Wireless LAN Security

CSE 6590

Fall 2010

Outline

- Wired Equivalent Privacy (WEP)
  - first security protocol defined in 802.11
- Wi-Fi Protected Access (WPA)
  - defined by Wi-Fi Alliance
- WPA2
- 802.11i

History

- In the early 1980s, the IEEE began work on developing computer network architecture standards
  - This work was called Project 802
- In 1990, the IEEE formed a committee to develop a standard for WLANs (Wireless Local Area Networks)
  - At that time WLANs operated at a speed of 1 to 2 million bits per second (Mbps)

IEEE 802.11 WLAN Standard

- In 1997, the IEEE approved the IEEE 802.11 WLAN standard
- Revisions
  - IEEE 802.11a
  - IEEE 802.11b
  - IEEE 802.11g
  - IEEE 802.11n

Controlling Access to a WLAN

- Access is controlled by limiting a device's access to the access point (AP)
- Only devices that are authorized can connect to the AP
  - One way: Media Access Control (MAC) address filtering
  - CCSF uses this technique (unfortunately)
  - See www.ccsf.edu/wifi

Controlling Access

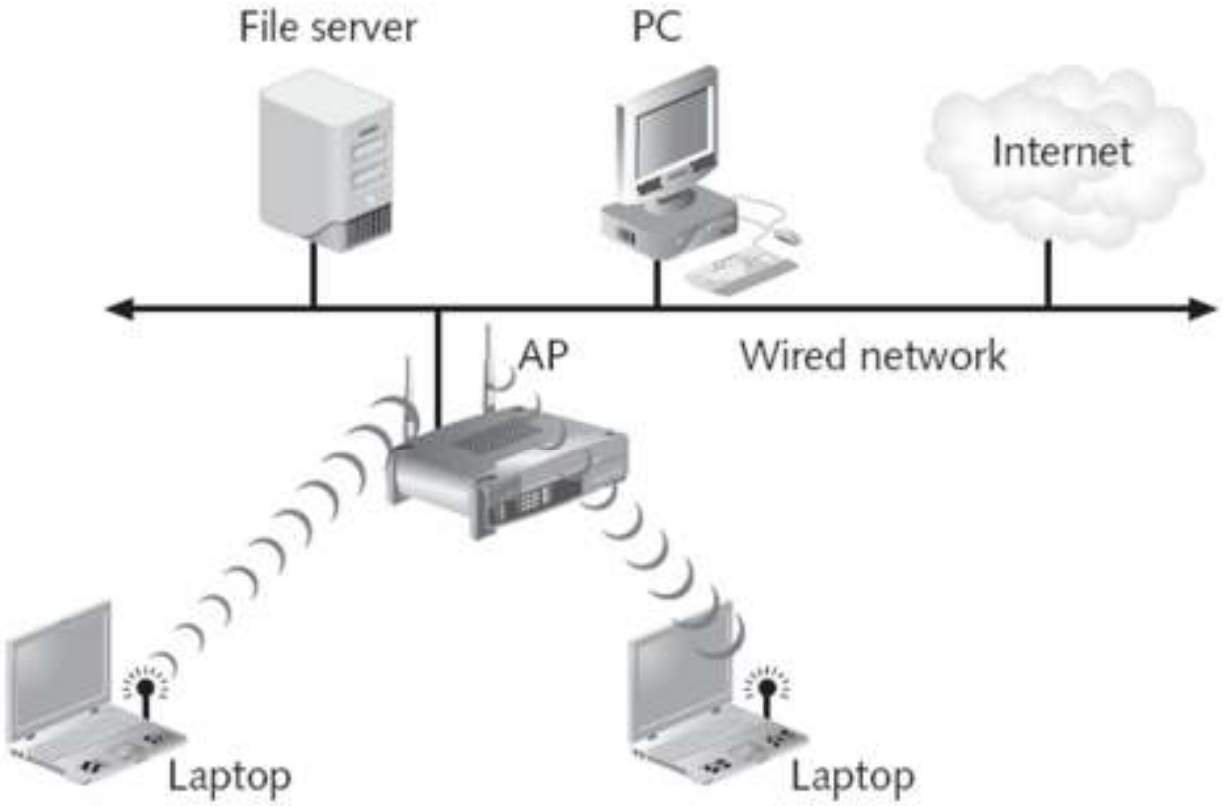


Figure 6-1 Central base station AP

MAC Address Filtering

Figure 6-2 MAC address filter

MAC Address Filtering

- Usually implemented by permitting instead of preventing
- CCSF does this
  www.ccsf.edu/wifi

MAC Address Filtering Weaknesses

- MAC addresses are transmitted in the clear
  - An attacker can just sniff for MACs
- Managing a large number of MAC addresses is difficult
- MAC address filtering does not provide a means to temporarily allow a guest user to access the network
  - Other than manually entering the user's MAC address into the access point

Wired Equivalent Privacy (WEP)

- Designed to ensure that only authorized parties can view transmitted wireless information
- Uses encryption to protect traffic
- WEP was designed to be:
  - Efficient and reasonably strong

10

WEP Keys

- WEP secret keys can be 64 or 128 bits long
- The AP and devices can hold up to four shared secret keys
  - One of which must be designated as the default key

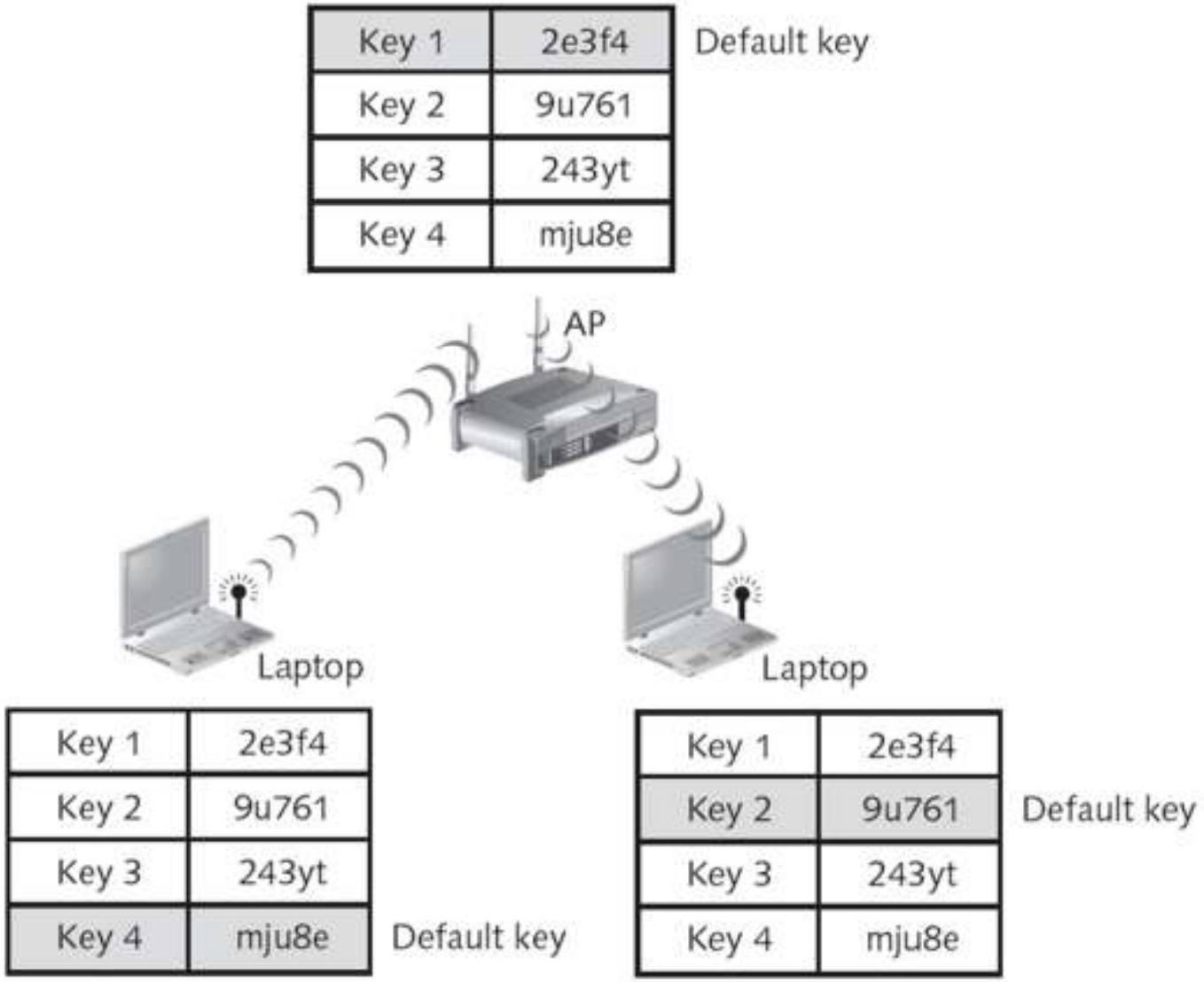


Figure 6-3 Default WEP key

WEP Encryption Process

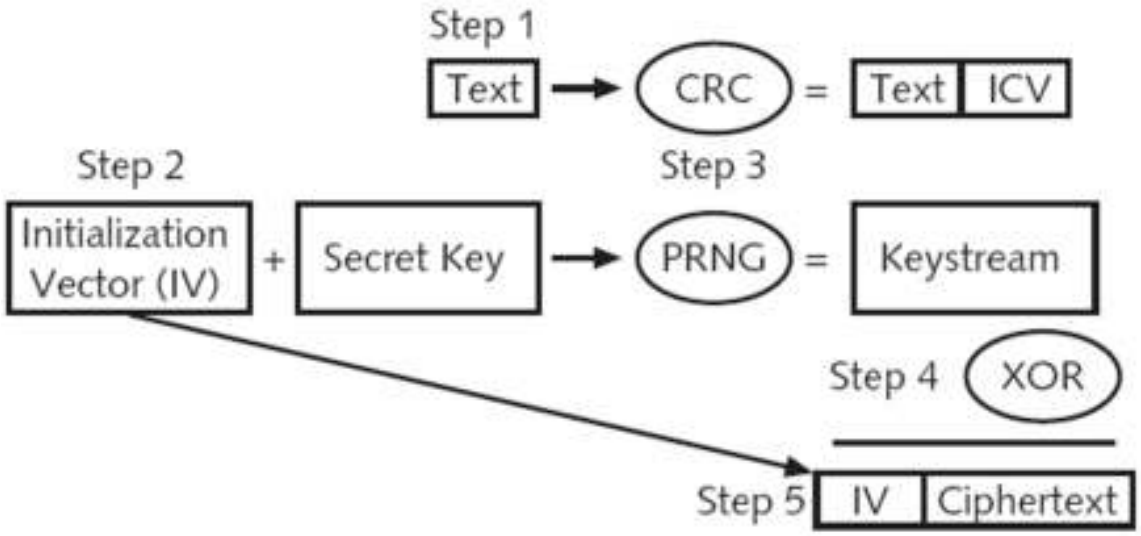
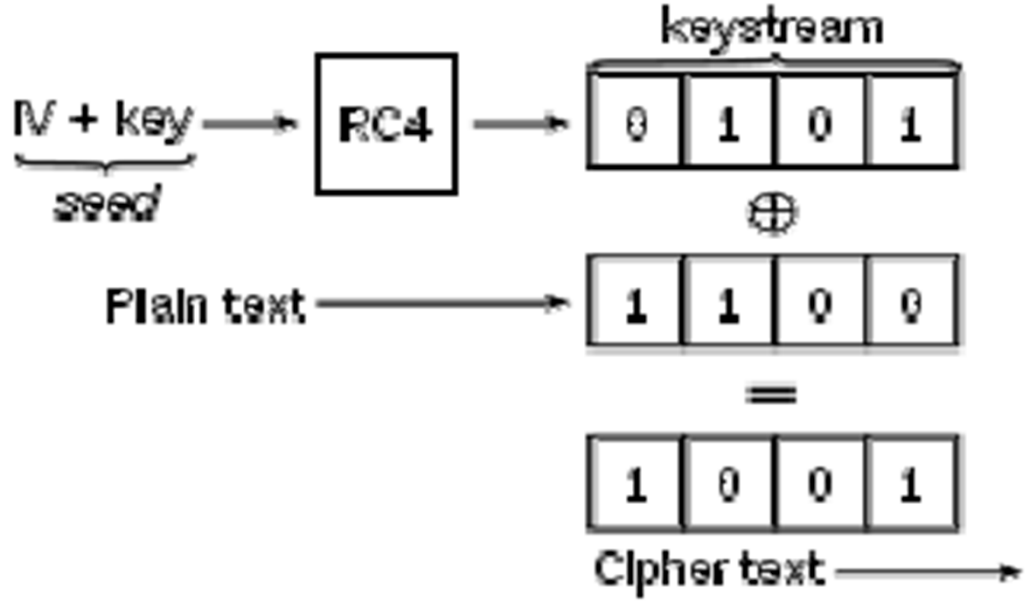


Figure 6-4 WEP encryption process

WEP Encryption Process (2)

- When a node has a packet to send, it first generates CRC for this packet as an integrity check value (ICV).
- Generates an IV; concatenates it with the secret key; applies RC4 to create RC4 key stream.
- Performs XOR operation on the above two streams, byte by byte, to produce ciphertext.
- Appends the IV to the ciphertext and transmits to the receiver.

WEP Encryption Process (3)



Transmitting with WEP

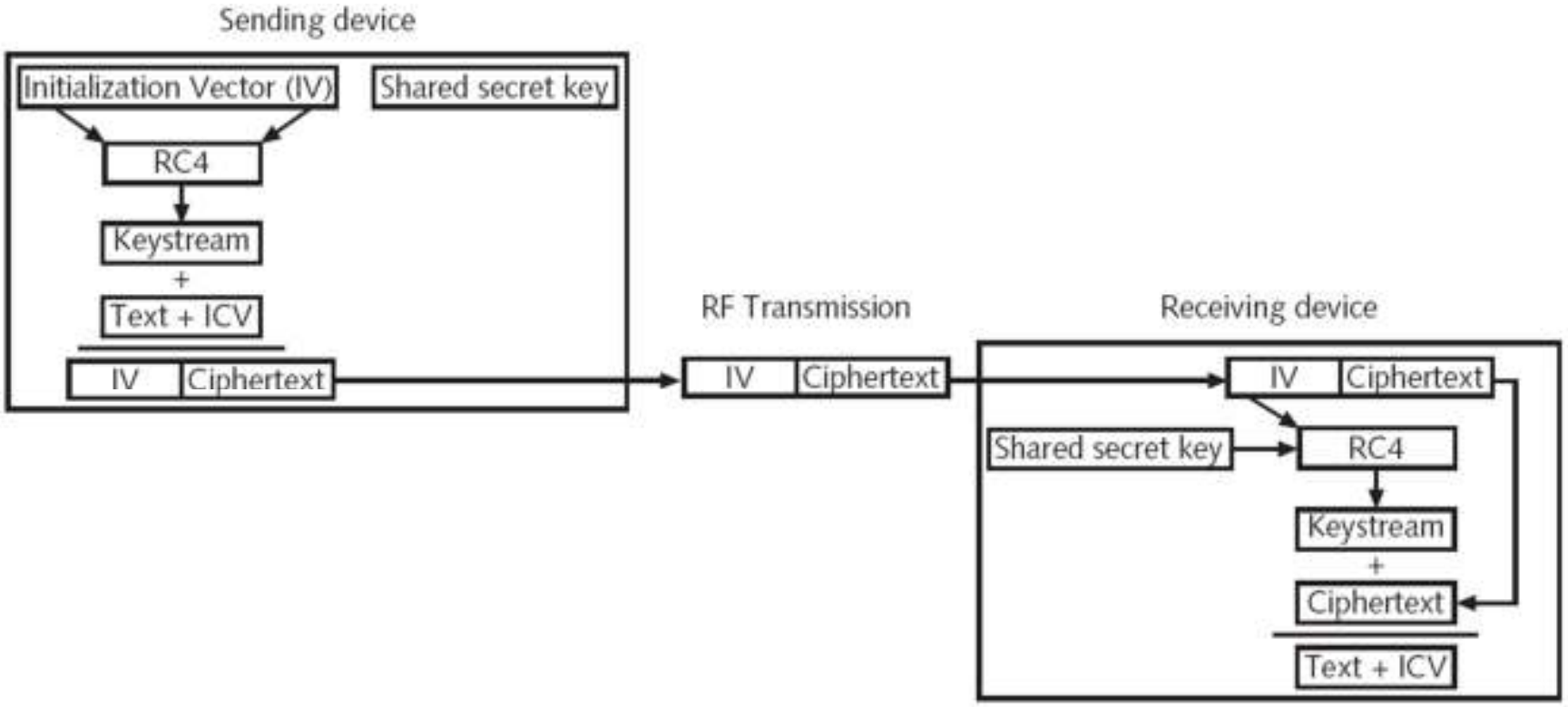


Figure 6-5 Transmitting with WEP

Analysis of WEP Encryption

- IV is 24-bit long $\Rightarrow 2^{24}$ choices.
- The probability of choosing the same IV value is more than 99% after only 12,00 frames.
- Only a few seconds elapse with 11Mbps and 1KByte frame size.
- IV values are sent in plain text $\Rightarrow$ attackers can detect a duplicate value and re-use past keys.

Device Authentication

- Before a computer can connect to a WLAN, it must be **authenticated**
- Types of authentication in 802.11
  - **Open system authentication**
    - Lets everyone in
  - **Shared key authentication**
    - Only lets computers in if they know the **shared key**

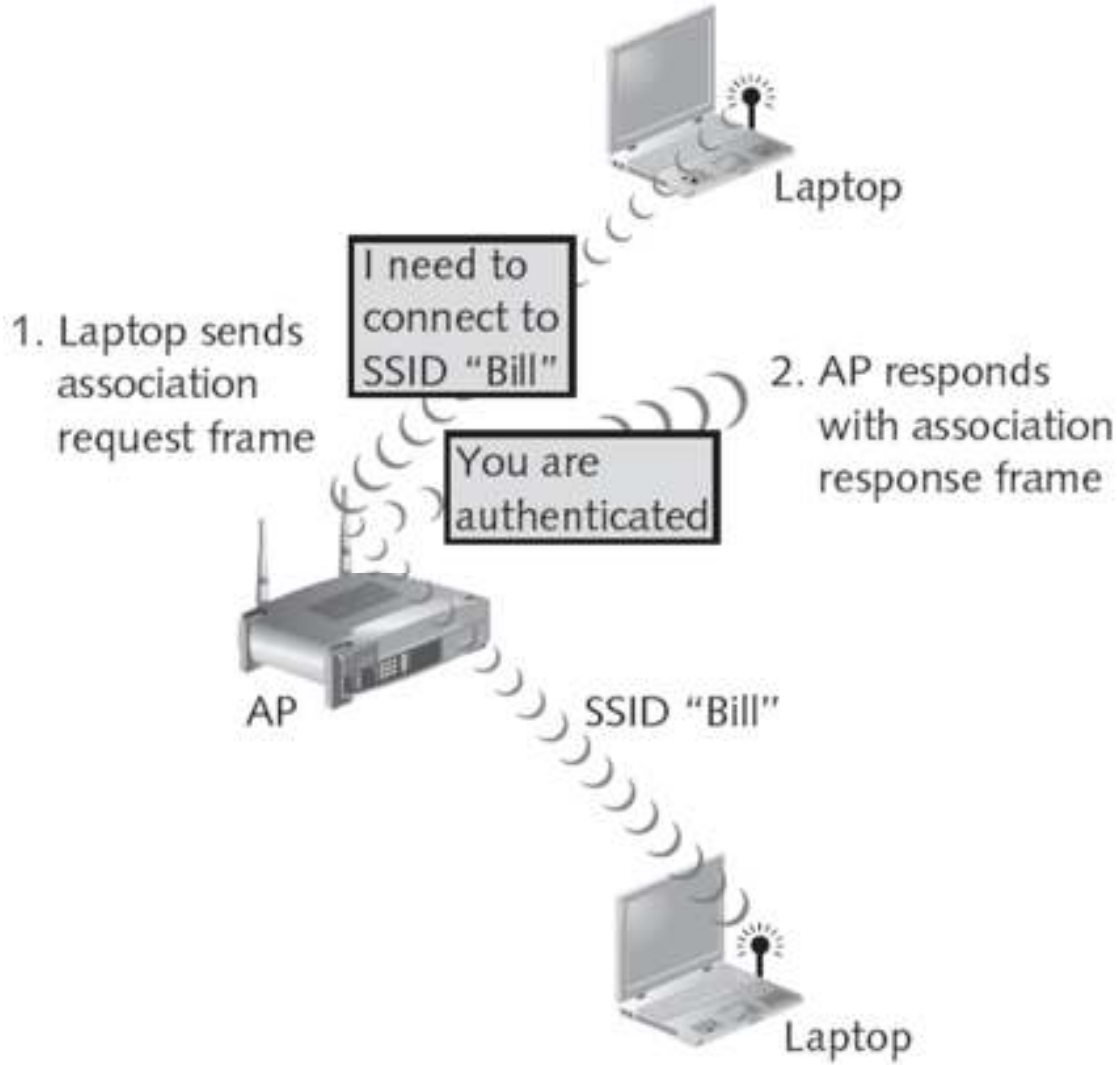


Figure 6-6 Open system authentication

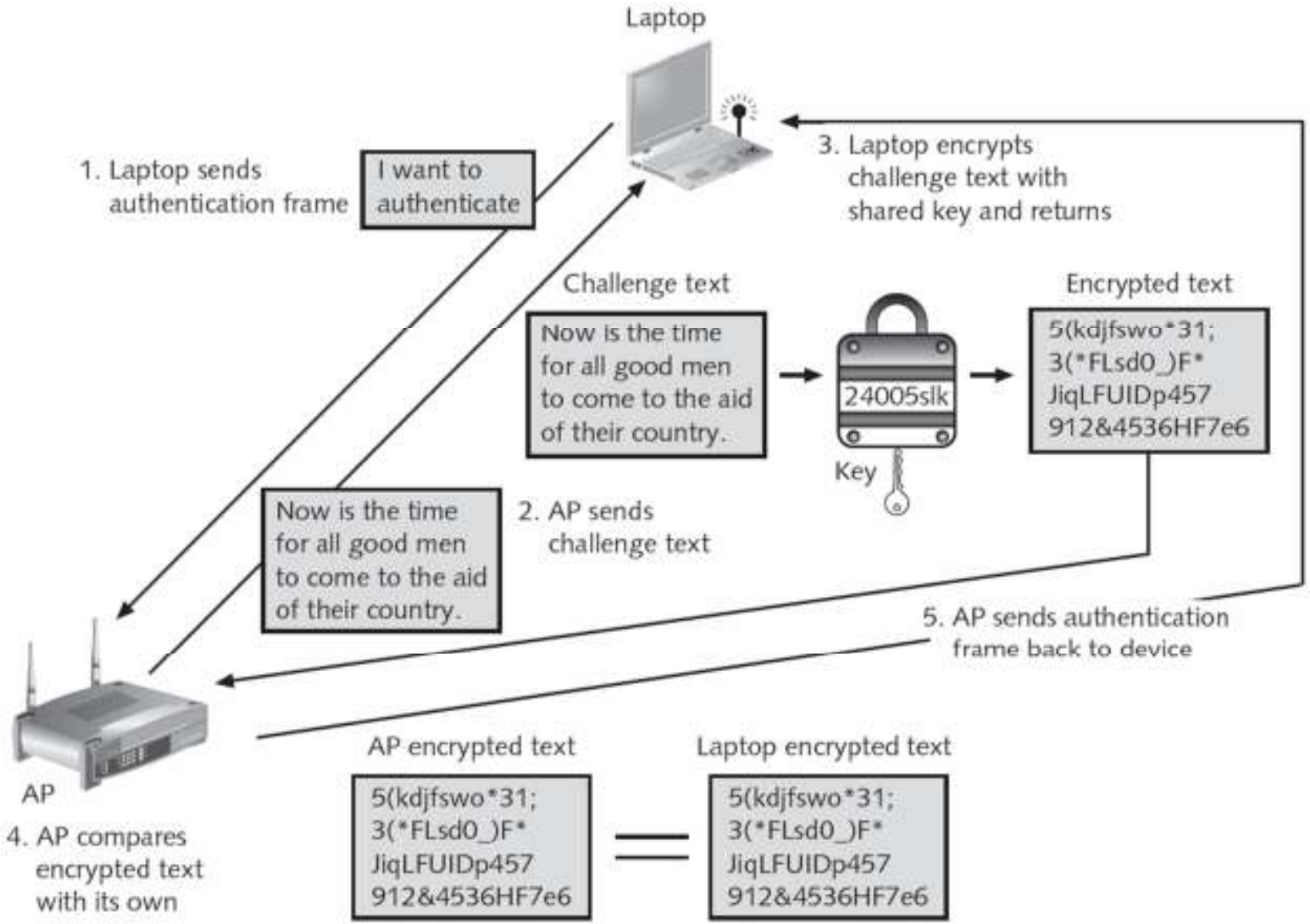


Figure 6-7 Shared key authentication

WEP Summary

- Authentication is first carried out via
  - open system authentication, or
  - shared key authentication

- Data packets are then encrypted using the WEP encryption process described above. Each packet requires a new IV.

WEP Weaknesses

- Static WEP keys (no periodic updates)
- High frequency of repeating the same IV
  - IVs are only 24-bit long
  - Packets can be replayed to force the access point to pump out IVs.
- CRC is weak in integrity check.
  - An attacker can flip a bit in the encrypted data and then change the CRC as well.
- Authentication is too simple.

WPA

WPA History

- Wireless Ethernet Compatibility Alliance (WECA)
  - A consortium of wireless equipment manufacturers and software providers
- WECA goals:
  - To encourage wireless manufacturers to use the IEEE 802.11 technologies
  - To promote and market these technologies
  - To test and certify that wireless products adhere to the IEEE 802.11 standards to ensure product interoperability

WPA History (2)

- In 2002, the WECA organization changed its name to **Wi-Fi (Wireless Fidelity) Alliance**
- In October 2003 the Wi-Fi Alliance introduced **Wi-Fi Protected Access (WPA)**
  - WPA had the design goal to protect both present and future wireless devices, addresses both wireless authentication and encryption
- PSK or 802.11X addresses authentication and TKIP addresses encryption

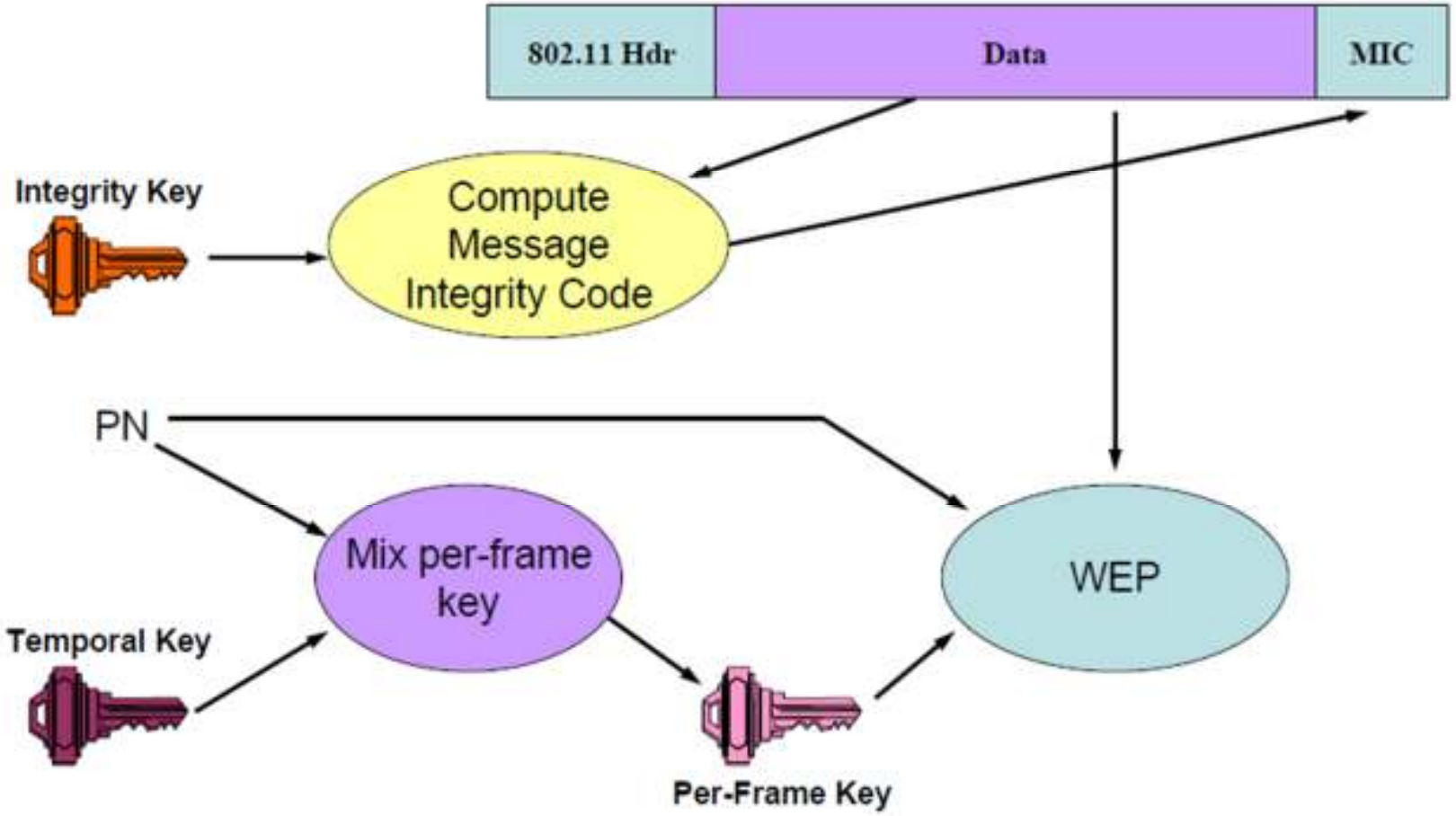
WPA: Improving WEP Encryption

- Key size increased to 128 bits
- Larger IVs: 48-bit long
- Changing security keys through Temporary Key Integrity Protocol (TKIP)
  - Encryption keys are changed (based on a master key) after a certain number of packets have been sent.
  - An IV is mixed with data (not concatenate).
- Ciphering scheme is the same as WEP
  - compatible with old wireless LAN cards

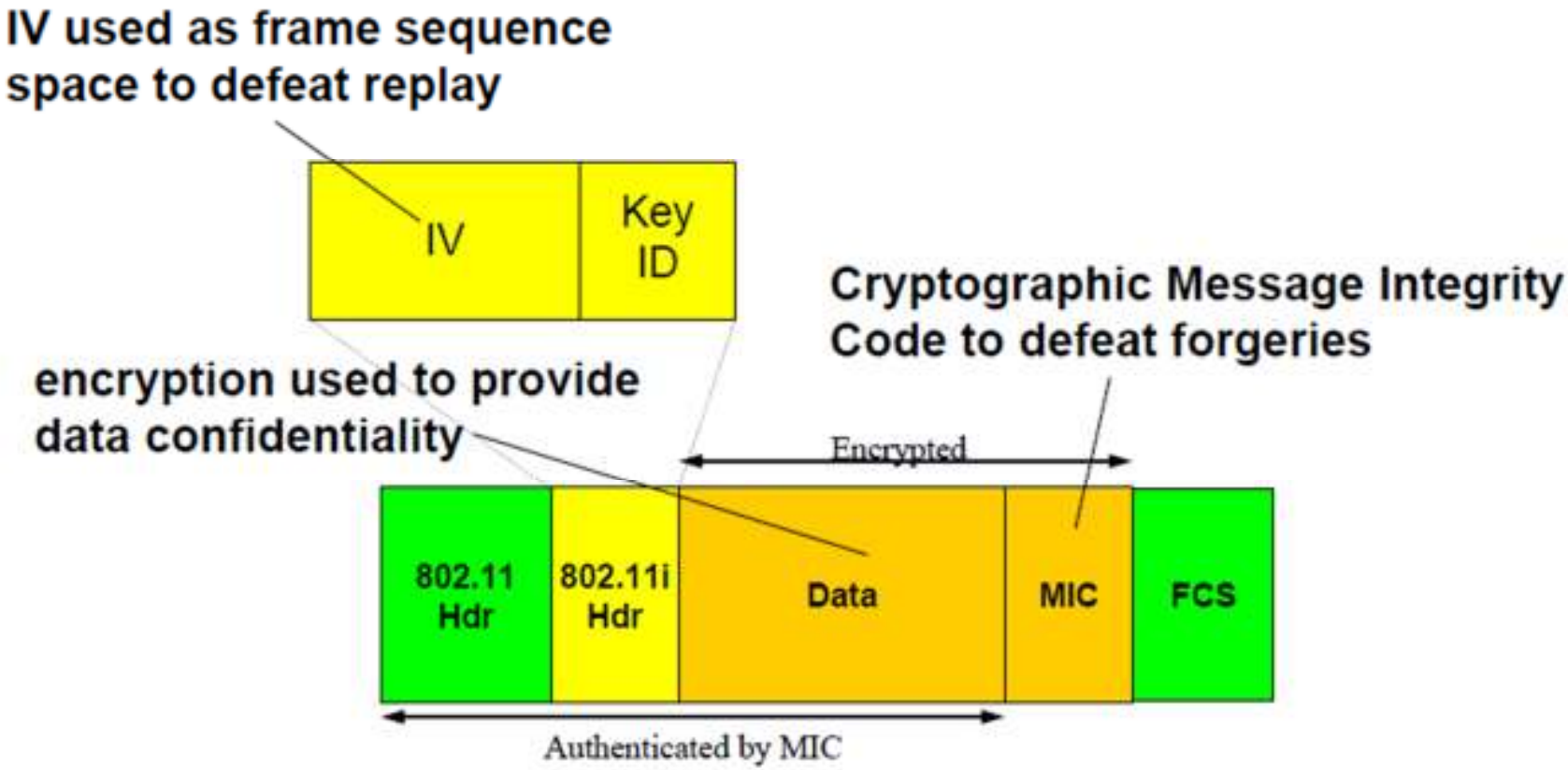
WPA: Improving Integrity Check

- WPA uses a new message integrity check scheme called Michael, replacing the CRC function in WEP.
- A frame counter is added to Michael to avoid replay or forgery attack.

TKIP Overview



Frame Format



WPA Authentication

Two options:

- PSK (inexpensive, home/personal networking)
- 802.11X (expensive, enterprise networking)

WPA Personal Security

- Pre-shared key (PSK) authentication
  - Uses a passphrase to generate the encryption key
- Key must be entered into both the access point and all wireless devices
  - Prior to the devices communicating with the AP
- The PSK is not used for encryption
  - Instead, it serves as the starting point (seed) for mathematically generating the encryption keys
- Results in a pair-wise master key (PMK)
- Followed by a 4-way handshake to handle key management and distribution, which uses the PMK to generate a pair-wise transient key (PTK).

WPA Personal Security (2)

Pre-Shared Key Weakness

- A PSK is a 64-bit hexadecimal number
  - Usually generated from a passphrase
    - Consisting of letters, digits, punctuation, etc. that is between 8 and 63 characters in length
- If the passphrase is a common word, it can be found with a dictionary attack

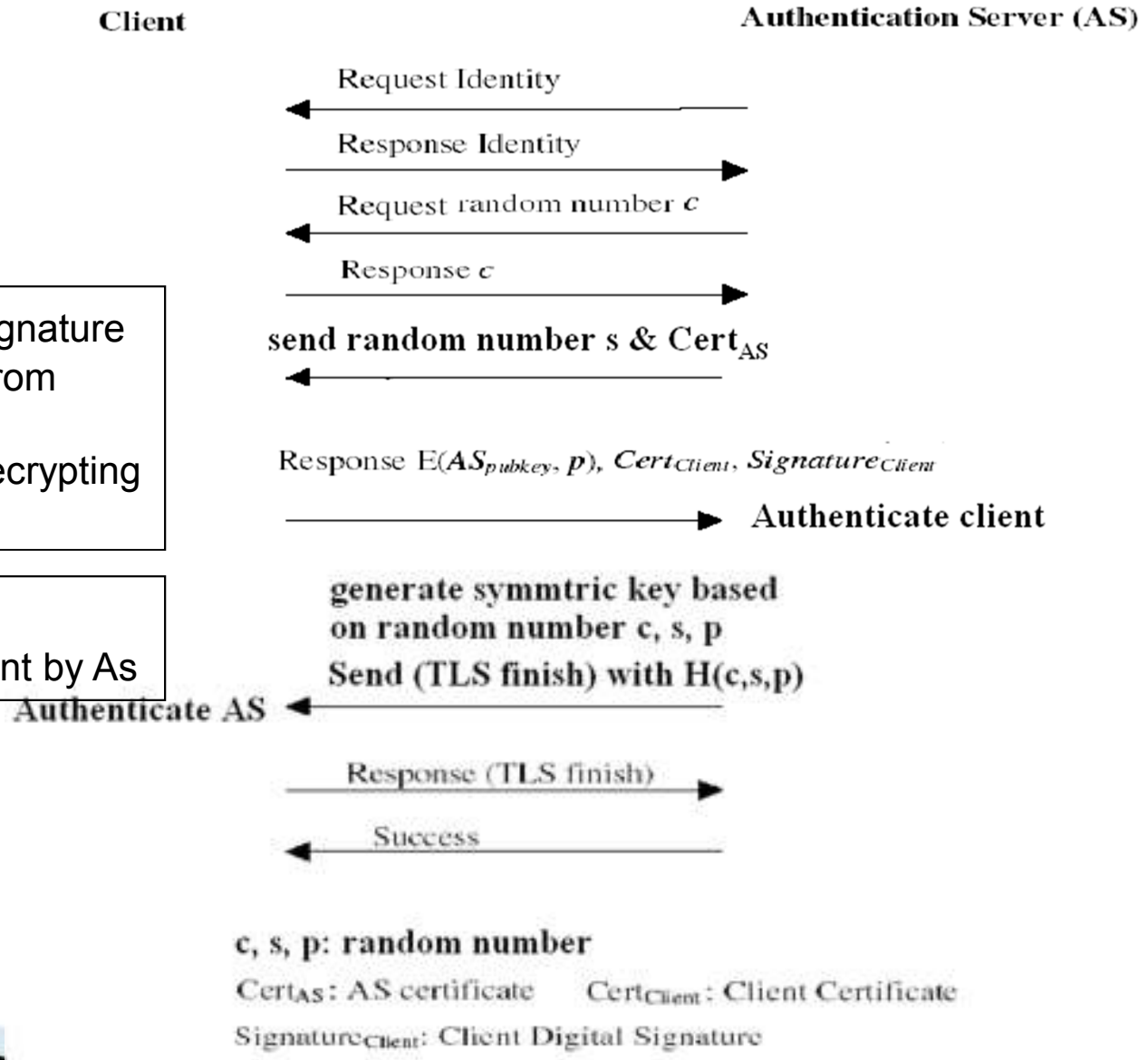
PSK Key Management Weaknesses

- People may send the key by e-mail or another insecure method
- Changing the PSK key is difficult
  - Must type new key on every wireless device and on all access points
  - In order to allow a guest user to have access to a PSK WLAN, the key must be given to that guest

WPA Authentication via 802.11X

- Three components:
  - Remote authentication dial-in user service (RADIUS)
  - authenticator (access point)
  - supplicant (client)
- Uses EAP authentication framework
  - EAP-PSK, EAP-TLS, EAP-TTLS, EAP-MD5
- Results in a pair-wise master key (PMK)
- Followed by a 4-way handshake to handle key management and distribution, which uses the PMK to generate a pair-wise transient key (PTK).

EAP–TLS

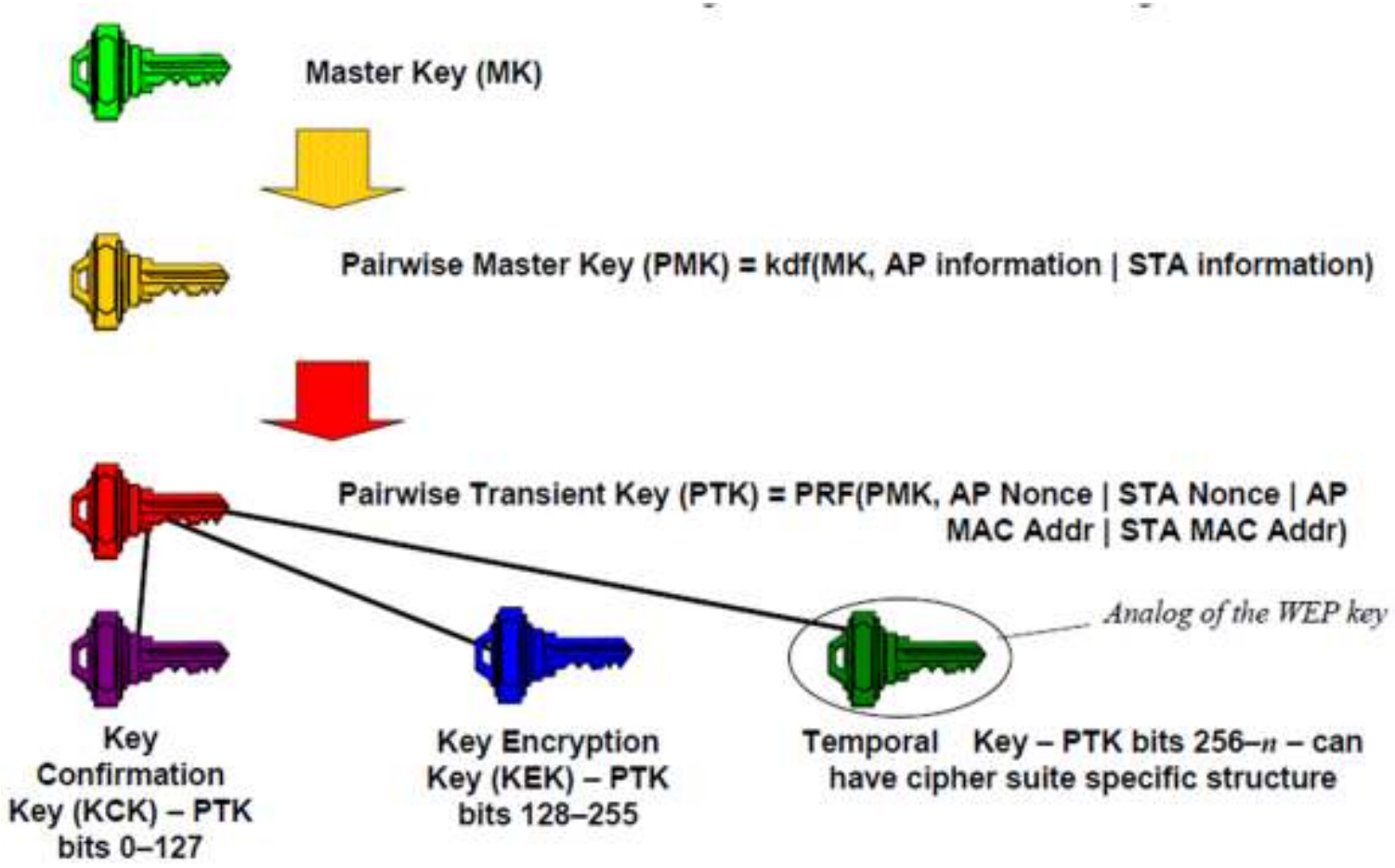


- AS verifies client's digital signature using client's public key got from client's certificate $Cert_{client}$
- Get random number p by decrypting with its private key

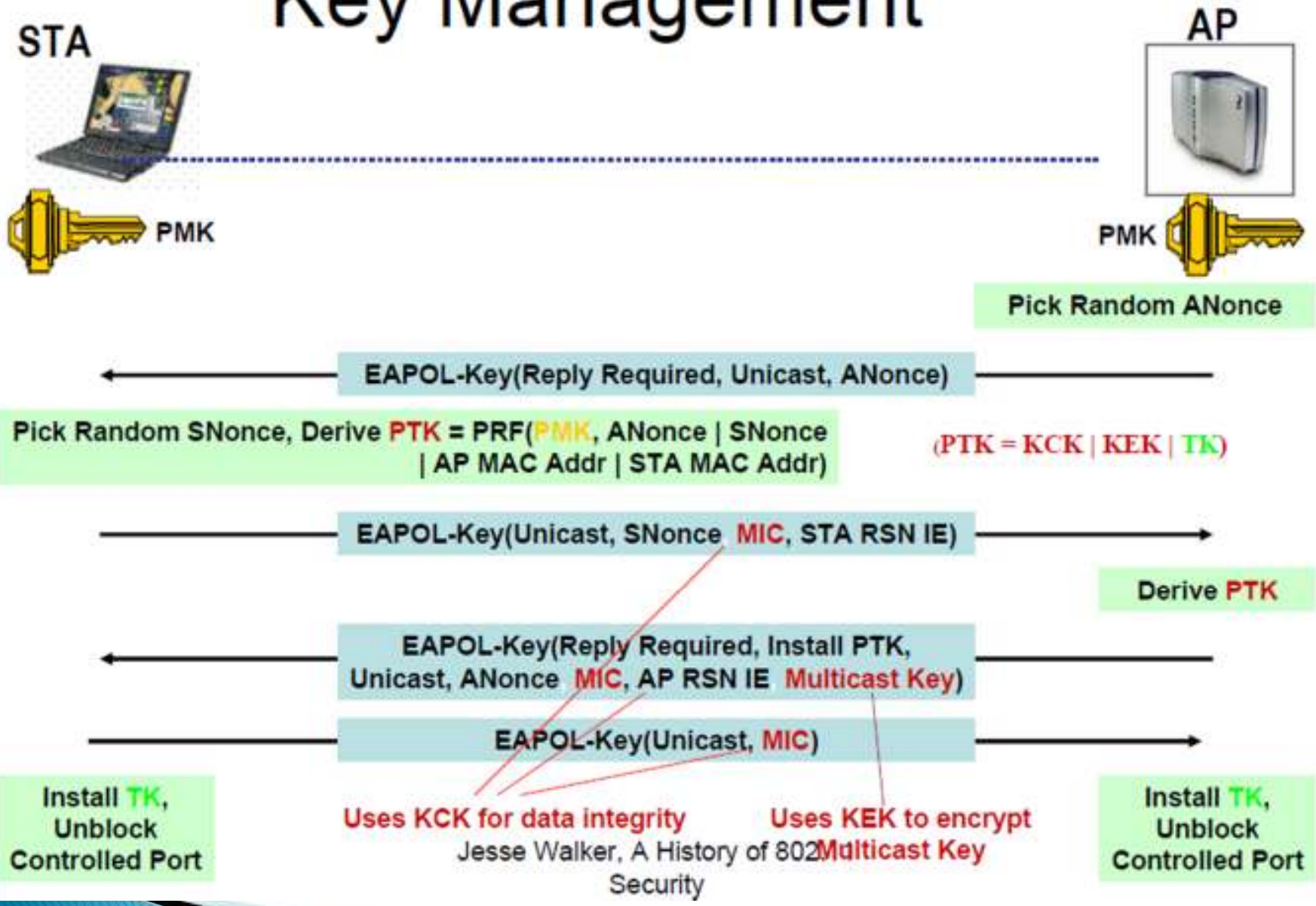
- Client calculates H(c,s,p), compares it with the value sent by As

4-way Handshake

Key Hierarchy



Key Management



Jesse Walker, A History of 802 Security

WPA2

WPA2 Personal Security

- Wi-Fi Protected Access 2 (WPA2)
  - Introduced by the Wi-Fi Alliance in September 2004
  - The second generation of WPA security
  - Still uses PSK (Pre-Shared Key) authentication
  - But instead of TKIP encryption it uses a stronger data encryption method called AES-CCMP

AES: Advanced Encryption Standard

CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

WPA2 Personal Security (2)

- PSK Authentication
  - Intended for personal and small office home office users who do not have advanced server capabilities
  - PSK keys are automatically changed and authenticated between devices after a specified period of time known as the *rekey interval*

WPA2 Personal Security (3)

- AES-CCMP Encryption
  - Encryption under the WPA2 personal security model is accomplished by **AES-CCMP**
  - This encryption is so complex that it requires special hardware to be added to the access points to perform it

WPA and WPA2 Compared

Security Model	Category	Security Mechanism	Security Level
WPA Personal Security	Authentication	PSK	Low-Medium (depends on length of passphrase)
WPA Personal Security	Encryption	TKIP	Medium
WPA2 Personal Security	Authentication	PSK	Medium
WPA2 Personal Security	Encryption	AES-CCMP	High

Table 6-1 Personal wireless security models

WPA2 Enterprise Security

- The most secure method
- Authentication uses IEEE 802.1x
- Encryption is AES-CCMP

Wireless Security Models

Security Model	Category	Security Mechanism	Security Level
WPA Enterprise Security	Authentication	802.1x	High
WPA Enterprise Security	Encryption	TKIP	Medium
WPA2 Enterprise Security	Authentication	802.1x	High
WPA2 Enterprise Security	Encryption	AES-CCMP	High

Table 6-2 Enterprise wireless security models

Security Model	Category	Security Mechanism	Security Level
WPA Personal Security	Authentication	PSK	Low-Medium (depends on length of passphrase)
WPA Personal Security	Encryption	TKIP	Medium
WPA2 Personal Security	Authentication	PSK	Medium
WPA2 Personal Security	Encryption	AES-CCMP	High

Table 6-1 Personal wireless security models

802.11i

- A superset of all WLAN security mechanisms including WEP, WPA and WPA2.
- PSK (personal) or 802.11X (enterprise) is used for authentication and key management.

Reference

- Section 6.3.1, Wireless Mesh Networks, by I. F. Akyildiz and X. Wang