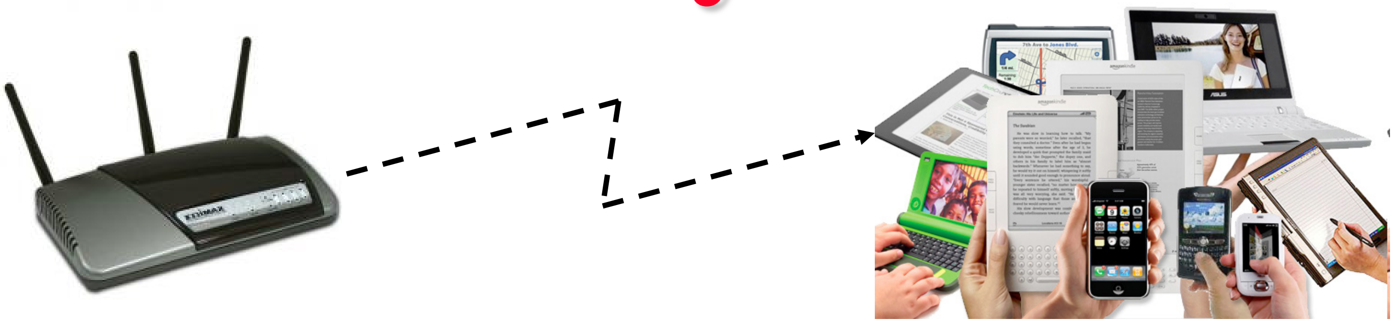
Wireless Network Security



Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-14/

Overview

1. Why Wireless is Insecure and What can we do about it?
2. IEEE 802.11 Wireless LAN Overview
3. Legacy 802.11 Security: WEP
4. IEEE 802.11i Wireless LAN Security: WPA, WPA2

These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 6th Ed, 2013.

Why Wireless is Insecure?

- **Channel**: Broadcast ⇒ Eavesdropping, Jamming, Active attacks on protocols
- **Mobility**: Portable devices ⇒ Not physically secured
- **Resources**: Limited memory and processing resources ⇒ Need simpler security
- **Accessibility**: May be left unattended

Wireless Network Threats

1. **Accidental Association**: Overlapping networks ⇒ unintentionally connect to neighbors

2. **Malicious Association**: Malicious access points (Free public WiFi) can steal passwords

3. **Ad-Hoc Networks**: Two computers can exchange data

4. **Nontraditional Networks**: Bluetooth can be used to eavesdrop

5. **MAC Spoofing**: Change MAC address to match a privileged computer

6. **Man-In-The-Middle Attacks**: Using rogue access point between the user and the real access point

7. **Denial of Service (DoS):** Keep the media busy

8. **Network Injection**: Spoof routing/management messages

Countermeasures

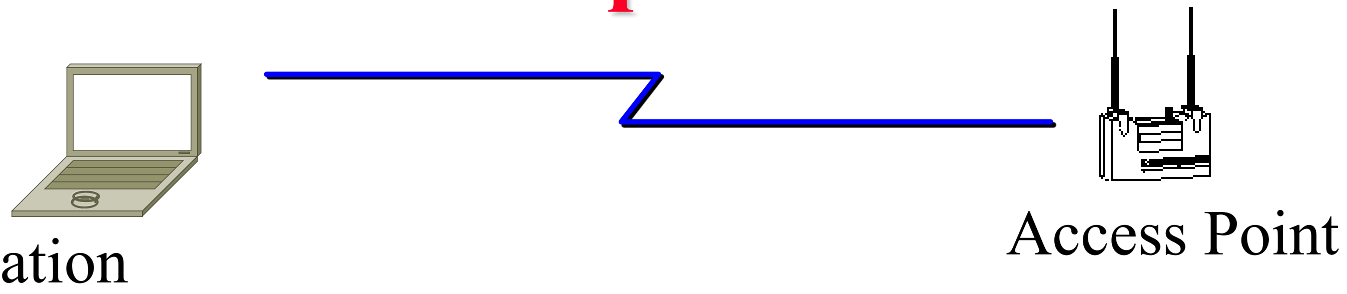
- Turn-off SSID broadcast
- Use Cryptic SSID names
- Reduce signal strength
- Locate APs away from boundary
- Use encryption
- Use IEEE 802.1x network access control
- Change the router's user ID from default
- Change the router's password from default
- MAC Filtering: Only specific MAC address connect

Mobile Device Security

Mobile ⇒ Dynamic/no boundary ⇒ Cloud

1. Lack of Physical security: Mobiles cannot be locked
2. Not all devices can be trusted
3. Untrusted networks between device and the organization
4. Wide variety of contents on mobiles than on other computers (music, video, games, …)
5. Apps from untrusted vendors
6. Data may get on unsecured device
7. Location information may be used for attack

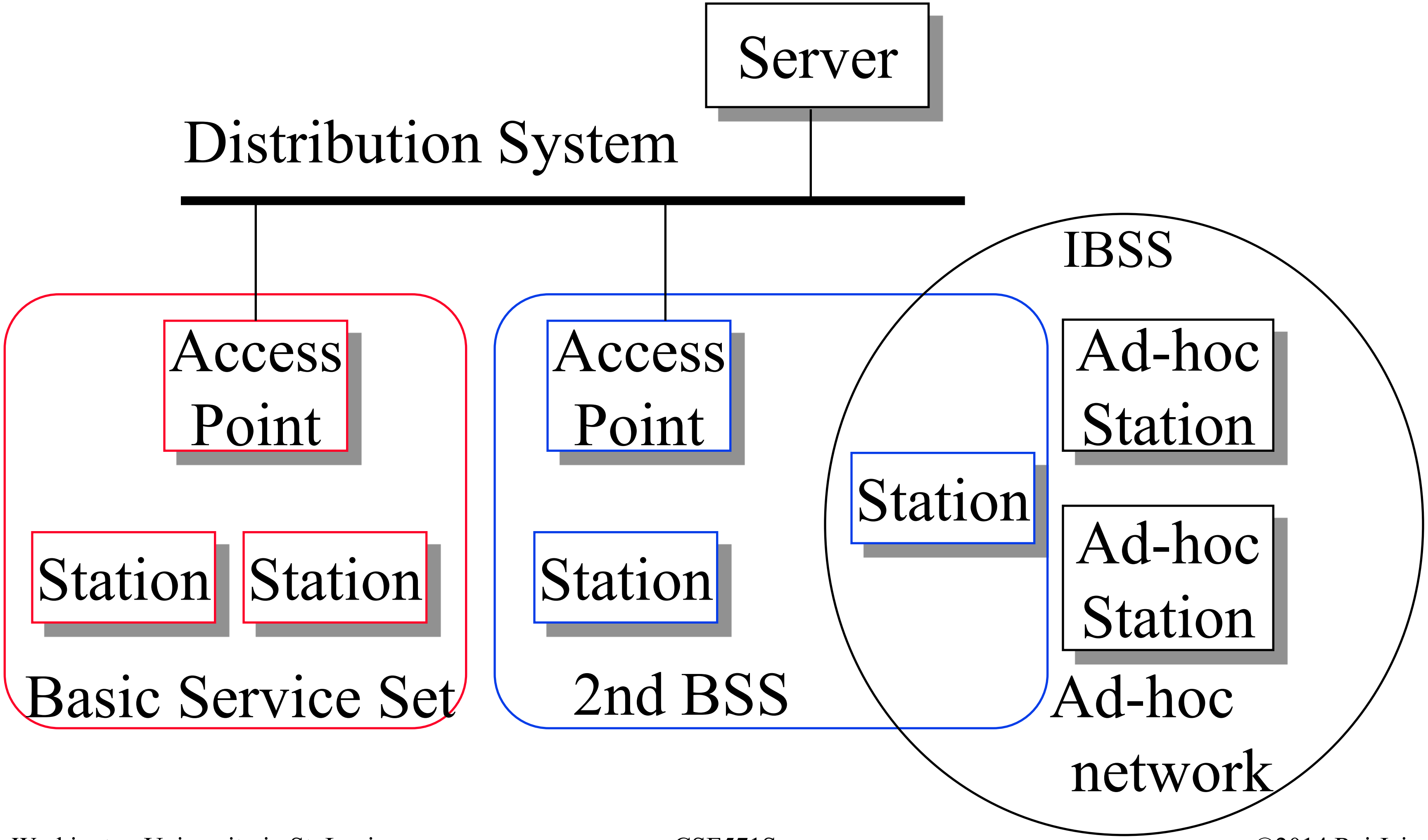
Wi-Fi Operation



- Access Points (APs) periodically broadcast a beacon with SSID (service set ID) and security level
- Subscriber stations listen to these beacons, measure signal strength and determine which AP to join
- Subscribers can also send a "Probe" to find AP's in the neighborhood
- AP authenticates the subscriber station using shared keys
- Subscriber stations and AP exchange encrypted packets
- Subscriber station send a "Disassociate" message and log off

Ref: http://en.wikipedia.org/wiki/Service_set_%28802.11_network%29

IEEE 802.11 Architecture



IEEE 802.11 Architecture (Cont)

- Basic Service Area (BSA) = Cell
- Each BSA may have several access points (APs)
- Basic Service Set (BSS)
  = Set of stations associated with one AP
- Distribution System (DS) - wired backbone
- Extended Service Area (ESA) = Multiple BSAs interconnected via a distribution system
- Extended Service Set (ESS)
  = Set of stations in an ESA
- Independent Basic Service Set (IBSS): Set of computers in ad-hoc mode. May not be connected to wired backbone.
- Ad-hoc networks coexist and interoperate with infrastructure-based networks

IEEE 802.11 Services

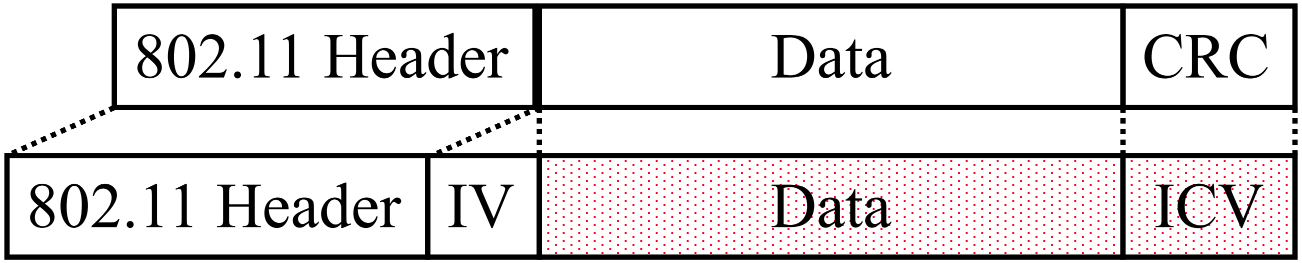
- **Association**: A STA connecting with an AP.
- **Disassociation**: Termination of association.
- **Re-association**: Transfer of association from one AP to another. Mobility within BSS, within ESS, between two ESSs.
- **MSDU Delivery**: Interchange of packets between STAs
- **Distribution**: Delivery of packets between STAs possibly via the backbone distribution system
- **Integration**: Interchange of packets between STAs and wired stations connected to LANs on the distribution system
- **Authentication**: The station is authenticated
- **De-authentication**
- **Privacy**: Encryption

Wired Equivalent Privacy (WEP)

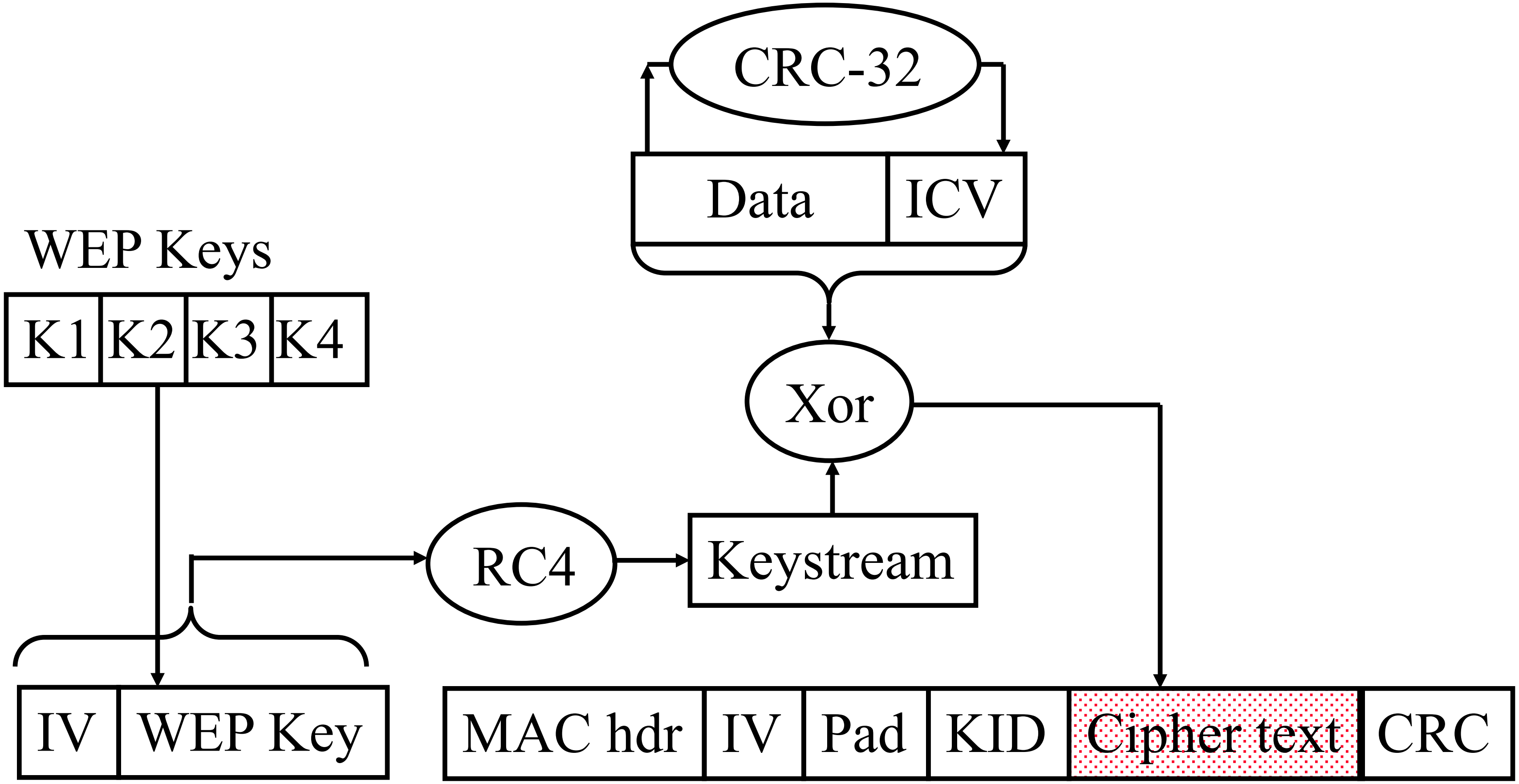
- WEP ⇒ Privacy similar to a wired network
  ⇒ Intellectual property not exposed to casual browser
  ⇒ Not protect from hacker
- First encryption standard for wireless. Defined in 802.11b
- Provides authentication and encryption
- Shared Key Authentication
  ⇒ Single key is shared by all users and access points

WEP Details

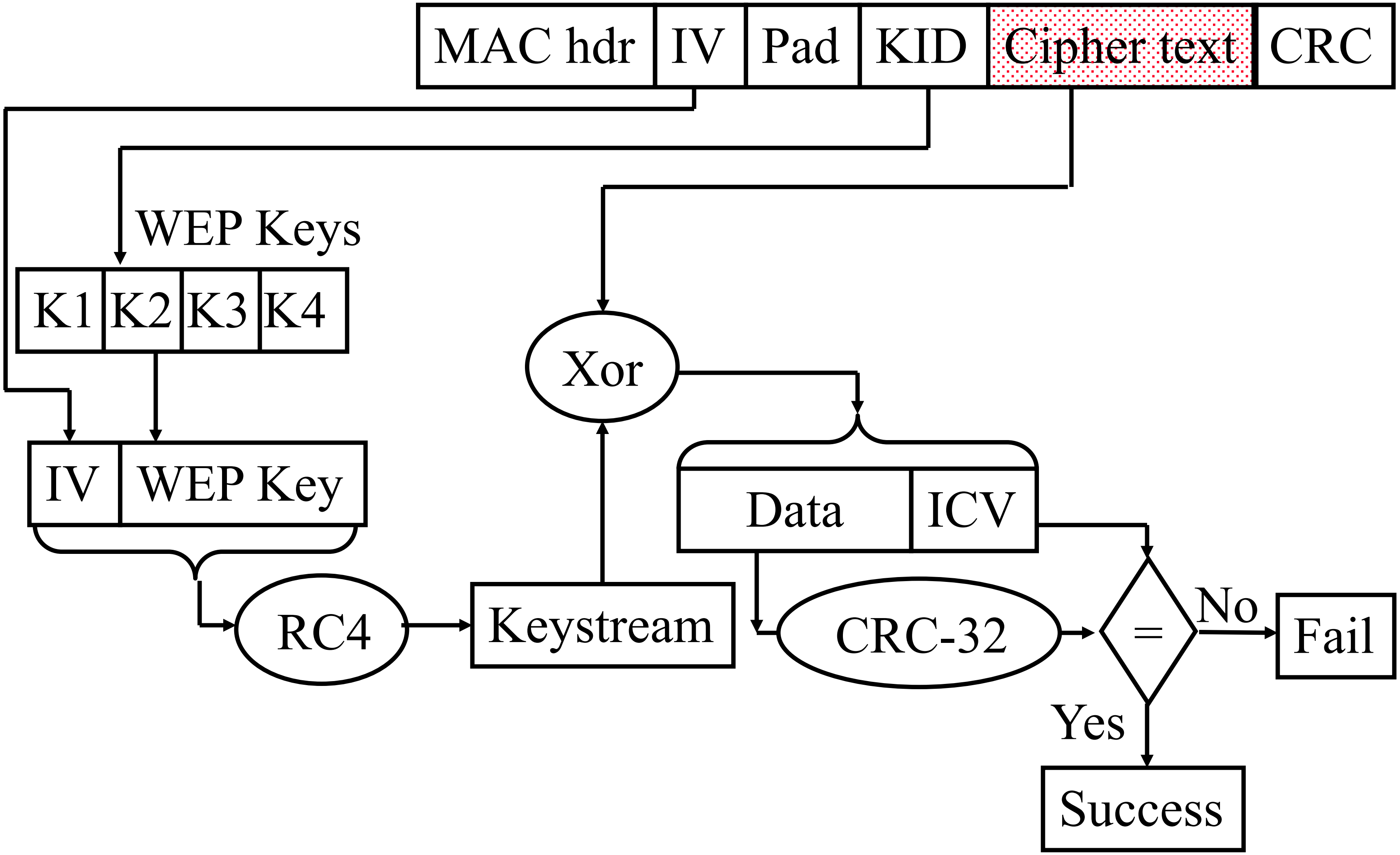
- Each device has 4 static WEP keys
- 2-bit key ID sent w Initialization Vector (IV) in clear in each packet
- Per-Packet encryption key =24-bit IV + one of pre-shared key
- Encryption Algorithm: RC4
  - Standard: 24 + 40 = 64-bit RC4 Key
  - Enhanced: 24 + 104 = 128 bit RC4 key
- WEP allows IV to be reused
- CRC-32 = Integrity Check Value (ICV)
- Data and ICV are encrypted under per-packet encryption key



WEP Encapsulation

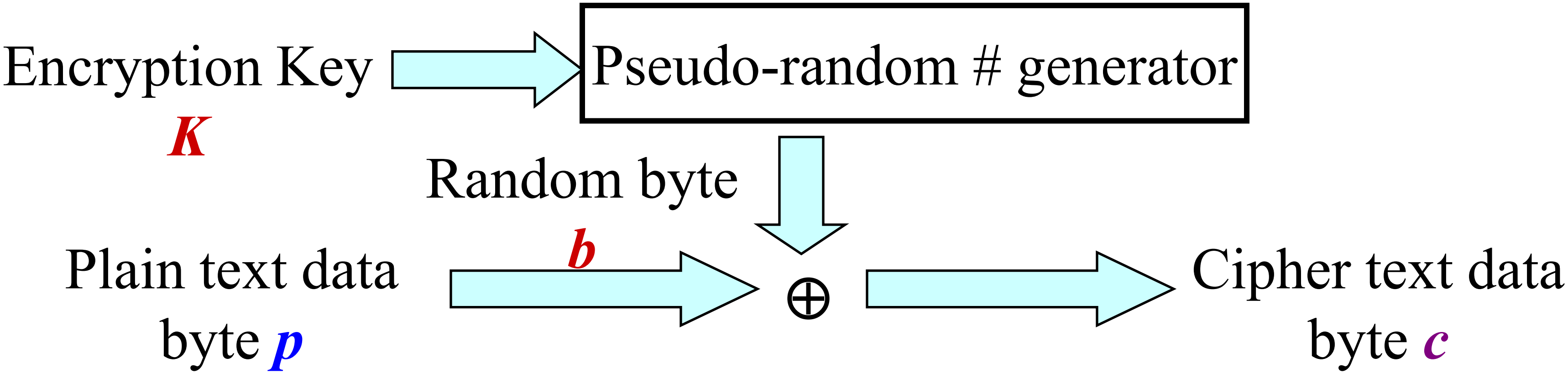


WEP Decapsulation



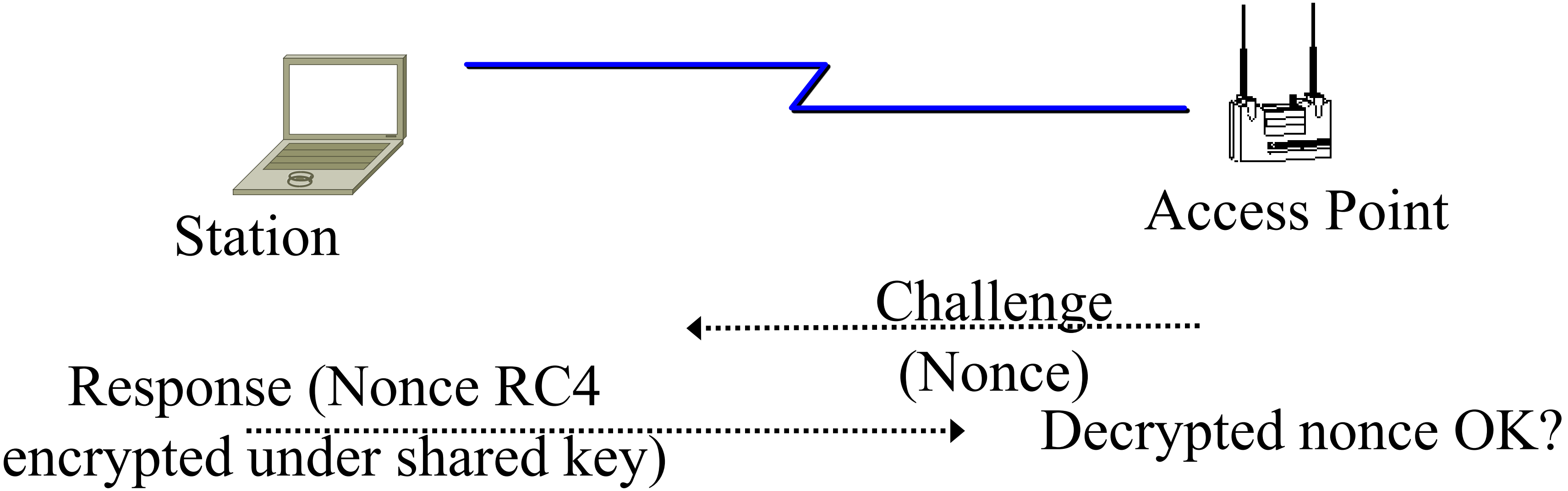
Ron's Cipher 4 (RC4)

- Developed by Ron Rivest in 1987. Trade secret. Leaked 1994.
- Stream Cipher
  - A pseudo-random stream is generated using a given key and xor'ed with the input
- Pseudo-random stream is called **One-Time pad**
- Key can be 1 to 256 octet
- See the C code in the textbook [KPS].



WEP Authentication

- Authentication is a via Challenge response using RC4 with the shared secret key.



Station

Access Point

Challenge (Nonce)

Response (Nonce RC4 encrypted under shared key)

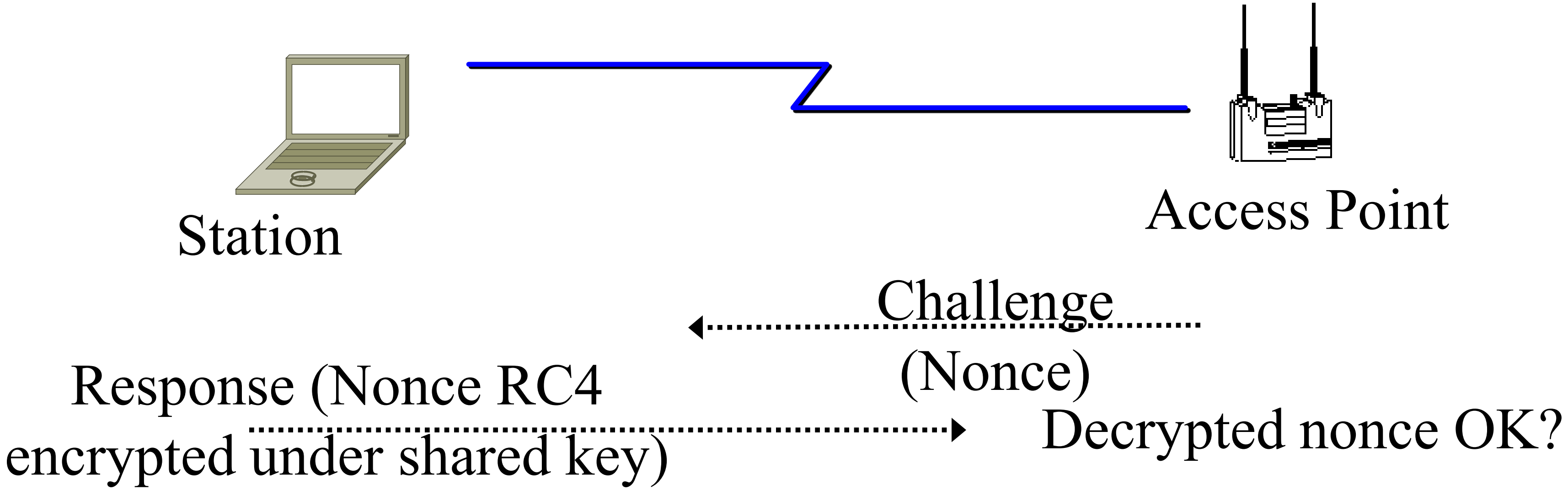
Decrypted nonce OK?

WEP Review

- Four 40-bit or 104-bit Keys are manually programmed in each subscriber station and AP
- A 24-bit IV and WEP key is used to form a 64b or 128b RC4 key
- A keystream is generated using the RC4 key
- A 32-bit CRC is added as “Integrity check value” (ICV) to the packet
- Plain text and keystream is xor’ed. A 32-bit CRC is added in clear.

Problems with WEP Authentication

- ❑ Record one challenge/response
- ❑ Both plain text and encrypted text are available to attacker
- ❑ XOR the two to get the keystream
- ❑ Use that keystream and IV to encrypt any subsequent challenges



Station

Access Point

Challenge (Nonce)

Response (Nonce RC4 encrypted under shared key)

Decrypted nonce OK?

Problem with Stream Cipher

- Consider two packets with the same IV ⇒ Same keystream **b**
- **c**1 = **p**1 ⊕ **b**; **c**2 = **p**2 ⊕ **b** ⇒ **c**1 ⊕ **c**2=**p**1 ⊕ **p**2
- Two packets w same IV ⇒ XOR = Difference in plain text
- 50% chance of using the same IV in 4823 packets.
- Recovered ICV matches ⇒ Plain text is correct
- Possible to recover all 2^{24} keystreams in a few hours

Problems with WEP ICV

- CRC is used as ICV
- CRC: Message polynomial is shifted and divided by CRC polynomial, the remainder is sent as CRC

$$\boldsymbol{p} = p_n x^n + p_{n-1} x^{n-1} + \ldots + p_0 x^0$$

- Remainder(**p**+**q**, c)

  = Remainder(**p**, c) + Remainder(**q**, c)
- ICV is linear: ICV(**p**+**q**) = ICV(**p**) + ICV(**q**)
- **Conclusion**: XOR any CRC-32 valid plain text to encrypted packet. The modified packet will pass the ICV after decryption.

WEP Problems

- No centralized key management
  Manual key distribution ⇒ Difficult to change keys
- Single set of Keys shared by all ⇒ Frequent changes necessary
- No mutual authentication
- No user management (no use of RADIUS)
- IV value is too short. Not protected from reuse.
- Weak integrity check.
- Directly uses master key
- No protection against replay

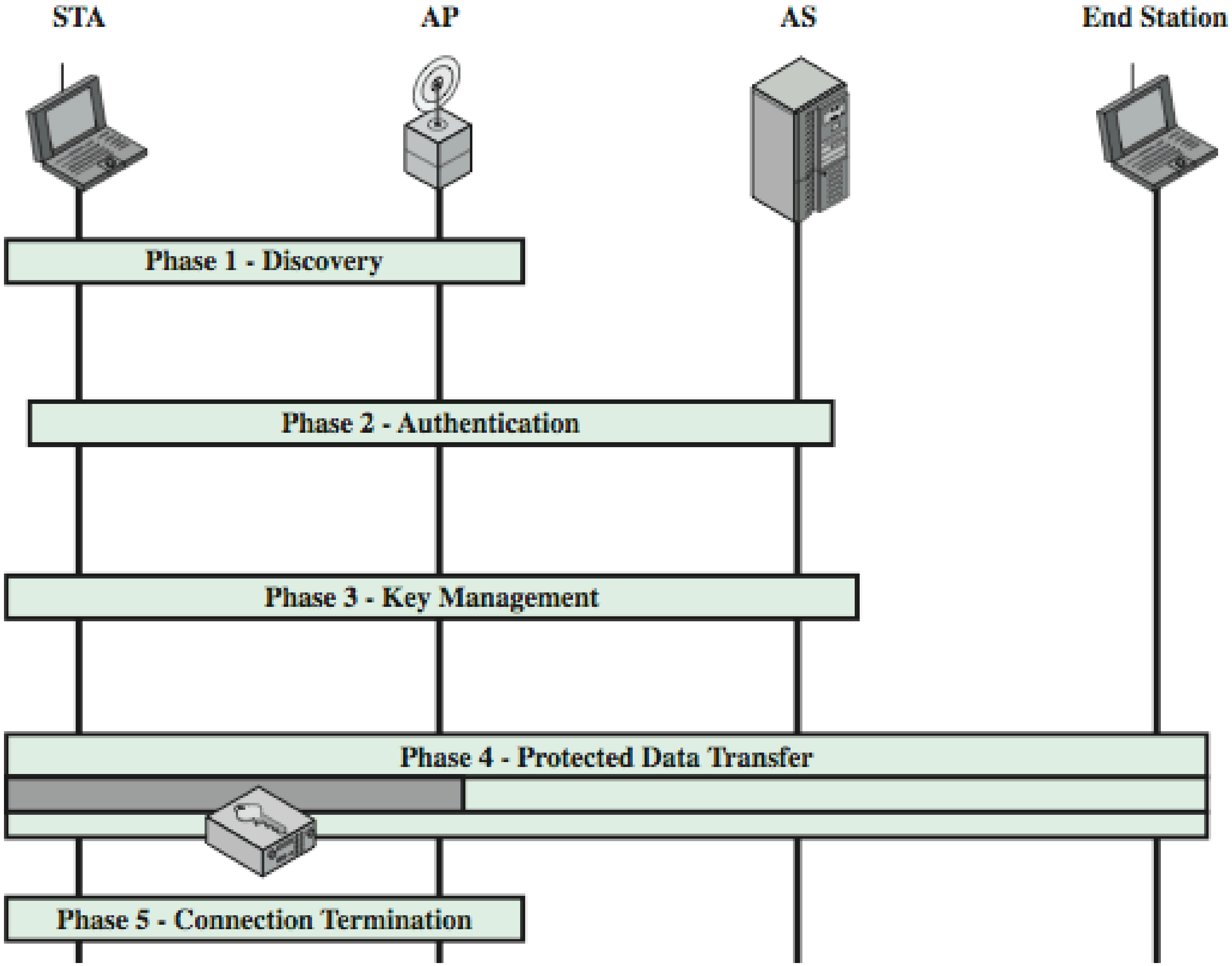
Ref: http://en.wikipedia.org/wiki/Wireless_security, http://en.wikipedia.org/wiki/Wireless_LAN_security, http://en.wikipedia.org/wiki/Cracking_of_wireless_networks

802.11i Wireless LAN Security

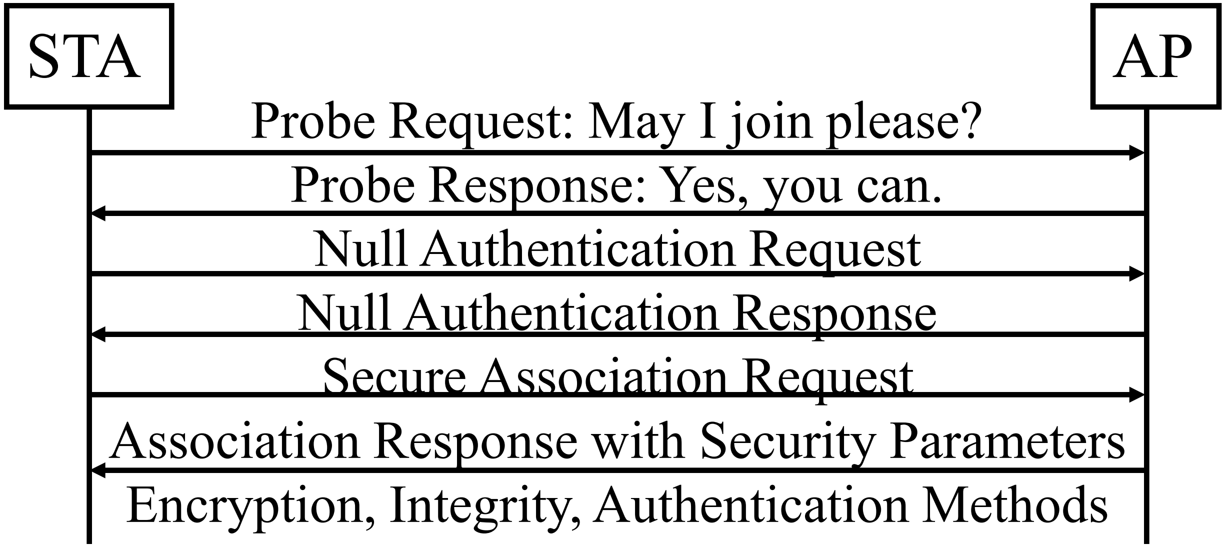
- Wi-Fi Alliance **Wi-Fi Protected Access (WPA)** Software modification to existing WEP systems
  - Key mixing function to generate per packet key
  - Sequence Number to protect against replay attacks
  - 64-bit message integrity check (MIC)
  - Uses the same RC4 encryption
- 802.11i **Robust Security Network (RSN) or WPA2** Requires hardware replacement
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
  - AES encryption with counter mode

Ref: http://en.wikipedia.org/wiki/IEEE_802.11i-2004, http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol, http://en.wikipedia.org/wiki/CCMP

802.11i Phases of Operation

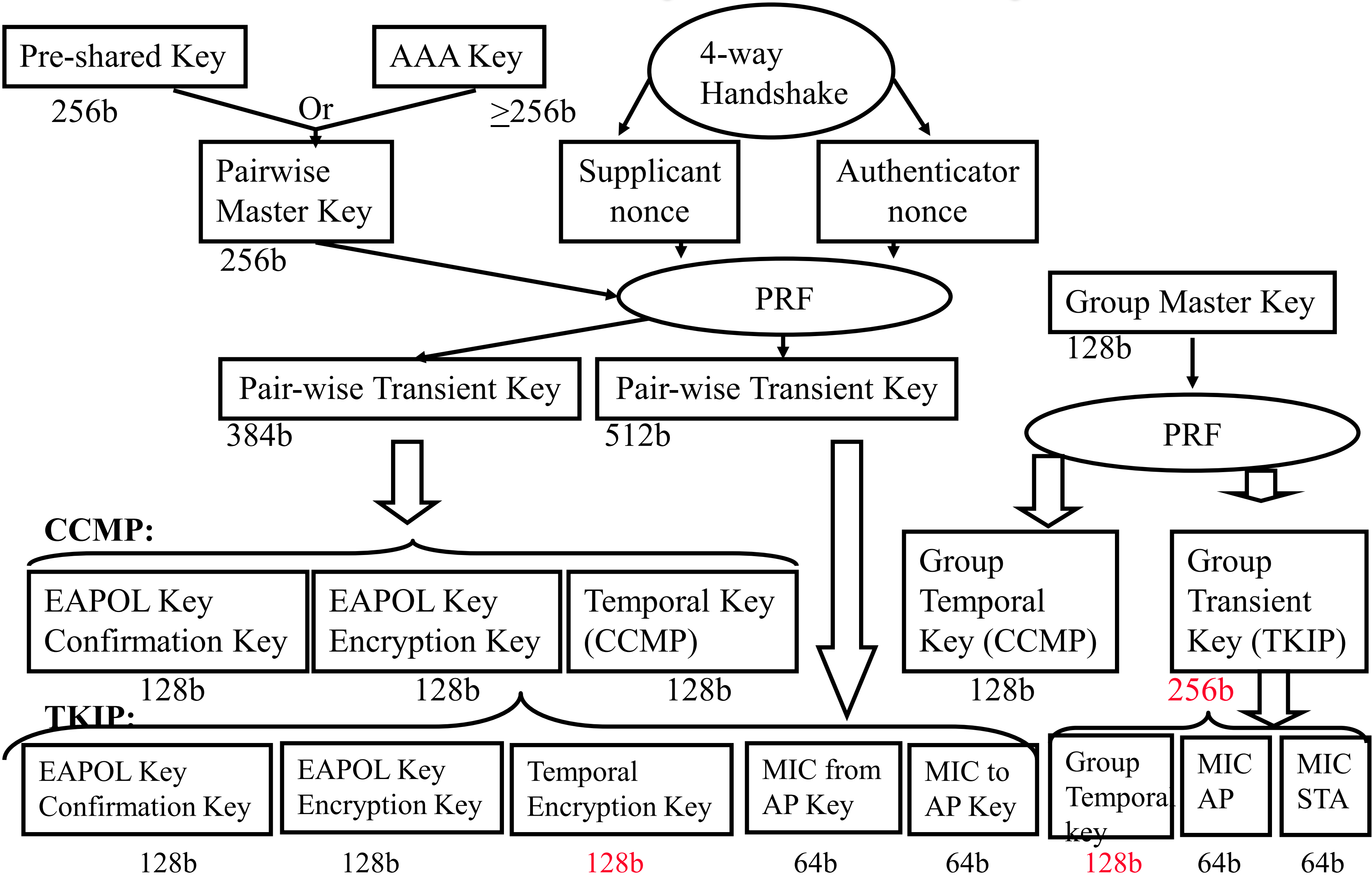


IEEE 802.11i Discovery Phase

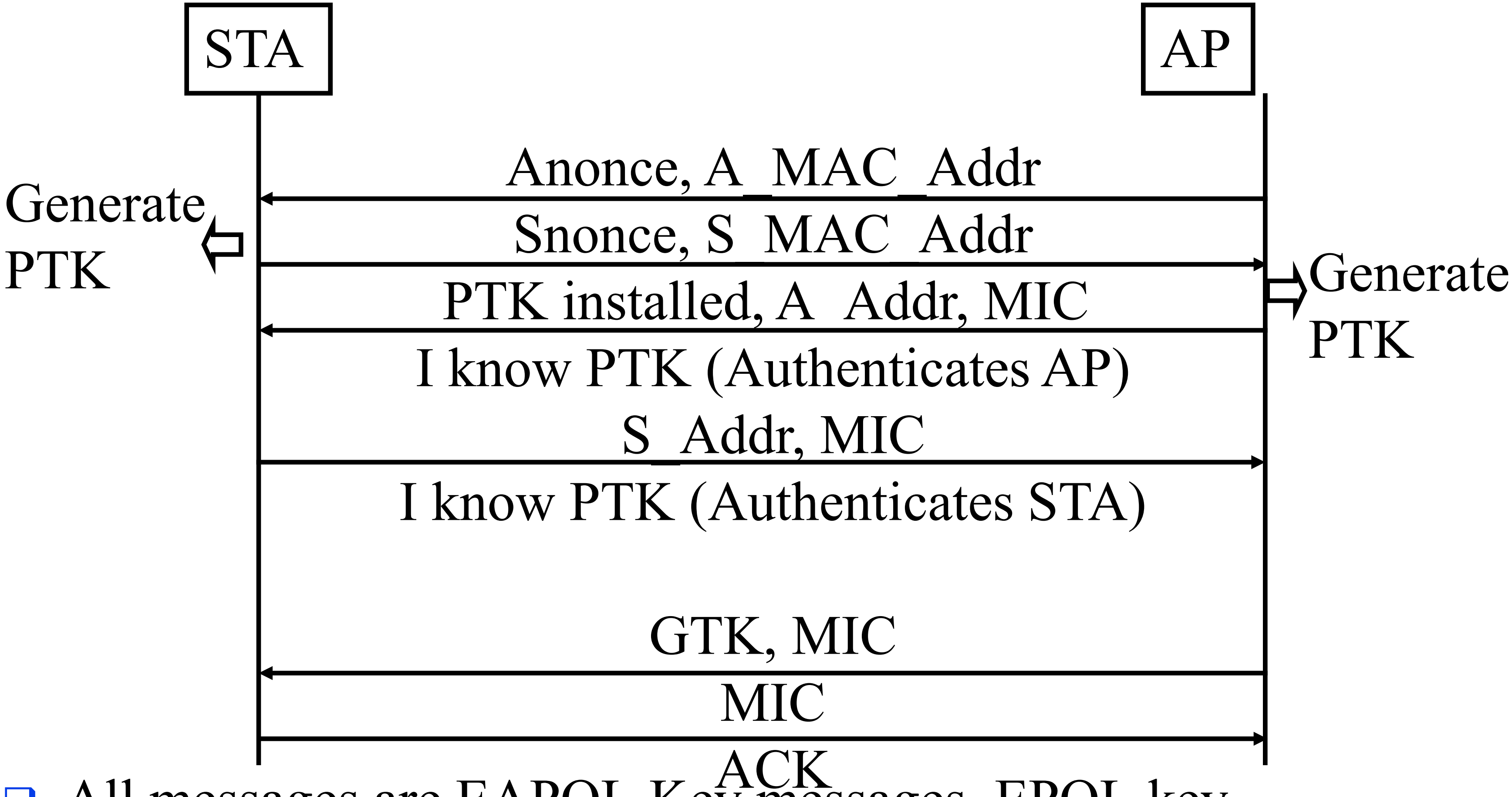

STA
AP
Probe Request: May I join please?
Probe Response: Yes, you can.
Null Authentication Request
Null Authentication Response
Secure Association Request
Association Response with Security Parameters
Encryption, Integrity, Authentication Methods

- Capability negotiation
  - Confidentiality and Integrity: WEP, TKIP, CCMP, vendor specific
  - Authentication: 802.1x, Pre-shared key, vendor specific

802.11i Key Hierarchy



Key Management



STA

AP

Generate PTK

Anonce, A_MAC_Addr

Snonce, S_MAC_Addr

Generate PTK

PTK installed, A_Addr, MIC

I know PTK (Authenticates AP)

S_Addr, MIC

I know PTK (Authenticates STA)

GTK, MIC

MIC

ACK

- All messages are EAPOL Key messages. EPOL key confirmation key is used to compute MIC for EPOL messages.

Ref: http://en.wikipedia.org/wiki/IEEE_802.11i-2004

802.11i Protected Data Transfer Phase

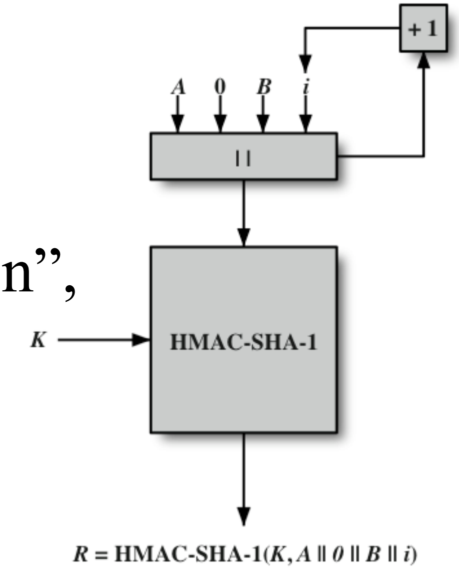
Two schemes for protecting data

- Temporal Key Integrity Protocol (TKIP)
  - S/w changes only to older WEP
  - Adds 64b Michael message integrity code (MIC) instead of 32b CRC in WEP
  - Encrypts MPDU plus MIC value using 128b RC4
- Counter Mode-CBC MAC Protocol (CCMP)
  - Uses cipher block chaining message authentication code (CBC-MAC) for integrity
  - Uses Counter mode AES for encryption

Ref: http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol, http://en.wikipedia.org/wiki/CCMP

IEEE 802.11i Pseudo-Random Fn

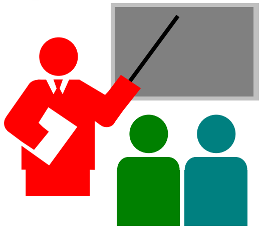
- PRF is required to generate nonces and keys.
- HMAC-SHA-1 is used for all
- 4 Inputs: K=Secret Key, A= Use specific text string, B= Use specific Data, length
- Set counter to 0 and take desired number of bits from the left (if less than 160)
- If more than 160 bits needed, run the function again with the next sequence number
- Example: Pair-wise Temporal Key for CCMP
  - PTK=PRM{PMK, "Pairwise key expansion", min(AP Addr, STA Addr)||max(AP-Addr, STA-Addr)||min(Anonce, Snonce)|| max(Anonce,Snonce), 384}



Security Problems Addressed

- No MAC address spoofing: MAC address included in both Michael MIC and CCMP MAC
- No replay: Each message has a sequence number (TSC in TKIP and PN in CCMP)
- No dictionary based key recovery: All keys are computer generated binary numbers
- No keystream recovery: Each key is used only once in TKIP. No keystream in CCMP.
- No Weak Key Attack: Special byte in IV in TKIP prevents weak keys. Also, keys are not reused.
- No rouge APs: Mutual authentication optional. Some APs provide certificates.
- **Not Addressed**: DoS attack using disassociation or deauthentication attack. Mgmt frames are still not encrypted.

Summary



1. Wireless networks and mobile devices are subject to more attacks than wired network or static devices
2. 802.11 LANs consist of Basic Service Areas connected via a wired distribution system into an Extended Service Area
3. 802.11 originally used Wired Equivalent Privacy (WEP) which used RC4 for encryption and CRC-32 for MAC. Both were trivial to attack.
4. TKIP or WPA provides per-packet key and 64-bit MIC using RC4.
5. RSN or WPA2 provides stronger encryption and authentication using AES.

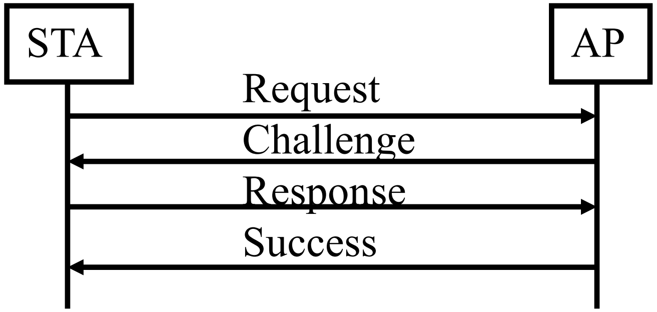
Homework 18

- WEP assumed all devices in the network share a secret key. The purpose of the authentication scenario is for the STA to prove that it possesses the secret key. As shown in the figure below, the STA sends a message to AP requesting authentication. The AP issues a challenge, which is a sequence of 128 random bytes sent as plain text. The STA encrypts the challenge with the shared key and returns it to the AP. The AP decrypts the incoming value and compares it to the challenge that it sent. If there is a match, the AP confirms that authentication has succeeded.

a. This authentication scheme is one-sided. How can it be made mutual?

b. What information does it provide to an attacker making it easy to attack?

c. The encryption scheme is RC4 stream cipher. How can a attacker create a valid response for any challenge after watching just one valid authentication.


STA
AP
Request
Challenge
Response
Success