Wireless LAN Security II: WEP Attacks, WPA and WPA2

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/cse571-07/

Overview

- Wireless Networking Attacks
- Wireless Protected Access (WPA)
- Wireless Protected Access 2 (WPA2)

Wireless Networking Attacks

1. MAC Address Spoofing Attack
2. Disassociation and Deauthentication Attacks
3. Shared Key Authentication Attacks
4. Known Plaintext Attack
5. Reaction Attack
6. Message Modification Attack
7. Inductive Attack
8. Reuse IV Attack
9. WEP Key Attacks
10. FMS Attack
11. Dictionary Attack on LEAP
12. Rouge APs
13. Ad-Hoc Networking Issues

MAC Address Spoofing Attack

- AP has list of MAC addresses that are allowed to enter the network
- Attacker can sniff the MAC addresses and spoof it

Disassociation and Deauthentication Attacks

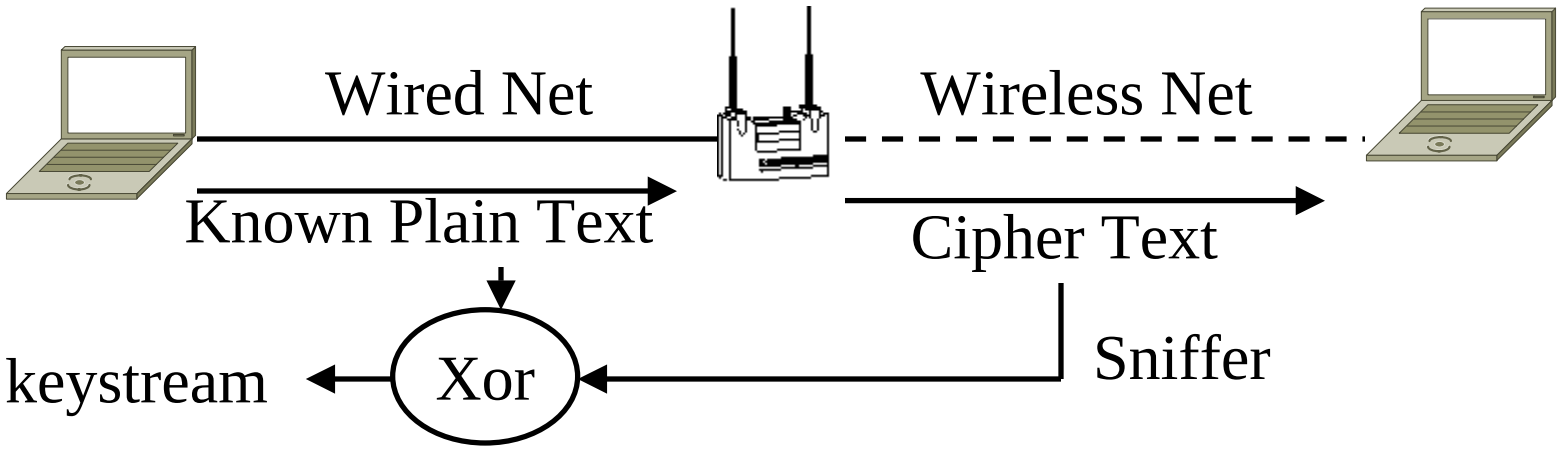
- WiFi stations authenticate and then associate
- Anyone can send disassociate packets
- Omerta, http://www.securityfocus.com/archive/89/326248 simply sends disassociation for every data packet
- AirJack, http://802.11ninja.net includes essid_jack which sends a disassociation packet and then listens for association packets to find hidden SSIDs that are not broadcast
- fata_jack sends invalid authentication requests spoofing legitimate clients causing the AP to disassociate the client
- Monkey_jack deauthenticates a victim and poses as the AP when the victim returns (MitM)
- Void11, www.wlsec.net/void11 floods authenticate requests to AP causing DoS

Shared Key Authentication Attacks

- Authentication challenge is sent in clear
- XOR of challenge and response ⇒ keystream for the IV
- Can use the IV and keystream for false authentication
- Collect keystreams for many IVs
- 24b IV ⇒ 2^{24} keystreams ⇒ 24 GB for 1500B packets
- Can store all possible keystreams and then use them to decrypt any messages

Known Plaintext Attack

- Wired attacker sends a message to wireless victim
- AP encrypts the message and transmits over the air
- Attacker has both plain text and encrypted text
  $\Rightarrow$ keystream



Reaction Attack

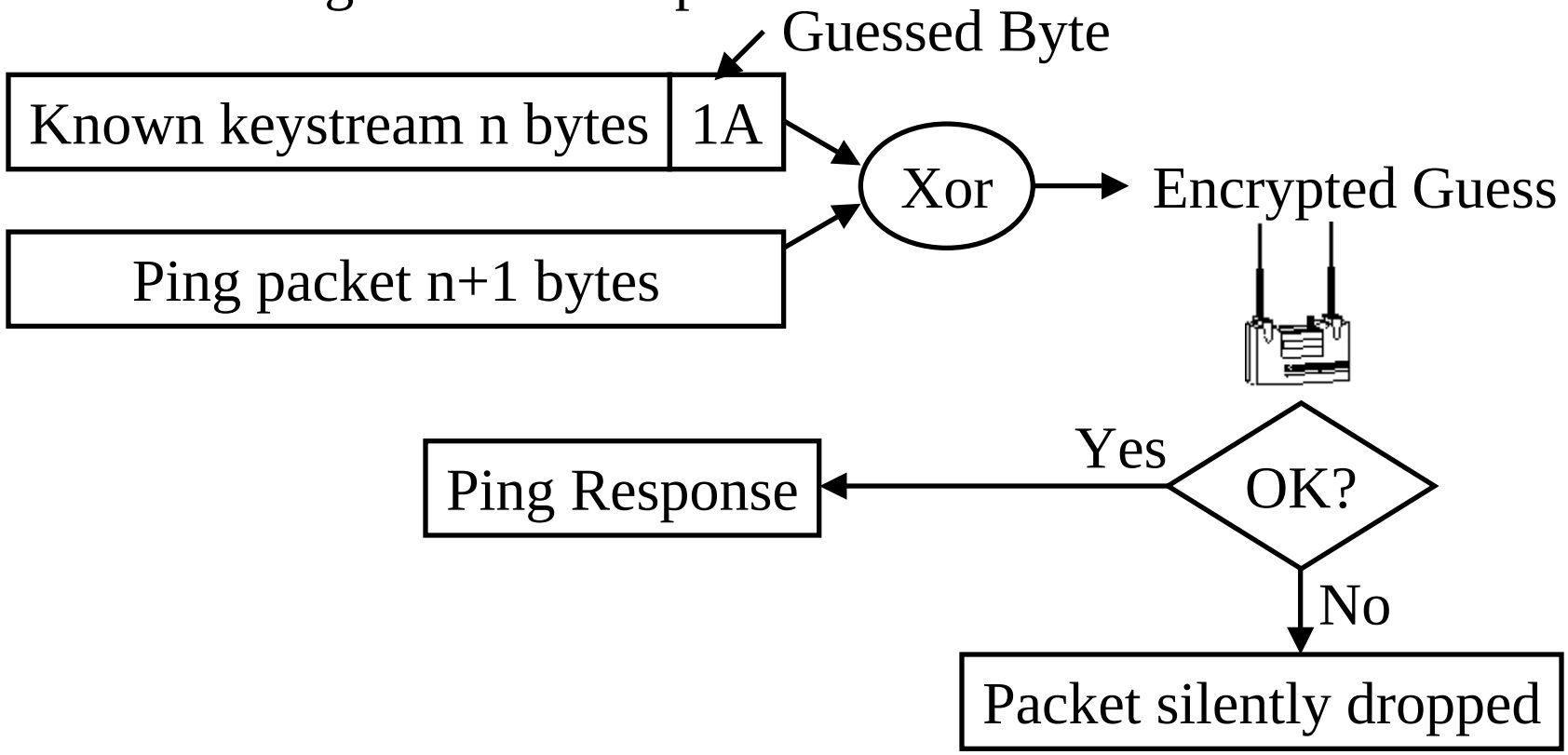
- ICV is a linear sum ⇒ Predictable
- Change a few bits and rebroadcast
  ⇒ TCP acks (short packets)
- Flip selected bits ⇒ Keystream bits are 0 or 1

Message Modification Attack

- Change the destination address to attacker's wired node
- Unencrypted packet will be delivered by the AP to the wired node

Inductive Attack

- If you know n bytes of keystream, you can find n+1st byte
- Send a ping request with 256 variations of the n+1st byte
- Whichever generates a response is the correct variation



Reuse IV Attack

- If you have keystream for a particular IV, you can keep using the same IV for which he has keystream

WEP Key Attacks

- 40-bit key or 104-bit key generated by a well-known pass-phrase algorithm
- wep_crack creats a table of keys for all dictionary words and uses them to find the key
- wep_decrypt tries random 40-bit keys to decrypt
  $\Rightarrow 2^{20}$ attempts = 60 seconds
- Dictionary based pass-phrase take less than 1 seconds

FMS Attack

- Scott Fluhrer, Itsik Mantin, and Adi Shamir
- Based on a weakness of the way RC4 initializes its matrix
- If a key is weak, RC4 keystream contains some portions of key more than other combinations
- Statistically plot the distribution of parts of keystreams $\Rightarrow$ Parts of key
- WEPcrack, http://wepcrack.sourceforge.net sniffs the network and analyzes the output using FMS to crack the keys
- AirSnort, http://airsnort.shmoo.com also sniffs and uses a part of FMS to find the key
- bsed-airtools includes dwepdump to capture the packets and dwepcrack to find the WEP key

Dictionary Attack on LEAP

- LEAP uses MS-CHAP v1 for authentication
- Capture the challenge and response
- Brute force password attack

Rouge APs

- AirSnarf, http://airsnarf.shmoo.com setups a rouge AP and presents an authentication web page to the user
- Can steal credit card numbers

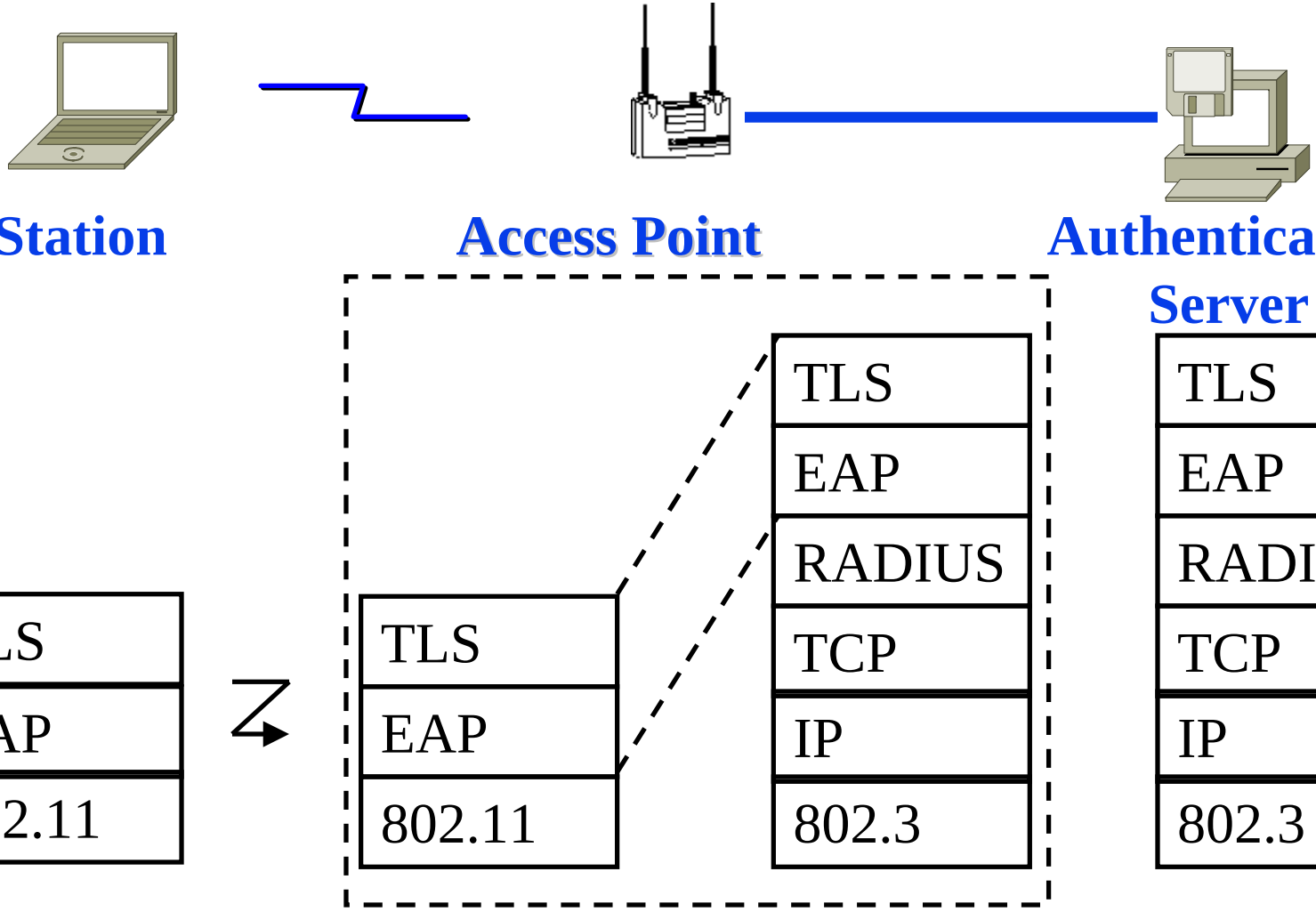
Ad-Hoc Networking Issues

- Computer-to-computer networking is allowed in XP
- Viruses and worms can be passed on if one of them is infected and the other does not have a personal firewall

IEEE 802.11i Security Enhancement

- Strong message integrity check
- Longer Initialization Vector (48 bits in place of 24b)
- Key mixing algorithm to generate new per-packet keys
- Packet sequence number to prevent replay
- Extensible Authentication Protocol (EAP)
  ⇒ Many authentication methods. Default=IAKERB
- 802.1X Authentication with Pre-shared key mode or managed mode with using RADIUS servers
- Mutual Authentication (Station-Key Distribution Center, Station-Access Point)
- AP sends security options in probe response if requested
- Robust Security Network (RSN)
  ⇒ Stronger AES encryption (AES-CCMP)

802.11 Security Protocol Stack

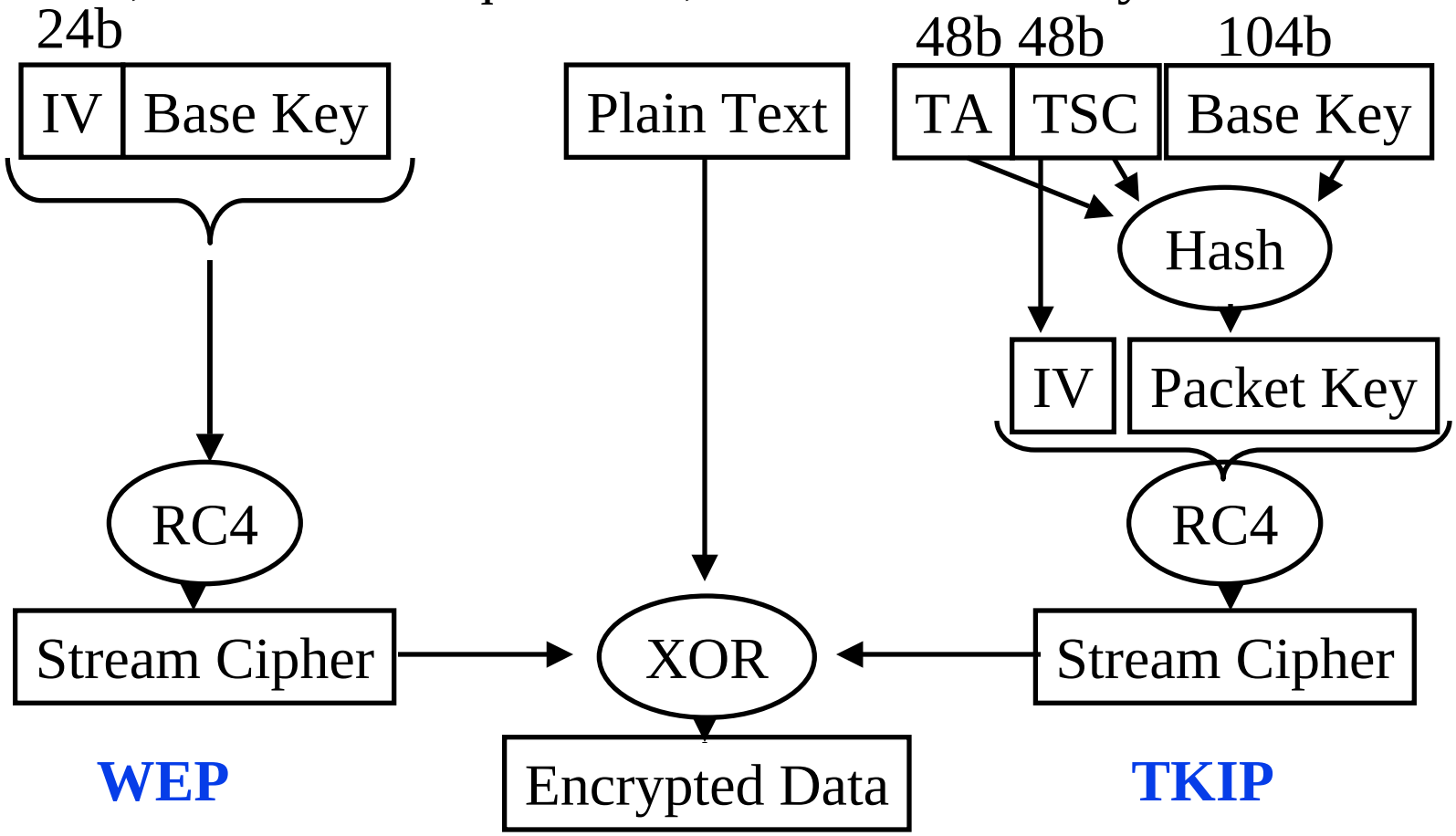


Wi-Fi Protected Access (WPA)

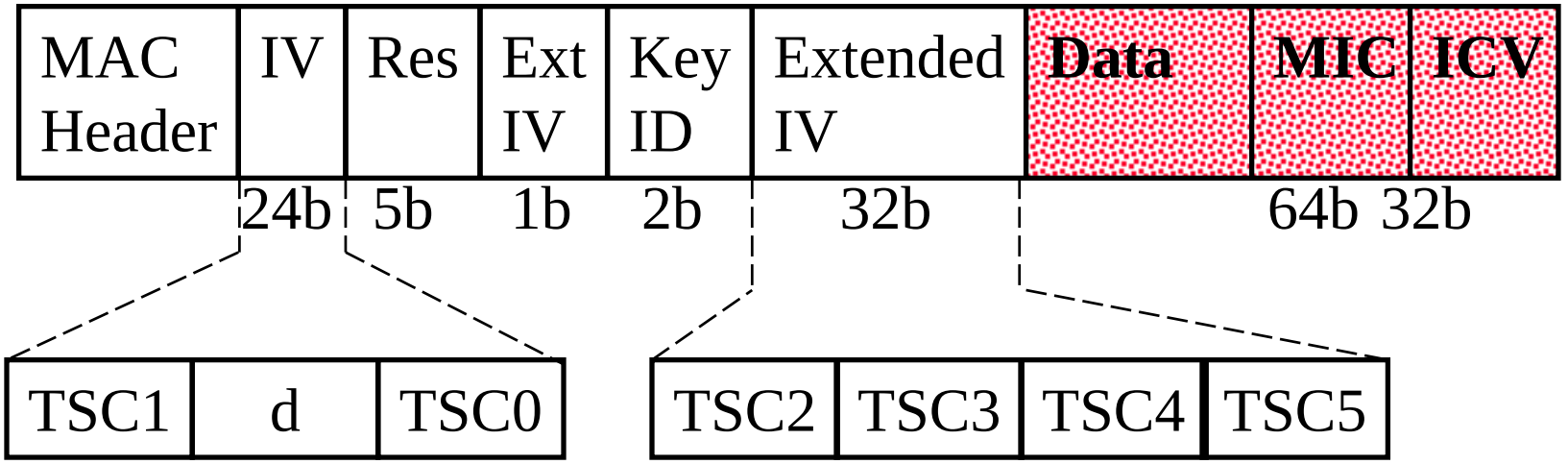
- Temporal Key Integrity Protocol (TKIP)
  - Longer IV + Key mixing to get Per-Packet Key + MIC
  - Use the same encryption (RC4) ⇒ Firmware upgrade
- All access points and subscribers need to use WPA
  WPA+WEP ⇒ WEP
- Separate keys for authentication, encryption, and integrity
- 48b TKIP sequence counter (TSC) is used to generate IV and avoid replay attack. Reset to 0 on new key and incremented.
- IV reuse is prevented by changing WEP key on IV recycling

Temporal Key Integrity Protocol (TKIP)

- WEP: Same base key is used in all packets
- TKIP: New packet key is derived for each packet from source address, 48b TKIP Seq counter, and 104b base key

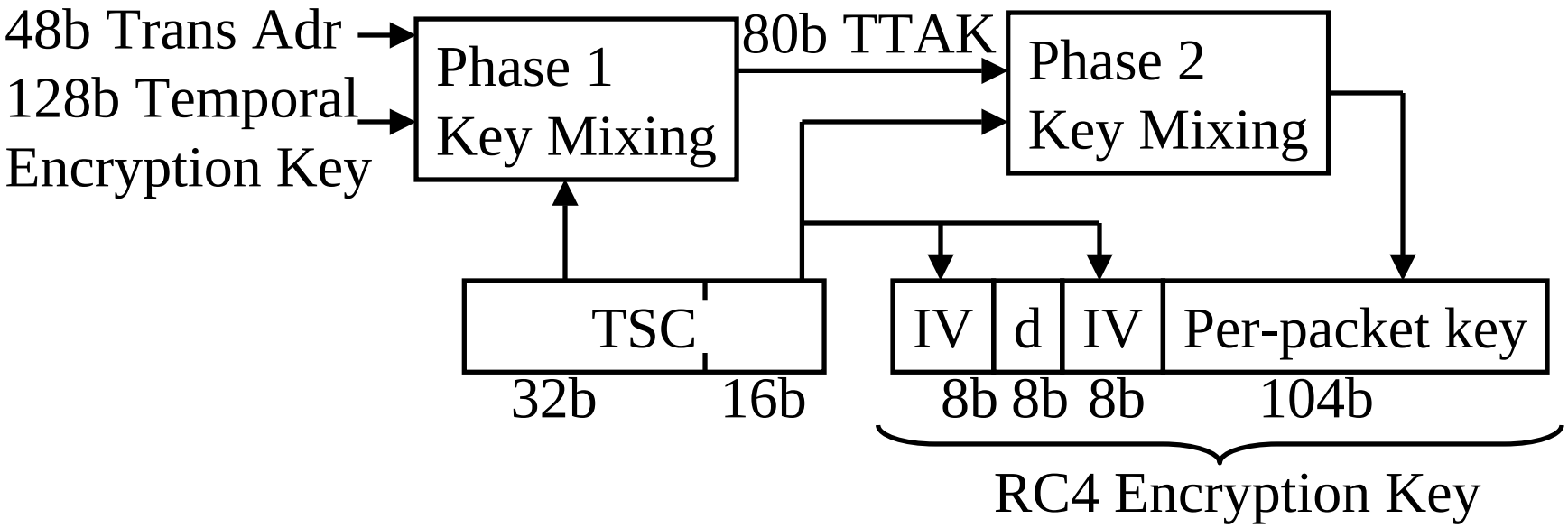


TKIP Packet Format



- Ext IV flag indicates if a longer IV is being used (and MIC is present)
- d is designed to avoid weak keys
- TSC is reset to zero on key change and is never reused with the same key ⇒ key is change on TSC cycling
- MIC is per MSDU. While ICV is per MPDU, i.e., fragment

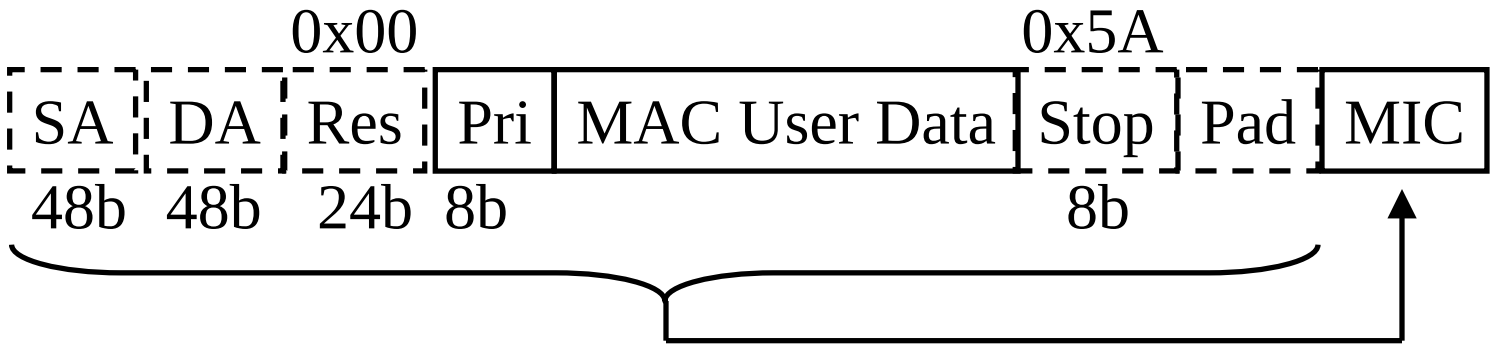
RC4 Encryption Key (TEK)



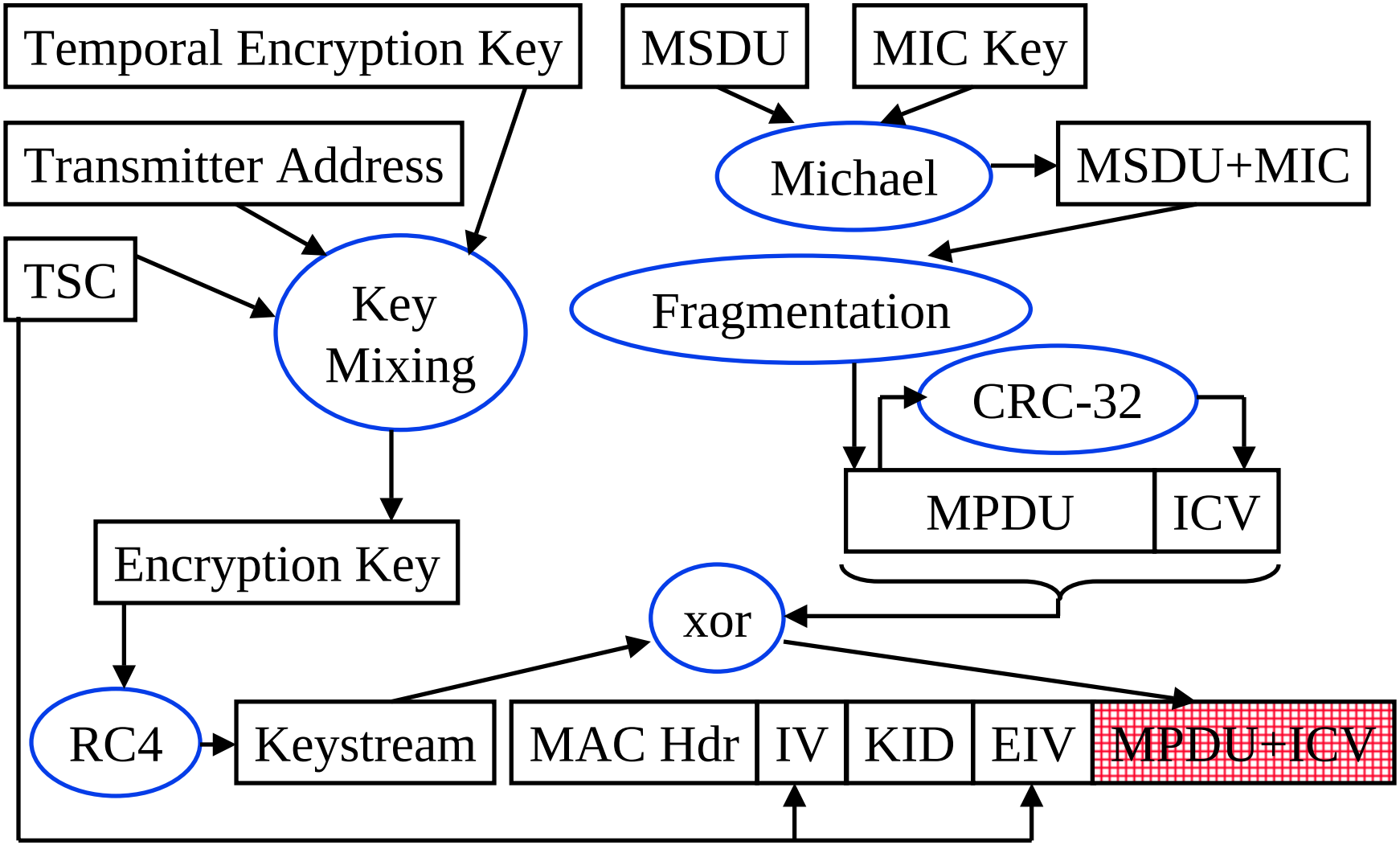
- Phase 1: Transmitters MAC address, TEK, and upper 32b of the IV are hashed together using an S-Box to produce 80b TKIP mixed Transmit Address and Key (TTAK)
- Phase 2: Lower 16 bits of TSC and TTAK are hashed to produce per-packet key
- d is a dummy byte designed to avoid weak keys.

Message Integrity Check (MIC)

- Michael – A non-linear integrity check invented by Neil Furguson. Designed for WPA.
- A separate 64b MIC key is derived from the master session key
- 64b Michael hash (MIC) is added to "MAC SDU"
- MIC is computed using a virtual header containing MAC destination and source address, stop, padding
- Padding is added to make length a multiple of 4B



TKIP Transmission



WEP vs. WPA

WEP	WPA
No centralized key management Manual key distribution => Difficult to change keys	EAP/TLS allows per session keys
Single set of Keys shared by all => Frequent changes necessary	RADIUS allows each user to be authenticated individually
Weak Encryption: RC4 is very weak => Challenge-Response can be used to obtain the shared key	RC4 is kept. Authentication key is different from encryption key
No mutual authentication	Mutual Authentication
No user management (no use of RADIUS)	RADIUS
IV value is too short. Not protected from reuse.	48-bit IV
Weak linear integrity check.	Michael – non-linear integrity check
Directly uses master key	Uses derived keys
No protection against replay	Protection against replay

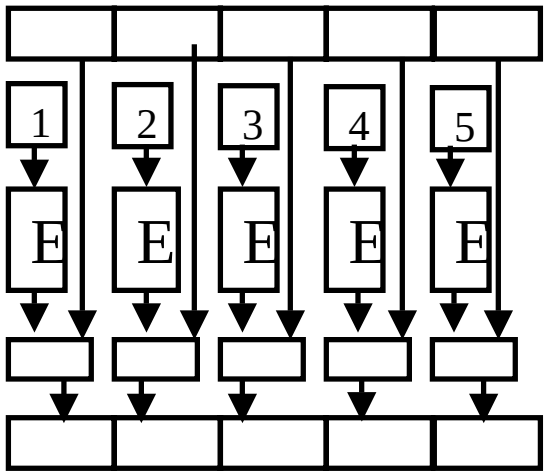
WPA2 (802.11i)

- Advanced Encryption Standard (AES)
  $\Rightarrow$ Need hardware support
- Counter mode (CTR) is used for encryption (in place of RC4)
- Cipher Block Chaining Message Authentication Code (CBC-MAC) is used for integrity (in place of Michael)
- CCM = CTR + CBC-MAC for confidentiality and integrity
- CCM Protocol (CCMP) header format is used (in place of TKIP header)
- 48b Packet number (PN) is used to prevent replay attacks
- Secure fast handoff preauthentication
- Secure de-association and de-authentication
- Security for peer-to-peer communication (Ad-hoc mode)

AES-CTR

- Advanced Encryption Standard (AES) in Counter Mode
- AES is a block cipher. It has many modes.
  802.11i uses Counter-Mode for encryption
- Counter is incremented for each successive block processed.
- Counter is encrypted and then xor'ed with data.

- Counter can be started at a arbitrary value.
- Repeating blocks give different cipher text



Message

Counter

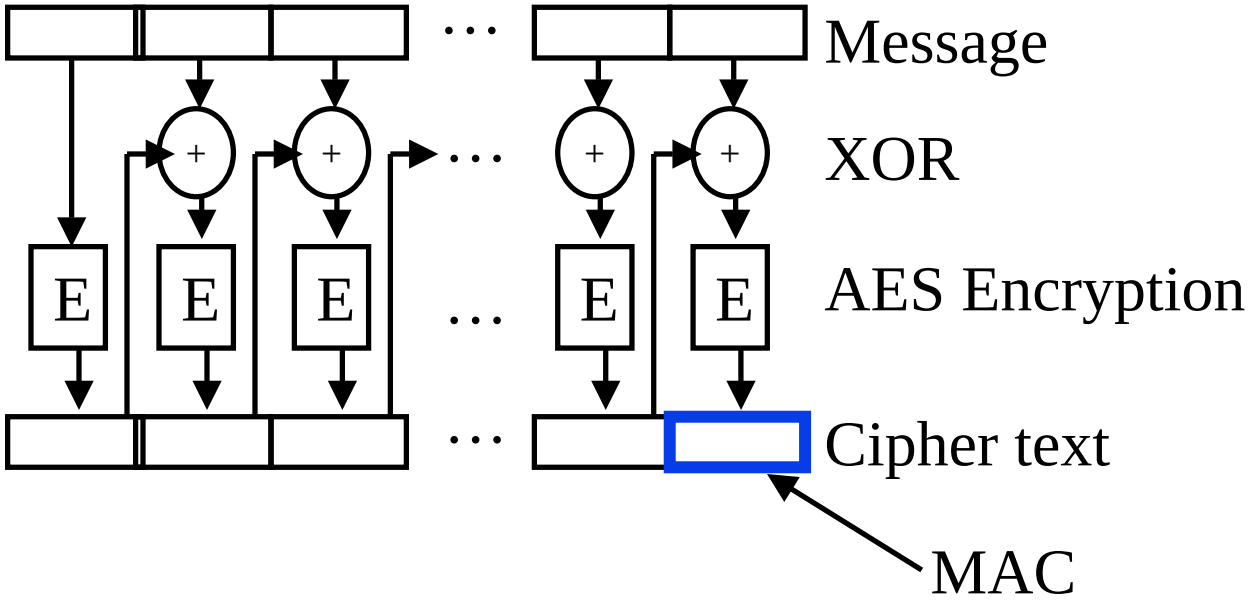
AES Encryption

XOR

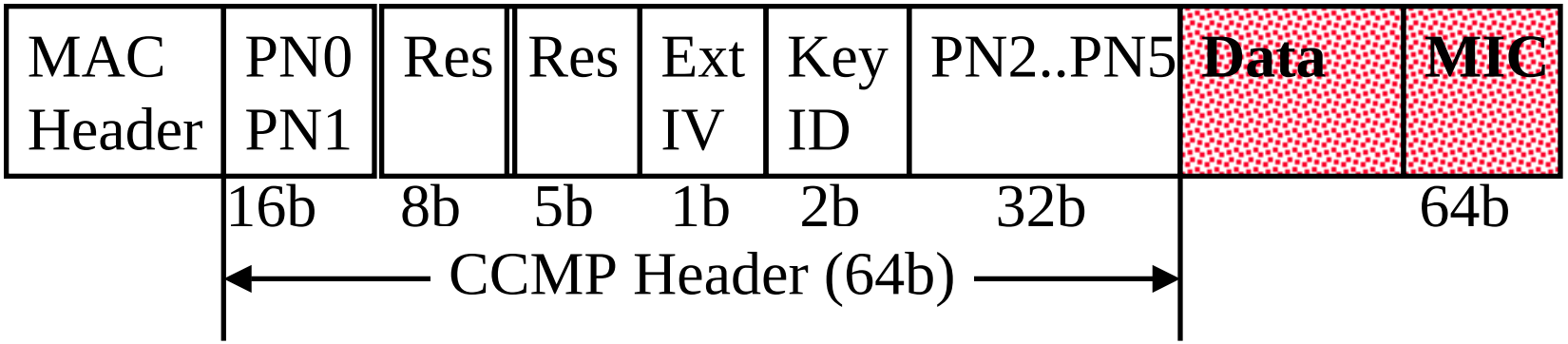
Cipher text

AES/CBC-MAC

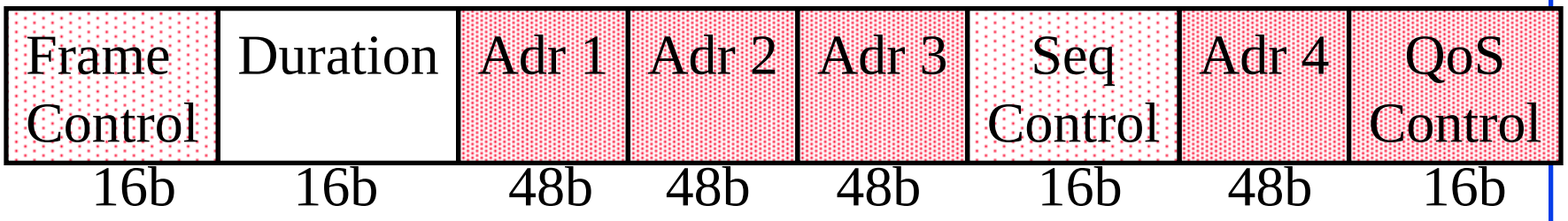
- Cipher-Block Chaining mode is used to produced a message authentication code



CCMP Packet Format

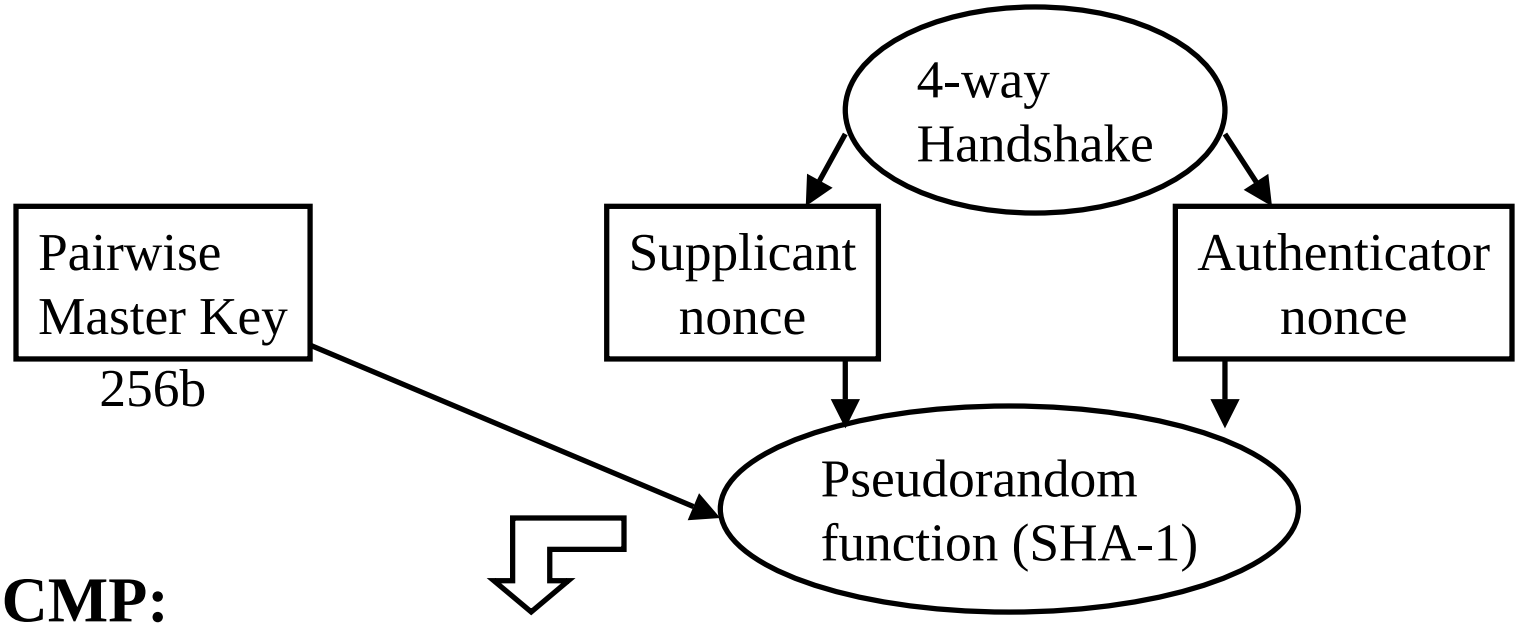


- Additional authentication data (AAD) is included in MIC calculation



- Some bits of frame control and seq control are zeroed out and duration is not included in ADA

802.11i Key Hierarchy



CCMP:

EAPOL Key Confirmation Key	EAPOL Key Encryption Key	Temporal Key (CCMP)
128b	128b	128b

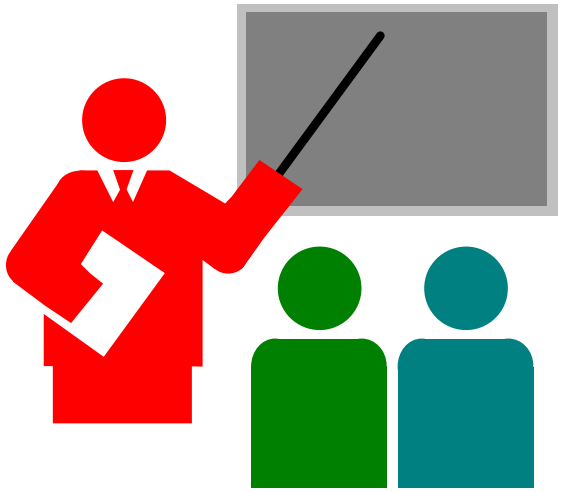
TKIP:

EAPOL Key Confirmation Key	EAPOL Key Encryption Key	Temporal Encryption Key	MIC from AP Key	MIC to AP Key
128b	128b	128b	64b	64b

Security Problems Addressed

- No MAC address spoofing: MAC address included in both Michael MIC and CCMP MAC
- Replay: Each message has a sequence number (TSC in TKIP and PN in CCMP)
- Dictionary based key recovery: All keys are computer generated binary numbers
- Keystream recovery: Each key is used only once in TKIP. No keystream in CCMP.
- FMS Weak Key Attack: Special byte in IV in TKIP prevents weak keys. Also, keys are not reused.
- 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



- WEP is a good training ground for security attacks
  Almost all components are weak
- TKIP provides a quick way to upgrade firmware and fix many of the flaws => WPA
- CCMP adds a stronger AES encryption and message integrity check but requires new hardware => WPA2
- Key management is provided by RADIUS, EAP, and 802.1x

References

- J. Edney and W.A. Arbaugh, “Real 802.11 Security: Wi-Fi Protected Access and 802.11i,” Addison-Wesley, 2004, 481 pp., ISBN:0321156209
- Krishna Shankar, et al, "Cisco Wireless LAN Security," Cisco Press, 2005, 420 pp, ISBN:1587051540
- A. A. Vladimirov, K.V. Gavrilenko, and A.A. Mikhailovsky, “Wi-Foo: The Secrets of Wireless Hacking,” Addison-Wesley, 2004, 560 pp., ISBN:0321202171