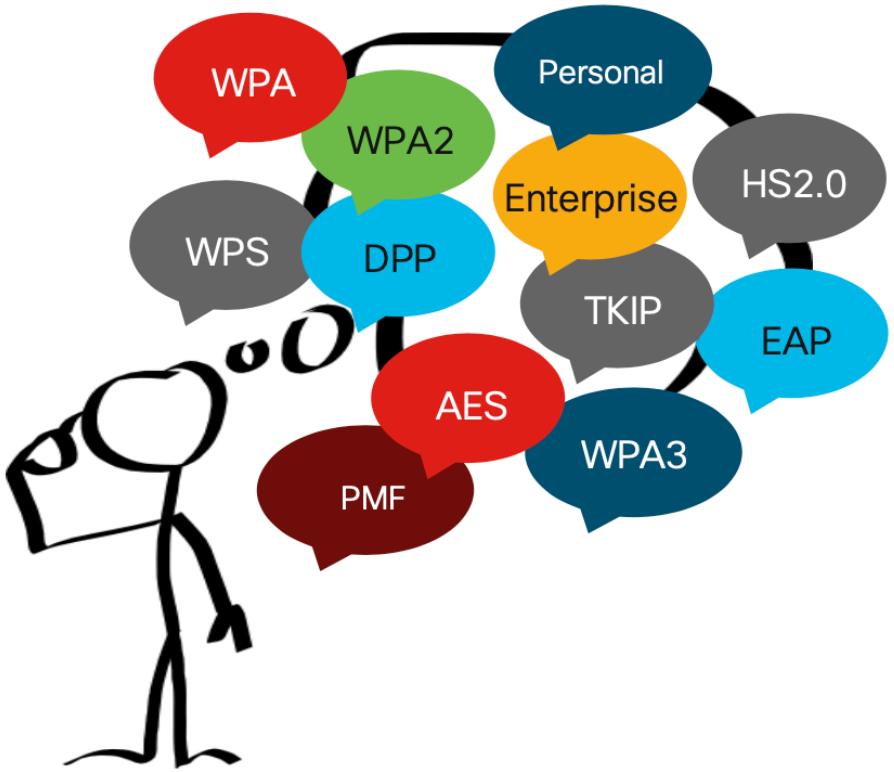
WLAN Security

by courtesy of Mohit Sethi (Ericcson) and Tuomas Aura (Aalto University)



Outline

- Wireless LAN technology
  - Threats against WLANs
- Real WLAN security: WPA2
  - WPA2-Personal (PSK)
  - WPA2 -Enterprise
- Real WLAN security: WPA3
  - Opportunistic Wireless Encryption (Enhanced Open)
  - Password Authenticated Key Exchange (PAKE: Dragonfly)
- Enterprise Security - EAP

WLAN Standards

- IEEE 802.11 standard defines physical and link layers for wireless Ethernet LANs
- Wi-Fi is an industry alliance to promote 802.11 interoperability
- Original 802.11-1997, latest 802.11-2016, amendments e.g. 802.11ae, 802.11aa
- Physical layer:
  - Uses unlicensed bands at 2.4 GHz (microwave ovens, Bluetooth) and 5 GHz
  - Up to 14 radio channels in the 2.4 GHz band, but only about 3 non-overlapping ones
- Link layer
  - Looks like Ethernet (802.3) to layers above
  - MAC protocol differs from 802.3 because one antenna cannot detect collisions while transmitting
    → explicit ACKs needed

WLAN Components

- Access point (AP) = bridge between wireless (802.11) and wired (802.3) networks
- Wireless station (STA) = PC or other device with a wireless network interface card (NIC)
  - To be precise, AP is also a STA
- Stations are identified by globally unique 48-bit MAC address
  - MAC = Medium Access Control, don't confuse with message authentication code
  - MAC address is assigned to each network interface card (NIC) by the manufacturer, which gets them from IEEE
- Infrastructure mode = wireless stations communicate only with AP
- Ad-hoc mode = no AP; wireless stations communicate directly with each other
- We will focus on infrastructure-mode WLANs

WLAN Structure

- Basic service set (BSS) = one WLAN cell (one AP + other wireless stations)
- The basic service set is identified by basic service set identifier (BSSID) = AP MAC address
- Extended service set (ESS) = multiple cells where the APs have the same service set identifier (SSID)
- The wired network is called distribution network in the standard; typically it is wire Ethernet
- APs in the same ESS can belong to the same IP network segment, or to different ones

WLAN threats

- Signal interception — sniffing
- Unauthorized network access — access to intranet or Internet access without authorization or payment
- Access-point misconfiguration
- Unauthorized APs — unauthorized ingress routes to intranet may bypass firewall
- Denial of service — logical attacks with spoofed signaling, signal jamming
- AP spoofing — stronger signal attracts STAs
- MitM attack by AP – especially free open AP

WLAN security goals

- Wireless LAN security protocols have following goals:
  - Data confidentiality and integrity — prevent sniffing and spoofing of data on the wireless link
  - Access control — allow access only for authorized wireless stations
  - Accounting — hotspot operators may want to meter network usage
  - Authentication — access control and accounting usually depend on knowing the identity of the wireless station or user
  - Availability — do not make denial-of-service attacks easy (radio jamming is always possible)
- Not all problems have been solved

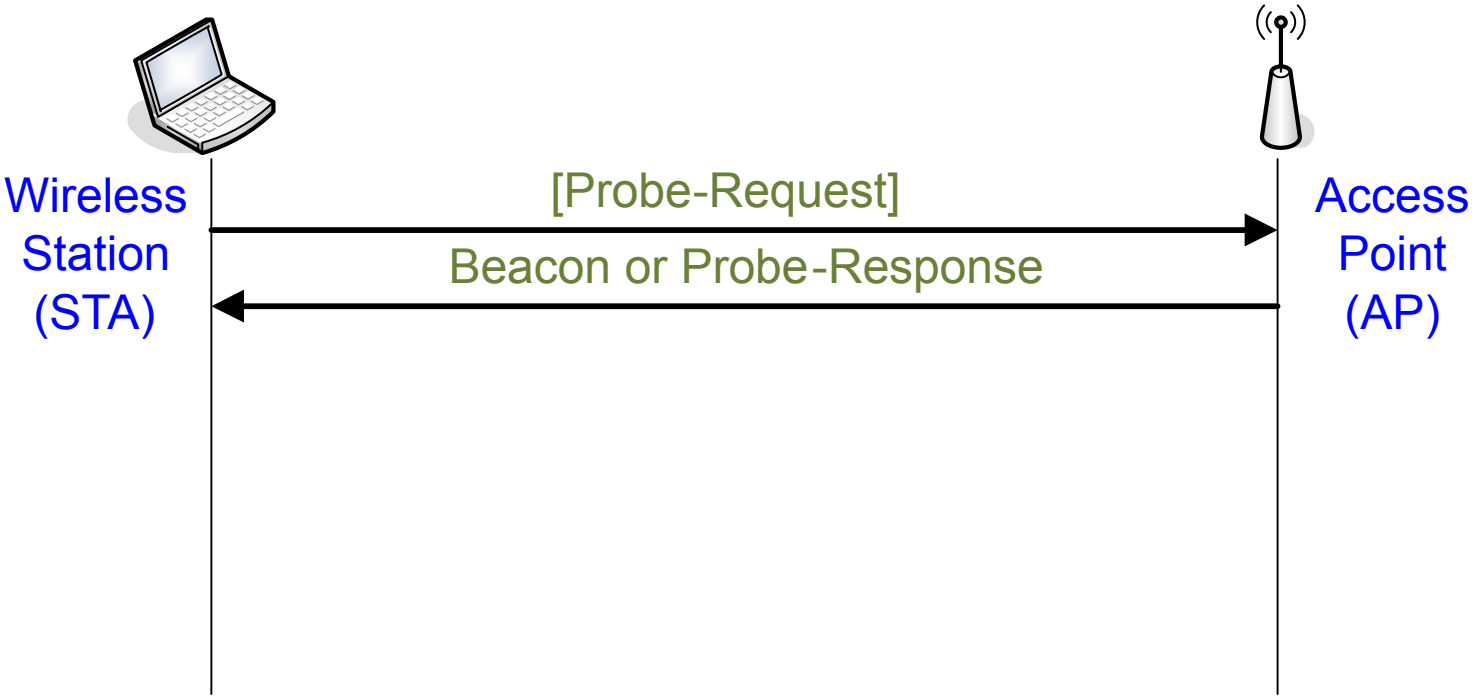
Weak WLAN security

- Disabling the SSID broadcast — attacker can sniff the SSID when other clients associate
- ACL of authorized MAC addresses — attacker can sniff and spoof another client's MAC address
- AP locations, directional antennas and metal foil to keep signal inside a building — hard to build a Faraday cage, and attacker can use a directional antenna with high gain

→ Weak security mechanisms are rarely worth the trouble

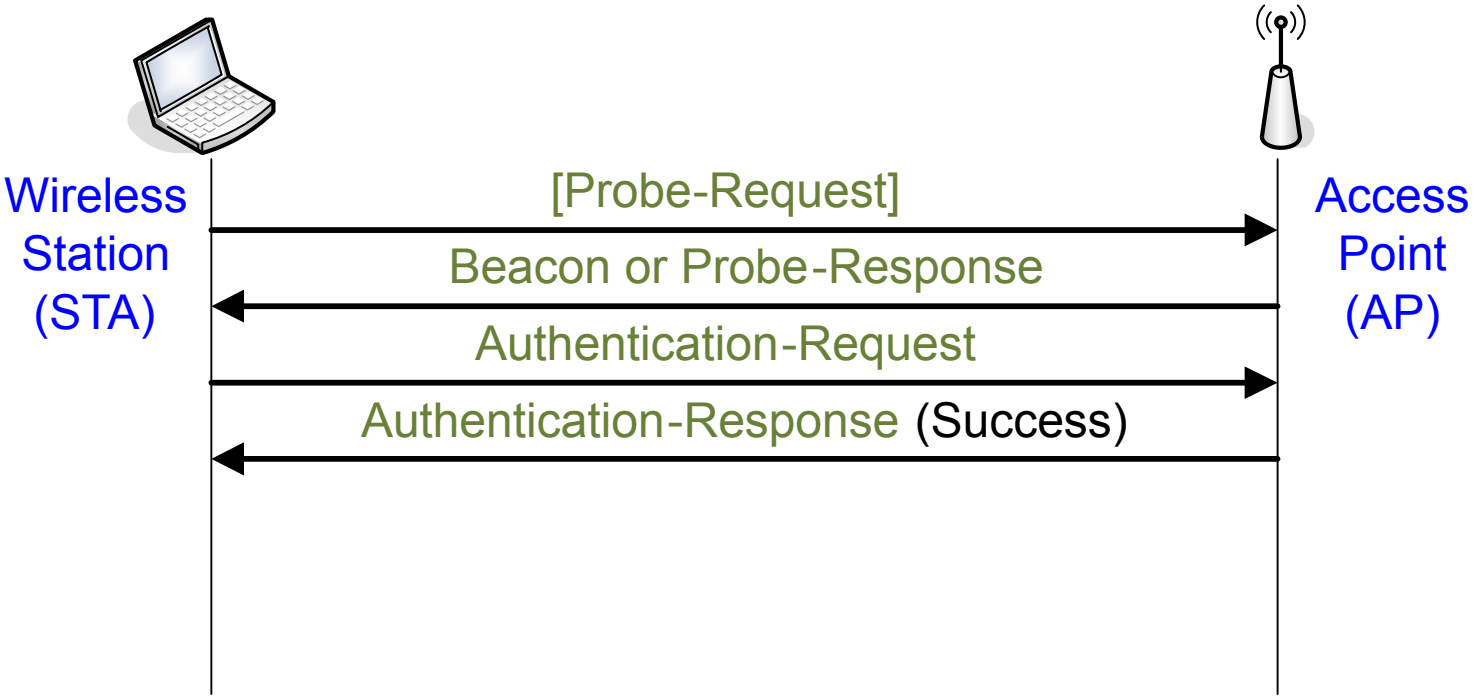
Joining an Open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



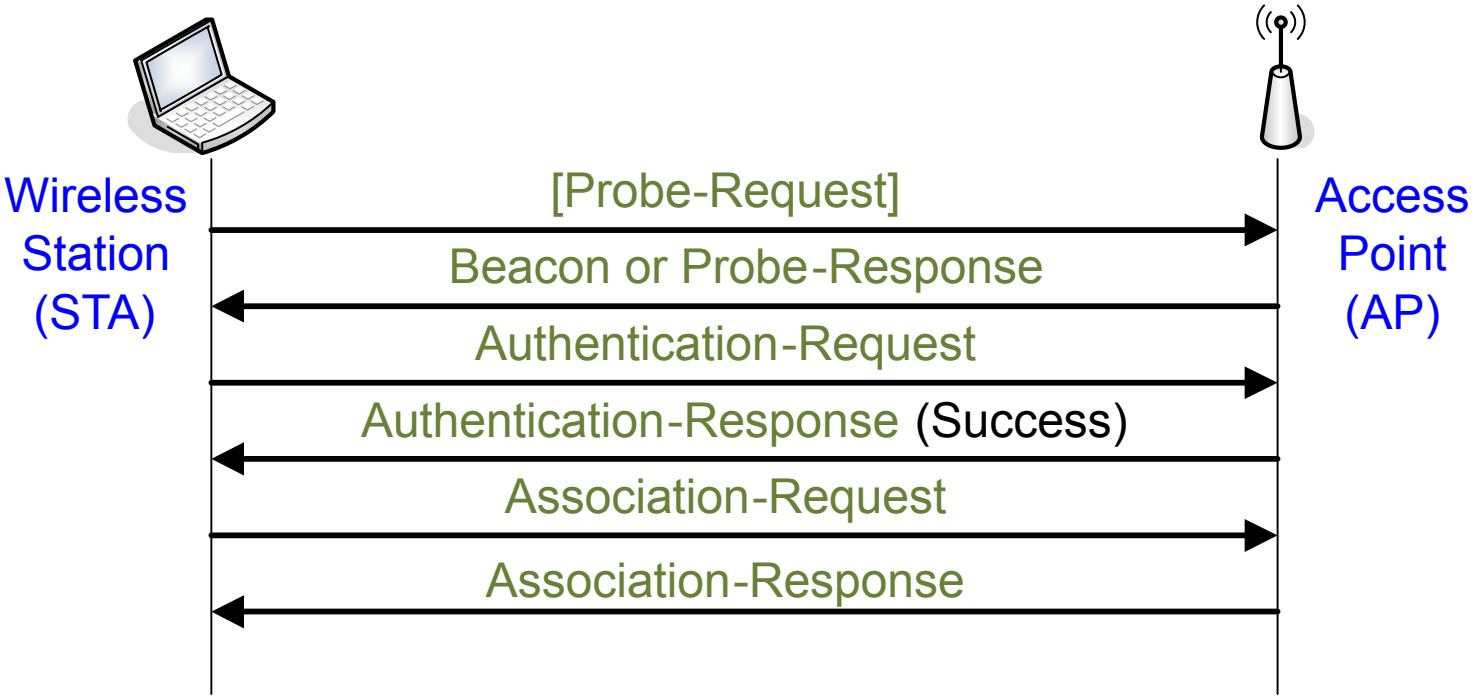
Joining an Open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



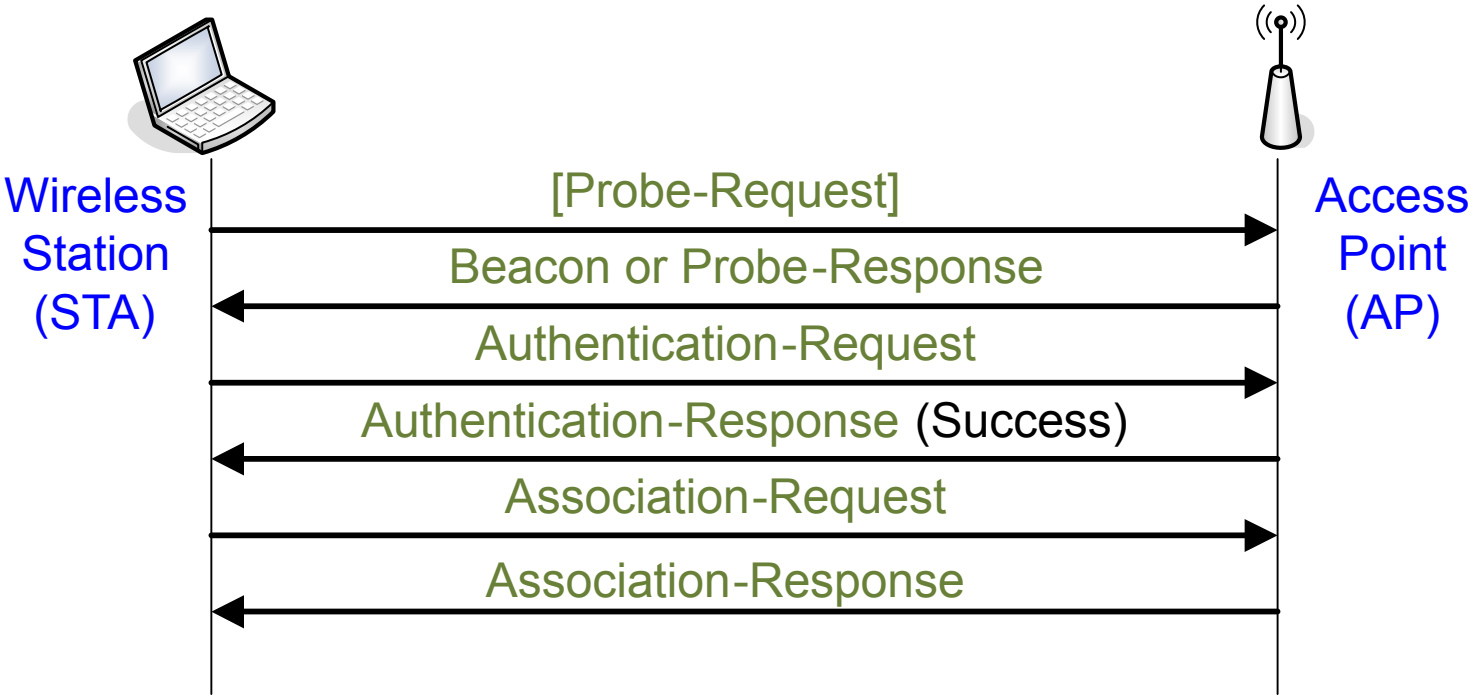
Joining an Open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



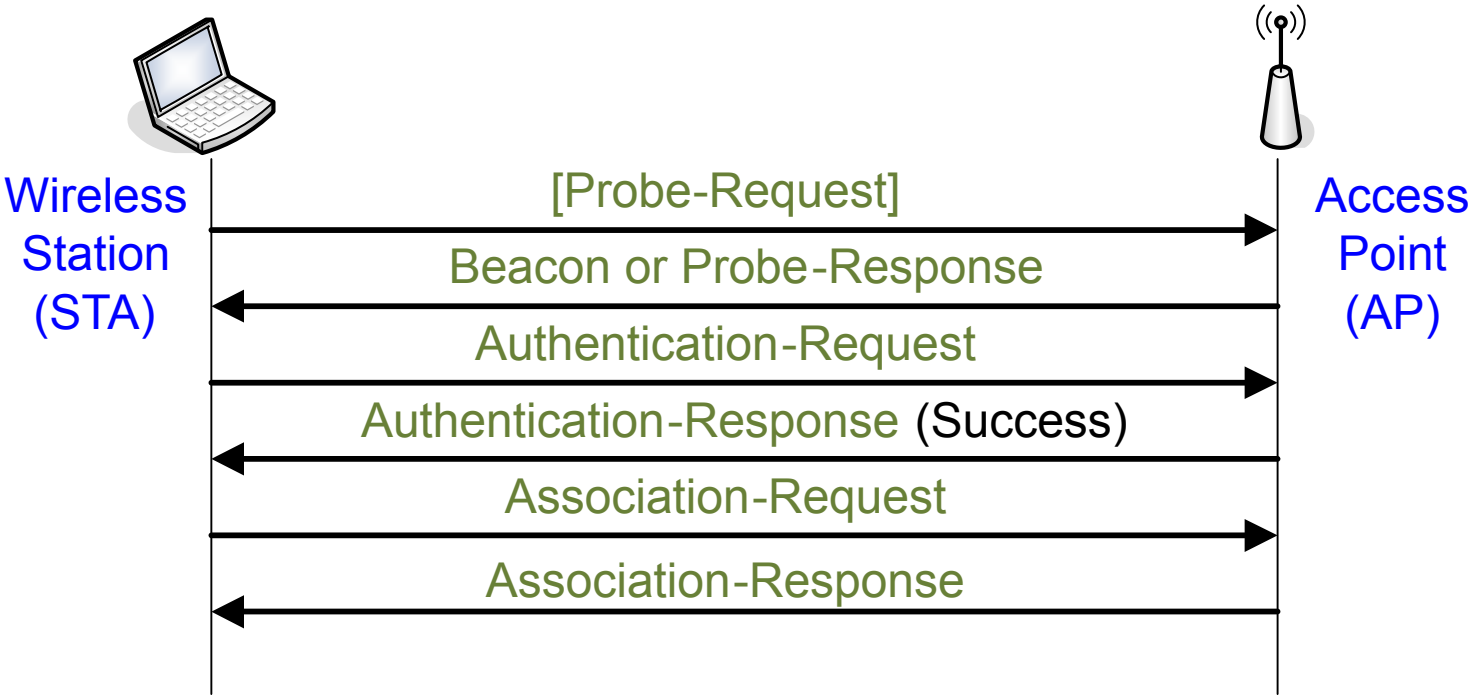
Joining an Open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off
- STA must specify SSID to the AP in association request



Joining an Open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off
- STA must specify SSID to the AP in association request

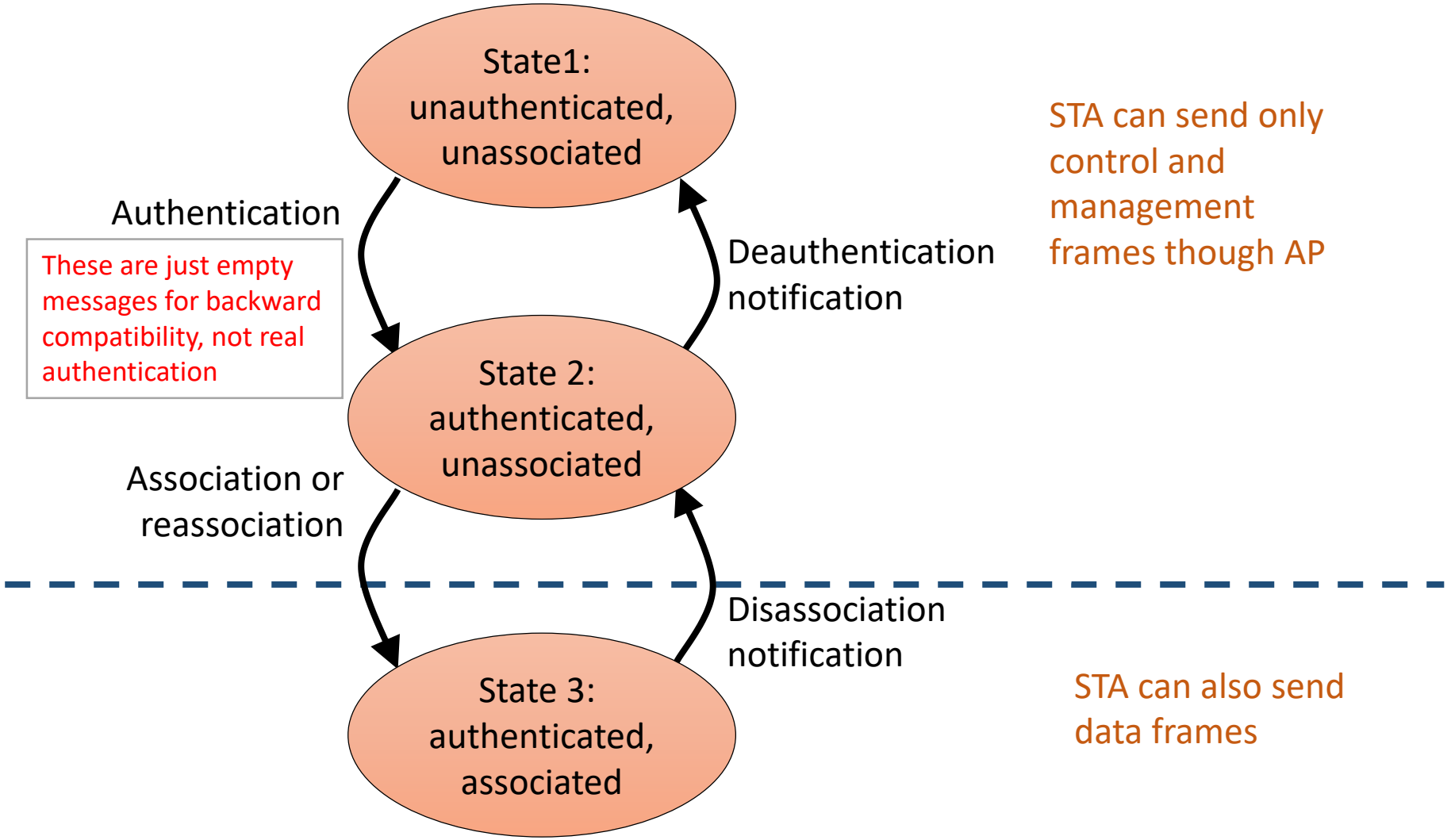


- Open system authentication = **no authentication**, empty authentication messages

Leaving a WLAN

- Both STA and AP can send a Disassociation Notification or Deauthentication Notification
- Include reason codes
  - station inactivity
  - station leaving

802.11 association state machine



REAL WLAN SECURITY: WPA2

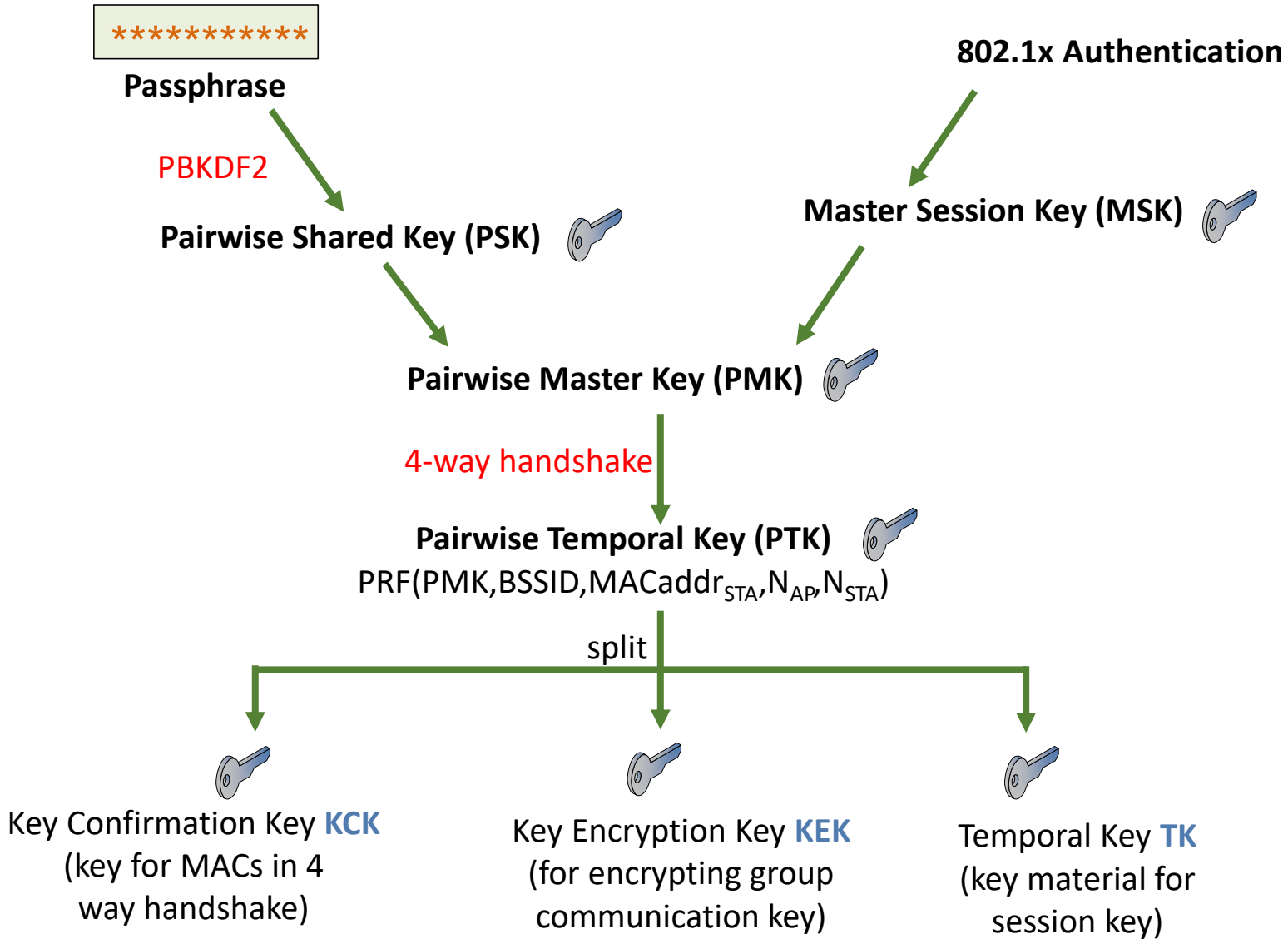
Real WLAN Security

- **Wireless Protected Access 2 (WPA2)**
  - WPA2 is the Wi-Fi alliance name for the 802.11i amendment to the IEEE standard, which is now part of 802.11-2016
  - Robust security network (RSN) = name of WPA2 in the standard
  - Uses 802.1X for access control
  - Uses EAP for authentication and key exchange, eg. EAP-TLS
  - Confidentiality and integrity protocol AES-CCMP

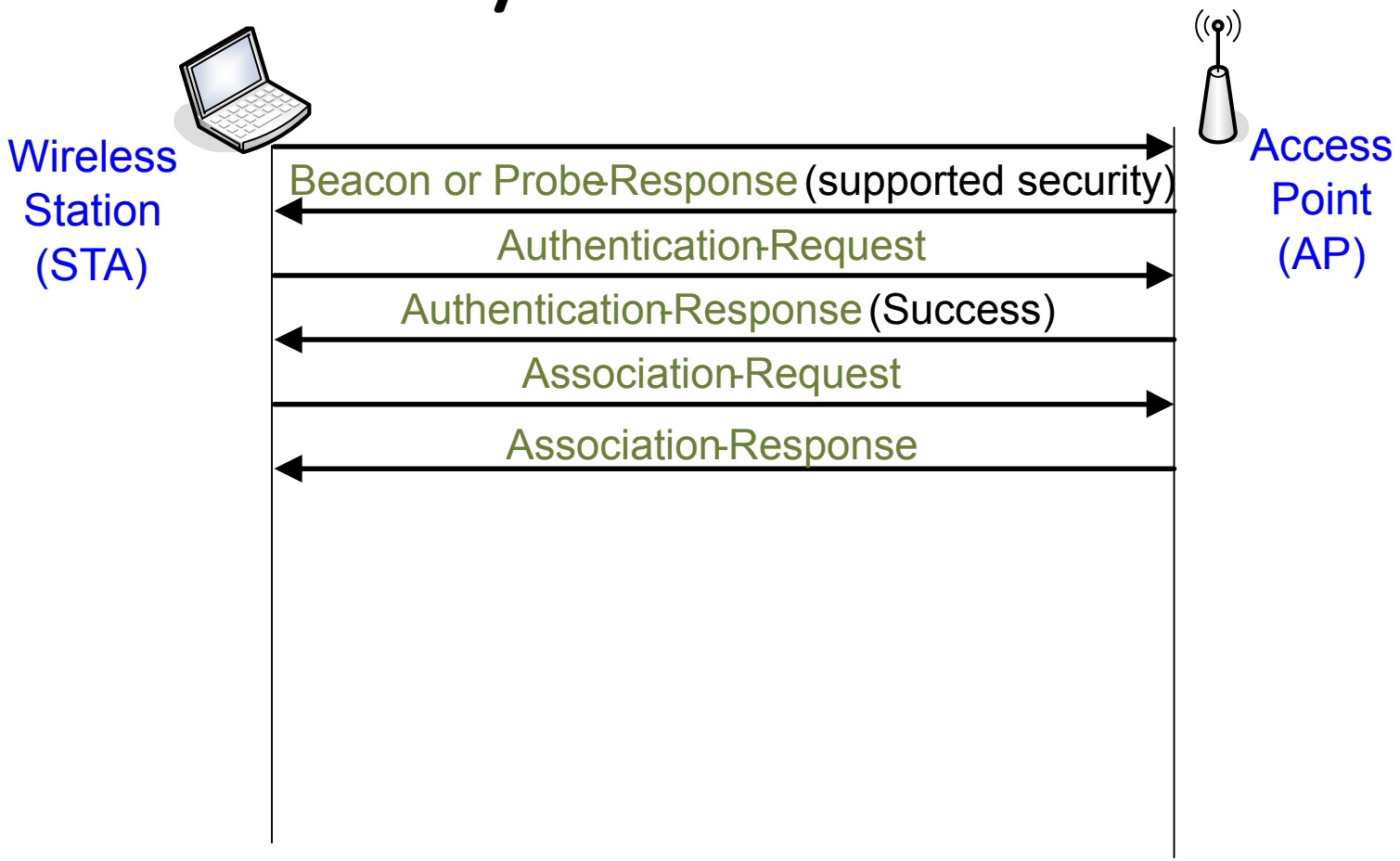
WPA2

- PSK Personal mode: Pre-Shared Keys
- Enterprise: strong authentication

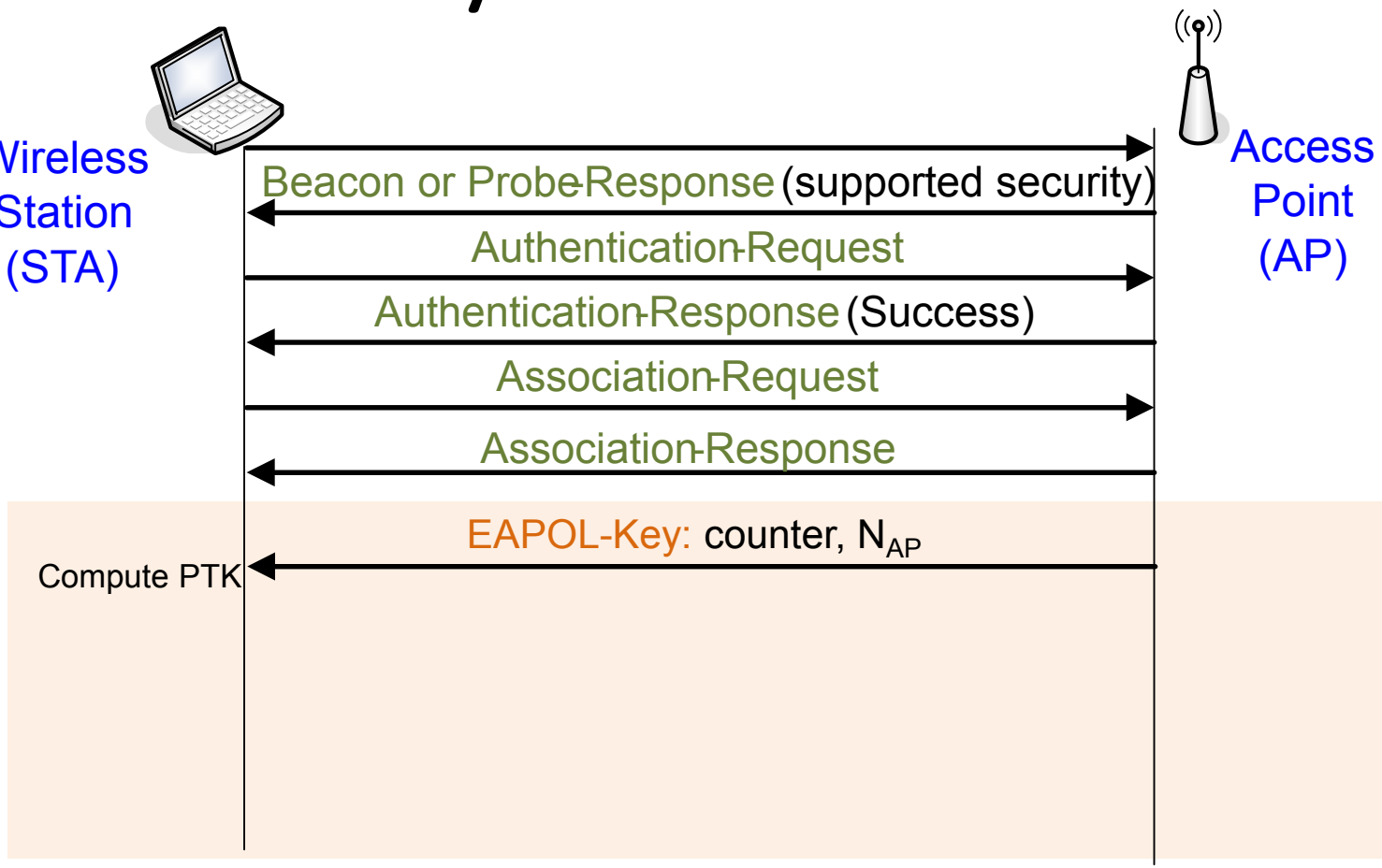
RSN Key Hierarchy



WPA2 - 4 way Handshake

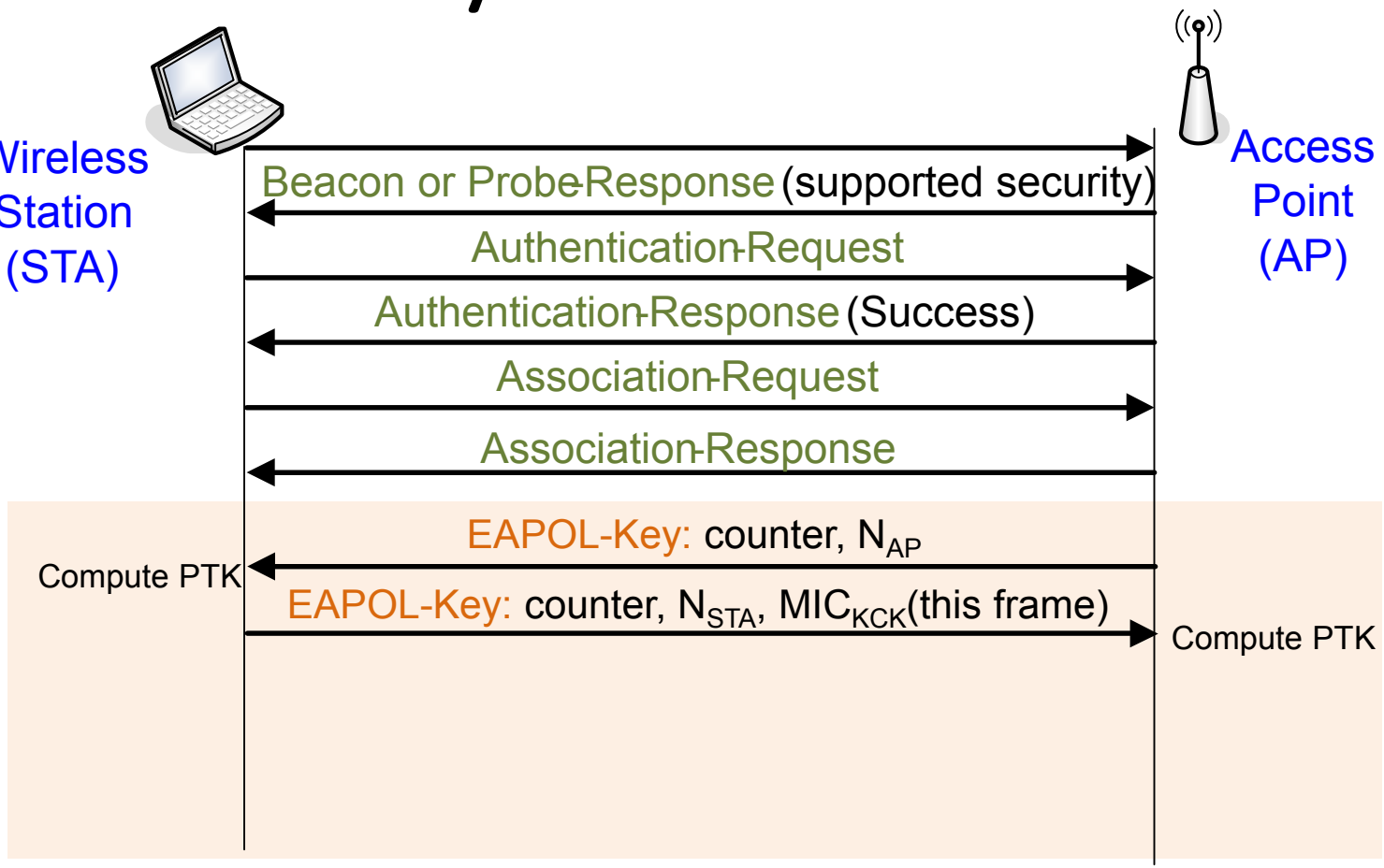


WPA2 - 4 way Handshake



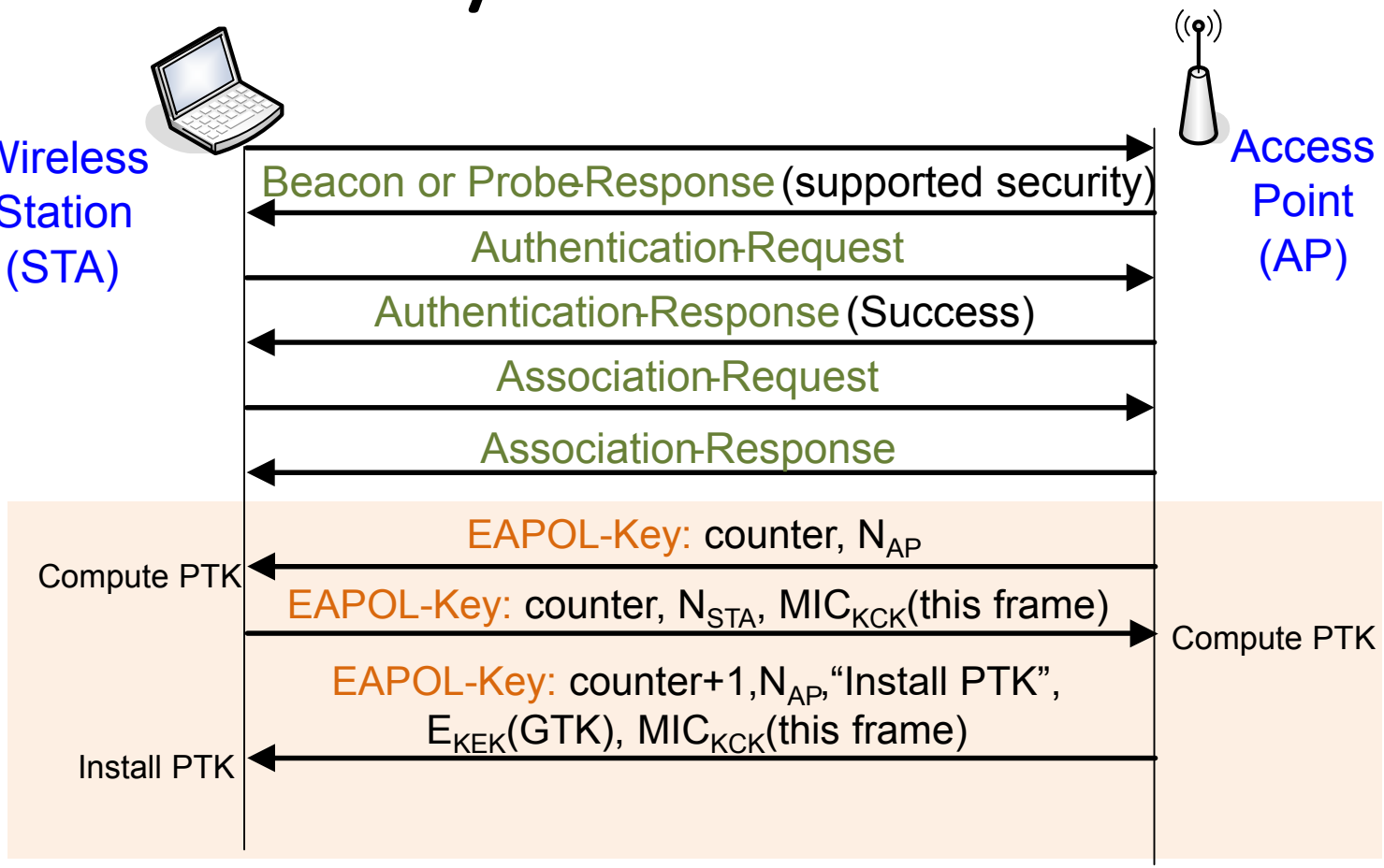
PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 - 4 way Handshake



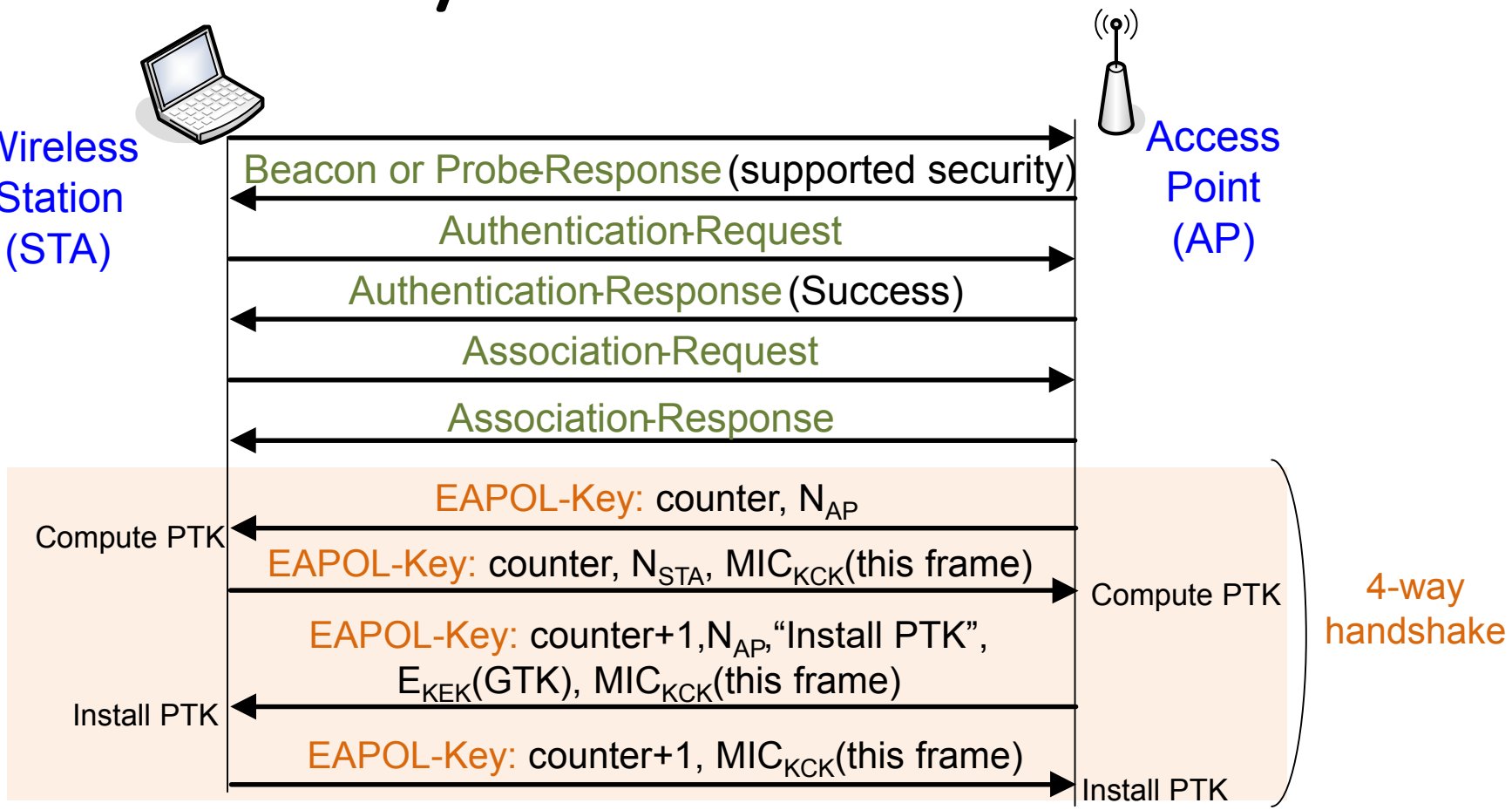
PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 - 4 way Handshake



PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 - 4 way Handshake

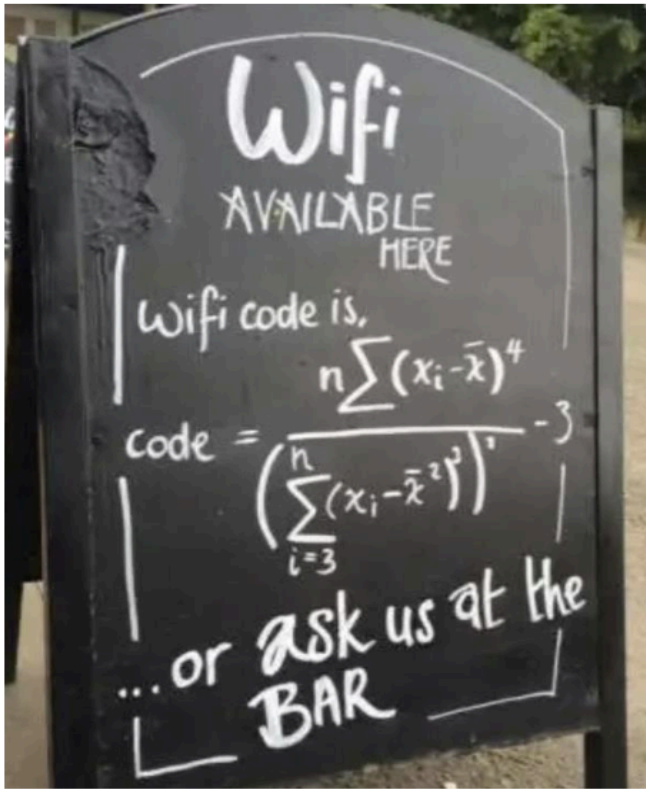


PMK = key derived from Passphrase /802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

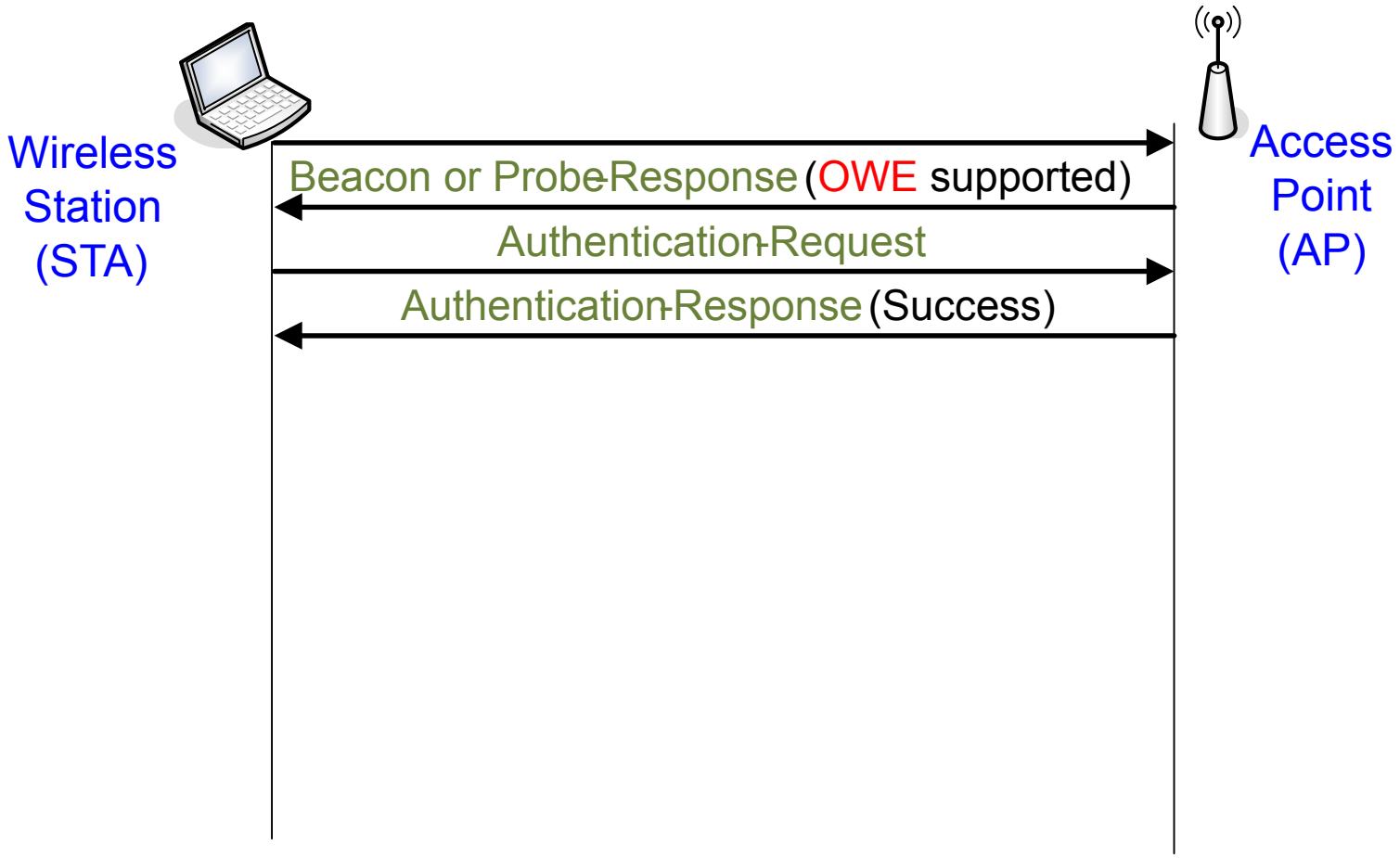
REAL WLAN SECURITY: WPA3

WPA3 Enhanced Open

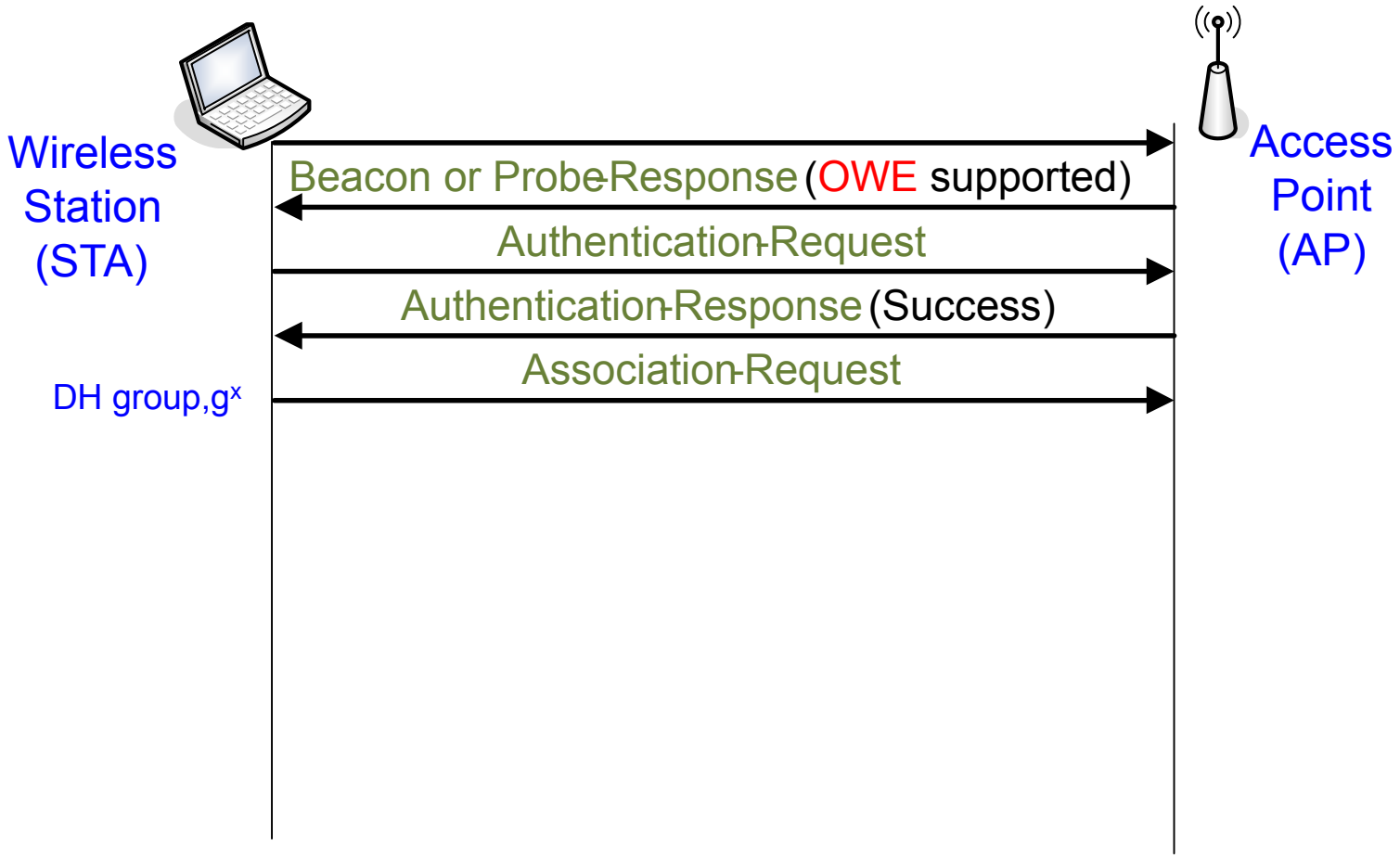
- Open networks used in cafes and airports
  - Better user experience than asking for passphrase
- WPA3 Enhanced Open provides Opportunistic Wireless Encryption (OWE) for open networks - RFC 8110
- Station and AP perform Diffie-Hellman (DH) exchange during association
- A PMK is derived from DH shared secret
- PMK is used in 4 - way handshake as before



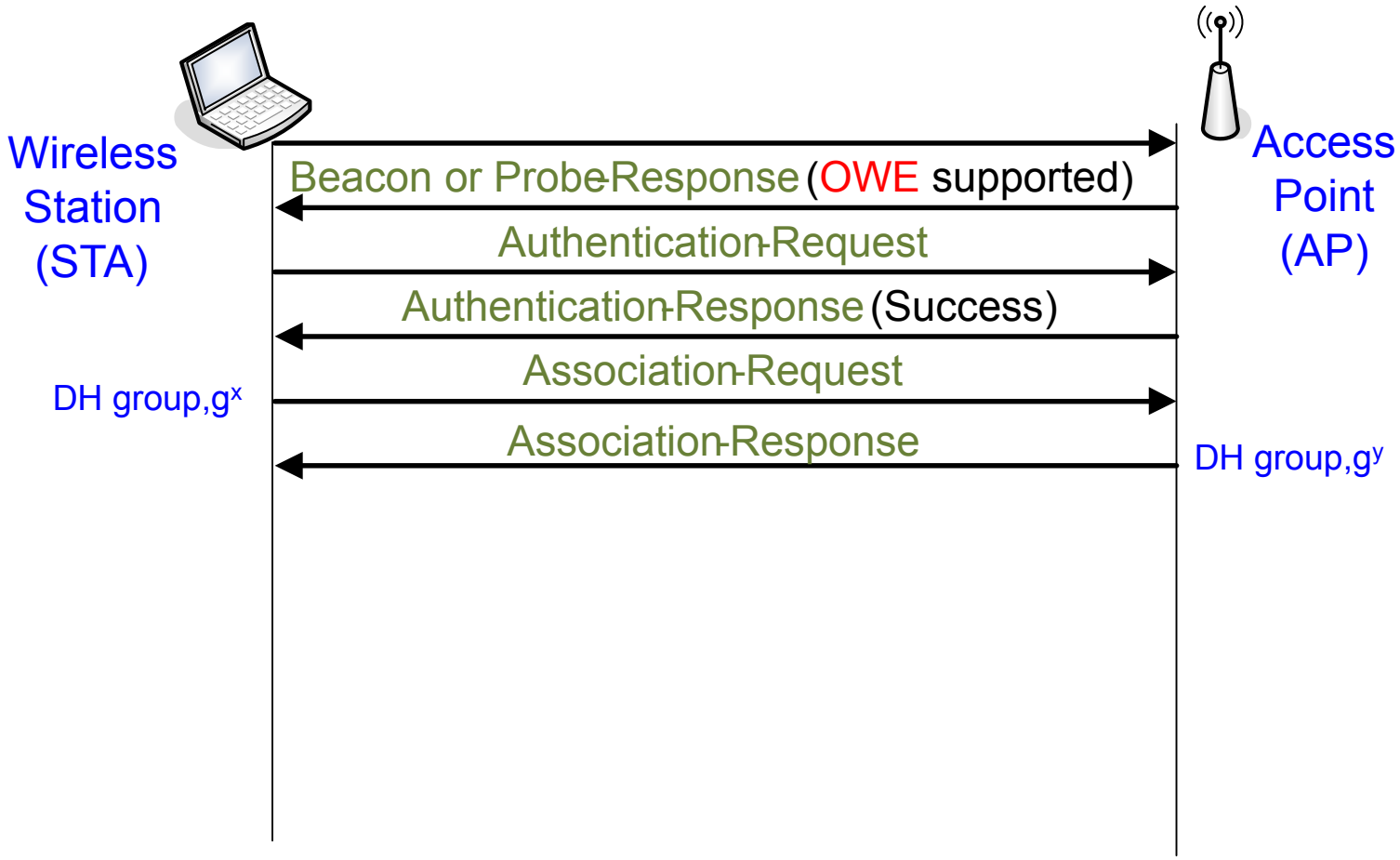
WPA3 Enhanced Open



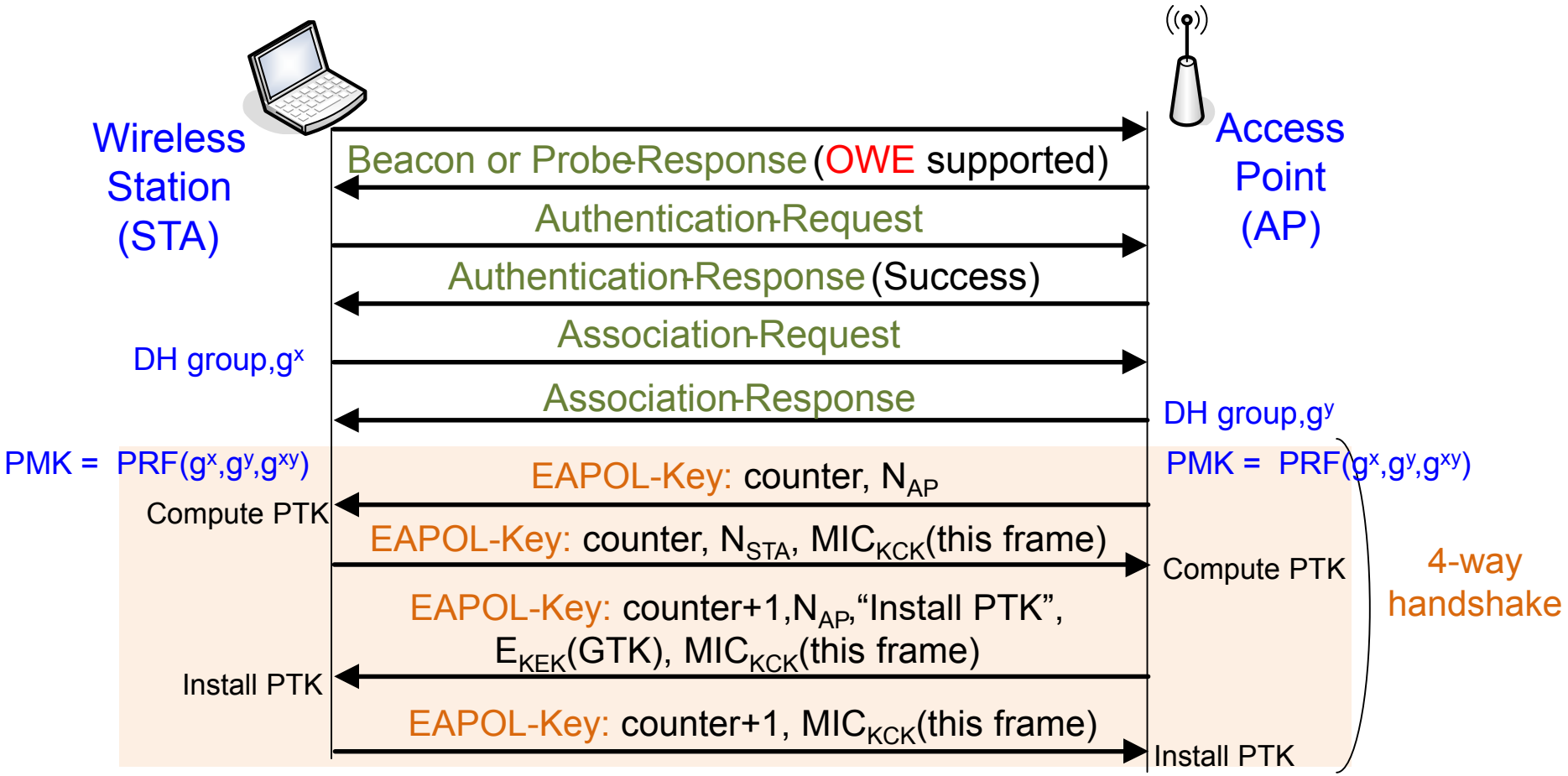
WPA3 Enhanced Open



WPA3 Enhanced Open



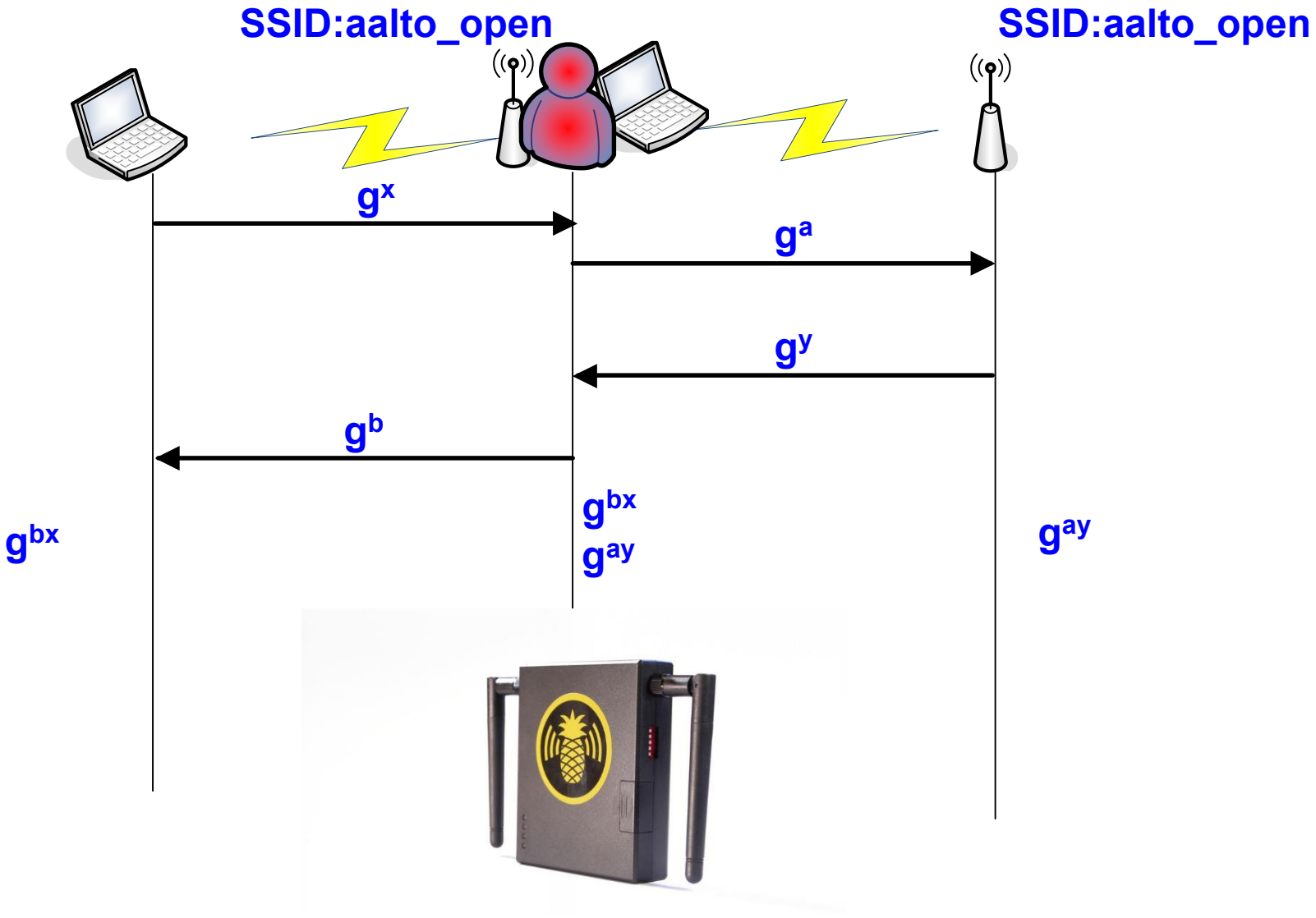
WPA3 Enhanced Open



WPA3 Enhanced Open

- Both ECC and FFC based Diffie-Hellman supported
- OWE is encryption NOT authentication
  - Susceptible to active MiTM attack
  - Does NOT prevent evil twin APs

WPA3 Enhanced Open - MitM



WPA3 Enhanced Open

- Both ECC and FFC based Diffie-Hellman supported
- OWE is encryption NOT authentication
  - Susceptible to active MiTM attack
  - Does NOT prevent evil twin APs
- No prior contact between Station and AP for PMK
- Better than open authentication:
  - Passive attacker now needs to be active
  - Attacker cannot inject packets without active MiTM first
  - Forward secrecy when private keys are deleted
- Can do client authentication later with captive portal

WPA2 PSK Weaknesses

- With WPA(2) – the password or PSK us used for both “authentication” and encryption
- Susceptible to attacks and tools to crack a password are easily downloadable from the Internet
- Given the messages from the 4-way Handshake, the attacker loops through all passwords in the database computing values using a candidate password until it is able to verify message 3 or message 4
- No *forward secrecy*– guess the password and get the session keys for all past, present, and future exchanges
- When used for network access through an AP it allows anyone in “earshot” to crack the password and connect
- Brute force attacks/Dictionary Attacks: Amazon Cloud attack: performs 2,400,000 password checks per minute at $0.23/min– the size of the dictionary really doesn’t matter now!

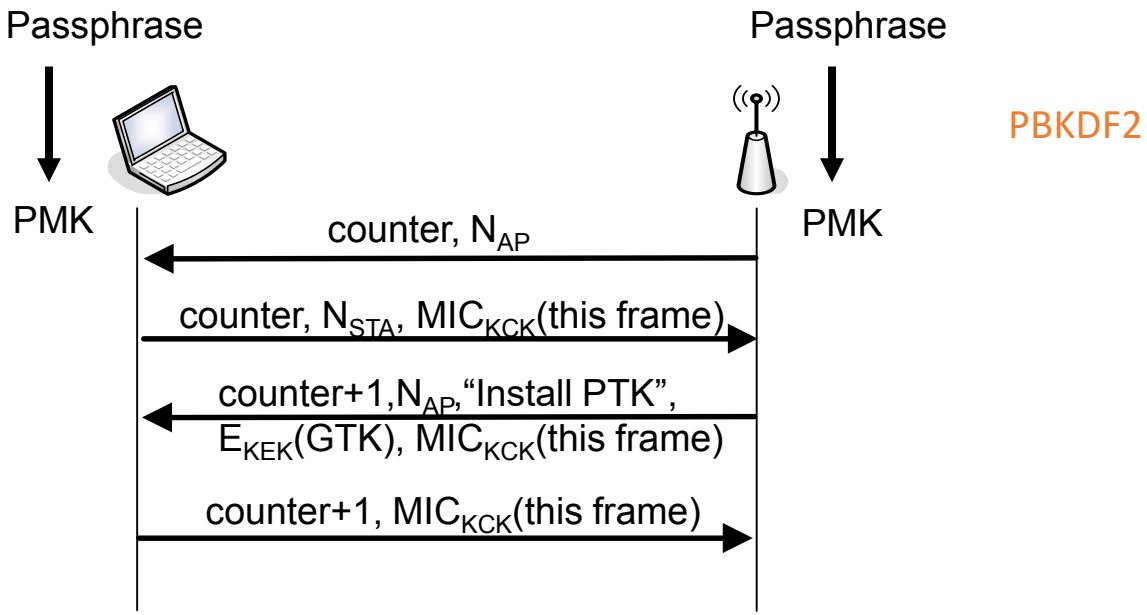
What is wrong with WPA2 PSK?

- With WPA2 PSK, your password is used to generate the PairwiseMasterKey(PMK)
- This is how the exchange works:
  - On both sides, make your weak passphrase (“password”) a bit stronger: PSK = pseudorandom (PBKDF2 algorithm) of Passphrase, SSID, SSIDlength, to produce a 256-bit string
  - The process is done the same way on the AP and client, so they have the same PSK. This PSK is the PMK.

PSK = PBKDF2 (PassPhrase, ssid, ssidLength, 4096, 256)

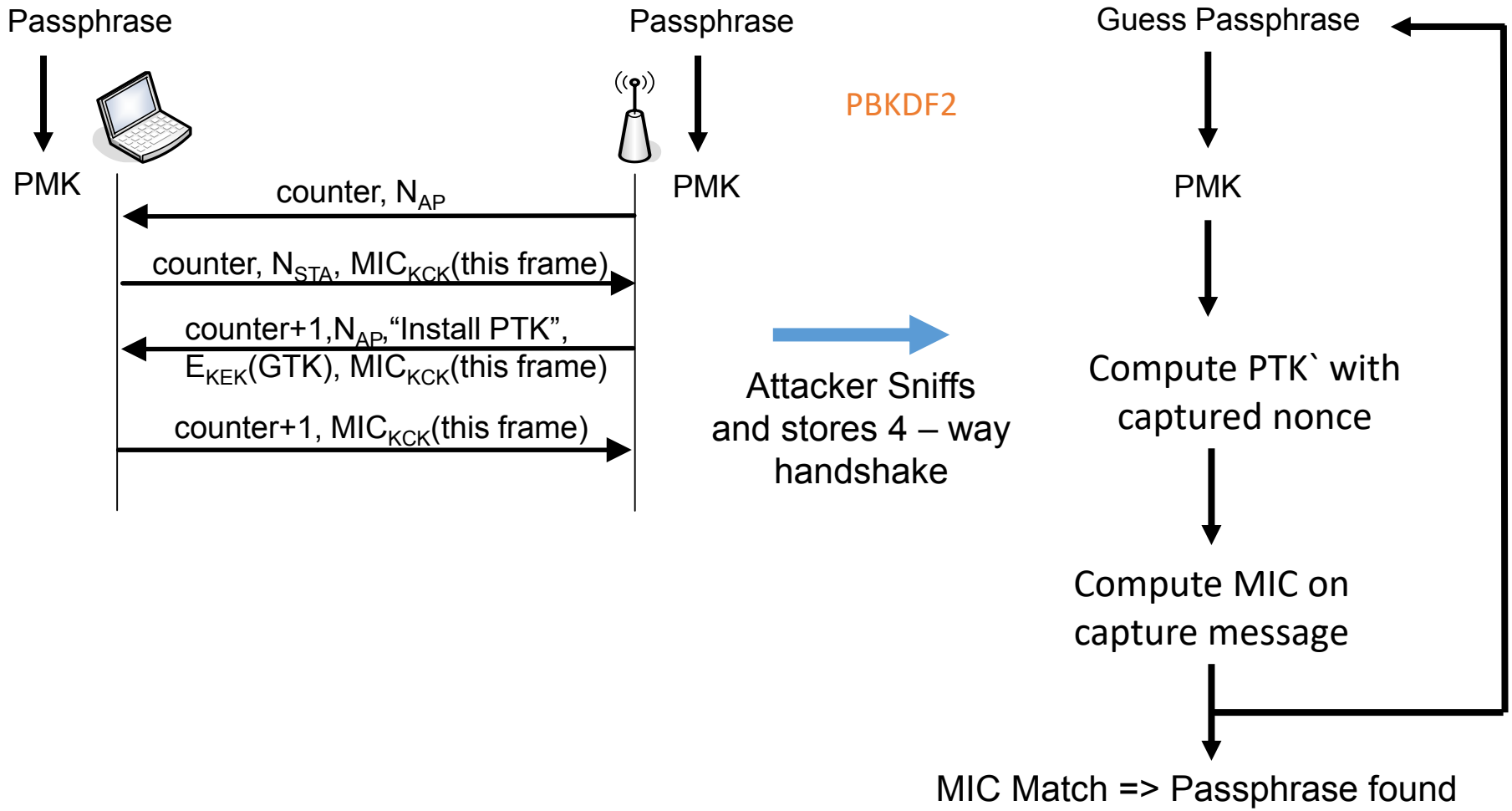
PSK = PBKDF2 (PassPhrase, ssid, ssidLength, 4096, 256)

WPA2 – Personal: Weakness

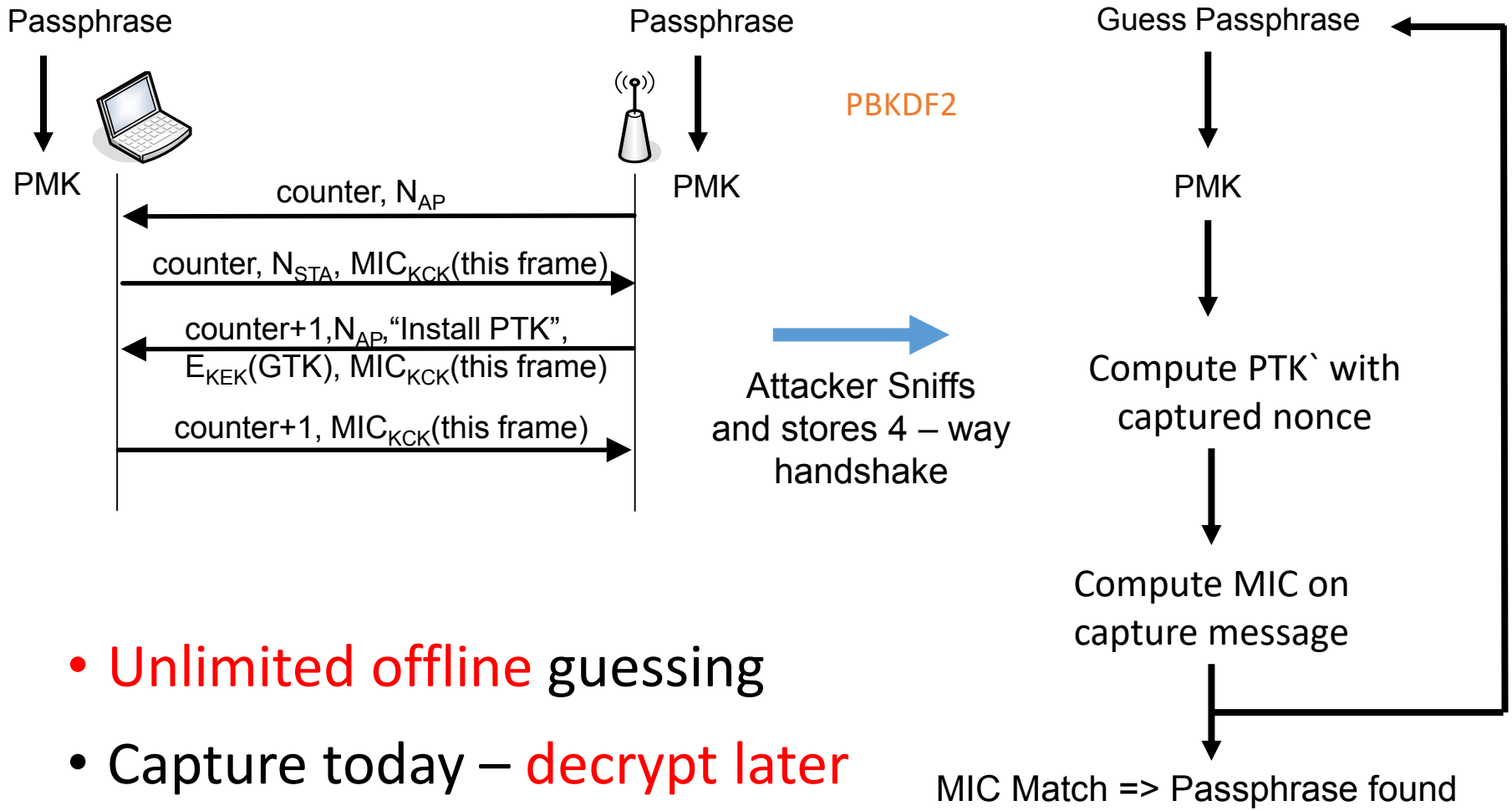


PBKDF2

WPA2 – Personal: Weakness



WPA2 – Personal: Weakness



- Unlimited offline guessing
- Capture today – decrypt later

Why is it easy to crack WPA2-Personal?

All I need is a capture of the 4-Way handshake

- How?– deauth the client

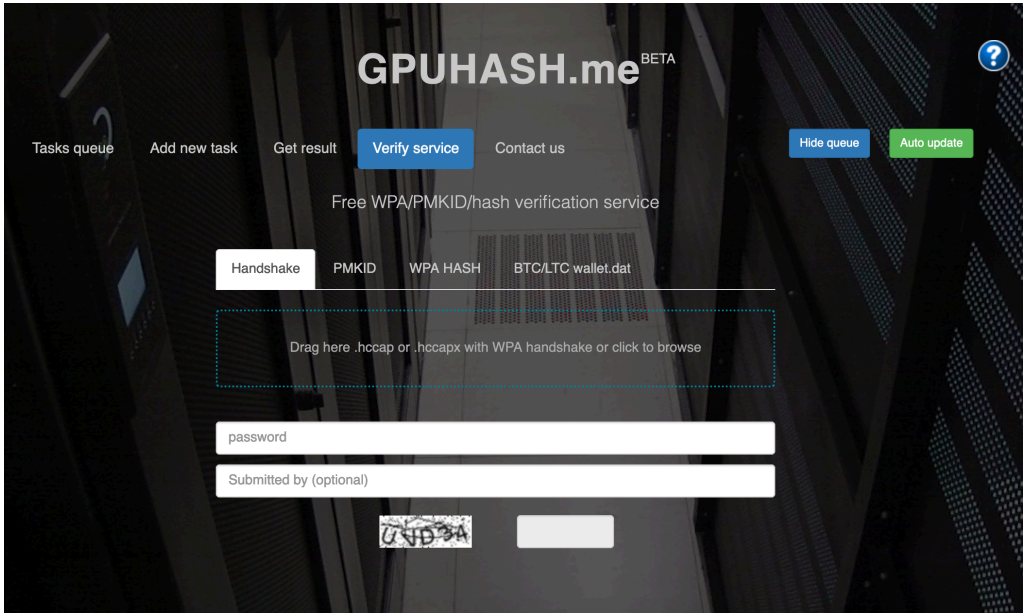
Upload the entire pcap

Customers/end users deploy weak passwords

Results in a easy access to the wired network (I don't care about capturing over the air data)

If the intent is to get wired side access MAC based auth + PSK is trivial to bypass

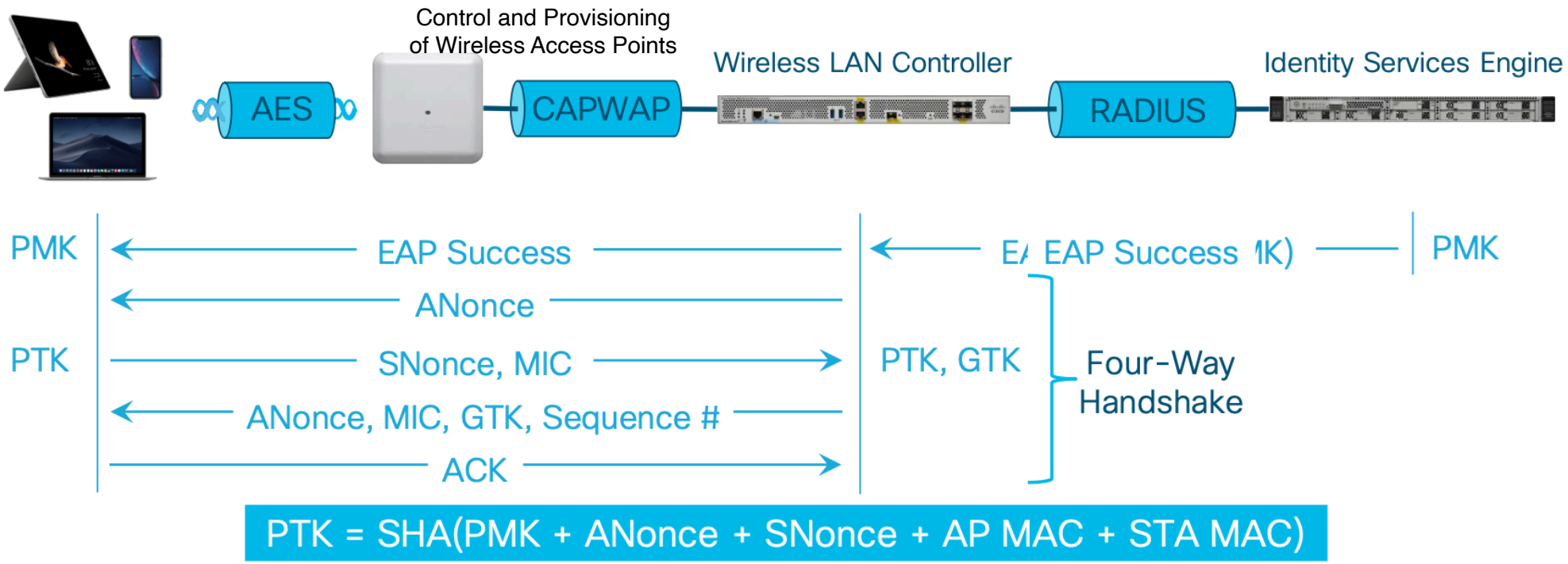
Think IoT, Medical devices, TV's etc etc



WPA3 PAKE : Dragonfly

- WPA3 uses Password Authenticated Key Exchange (PAKE) for preventing password guessing
- WPA3 uses a variant of Dragonfly – RFC 7664 as PAKE
- Original protocol called Simultaneous Authentication of Equals (SAE) defined in 802.11s in 2016
  - Standard for security in mesh networks
- Offline attacker can perform only one password guess on data before it is useless
- A live attacker physically present in the network can perform more guesses but devices can setup protection against such repeated guessing - denial of service (DoS)

What about WPA2 Enterprise?



Caution: Threat shifts from a weak PSK to weak user passwords for logon

Key Reinstallation AttaCK (KRACK)

- Once a target network is selected, the attacker clones the real AP onto a separate channel called the Rogue Access Point
- Attacker will send spoofed 802.11 management frames from the Rogue AP in an attempt to get clients to connect to it instead of the real AP, resulting in a man-in-the-middle position
- Right before the 3rd step of the 4-way handshake, a forged ANonce from the Rogue AP is sent forcing the target to re-install the shared key, essentially repeating step 1
- As this process repeats multiple times, the key becomes predictable allowing the attacker to decrypt packet data. It may also be possible for the attacker to inject malicious packets

Mitigation PMF

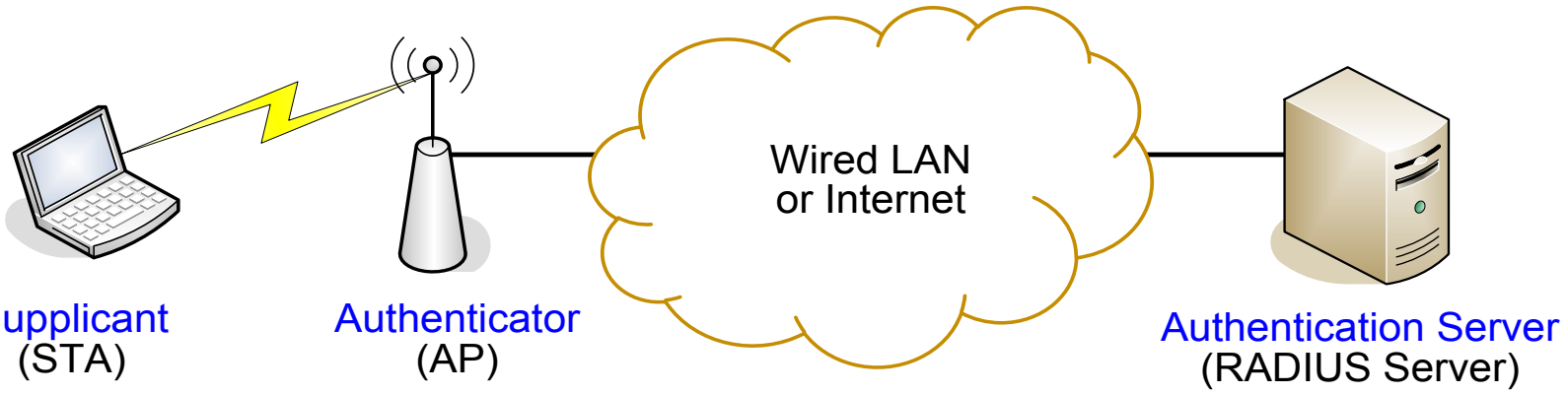
- Implementing Protected Management Frame (802.11w) will helps mitigate Man-in- the-Middle attacks
- The 802.11w protocol applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service.
- These include: Disassociation, De-authentication, and Robust Action frames (Like FT).

REAL WLAN SECURITY: 802.1X

IEEE 802.1X

- **Port-based access control** — originally intended for enabling and disabling physical ports on switches and modem banks
- Conceptual controlled port at WLAN AP
- Uses Extensible Authentication Protocol (EAP) to support many authentication methods;
- Starting to be used also in Ethernet switches

802.11/802.1X architecture



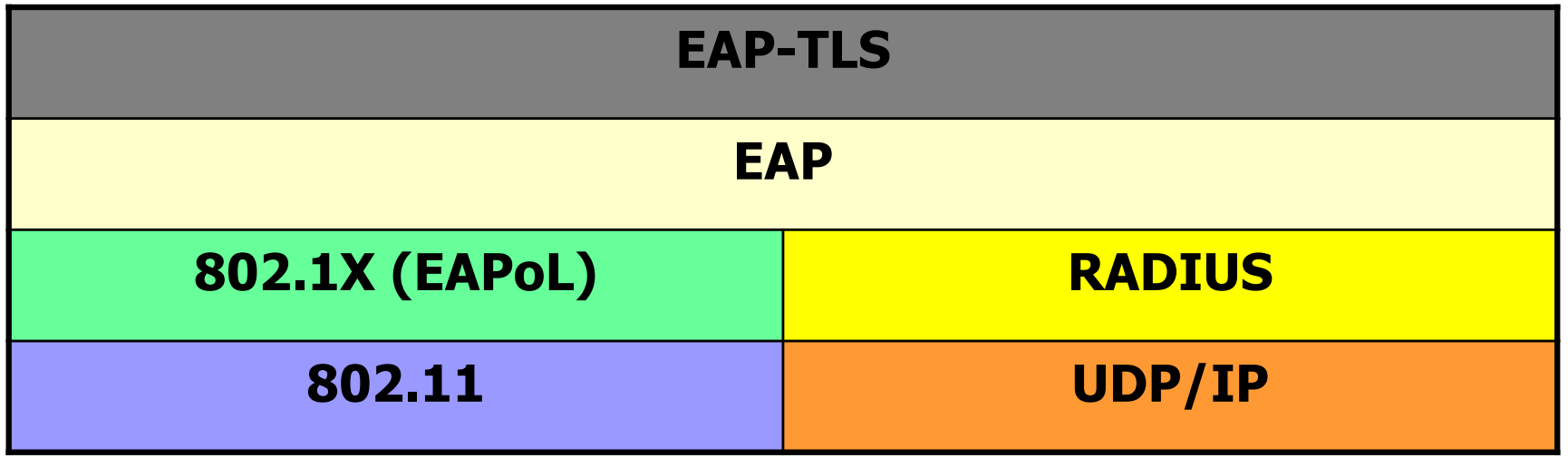
- Supplicant wants to access the wired network via the AP
- Authentication Server (AS) authenticates the supplicant
- Authenticator enables network access for the supplicant after successful authentication

EAP

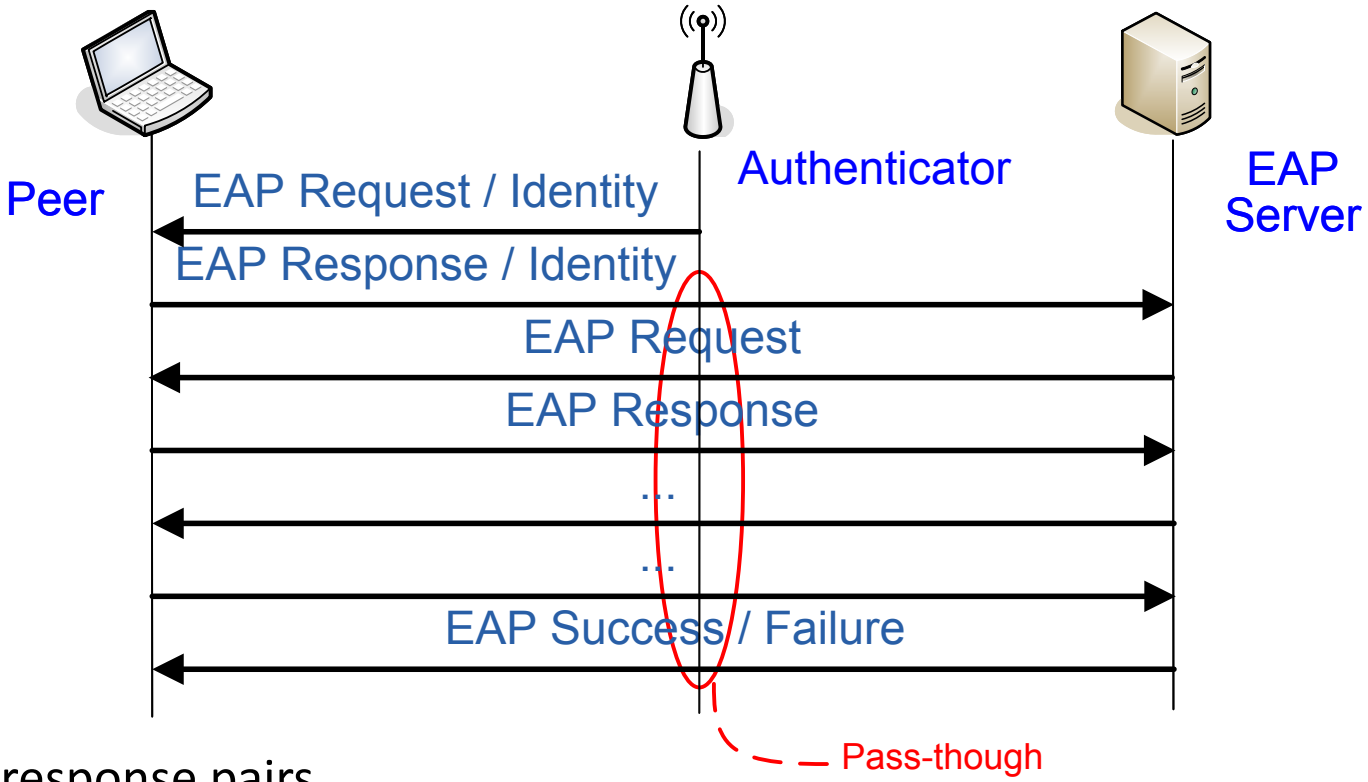
- **Extensible authentication protocol (EAP)** defines generic authentication message formats: Request, Response, Success, Failure
- Security is provided by the authentication protocol carried inside EAP, not by EAP itself
- EAP supports many authentication protocols: EAP-TLS, PEAP, EAP-SIM, ...
- Used in 802.1X between supplicant and authentication server
- EAP term for supplicant is peer, reflecting the original idea that EAP could be used for mutual authentication between equal entities

802.1x Architecture

- Allows choice of auth. methods using EAP
  - Chosen by peers at authentication time
  - Access point doesn't care about EAP methods
- Requires some authentication server
  - RADIUS is the de facto back-end protocol

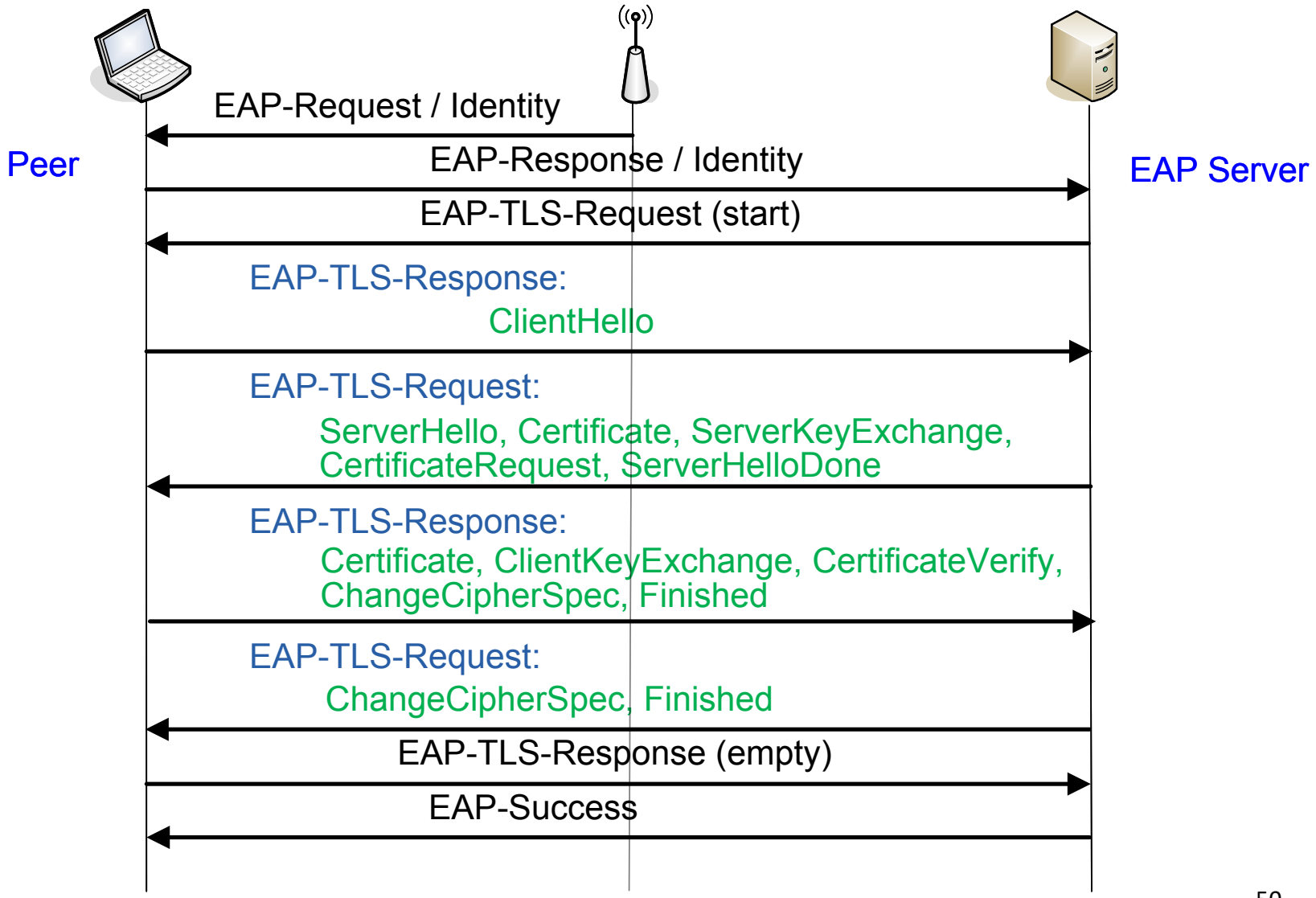


EAP protocol

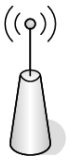


- Request-response pairs
- User identified by **network access identifier (NAI)**: username@realm
- Allows multiple rounds of request-response, originally for mistyped passwords
- Additionally, the EAP server will tell Authenticator to open the port

EAP protocol example – EAP TLS

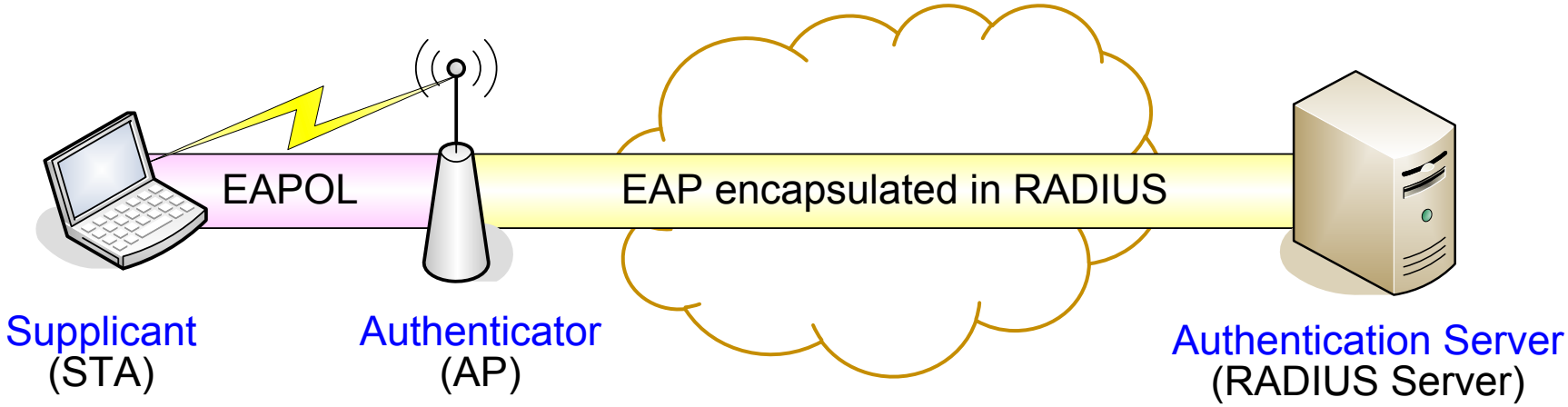


Terminology

			
TLS	Client		Server
EAP/AAA	Peer	Authenticator	EAP server / Backend authentication server
802.1X	Supplicant	Authenticator	Authentication server (AS)
RADIUS		Network access server (NAS)	RADIUS server
802.11	STA	Access point (AP)	

Confused yet?

EAP encapsulation

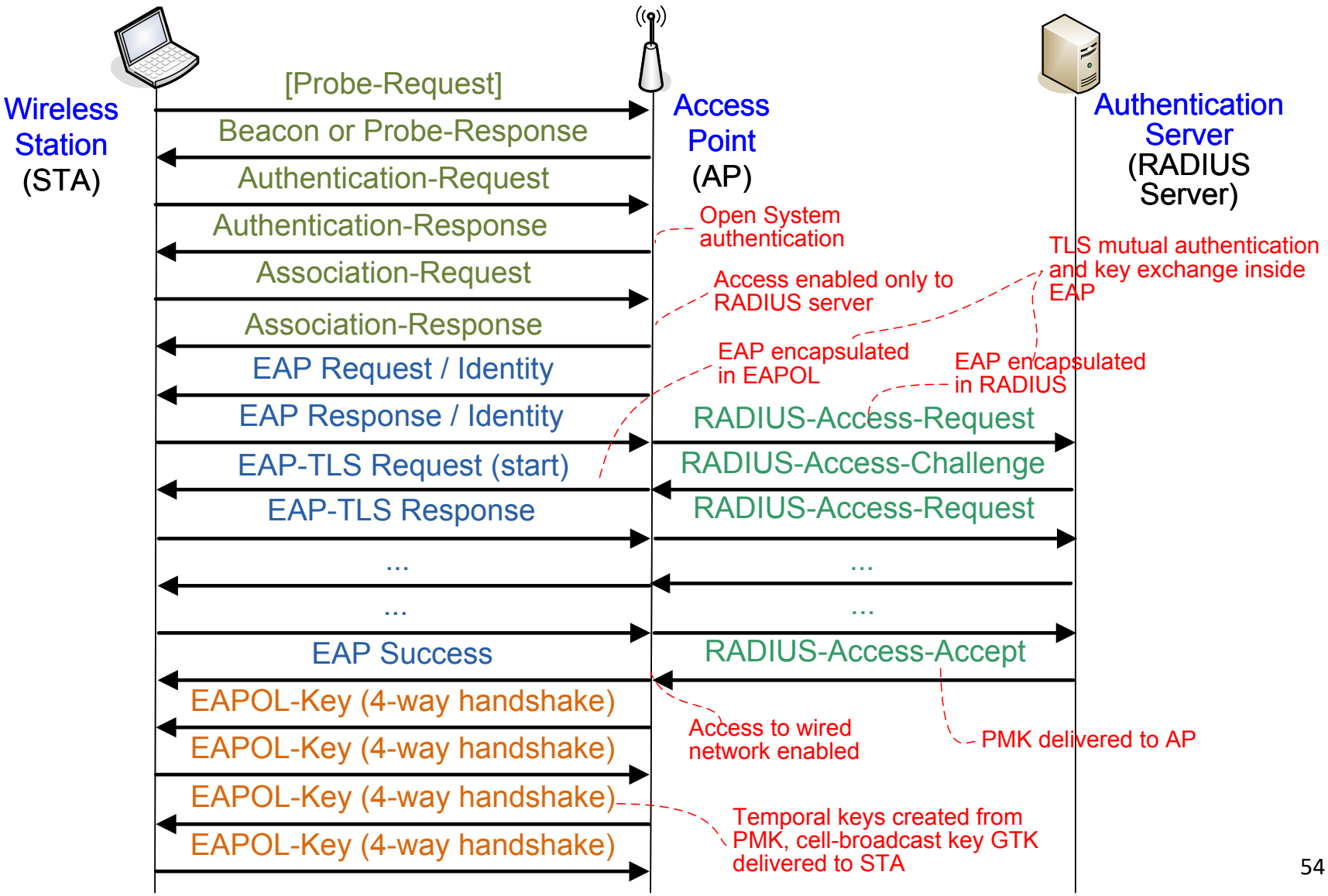


- On the wire network, EAP is encapsulated in RADIUS attributes
- On the 802.11 link, EAP is encapsulated in EAP over LAN (EAPOL)
- In 802.1X, AP is a pass-through device: it copies most EAP messages without reading them

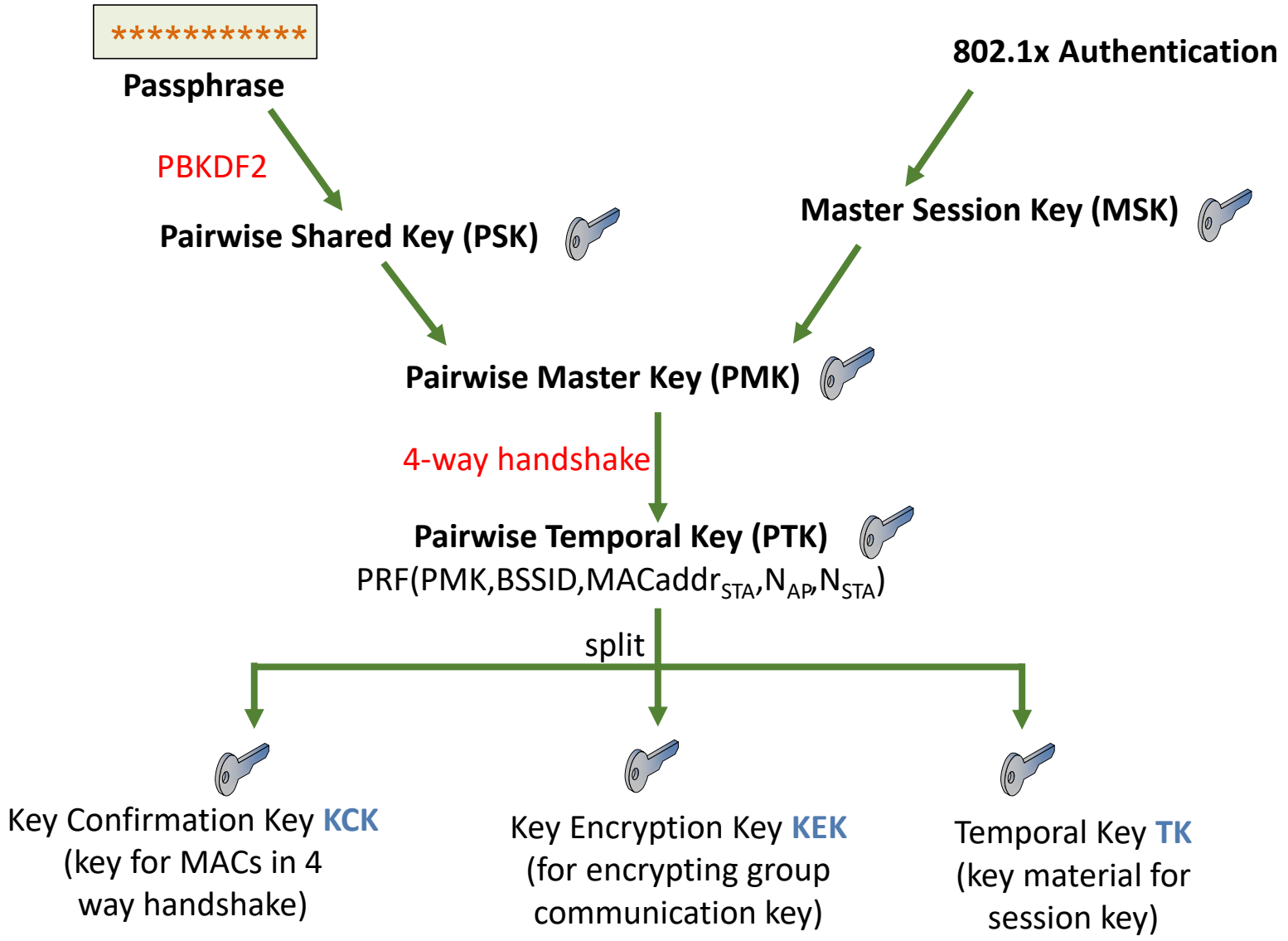
RADIUS

- Remote access dial-in user service (RADIUS)
  - Originally for centralized authentication of dial-in users in distributed modem pools
- Defines messages between the network access server (NAS) and authentication server:
  - NAS sends Access-Request
  - Authentication server responds with Access-Challenge, Access-Accept or Access-Reject
- In WLAN, AP is the NAS
- EAP is encapsulated in RADIUS Access-Request and Access-Challenge; as many rounds as necessary
- RADIUS has its own security protocol based on shared keys between the endpoints (AP and server)

EAP protocol in context



RSN Key Hierarchy



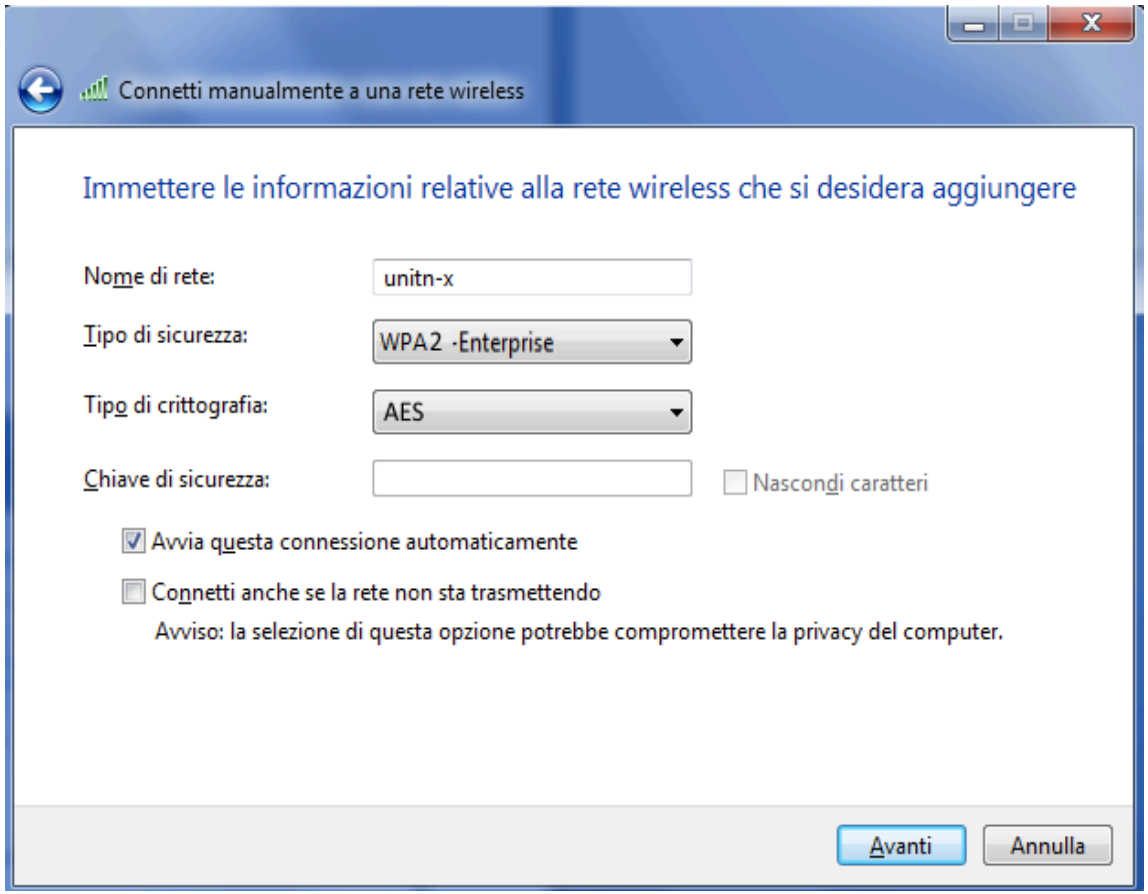
What does WPA2/3 achieve

- Authentication and access control prevents unauthorized network access
- Mutual authentication prevents association with rogue access points
- Encryption prevents data interception on wireless link
- Strong integrity check prevents data spoofing on wireless link
- 802.11w: management frame authentication
  - New key IGTK sent by STA in the four-way handshake (msg 3), management frames after that authenticated with MIC
  - Prevents deauthentication and disassociation spoofing after the four-way handshake (but not before)

Eduroam case study

- Eduroam is a federation for wireless roaming between educational institutions
- User is registered at the home university, which has a RADIUS server (AAAH)
- National educational and research network (NREN), e.g. GARR, operates a national roaming broker
- National brokers are connected to a regional broker for international roaming
- EAP authentication: user's home institution determines the EAP authentication method
  - UNITN uses PEAP
- Users identified by NAI: username@realm
  - NAI for UNITN users: firstname.lastname@unitn.it
- In PEAP, the outer NAI only needs to have only correct realm, but Aalto seems to require the username to be correct as well (should test if this is still the case)

Eduroam case study



- Eduroam uses WPA2 with AES encryption
- UNITN RADIUS server is radius.org.unitn.ot
- UNITN user's NAI looks like the email address, e.g. bruno.crispo@unitn.it
- UNITN users are authenticated with EAP-PEAP Microsoft's proprietary EAP method with TLS for the server authentication and password for the client
- Roaming between universities enabled by federation between RADIUS servers

Eduroam case study

- IN EAP-TLS and PEAP, the client authenticates the RADIUS server based on a certificate
- To verify the certificate, the client needs to know:
  - trusted Cas
  - name of the RADIUS server
- On many clients, any commercial CA and any name in the certificate is accepted anyone with any commercial certificate can set up a fake AP and pretend to be the RADIUS server