09 Wireless Security

2020 Spring

Information Security

Teacher: Po-Wen Chi

neokent@gapps.ntnu.edu.tw

June 9, 2020

Department of Computer Science and Information Engineering,

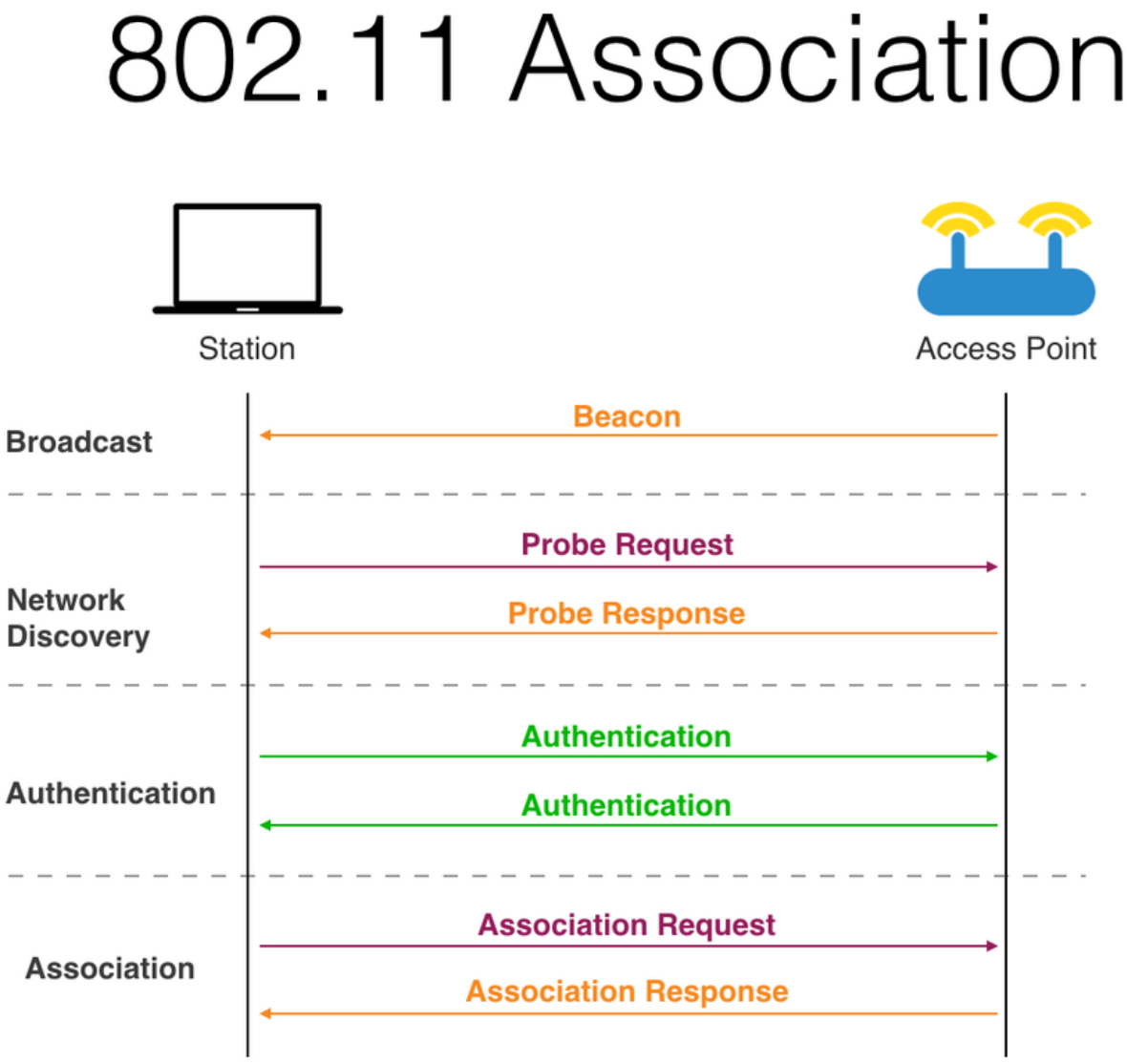
National Taiwan Normal University

IEEE802.11 Review

IEEE802.11

- IEEE 802.11 is part of the IEEE 802 set of **LAN** protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN).
- Frequency: including but not limited to 2.4, 5, and 60 GHz frequency bands.
  - 802.11b and 802.11g use the 2.4 GHz ISM band.

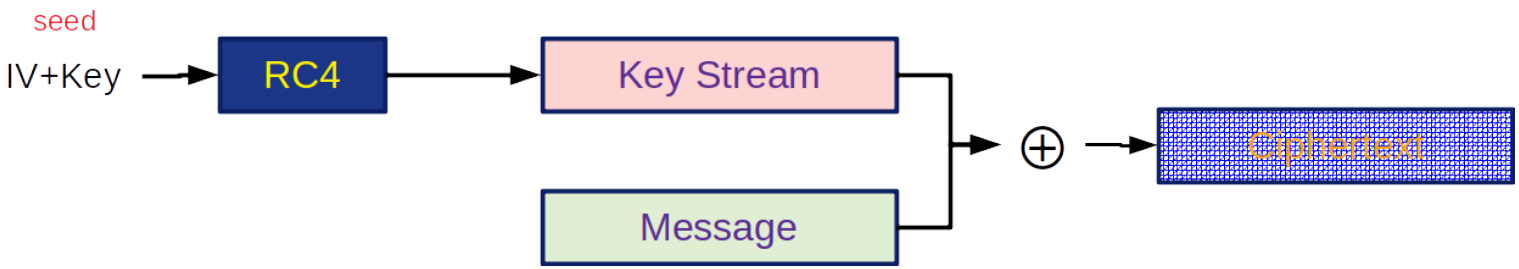
IEEE802.11 Association Process



WEP: Wired Equivalent Privacy

WEP

- Wired Equivalent Privacy.
- The original 802.11 standard ratified in 1997.
- Based on RC4.
  - IV: 24bits = 3 bytes.
  - Key: 40bits or 104bits.



WEP Problems

1. IV is not long enough.
   - So the key stream will be easily repeated.
   - Crack WEP: `https://blog.gtwang.org/linux/aircrack-ng-cracking-wep-wifi-using-the-raspberry-pi/`
2. RC4 is not a good cipher.
   - The PRF is not good enough.

Current Status

- Most APs do not support WEP.
  - If you enable the hotspot feature on your mobile phone, can you select WEP as the security mode?

Current Status

- Most APs do not support WEP.
  - If you enable the hotspot feature on your mobile phone, can you select WEP as the security mode?
- However, some AP vendors insist that this is a mandatory feature for the compatibility issue.

Some Solutions in the Past

- **MAC filter**.
  - Every network adapter has its own MAC address.
  - So we can use **blacklist** or **whitelist** to protect our wireless network.

Some Solutions in the Past

- **MAC filter**.
  - Every network adapter has its own MAC address.
  - So we can use **blacklist** or **whitelist** to protect our wireless network.
  - Quiz: Do you agree that this is a good solution?

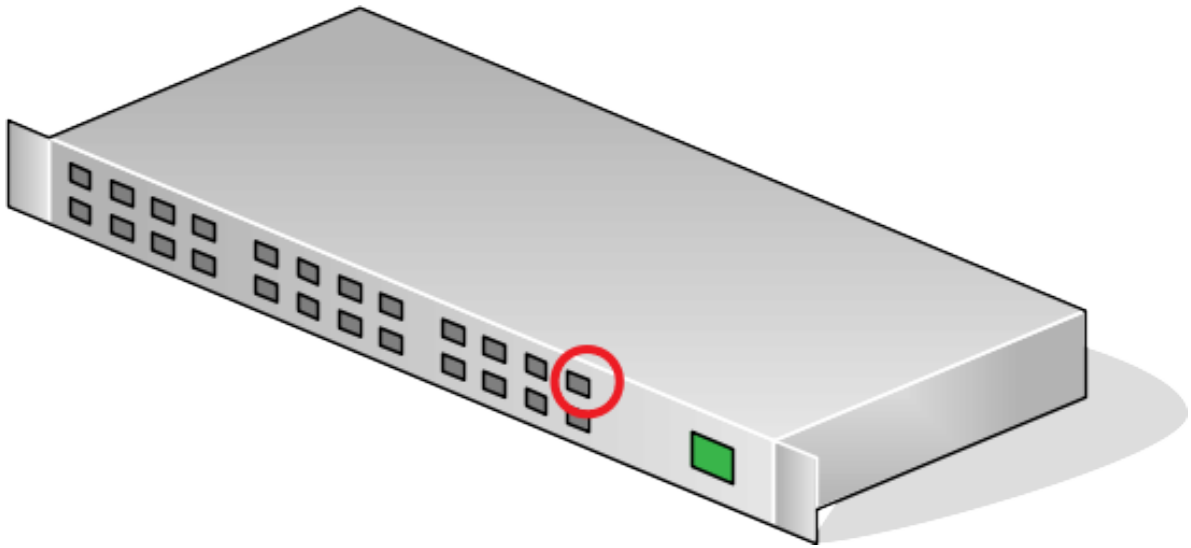
Some Solutions in the Past

- **MAC filter**.
  - Every network adapter has its own MAC address.
  - So we can use **blacklist** or **whitelist** to protect our wireless network.
  - Quiz: Do you agree that this is a good solution?
- IEEE 802.1X.

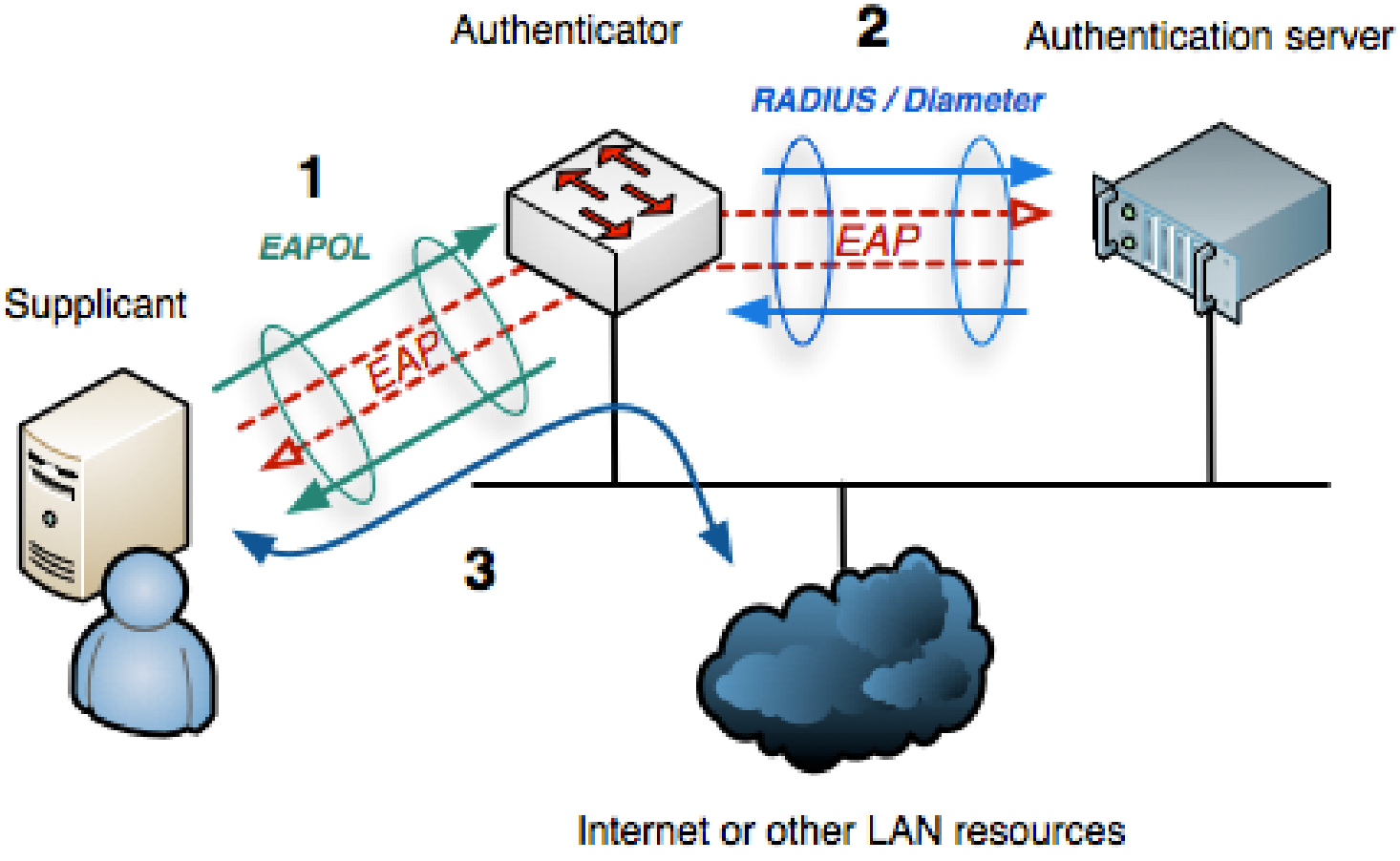
IEEE 802.1X

IEEE 802.1X

- Actually, this is not a wireless protocol.
- **Port-based** network access control.



Authentication Process



Roles

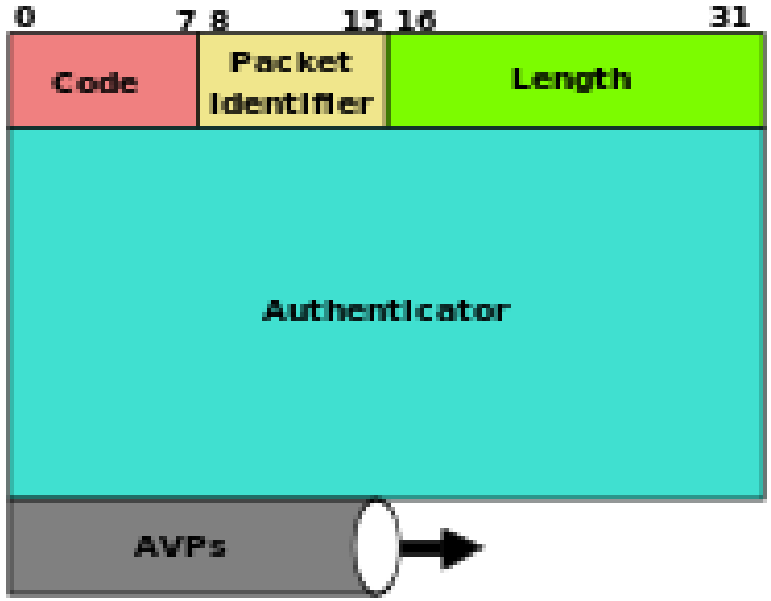
- **Supplicant:**
  - A client device that wishes to access the network.
- **Authenticator:**
  - A network device which determines pass or not.
- **Authentication Server:**
  - A server that stores user credentials.

Radius

- **Remote Authentication Dial In User Service.**
- AAA Protocol:
  1. Authentication.
  2. Authorization.
  3. Accounting.

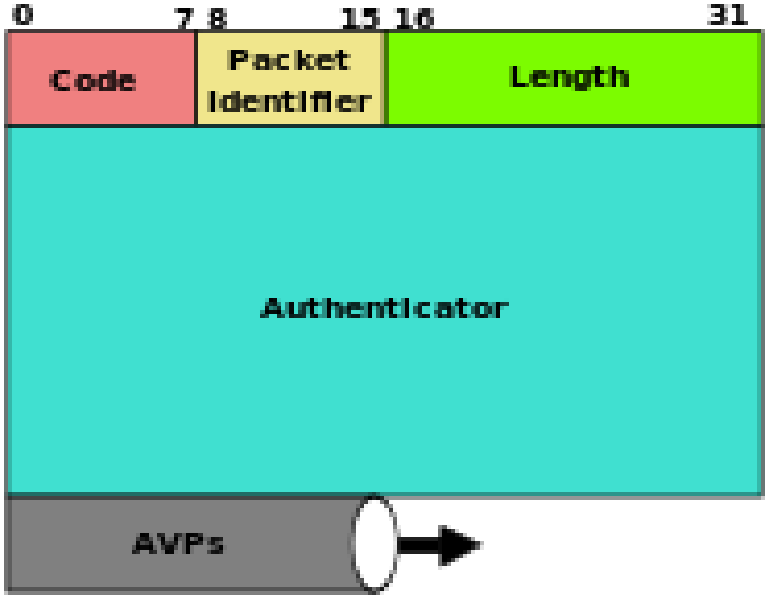
Radius Protocol

- Code:
  - Access Request.
  - Access Accept.
  - Access Reject.
  - ...
- Identifier: Used to match request and response.
- Length.
- Authenticator (16 bytes).



Authenticator Field

The Authenticator field in an Accounting-Response packet is called the Response Authenticator, and contains a one-way MD5 hash calculated over a stream of octets consisting of the Accounting-Response Code, Identifier, Length, the Request Authenticator field from the Accounting-Request packet being replied to, and the response attributes if any, followed by the shared secret. The resulting 16 octet MD5 hash value is stored in the Authenticator field of the Accounting-Response packet.



EAP

- **Extensible Authentication Protocol.**
- EAP defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages.
  - EAPoL.
  - EAPoRadius.

Let's see the real packets.

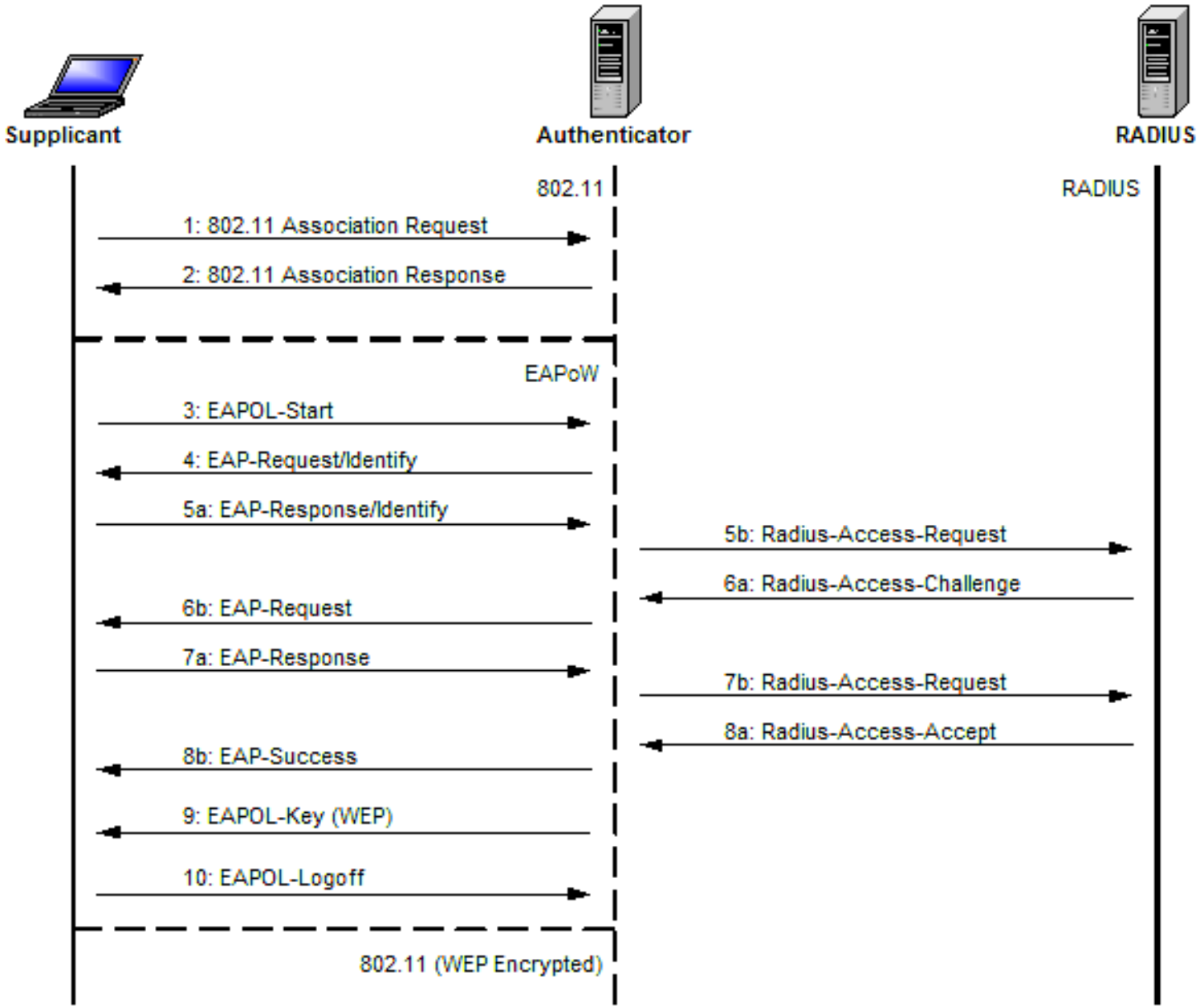
EAP Methods

- Lightweight Extensible Authentication Protocol (LEAP)
- EAP Transport Layer Security (EAP-TLS)
- EAP-MD5
- EAP Protected One-Time Password (EAP-POTP)
- EAP Pre-Shared Key (EAP-PSK)
- EAP Password (EAP-PWD)
- EAP Tunneled Transport Layer Security (EAP-TTLS)
- EAP Internet Key Exchange v2 (EAP-IKEv2)
- EAP Flexible Authentication via Secure Tunneling (EAP-FAST)
- EAP Subscriber Identity Module (EAP-SIM)
- EAP Authentication and Key Agreement (EAP-AKA)
- EAP Authentication and Key Agreement prime (EAP-AKA')
- EAP Generic Token Card (EAP-GTC)
- EAP Encrypted Key Exchange (EAP-EKE)

Diameter

- A AAA protocol **evolved** from Radius.
  - Support for SCTP.
  - Capability negotiation.
  - Application layer acknowledgements.
  - Extensibility; new commands can be defined.
  - Aligned on 32 bit boundaries.
- Quiz: Why called Diameter?

WiFi Access with IEEE802.1X



WiFi Access with IEEE802.1X

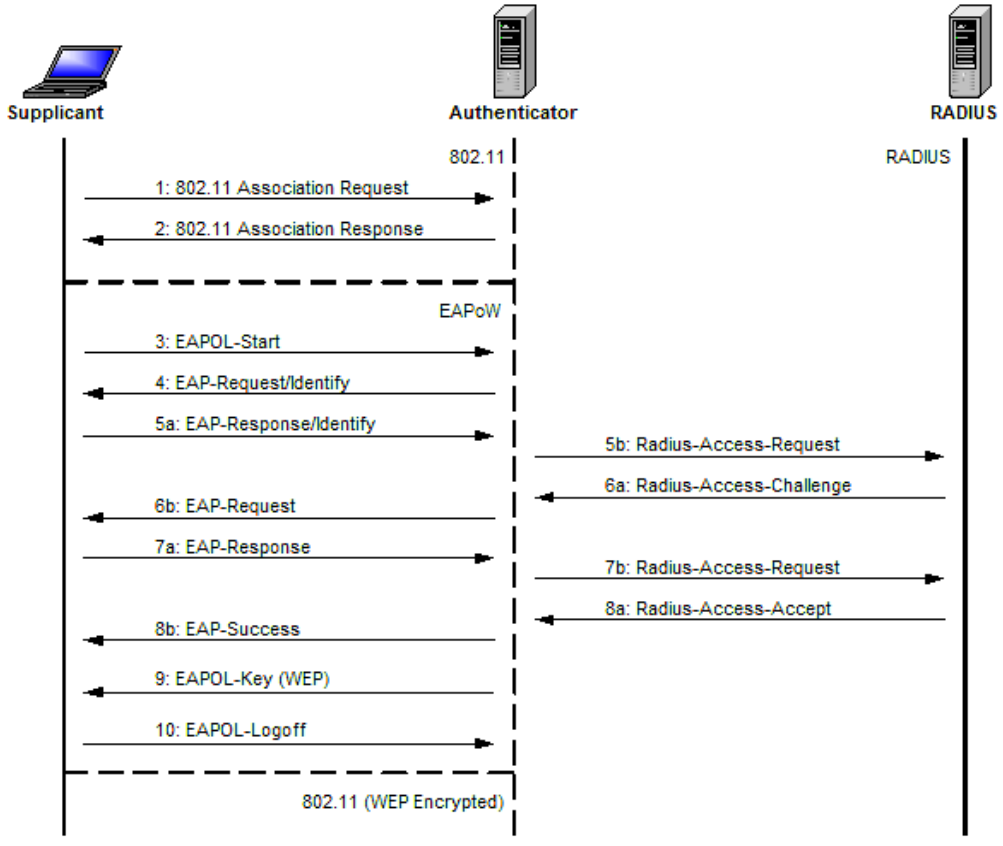


Figure 2: Sample 802.11/EAPoW Exchange

WEP key is **dynamically** generated.

WiFi Access with IEEE802.1X

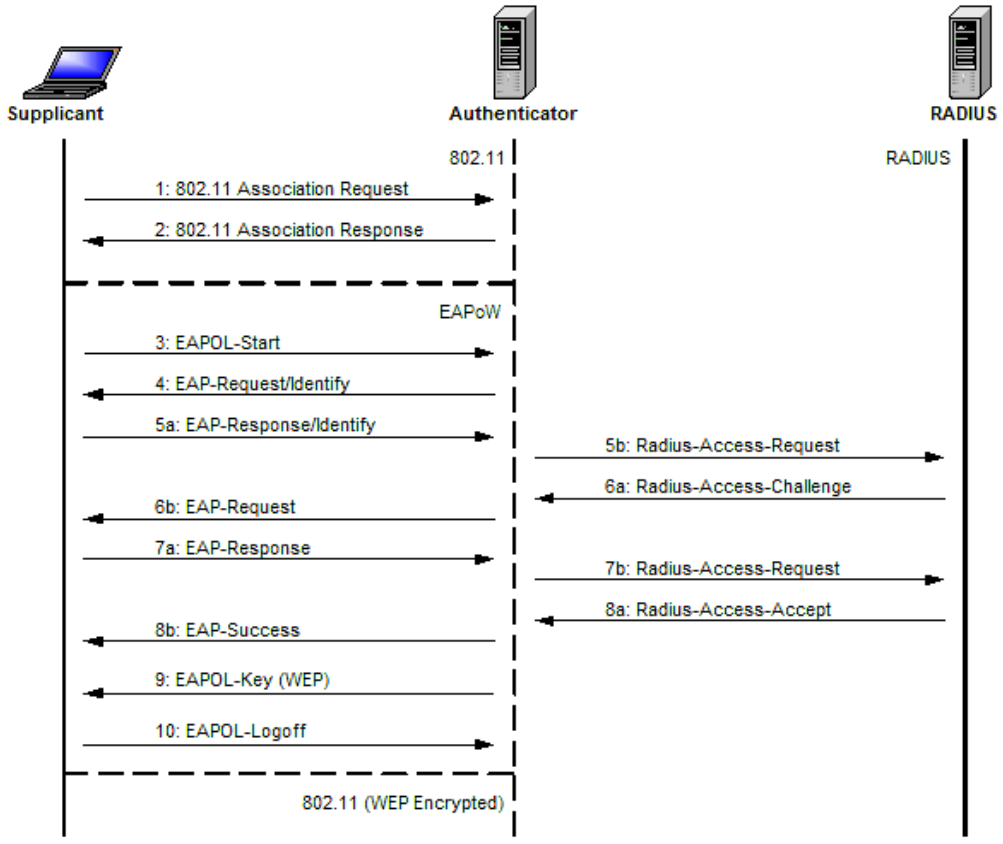


Figure 2: Sample 802.11/EAPoW Exchange

WEP key is **dynamically** generated.

So What? WEP is still not secure.

Quiz

Will the authenticator get the user credential?

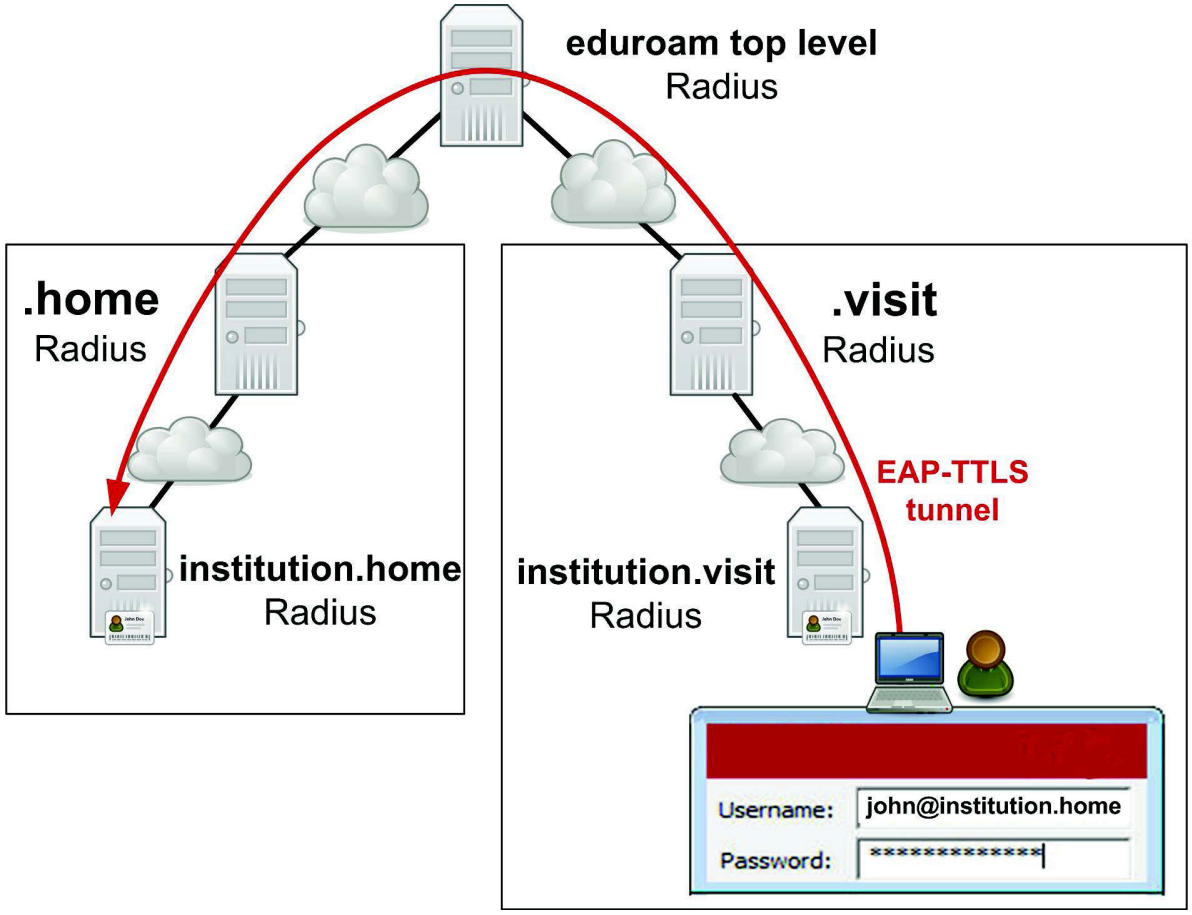
Quiz

Will the authenticator get the user credential?

No.

Eduroam

Eduroam (education roaming) is the secure, world-wide roaming access service developed for the international research and education community.



How to Apply Eduroam

- https://www.itc.ntnu.edu.tw/index.php/wirelessnetwork/
- https://roamingcenter.tanet.edu.tw/?page_id=2043

WPA: Temporal Key Integrity Protocol (TKIP)

WiFi Standard

Quiz: Who define WiFi standard?

1. IEEE.
2. WiFi Alliance.

WiFi Alliance

- Wi-Fi Alliance is a **non-profit** organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of **interoperability**.
  - Making SPEC is too slow.
  - SPEC is too complicated.
  - Plugfest.
- The Wi-Fi Alliance owns and controls the "Wi-Fi Certified" logo.

WiFi Alliance

- Wi-Fi Alliance is a **non-profit** organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of **interoperability**.
  - Making SPEC is too slow.
  - SPEC is too complicated.
  - Plugfest.
- The Wi-Fi Alliance owns and controls the "Wi-Fi Certified" logo.

Naming

- IEEE:
  - IEEE802.11i.
  - IEEE802.11i has been integrated into IEEE802.11.
- WiFi Alliance:
  - WPA.
  - WPA2.

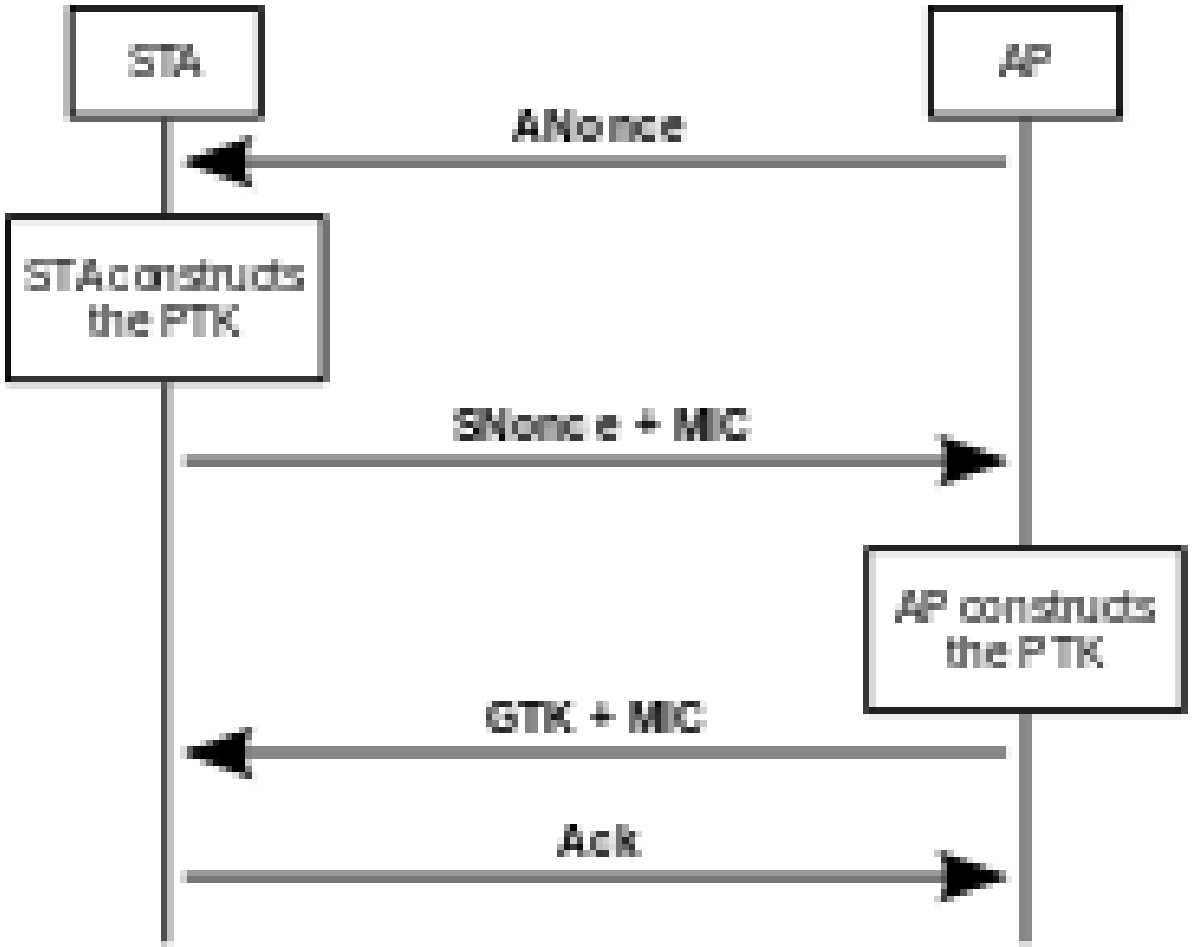
Question: How to improve WiFi Security.

Security Requirements

- The secret key should not be used too frequently.
  - We need a **temporary** key.
- WEP is not secure anymore.
  - We need another encryption algorithm.

Four-Way Handshake

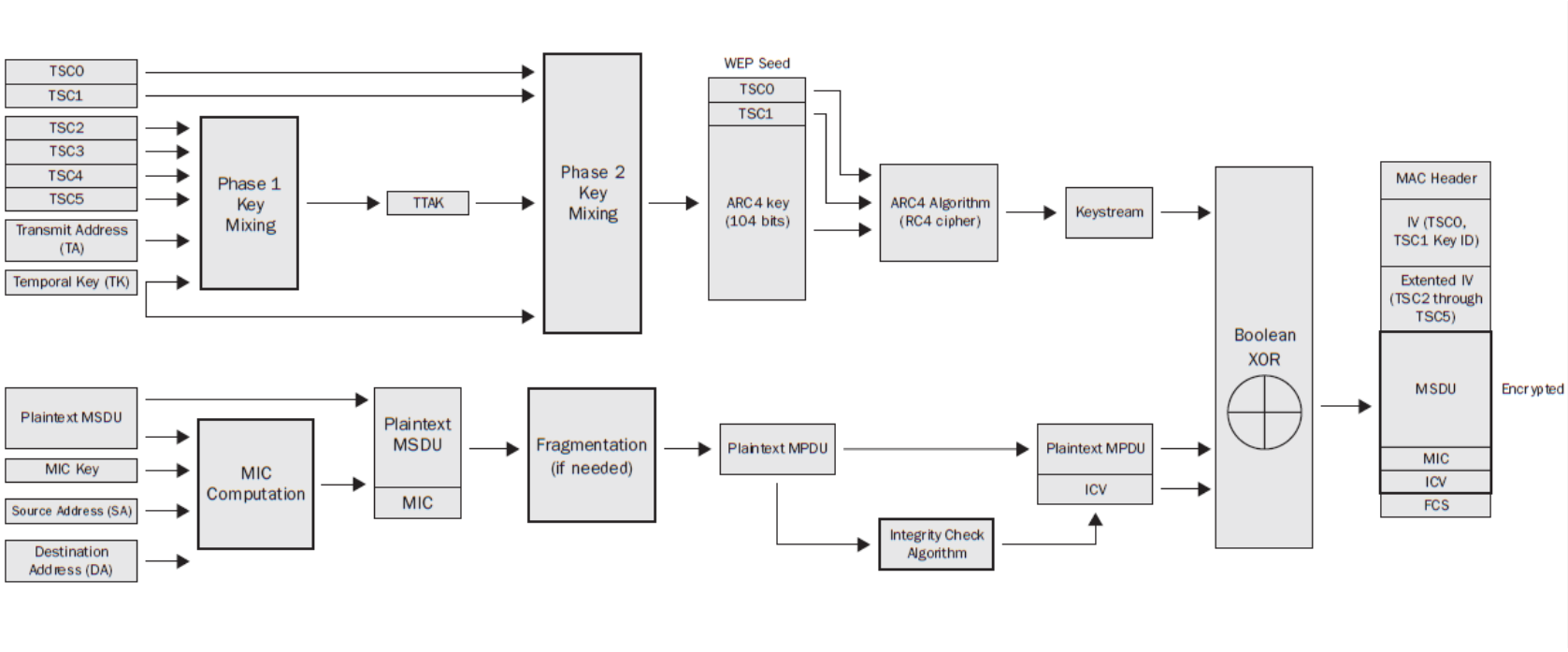
The four-way handshake is designed so that the AP and wireless client can independently prove to each other that they know the **PSK/PMK**, without ever disclosing the key.



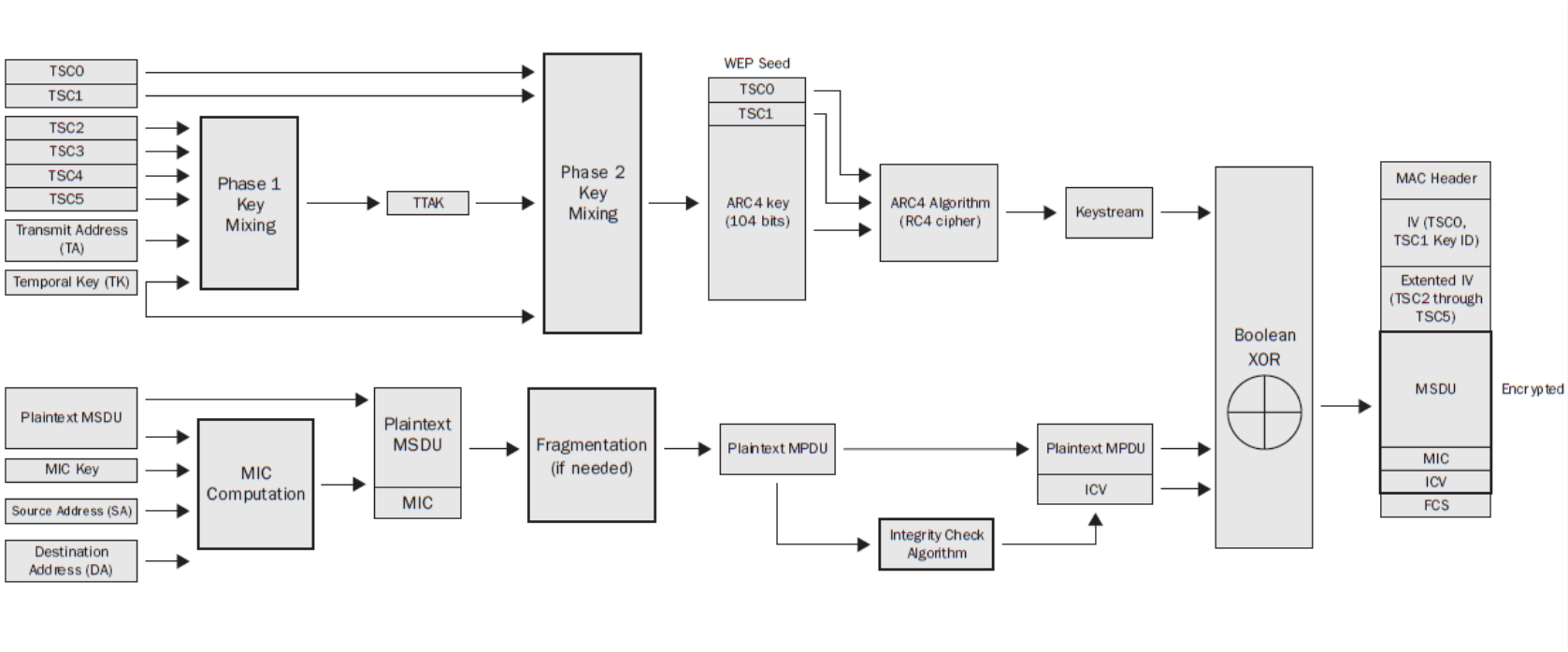
WPA: TKIP

- WEP is not secure because of **short IV**.
- Solution: make IV longer.
- Advantage: compatible with WEP.

TKIP


TSC0
TSC1
TSC2
TSC3
TSC4
TSC5
Transmit Address (TA)
Temporal Key (TK)
Phase 1 Key Mixing
TTAK
Phase 2 Key Mixing
WEP Seed
TSC0
TSC1
ARC4 key (104 bits)
ARC4 Algorithm (RC4 cipher)
Keystream
Boolean XOR
MAC Header
IV (TSC0, TSC1 Key ID)
Extented IV (TSC2 through TSC5)
MSDU
MIC
ICV
FCS
Encrypted
Plaintext MSDU
MIC Key
Source Address (SA)
Destination Address (DA)
MIC Computation
Plaintext MSDU
MIC
Fragmentation (if needed)
Plaintext MPDU
Integrity Check Algorithm
Plaintext MPDU
ICV

TKIP



Unfortunately, short IV is just one vulnerability in WEP. RC4 is another one.

Summary

You should not use TKIP.

WPA2

WPA2

- Basic idea: no more RC4, use AES instead.
  - AES-CCMP: AES counter mode with CBC MAC.
- Two types:
  - **WPA2-personal**: Shared Key.
  - **WPA2-enterprise**: Authentication server.

Currently, you should use this as your AP security mode.

Rogue AP

Rogue AP

- Rogue AP is a wireless access point that has been installed on a secure network **without explicit authorization** from a local network administrator.
- For example, you can setup an AP with ssid called ntnu, right?

Quiz

1. How to detect Rogue APs?

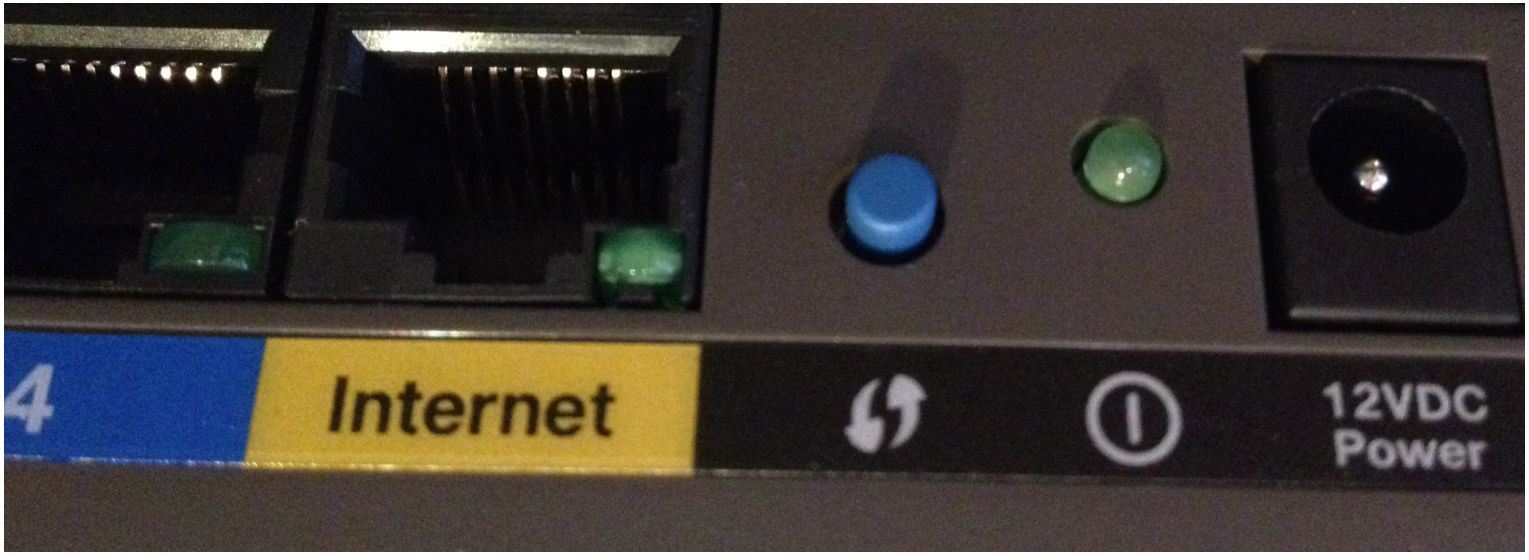
Quiz

1. How to detect Rogue APs?
2. How to prevent yourself from accessing rogue AP?

WPS

WPS

- **Wi-Fi Protected Setup** is a network security standard to create a secure wireless home network for **dumb users**.
- Oriented by Wi-Fi Alliance.



WPS Mode

- PIN mode (Mandatory)
  - Eight-digit number used to add new WPA enrollees to the network.
  - Last digit is a checksum.
- Push button mode.
- NFC mode.

How WPS Works?

WPS-enabled Printer

Wi-Fi Protected Setup PIN Method

AP advertises Wi-Fi Protected Setup capability in beacon

Printer sends probe request to AP to indicate it is capable of WPS configuration

User enters 8-digit PIN from printer packaging via the AP web interface to begin WPS

Authentication phase commences using PIN as shared secret

AP delivers encrypted WPA-PSK key and SSID to printer

Standard WPA four-way authentication can now begin

WPS-enabled Access Point (AP)

Quiz

How to attack WPS?

Quiz

How to attack WPS?

Eight-digit only. Are you kidding?

`https://tools.kali.org/wireless-attacks/reaver`

IEEE802.11w

IEEE802.11w

- All slides before are talking about the user data encryption. How about the management frame?
- Quiz: what will happen if we do not protect management frames? Please describe an attack.

IEEE802.11w

- All slides before are talking about the user data encryption. How about the management frame?
- Quiz: what will happen if we do not protect management frames? Please describe an attack.
  - Inject a deauthentication frame.

IEEE802.11w

- Single and unified solution needed for all IEEE 802.11 Protection-capable Management Frames.
- It uses the existing security mechanisms rather than creating new security scheme or new management frame format.
- It is an optional feature in 802.11 and is required for 802.11 implementations that support TKIP or CCMP.
- Its use is optional and can be negotiable between STAs.

IEEE802.11 Mgmt Frames

Unprotected:

- **Beacon** and **probe** request/response.
- Announcement traffic indication message (ATIM).
- **Authentication**.
- **Association request/response**.
- Spectrum management action.

Protected:

- **Disassociation** and **deauthentication**.
- Radio measurement action for infrastructure BSS (802.11k frames).
- QoS action frame (802.11e frames).
- Future 11v management frames (802.11v frames).

Other Attacks on WiFi

Quiz

- Do you know what **CSMA/CD** is?
- Do you know what **CSMA/CA** is?
- Do you know how **RTS/CTS** works?
- Do you know what **Binary Exponential Backoff** is?

Quiz

Today, if someone uses an unfair dice which always gets 1 when backoff, what will happen?

Quiz

Can you launch this attack by modifying wifi driver?

Quiz

How to detect this attack?

WPA2 Crack: KRACK

4-Way Handshake

- The 4-way handshake provides mutual authentication and session key agreement.
- Though history and security proofs though, the 4-way handshake is vulnerable to **key reinstallation attacks**.
  - It is human beings who implement it.
- Concept:
  1. When a client joins a network, it executes the 4-way handshake to negotiate a fresh session key.
  2. The client will install this key after receiving message 3 of the handshake.
  3. What will happen if message 3 is lost?

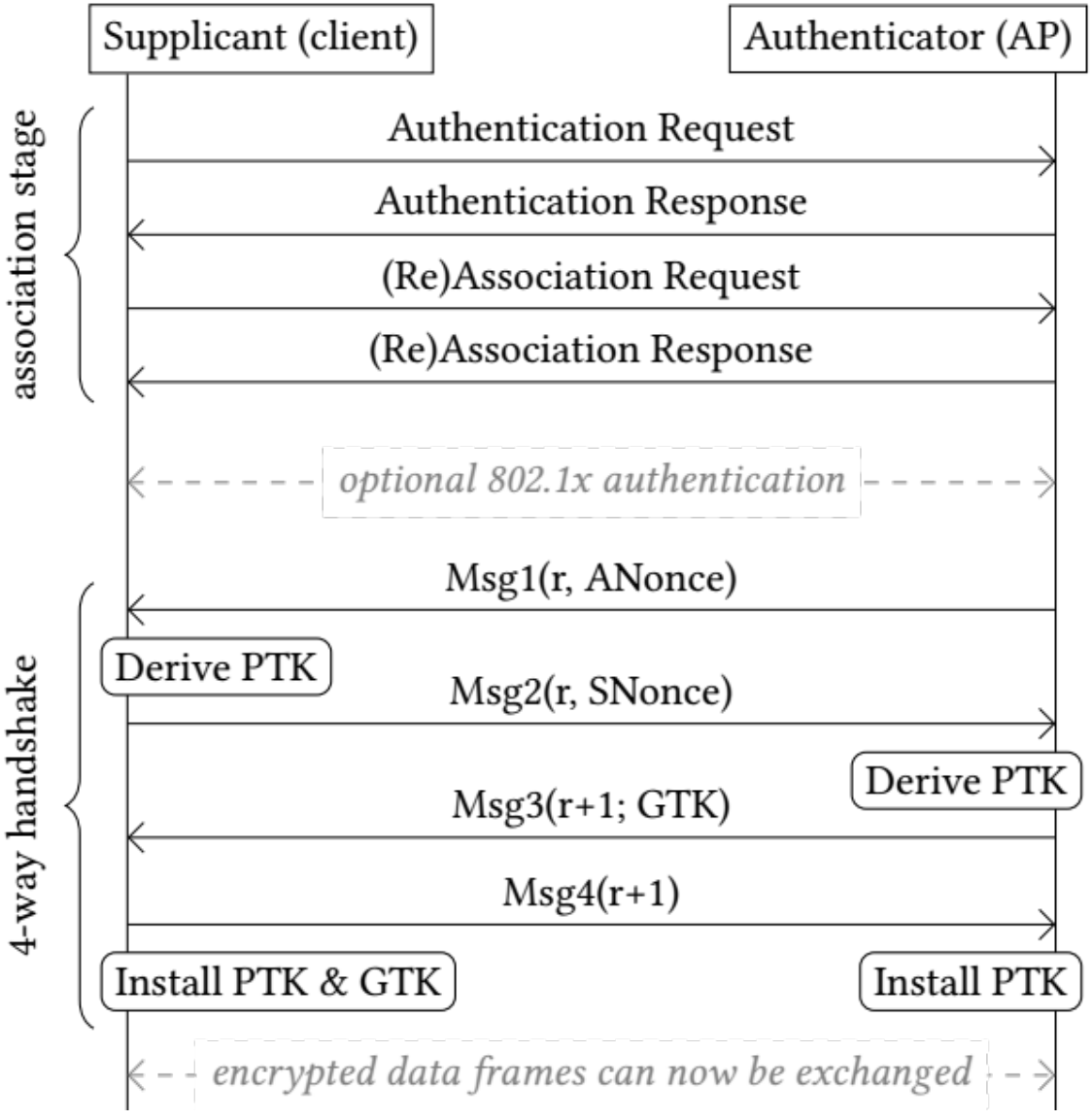
4-Way Handshake

- The 4-way handshake provides mutual authentication and session key agreement.
- Though history and security proofs though, the 4-way handshake is vulnerable to **key reinstallation attacks**.
  - It is human beings who implement it.
- Concept:
  1. When a client joins a network, it executes the 4-way handshake to negotiate a fresh session key.
  2. The client will install this key after receiving message 3 of the handshake.
  3. What will happen if message 3 is lost?
  4. AP will retransmit message 3.

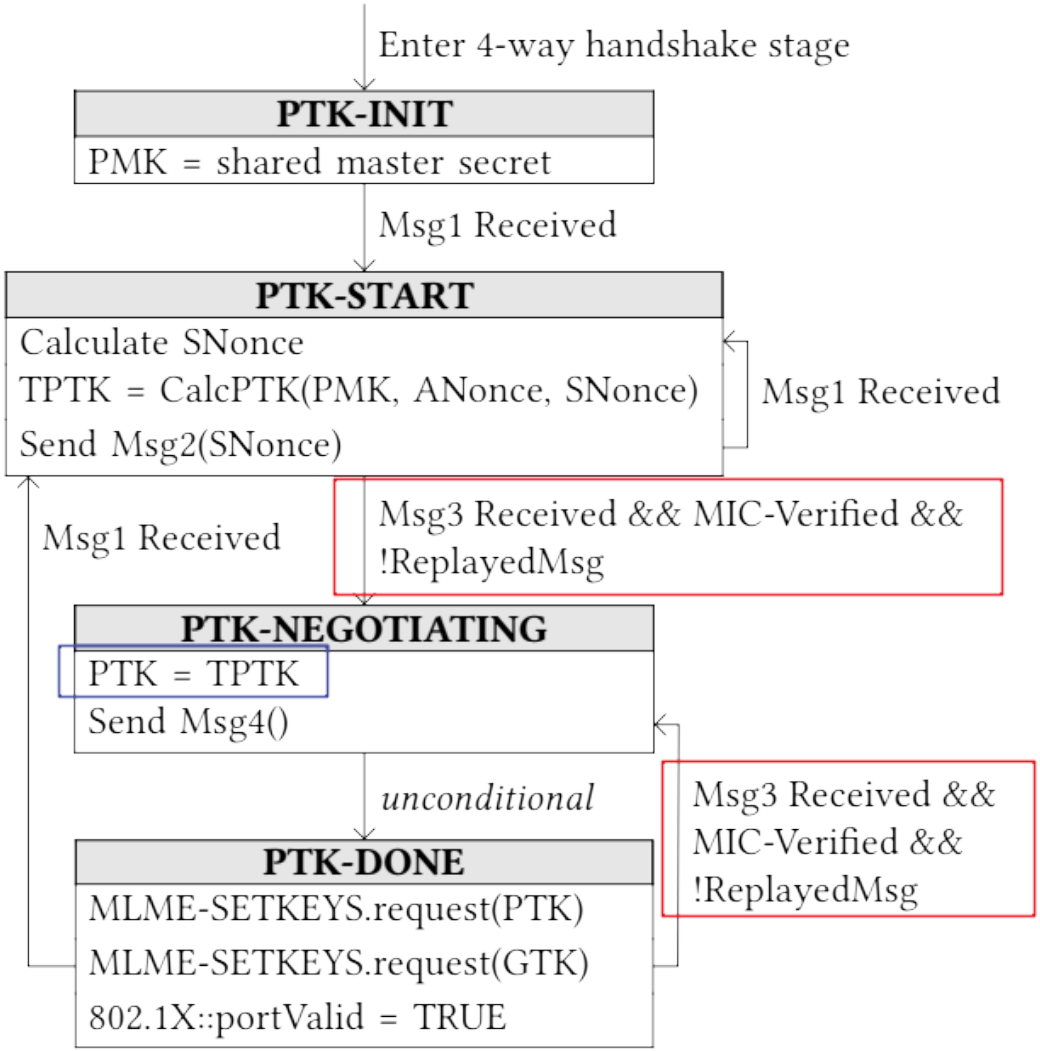
4-Way Handshake

- The 4-way handshake provides mutual authentication and session key agreement.
- Though history and security proofs though, the 4-way handshake is vulnerable to **key reinstallation attacks**.
  - It is human beings who implement it.
- Concept:
  1. When a client joins a network, it executes the 4-way handshake to negotiate a fresh session key.
  2. The client will install this key after receiving message 3 of the handshake.
  3. What will happen if message 3 is lost?
  4. AP will retransmit message 3.
  5. The client will reinstall the same session key and **reset the counter**.

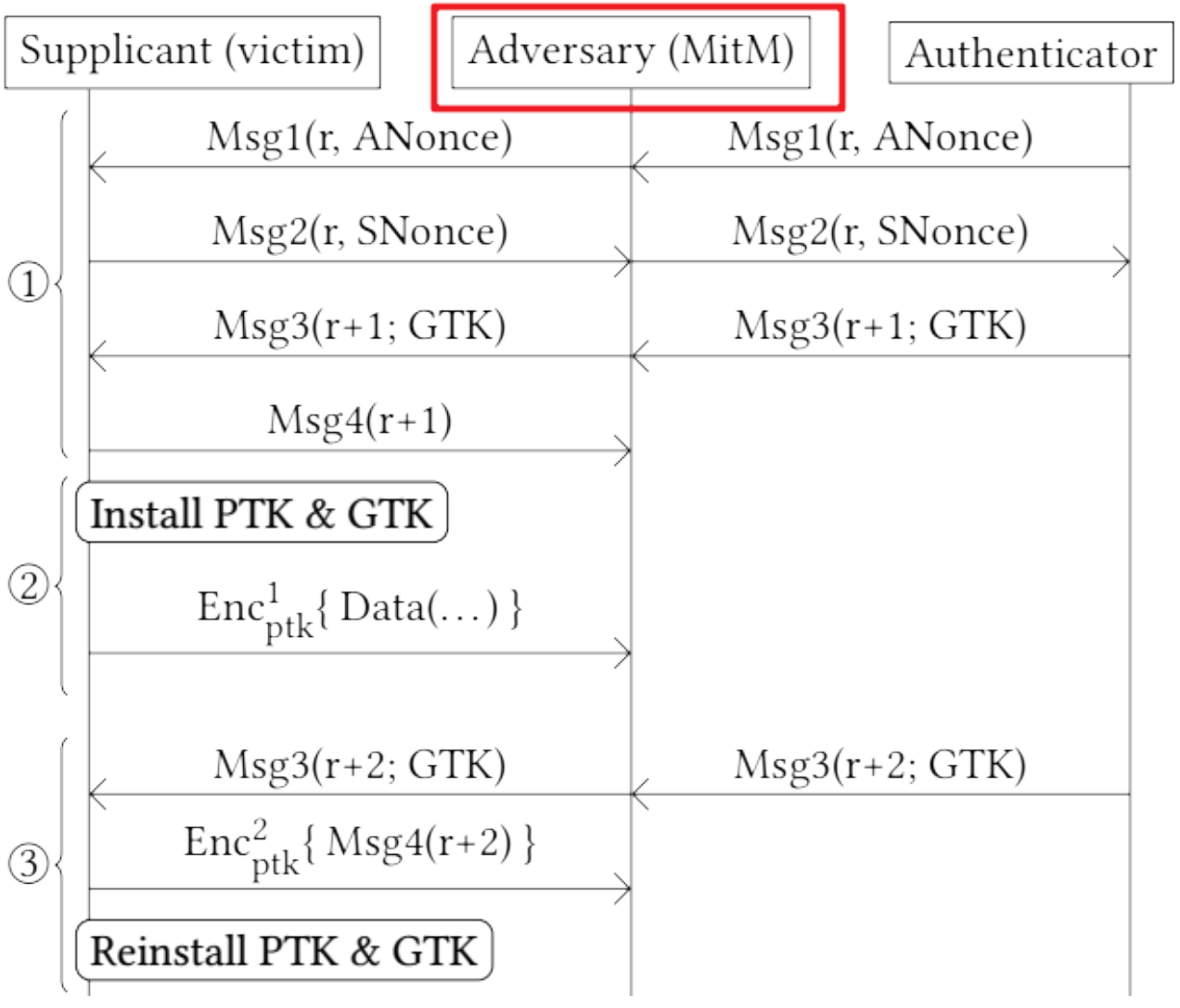
4-Way Handshake



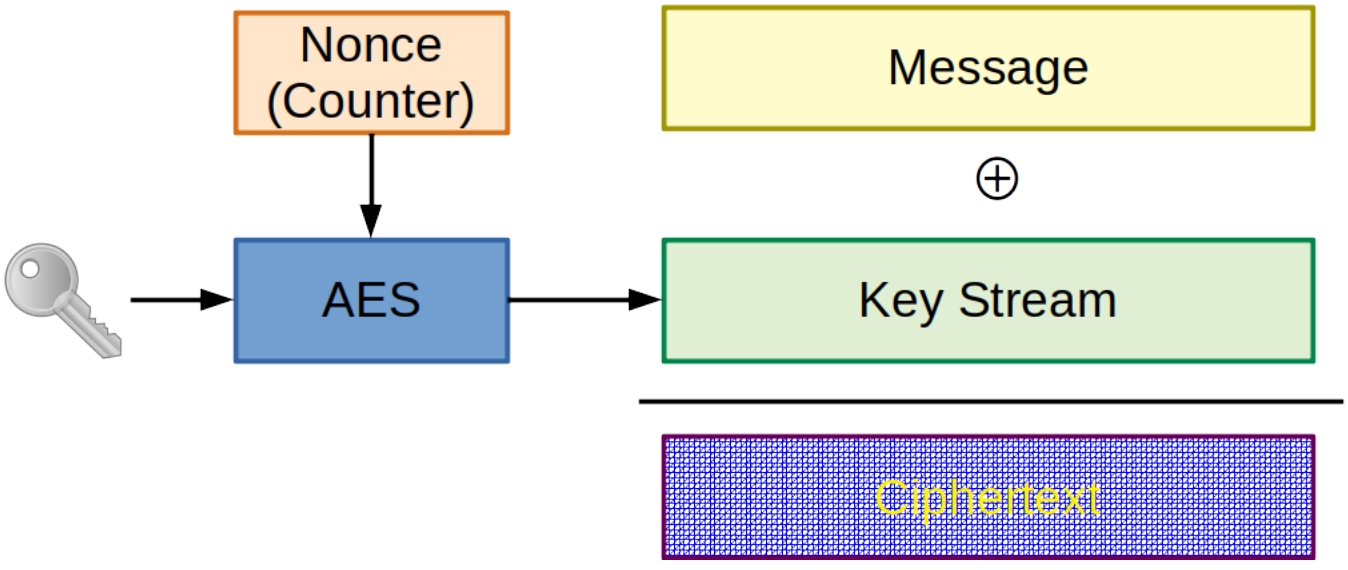
4-Way Handshake in IEEE802.11 Standard



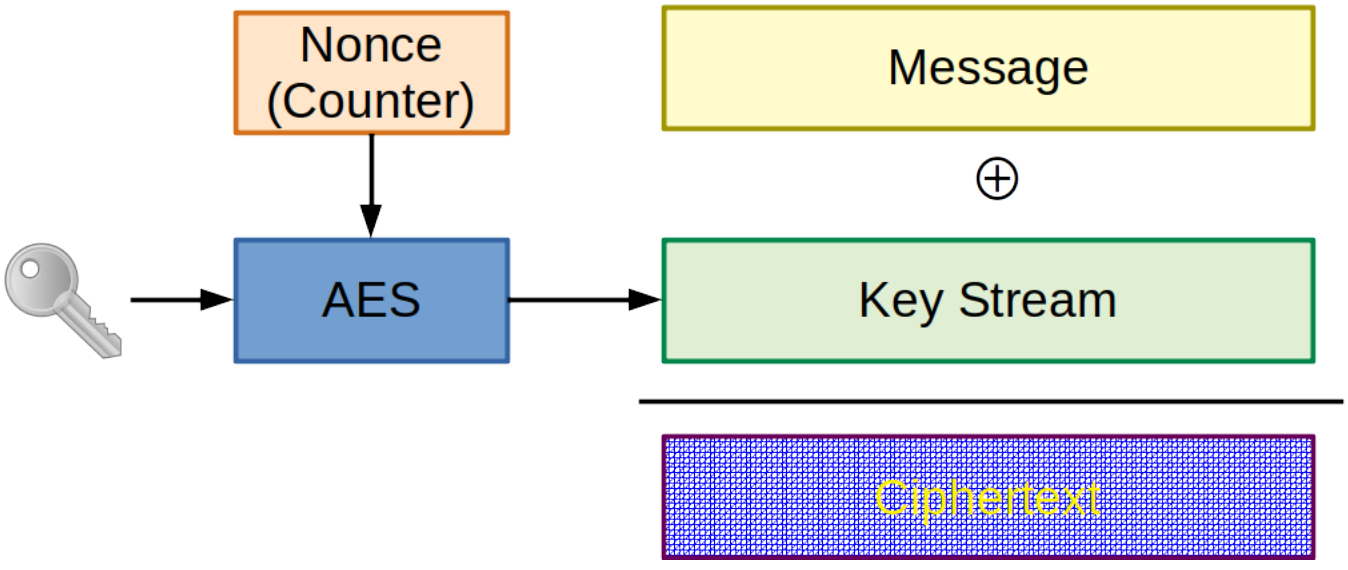
Man in the Middle Attack



AES-CCMP: AES Counter Mode with CBC MAC



AES-CCMP: AES Counter Mode with CBC MAC



Quiz: What will happen if nonce is reset?

Reference

https://www.krackattacks.com/

WPA3

Wi-Fi CERTIFIED WPA3

WPA3™ is the next generation of Wi-Fi security and provides cutting-edge security protocols to the market. Building on the widespread success and adoption of Wi-Fi CERTIFIED WPA2™, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission critical networks.

WPA3 Features

1. A More Secure Handshake.
2. Open Wi-Fi Network Security.
3. Enables easy connectivity to devices with out display.
4. 192-bit security suite.

Simultaneous Authentication of Equals

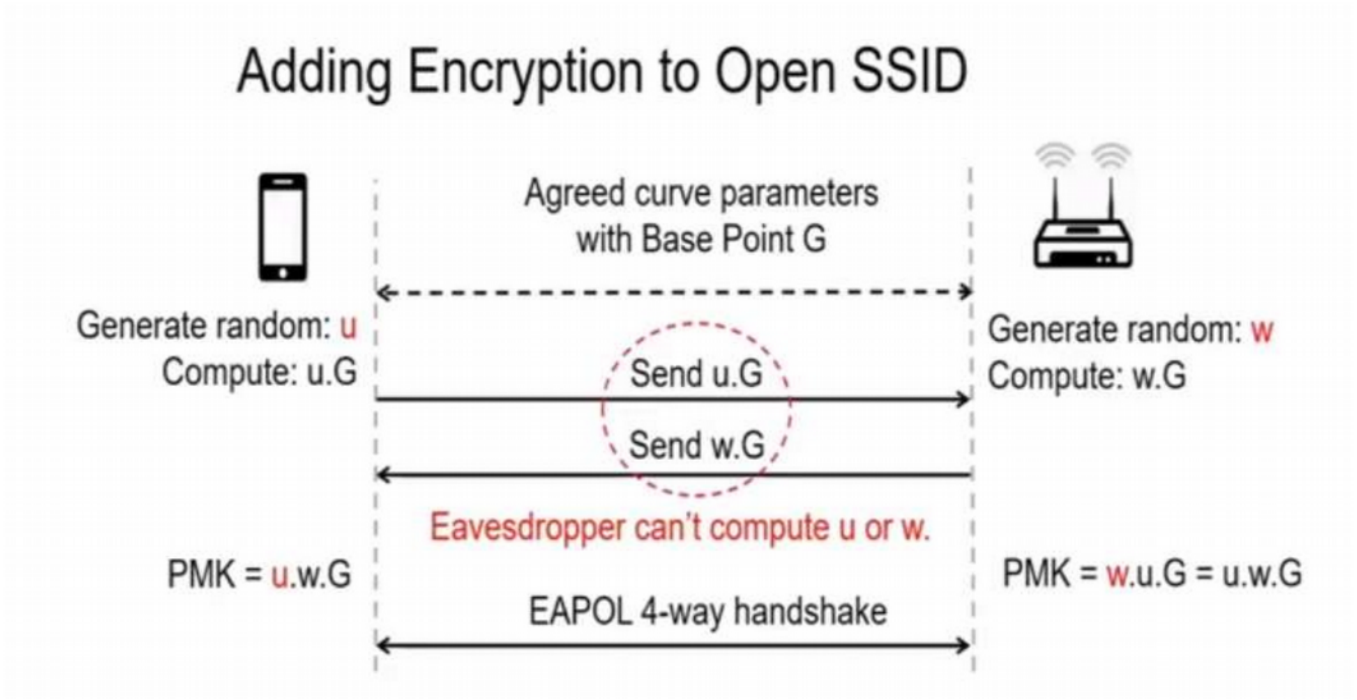
- Each peer can **commit** at any time.
- A peer can **confirm** only after it has committed and the other peer has committed.
- A peer can **accept** after its peer has confirmed and the confirmation has been verified.

Simultaneous Authentication of Equals

- Each peer can **commit** at any time.
- A peer can **confirm** only after it has committed and the other peer has committed.
- A peer can **accept** after its peer has confirmed and the confirmation has been verified.

Just like Diffie-Hellman.

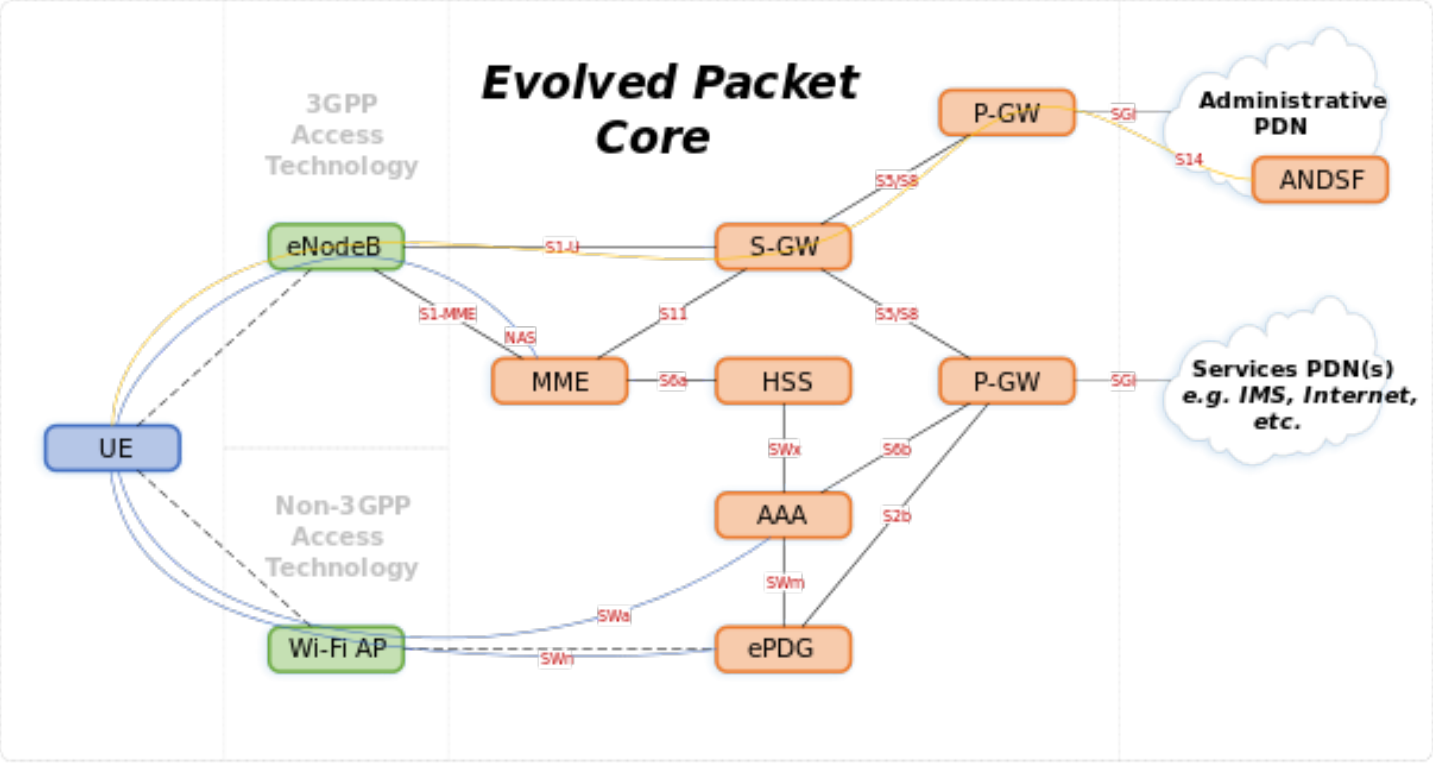
Opportunistic Wireless Encryption



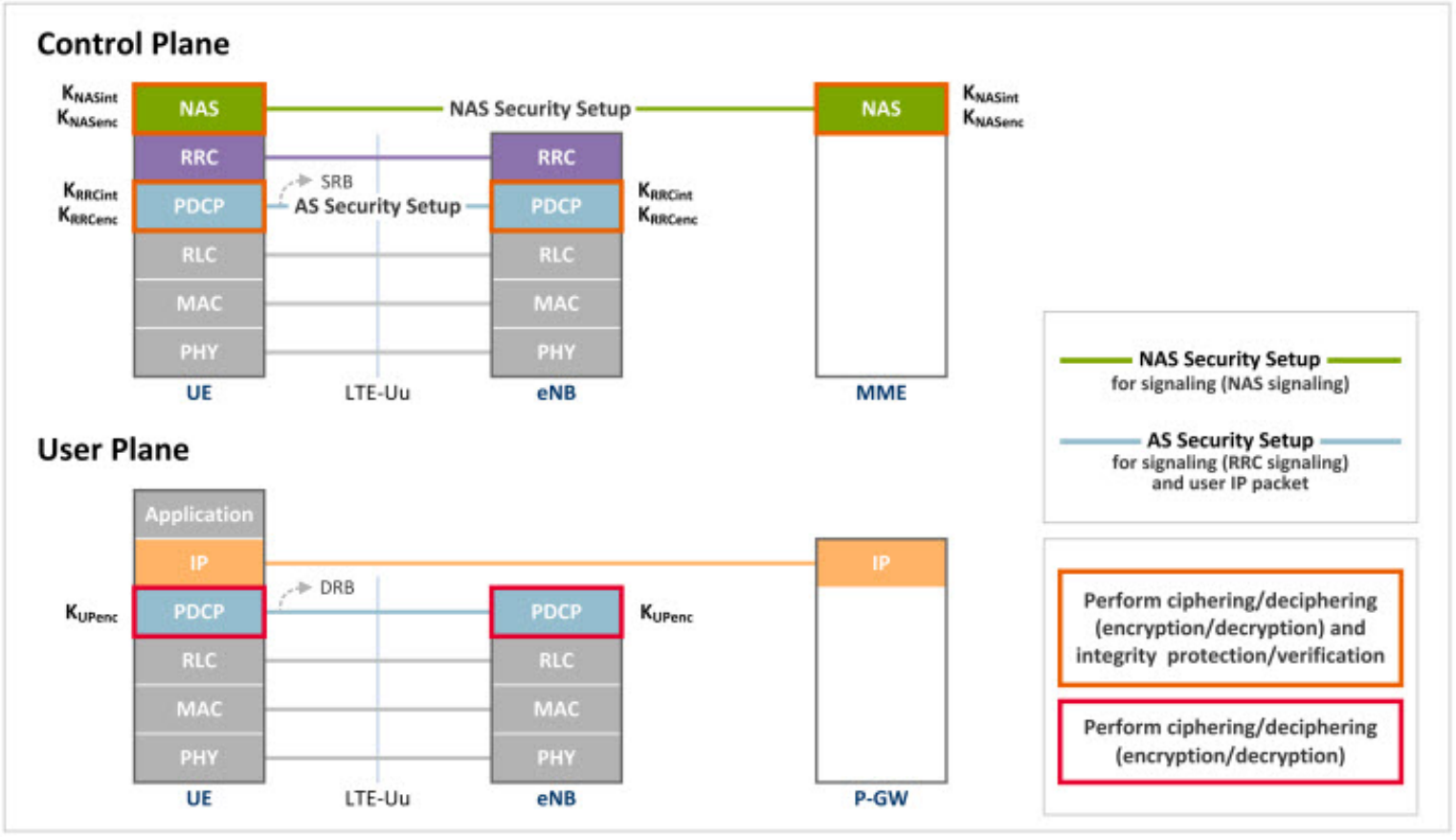
- Strengthen user privacy in open networks through individualized data encryption.
- Encryption only, no authentication.

LTE

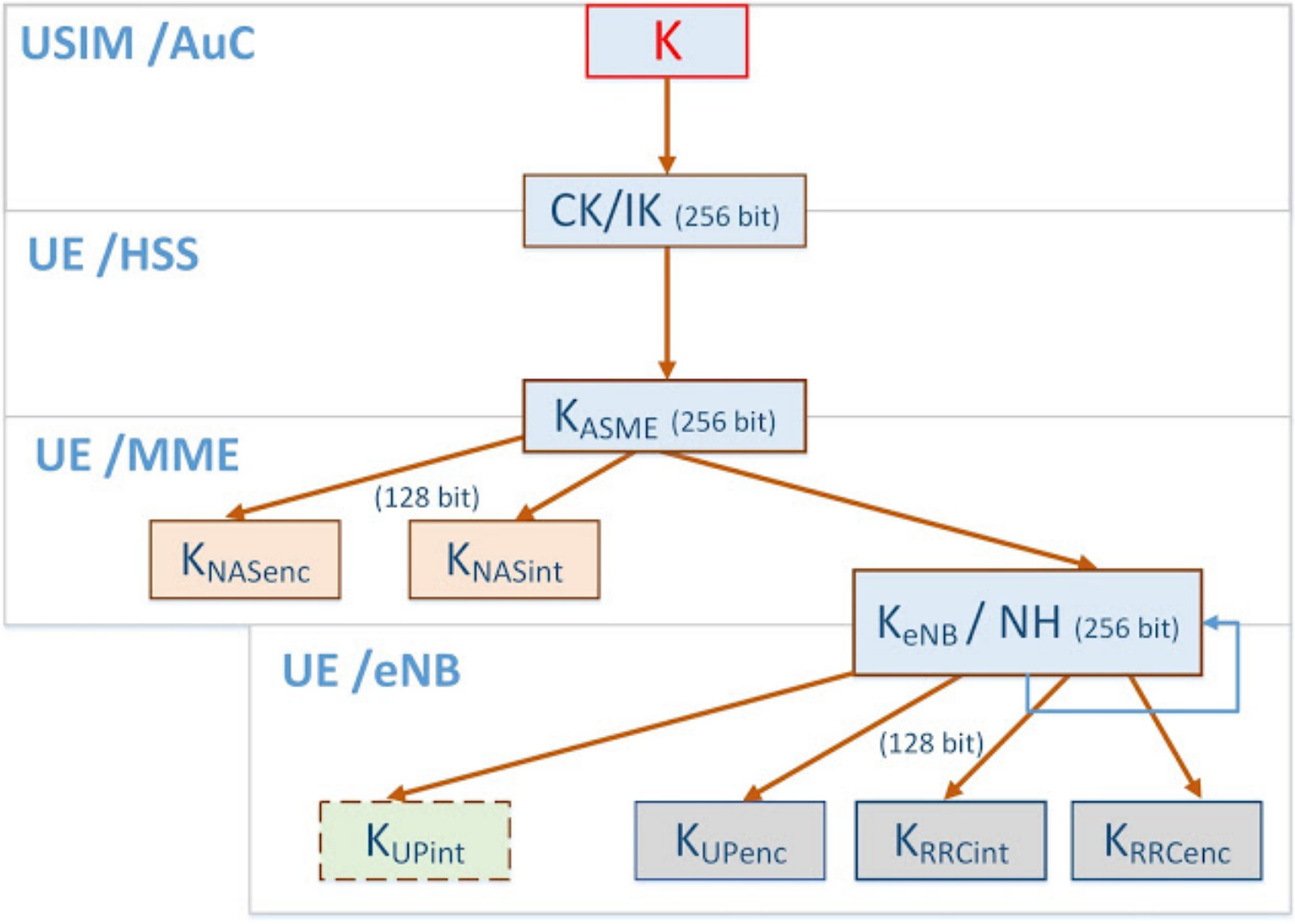
LTE EPC Architecture



LTE Control Plane vs. Data Plane



LTE Key Hierarchy



EPS Authentication and Key Agreement