption algorithm in Internet Protocol Security (IPSec) VPNs
  - Supports three key sizes—128, 192, and 256 bits—although it uses a fixed block size of 128 bits

WPA2 with Counter Mode Cipher Block Chaining

- **Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)** is the security encryption protocol defined by 802.11i WPA2
- CCMP provides security via:
  - Data confidentiality via encryption
  - Authentication
  - Access control with layer management
- CCMP considered to be mandatory for Robust Security Network (RSN) compliance

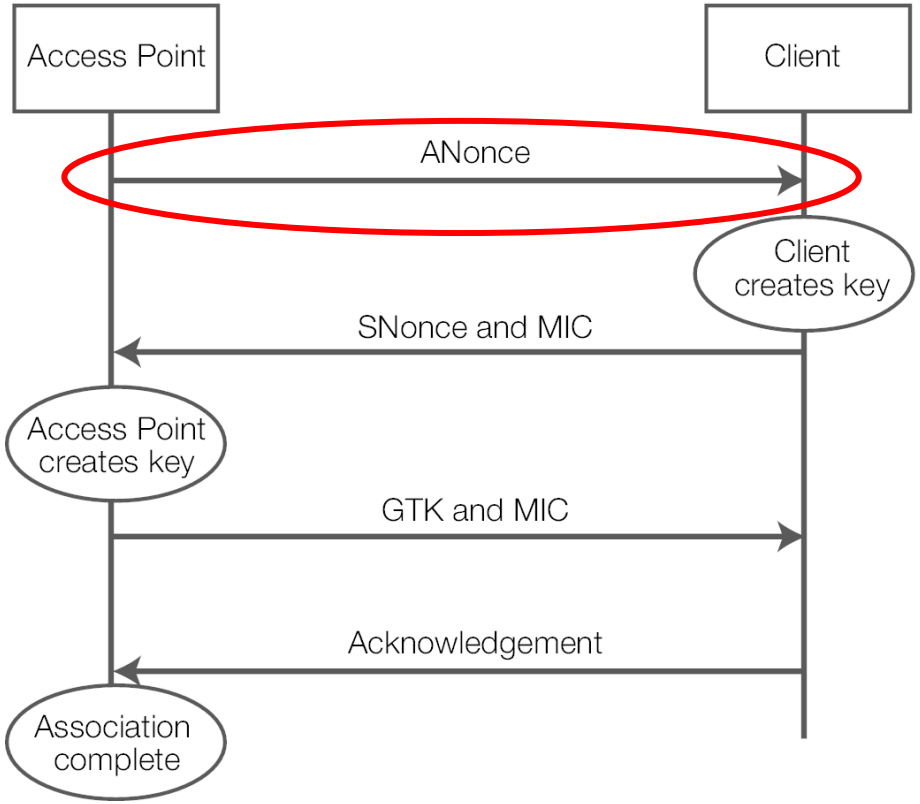
WPA2 Association Process

- Wi-Fi Protected Access 2 (WPA2) uses a four-way handshake for association



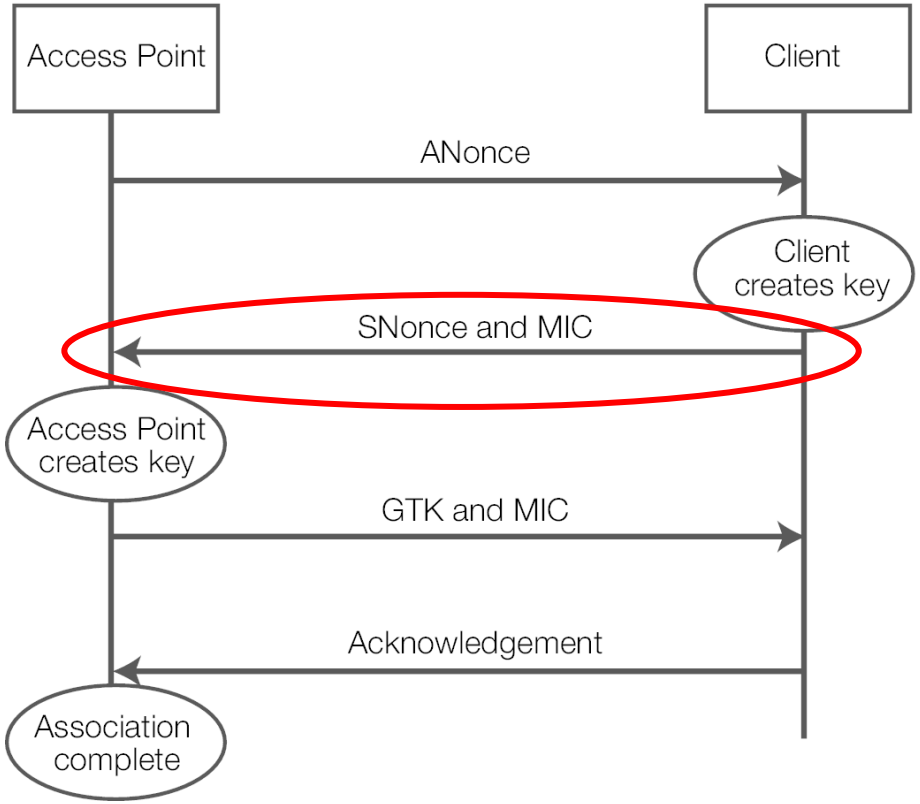
WPA2 Association Process

- The AP sends a nonce-value (ANonce) to the STA together with a Key Replay Counter, which is a number that is used to match each pair of messages sent, and discard replayed messages. The STA now has all the attributes to construct the Pairwise Transit Key (built with Pre-shared Key).



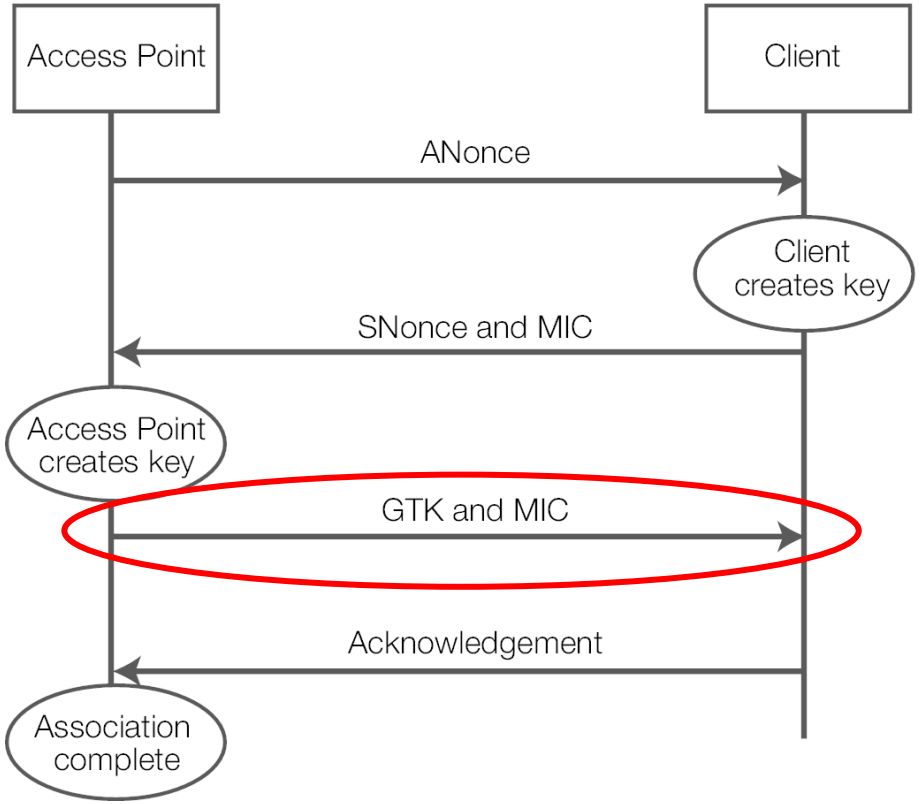
WPA2 Association Process

- The STA sends its own nonce-value (SNonce) to the AP together with a Message Integrity Code (MIC), including authentication, which is really a Message Authentication and Integrity Code (MAIC), and the Key Replay Counter which will be the same as Message 1, to allow AP to match the right Message 1.



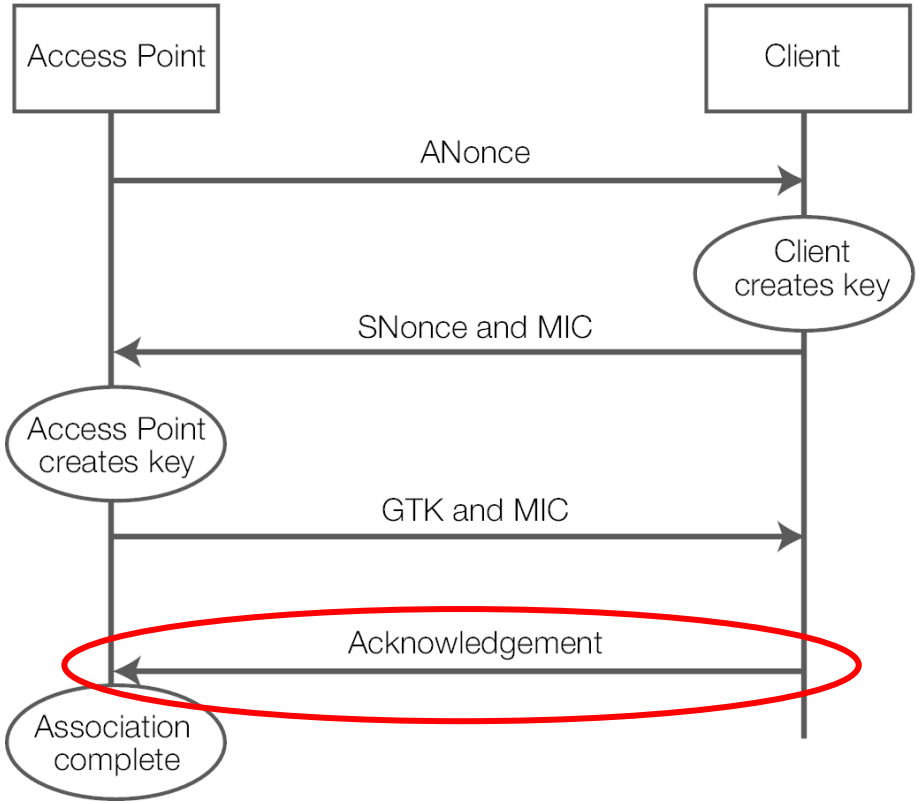
WPA2 Association Process

- The AP verifies Message 2, by checking MIC, RSN, ANonce and Key Replay Counter Field, and if valid constructs and sends the Group Temporal Key with another MIC.



WPA2 Association Process

- The STA verifies Message 3, by checking MIC and Key Replay Counter Field, and if valid sends a confirmation to the AP.



Observing the WPA2 Process

Wpa.full.cap- neat process

Wpa.badpassphrase.cap

Nokia network join pcap - common process

WPA3 Personal

- Simultaneous Authentication of Equals (SAE) or Dragonfly Key Exchange
- Uses hash of generated authentication key unique to each session
- Resistant to offline password cracking because of per-session keys
- Forward secrecy: Protects data traffic even if a password is compromised after the data was transmitted

WPA3 Example

https://www.cloudshark.org/captures/2b697549a818

WPA3 Enterprise

- Stronger encryption
- Offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data:
- Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)
- Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

WPA3 Vulnerabilities

- Downgrade attack on WAPs that enable backward compatibility
- CVE-2019-13377: Timing-based side-channel attack against WPA3's Dragonfly handshake when using Brainpool curves.
- CVE-2019-13456: Information leak in FreeRADIUS' EAP-pwd due to aborting when needing more than 10 iterations.
- As of 2023 these known CVEs were patched

WPA2/3 Vulnerabilities

- https://www.top10vpn.com/research/wifi-vulnerabilities/?is=6fa78154dbea9fd6a29caa59a8a9433f63d310cc0d643f0f38e7e9ff5be35bf6
- Details
- https://www.top10vpn.com/assets/2024/01/Top10VPN-Vanhoef-WiFi-Vulnerabilities.pdf?is=6fa78154dbea9fd6a29caa59a8a9433f63d310cc0d643f0f38e7e9ff5be35bf6

Eduroam Android Access

- EAP method: PEAP
- Identity: Your NetID username
- Password: Your NetID password
- CA certificate: Use System Certificates
- Domain: portal.connect.unr.edu
- * Select the View More Button for additional settings
- Phase 2 authentication: MSCHAPV2 – This is deprecated and EAP-TLS is recommended
- Anonymous Identity: Remove the word "Anonymous" so the input is left blank
- MAC address type: Phone MAC

Wi-Fi CERTIFIED Enhanced Open

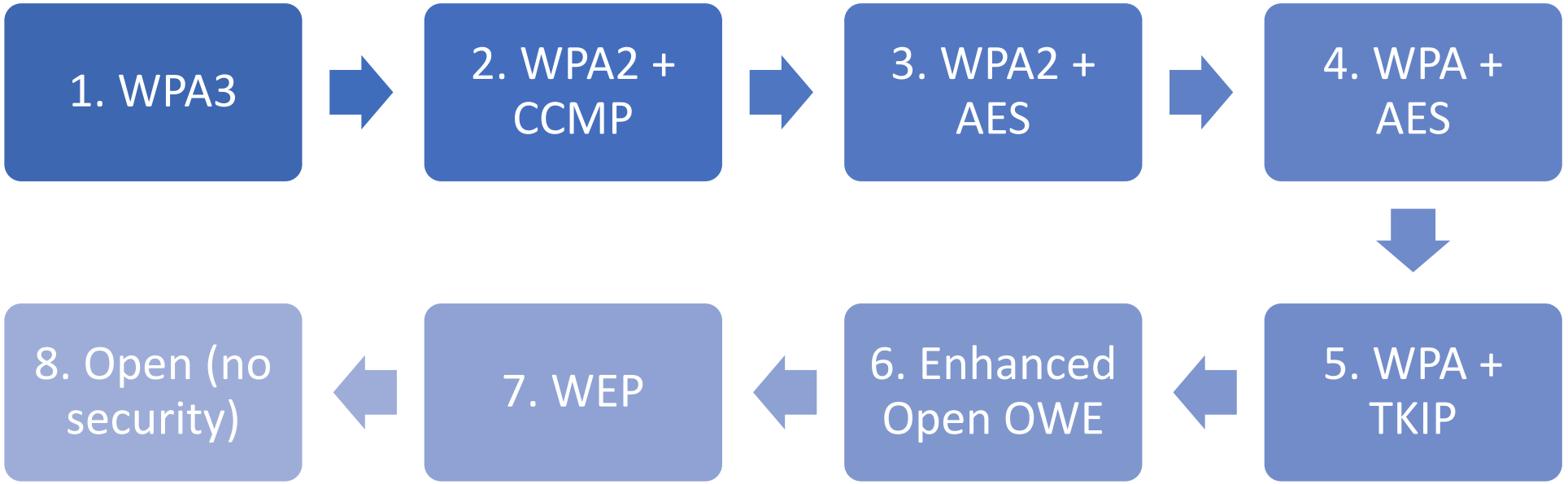
- Preserves convenience of open networks
- Provides some protection through encryption using Opportunistic Wireless Encryption (OWE)
- Unauthenticated Diffie-Hellman exchange is used to exchange ephemeral public keys
- Public keys are used in traditional 4-way handshake to generate encryption key for traffic.

OWE PCAP

- In association packets:
  - Tagged parameters, RSN (Robust Security Network) Information – Auth protocol is OWE
  - Tagged parameters look for Diffie-Hellman parameter

Order of Preference for Wi-Fi Data Protection

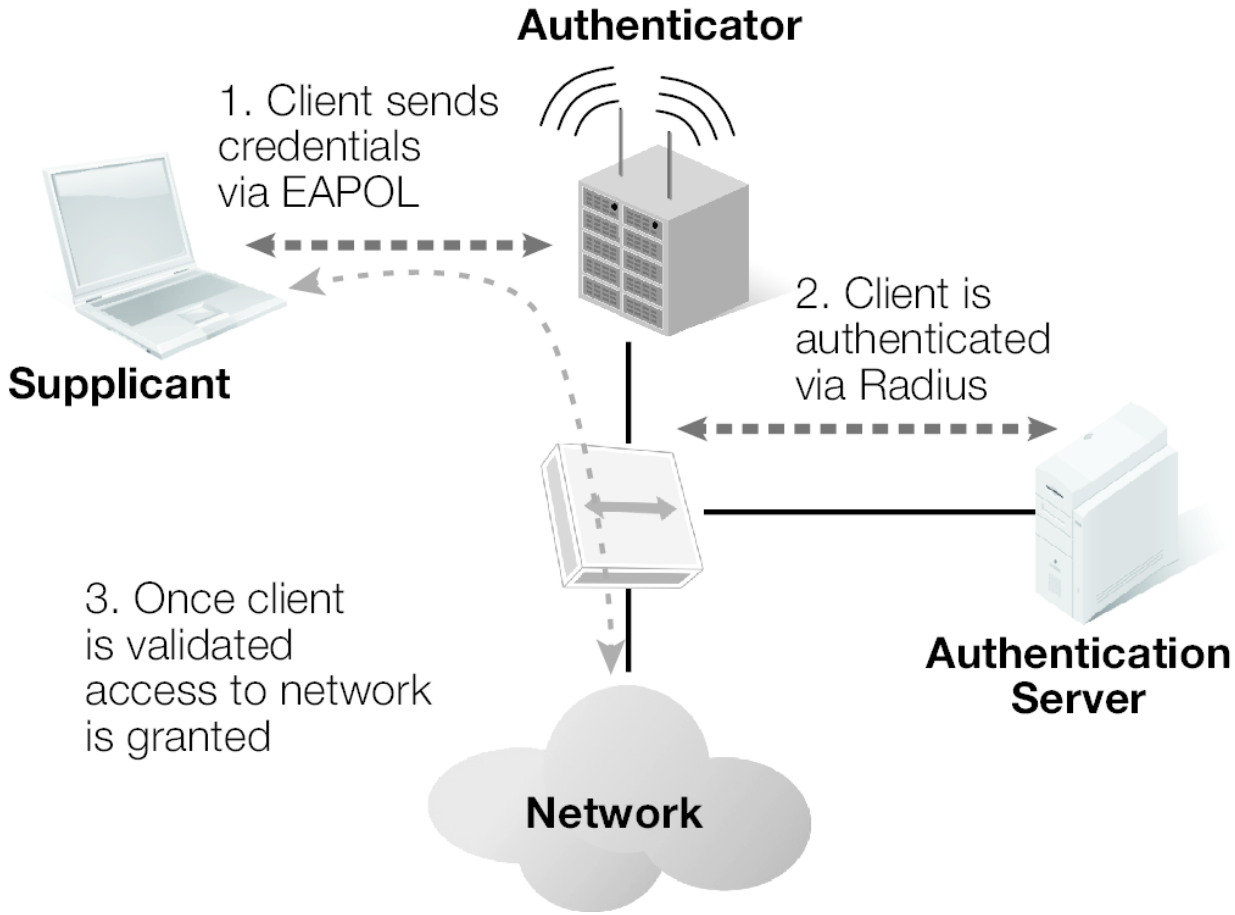
- When more than one type of Wi-Fi data protection is available, choose in this priority order.



Implementing Authentication and Access Control

- 802.1X specifies entities for per-user and per-device authentication:
  - **Supplicant:** A client device looking to connect to the network
  - **Authenticator:** A network device such as a switch or access point
  - **Authentication server:** A server supporting an authentication protocol such as Extensible Authentication Protocol (EAP) or RADIUS

Implementing Authentication and Access Control (Cont.)



Extensible Authentication Protocol (EAP)

- A method of encapsulation for securely transporting keying material for encryption over wireless and Point-to-Point Protocol (PPP) networks
- Also used over LANs between authenticator and authentication server
  - Referred to as EAP over LAN (EAPoL)

Extensible Authentication Protocol (EAP) (Cont.)

- Transports authentication requests, challenges, notifications, etc. across network
- Creates a secure tunnel using Transport Layer Security (TLS)
- Credentials are passed through tunnel to authentication server
- Does not need to know authentication method
- Can accommodate username and password, certificates, tokens, biometrics, and more
- Closely associated with RADIUS

EAP-TLS

- EAP-TLS is the authentication protocol most commonly deployed on WPA2-Enterprise networks to enable the use of X.509 digital certificates for authentication.
- Uses asymmetric encryption (public key certificates) to create tunnel for EAP process
- Wpa-eap-tls.pcap
- Decryption keys:
- a5001e18e0b3f792278825bc3abff72d7021d7c157b600470ef730e2490835d4
  79258f6ceeecedd3482b92deaabdb675f09bcb4003ef5074f5ddb10a94ebe00a
  23a9ee58c7810546ae3e7509fda9f97435778d689e53a54891c56d02f18ca162

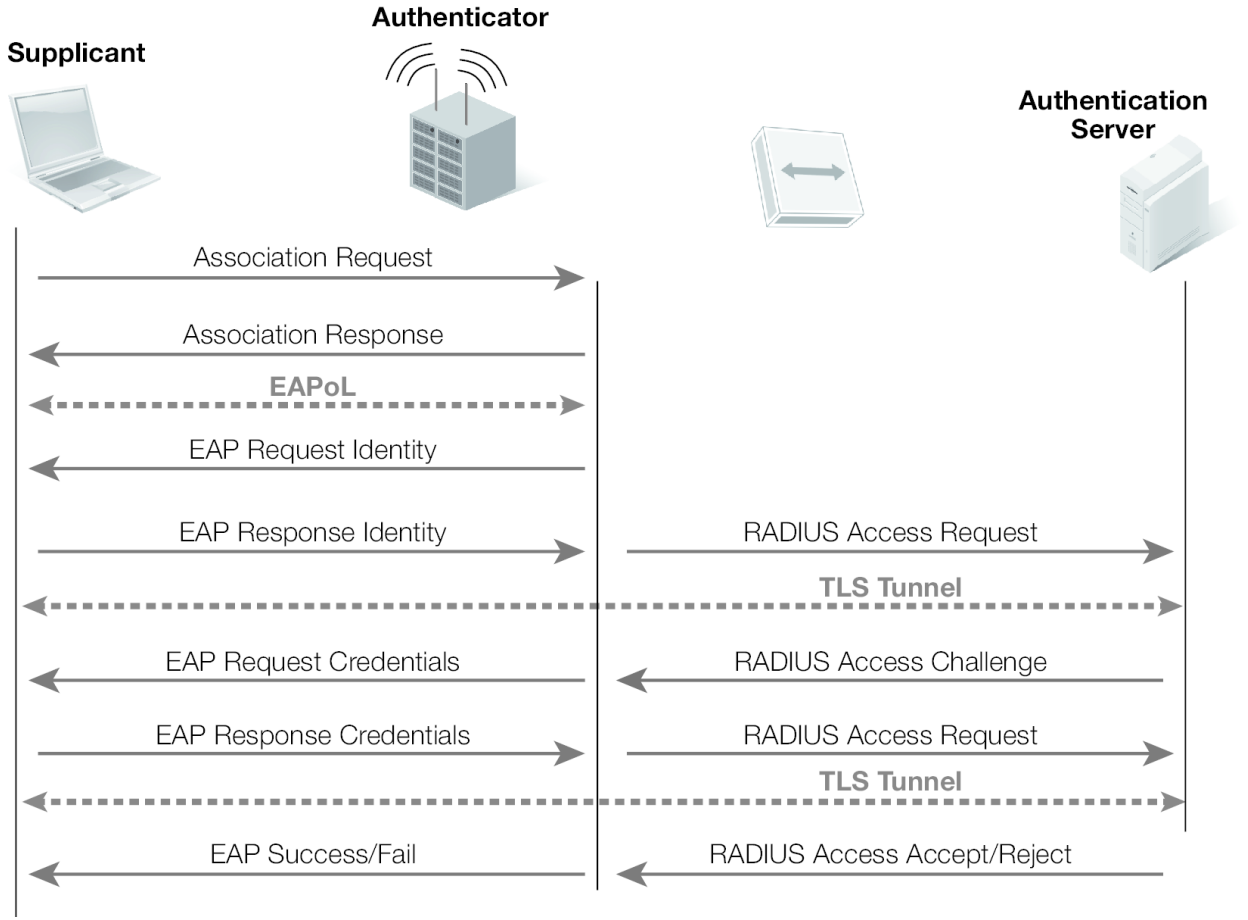
Remote Authentication Dial-In User Service (RADIUS)

- A network protocol that provides authentication, authorization, and accounting (AAA) services for devices or users connecting to a network
- Can also use TACACS+
  - Uses TCP, encrypts data and separates authentication from authorization

Remote Authentication Dial-In User Service (RADIUS) (Cont.)

- When attempting to connect, device (or user) is challenged by network access server (NAS) device with a request for credentials
- NAS passes user credentials to RADIUS server
- If credentials are verified, RADIUS server returns access accept response
- Access point is a conduit for passing authentication messages between the supplicant and the authentication server

Remote Authentication Dial-In User Service



Wi-Fi Guest Policies

- Guests may include vendors, clients, suppliers, others
- Establish rules for visitor authentication and policy control
  - Allow genuine visitors and guests access to Internet and perhaps some intranet services
  - Restrict them from corporate LAN
- Some organizations do not offer guest Wi-Fi access because of security concerns

Guest Access and Passwords

Open access

- Guest access available to anyone who can receive the wireless signal

Common guest password

- Low-security method, visitors share a well-known password for user authentication

Provisioned guest access

- Each guest is given a unique, time-limited password

Captive Portal

- All HTTP traffic is re-directed to the captive portal
- Login is required to obtain IP address with access to the Internet
- https://ui.linksys.com/LAPAC2600/V1.0.00.004/Menu_Conf.htm# Captive Portal Options

Summary

- Wireless encryption standards and appropriate uses
- Wireless authentication and guest policies