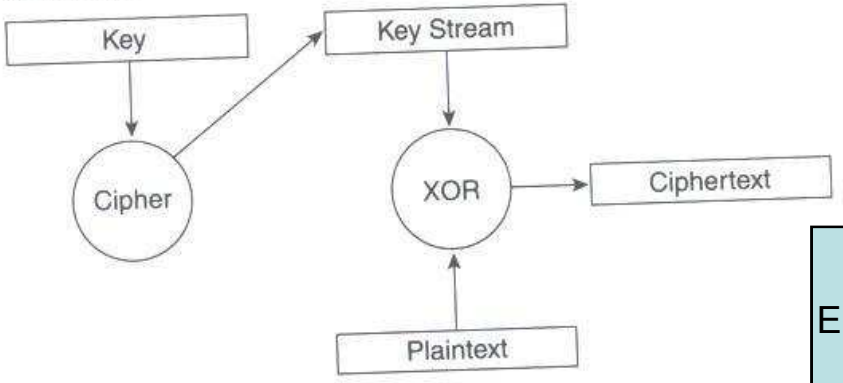
802.11 Security

Wireless security

- Any station within range of the RF receives data
- Two security mechanism
  - A means to decide who or what can use a WLAN – authentication
  - A means to provide privacy for the wireless data – encryption

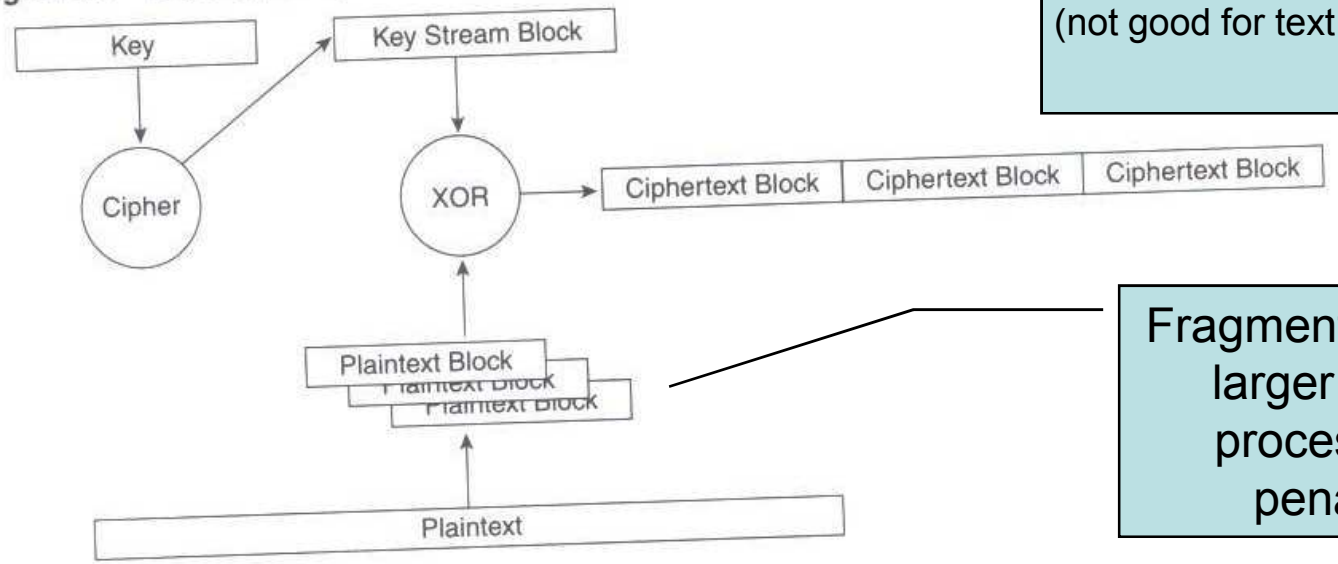
Encryption concepts

Figure 4-2 *Stream Cipher Operation*



Electronic Code Book (ECB): the same plain text input always produce the same ciphertext (not good for text < 40 sym.)

Figure 4-3 *Block Cipher Operation*

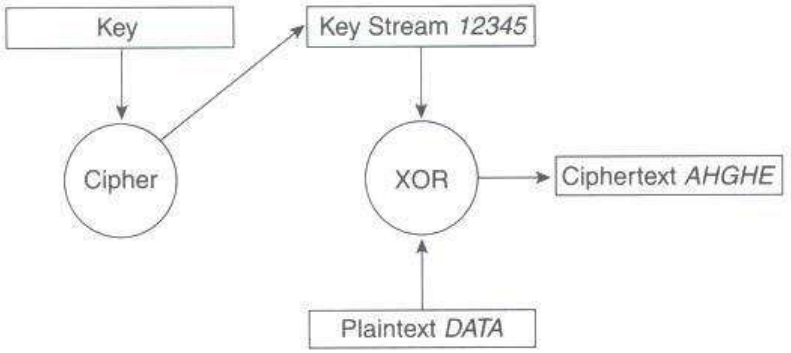


Fragmentation → larger CPU processing penalty

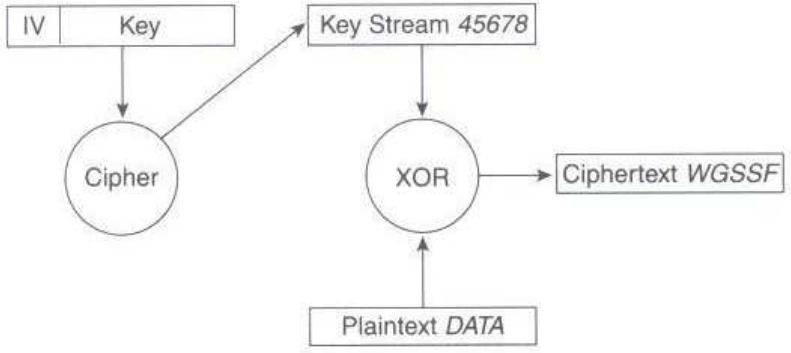
Initialization vector

- ECB → the same plaintext input always produce the same ciphertext
- 802.11 recommends to change Initialization Vector (IV) on a per-frame basis

Figure 4-4 *Encryption and Initialization Vectors*



1. Stream Cipher Encryption Without an Initialization Vector



2. Stream Cipher Encryption with an Initialization Vector

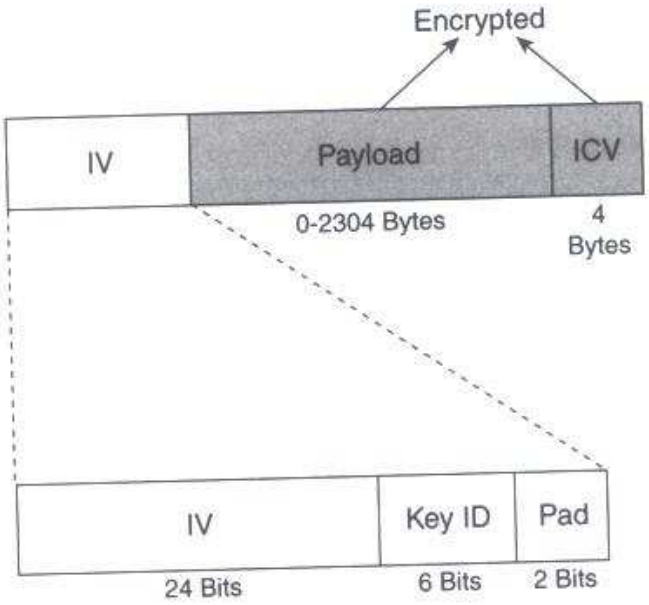
Encryption in 802.11

- Privacy → WEP
- WEP is based on RC4 symmetric stream cipher
- Symmetric → WEP keys (40 or 104 bits) statically configured both on APs and clients
- Why Wep?
  - Low computational overhead
  - In 1997 WLAN devices were application-specific devices (low computational power)
  - Wep can be written in 30 lines of code

Wep

- To avoid ECB, Wep uses a 24-bit IV
- IV must change on a per-frame basis (to avoid collision = same key and same IV)
- ICV = integrity check value

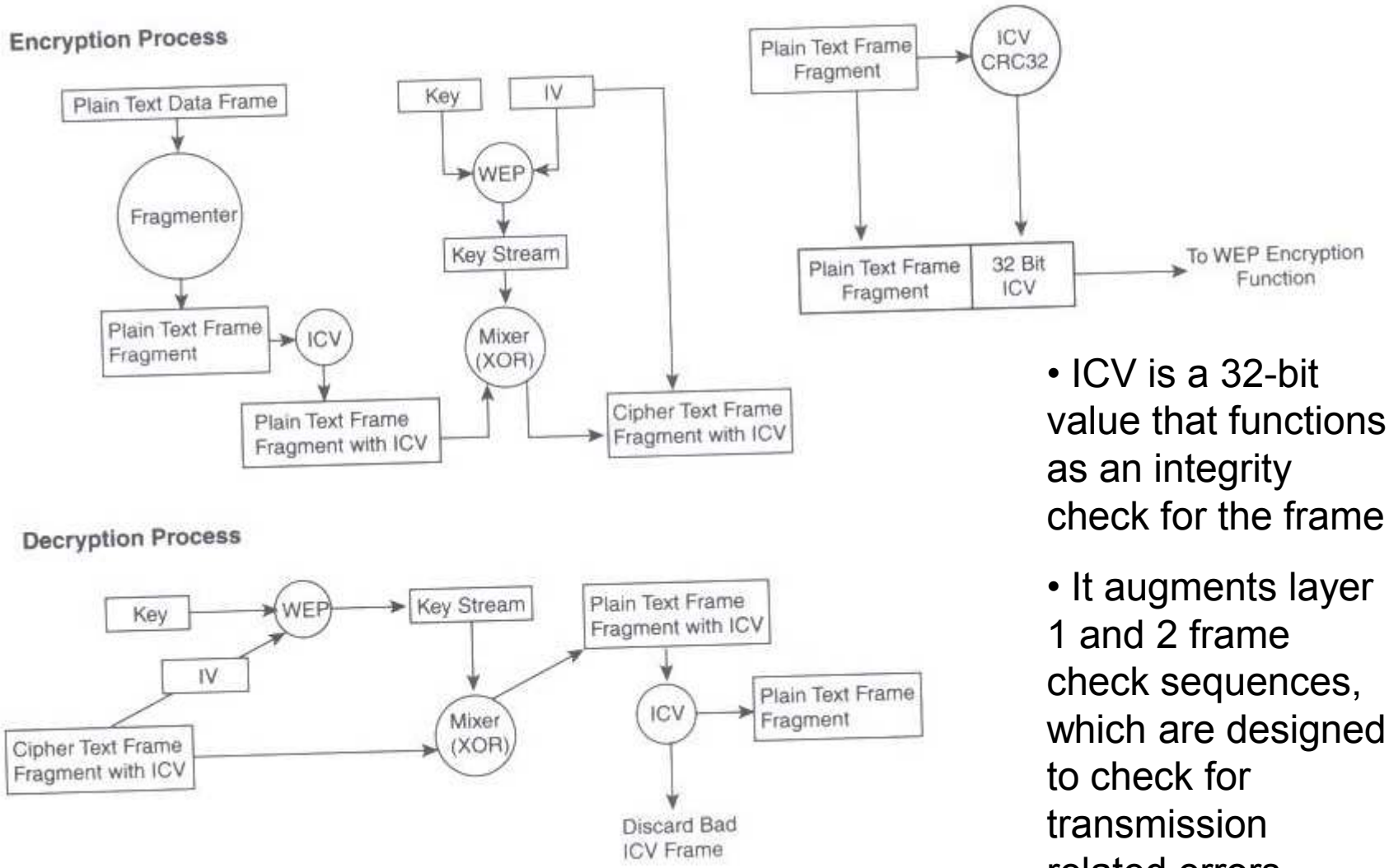
Figure 4-5 *A WEP-Encrypted Frame*



Wep

- Up to 4 key statically configured, used only one at a time
- Wep encryption is used only on
  - data frames (payload encryption)
  - and during Shared Key authentication
- Wep encrypts data or payload and the integrity check value, all other fields are transmitted without encryption

Encryption and decryption



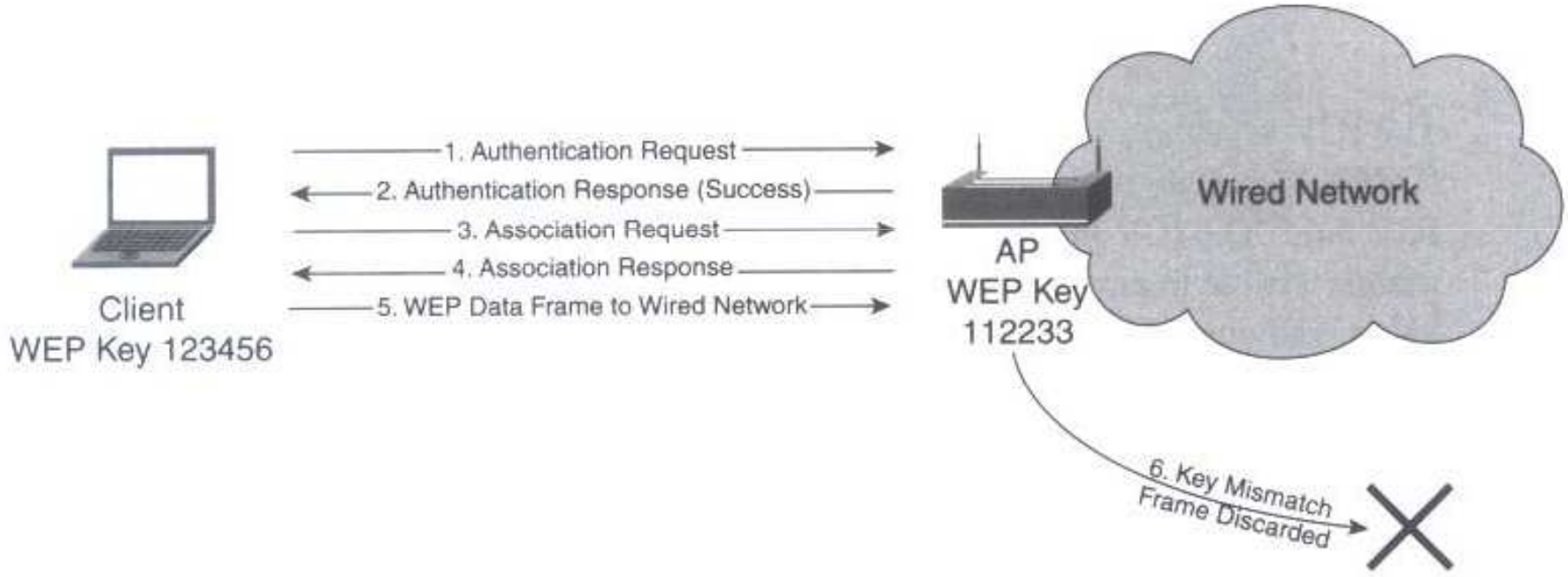
- ICV is a 32-bit value that functions as an integrity check for the frame
- It augments layer 1 and 2 frame check sequences, which are designed to check for transmission related errors

Authentication mechanism in 802.11: open authentication

- Null authentication algorithm.
  - The AP grants any request for authentication
  - Access control relies on preconfigured WEP key on the client and AP.
  - If the client and AP do not have WEP enabled → no security and privacy at all
- If the client is configured with a key that differs from the key on the AP, the client will be unable to encrypt/decrypt data frames correctly, and the frames will be discarded

Open authentication

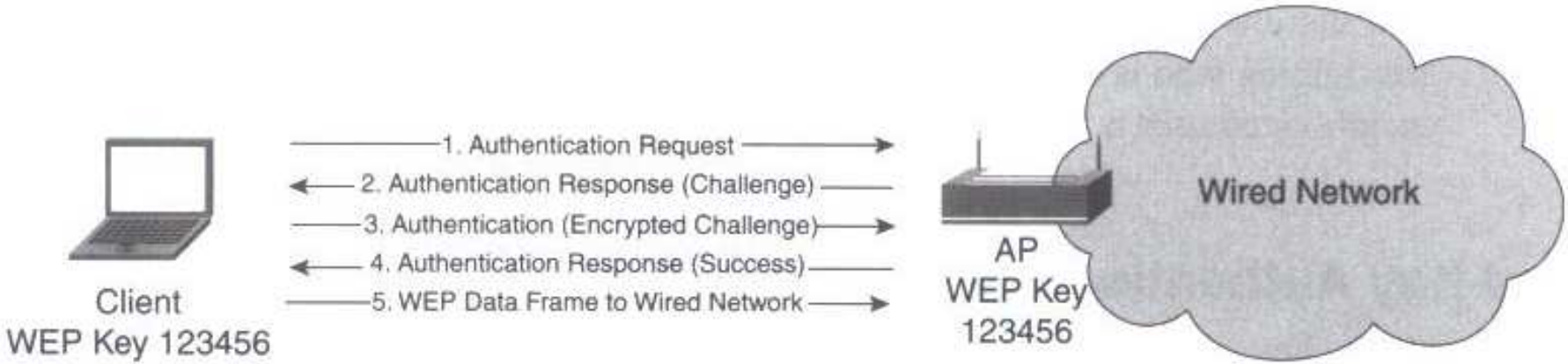
Figure 4-9 *Open Authentication with Differing WEP Keys*



Authentication mechanism in 802.11: shared key authentication

- The client and the AP MUST have Wep enabled and have matching WEP keys

Figure 4-10 *Shared Key Authentication Process*



MAC address authentication

- Not specified in 802.11, but supported by many vendors
- It verifies the client's MAC address against a list of allowed addresses

Figure 4-11 *MAC Address Authentication Process*

Vulnerability

- Open authentication: no way for the AP to determine whether a client is valid.
- MAC address authentication
  - MAC addresses are sent unencrypted in all 802.11 frames
  - Spoofing of valid MAC addresses
    - MAC Spoofing is possible with network interface cards (NICs) that allow the universally administrated address (UAA) to be overwritten with a locally administrated addresses (LAA)

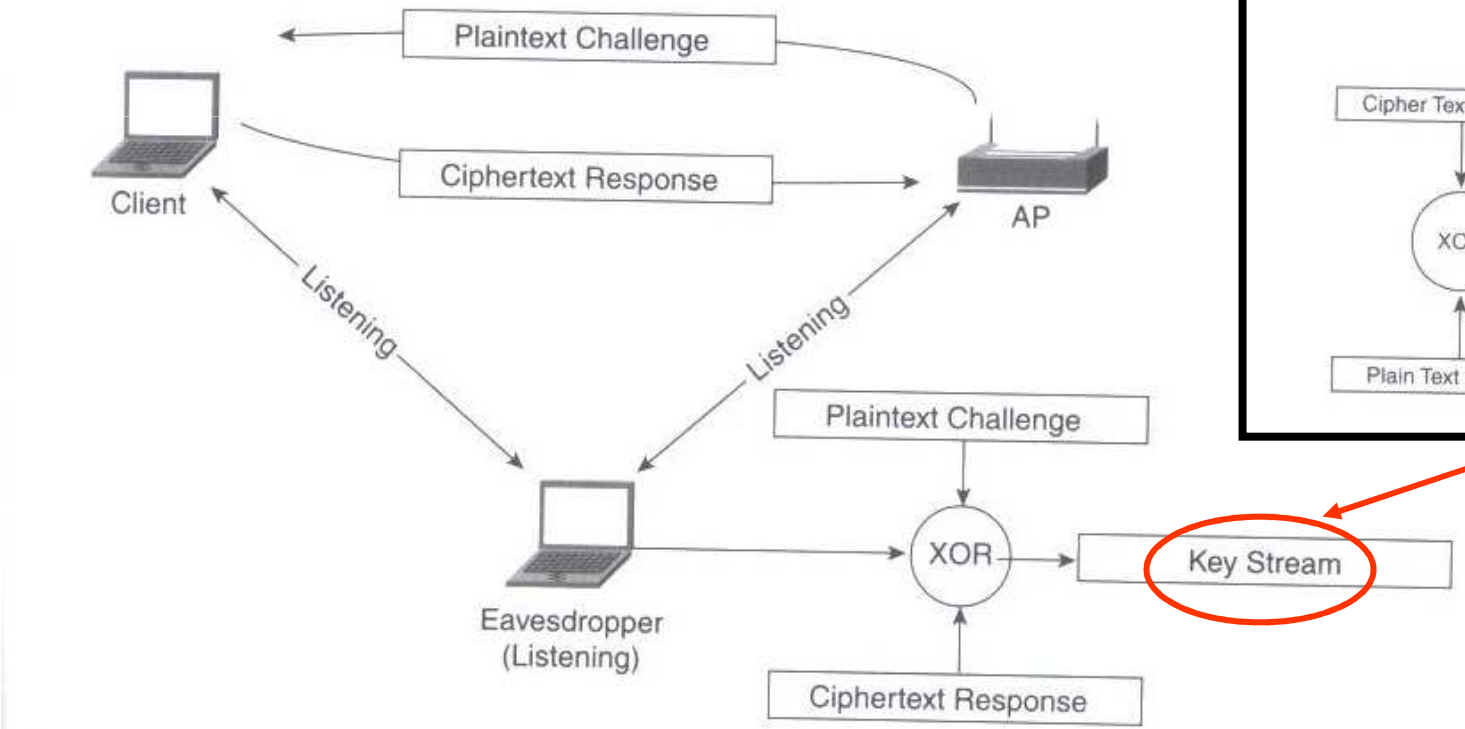
XOR properties

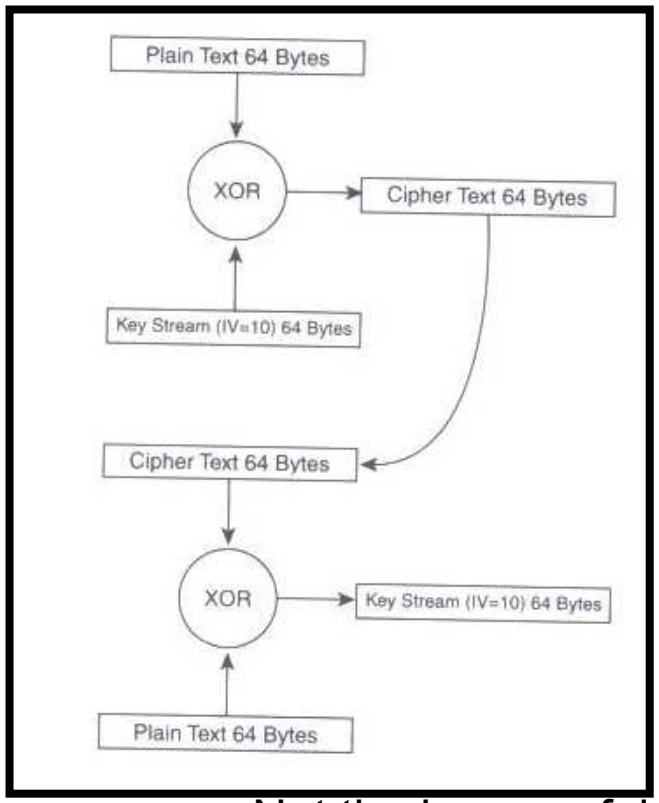
0 xor 0 = 0
0 xor 1 = 1
1 xor 0 = 1
1 xor 1 = 0

- (A xor B) xor A = B
  - If the attacker obtains (A xor B) by knowing A it gets the secret B
- (A xor B) xor B = A
- A xor A = 0
- (A xor K) xor (B xor K) = A xor B
  - If K is the same key used to encrypt A and B, and the attacker listens (A xor K) and (B xor K), it is able to compute (A xor B), which facilitates the solution.

Shared key vulnerabilities

Figure 4-13 *Shared Key Authentication Vulnerability*





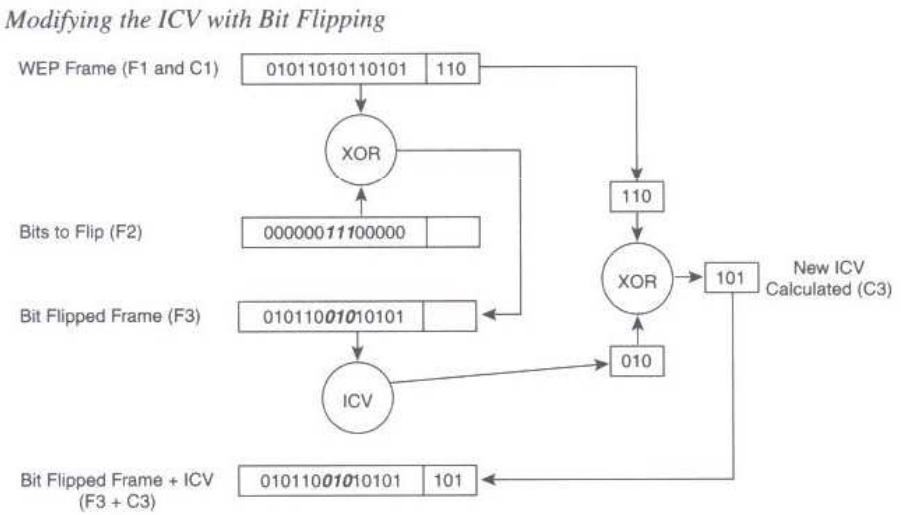
Not the key: useful to decrypt frames for a given IV and WEP key pair and for a specific length

WEP encryption vulnerabilities

- Fluhrer, Mantin and Shamir → you could derive a WEP key by passively collecting particular frames from a WLAN
- Some IVs, weak IVs, can reveal key bytes after statistical analysis
- You can derive WEP keys of either 40 or 104-bit key length after as few as 4 million frames.
- Passive attack: the attacker simply eavesdrops on a BSS and collects transmitted frames.
- Unlike Shared key authentication vulnerability, this attack can derive the actual WEP key, not just the key stream

Bit flipping attack

- The attacker captures a frame from the WLAN
- The attacker flips random bits in the data payload of the frame
- The attacker modifies the ICV
- The attacker transmits the modified frame
- The receiver receives the frame and accepts the modified frame
- The receiver forward the frame at the upper layer
- Because bits are flipped → layer 3 checksum fails
- The IP generates a PREDICTABLE error
- The attacker sniffs the encrypted error message
- The attacker derives the keystream Similar to shared key attack



Static Wep Key

- 802.11 specification does not specify key-management mechanisms
- Static pre-shared keys
- 802.11 authenticate the device → loss or theft problem
- Manually rekeying all wireless devices → scalability problem

Secure 802.11

- The WLAN industry recognizes vulnerabilities in 802.11
- Requirements: authentication and encryption scalable and manageable.
- 802.11i not already a standard
- A subset of 802.11i called Wi-Fi Protected Access (WPA)

roadmap

WEP: weak
and mixed
- privacy
- authentication

roadmap

WEP: weak and mixed
• privacy
• authentication

IEEE 802.11i: a new security architecture
Concept: Robust Security Network Association
In addition to wep:
- •crypto-mechanism with integrity functions
- •Protects headers and payload
- •Anti-replay mechanism
- •Extended IV

New crypto mechanisms (+frame encapsulation)
New advanced authentication schemes (STA - AP)
New advanced session key management schemes

roadmap

WEP: weak and mixed
• privacy
• authentication

IEEE 802.11i: a new security architecture
Concept: Robust Security Network Association
In addition to wep:
- •crypto-mechanism with integrity functions
- •Protects headers and payload
- •Anti-replay mechanism
- •Extended IV

New crypto mechanisms (+frame encapsulation)
New advanced authentication schemes (STA - AP)
New advanced session key management schemes

Wi-fi Alliance proposes **WPA**
Compliant with existing HW
Adopts a subset of IEEE 802.11i solutions (specifically, IEEE 802.1x authentication) and TKIP to enforce key protection

WPA2: adopts 5 EAP schemes

roadmap

IEEE 802.11i: a new standard security architecture

Association:

802.11: Beacon, Probe response indicate AP, ssid…
802.11i : … + security capabilities (authentication and crypto)
a STA can select mechanisms in association request packets

Authentication:

•**802.11i** mandates use of Std 802.1x (for authentication)
that can be applied over different MACs (Ethernet, Wifi…) but it does not specify which EAP methods to use for credentials. It only specifies that such a method must ensure mutual authentication and session key generation and management.

•**802.1x:** port-based network access control: supplicant, authenicator, auth-server.

- based on EAPOL protocol framework: which auth. mechanism to use?
  Supports different credentials: shared secret (EAP-MD5), X.509 digital certificates (EAP-TLS), hybrid (EAP-TTLS, PEAP), telephone-like (EAP-SIM…)

•or RADIUS protocol (see next slide)

EAPOL: extensible authentication protocol over Lan
RADIUS: remote authentication dial-in user service

roadmap

…. IEEE 802.11i: a new standard security architecture
Association:…
Authentication:
•**802.11i** mandates use of Std 802.1x (for authentication)
•**802.1x:** port-based network access control: supplicant, authenicator, auth-server.
•RADIUS protocol: controls AAA (Authentication, Authorization, Accounting)

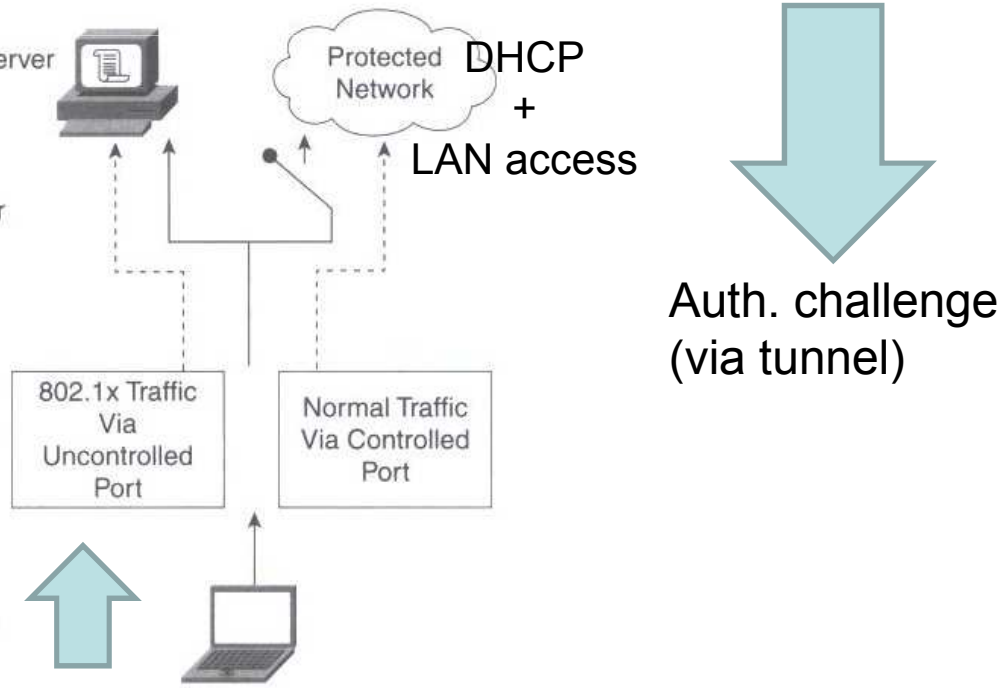
Check on local DB or remote SQL, Kerberos, LDAP, active directory service

e.g. Radius Server (AS)

EAP, PAP, CHAP
(secure auth. mechanism +
secure pairwise master key)

Network Access Server (NAS)

Radius Req(Userid, passwd, MAC, etc.)



Auth. challenge
(via tunnel)

EAPOL: extensible authentication prot
RADIUS: remote authentication dial-in

roadmap

IEEE 802.11i: a new standard security architecture

Association:…
Authentication: …
Encryption: IEEE 802.11i defines 2 protocols for frame protection (based on AES):

- TKIP: temporary key integrity protocol (base for WPA)
  - 64bit message integrity (MIC)
  - 128bit IV (initialization vector)
  - per packet re-keying
- CCMP (CBC-MAC): (base for WPA2) Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (based on AES)

Wireless security

- The authentication framework: “securely communicating messages between the client, AP, and authentication server
- The authentication algorithm: “validates user credentials”
- The data privacy algorithm: “provides data privacy across the wireless medium for data frames”
- The data integrity algorithm: “provides data integrity across the wireless medium to ensure to the receiver that the data frame was not tempered with”

The authentication framework

802.11 is missing some key components to provide effective authentication:

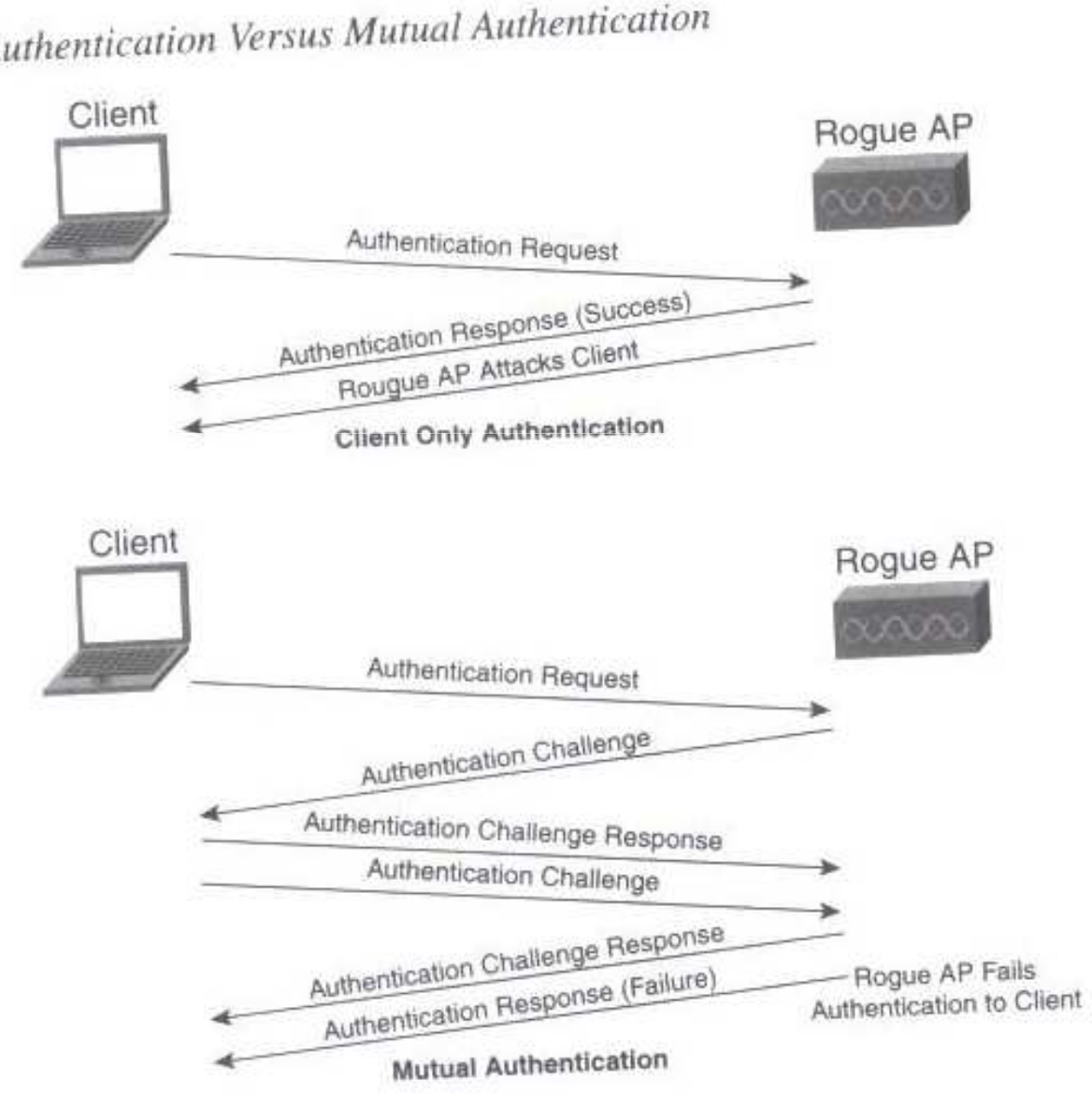
- Centralized, user-based authentication
- Dynamic encryption keys
- Encryption key management
- Mutual authentication

Centralized user-based authentication

- Device-based authentication does not prevent unauthorized accesses
- Logistical issues: lost or stolen devices, employee termination → manually rekeying
- Centralized user-based management via authentication, authorization, accommodation (AAA) servers (RADIUS)
- User-based authentication → user-specific encryption keys
- You only need to disable a user account to prevent accesses

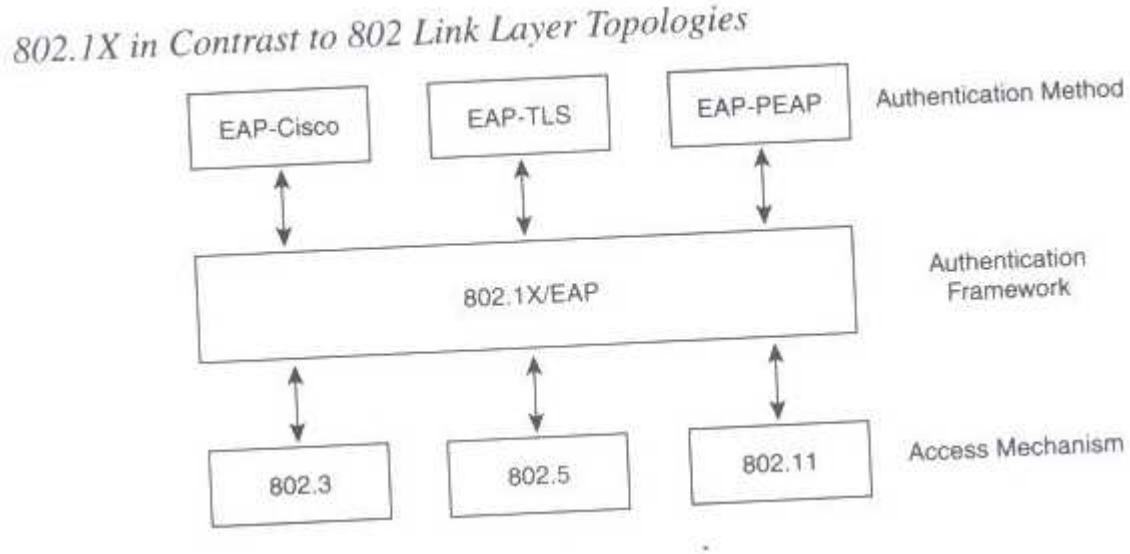
Mutual authentication

- "two-way": network authenticating the client and vice versa
- 802.11: the AP authenticates the client
- A rogue AP can pose as a valid AP and subvert the data on the client's machine



802.1X

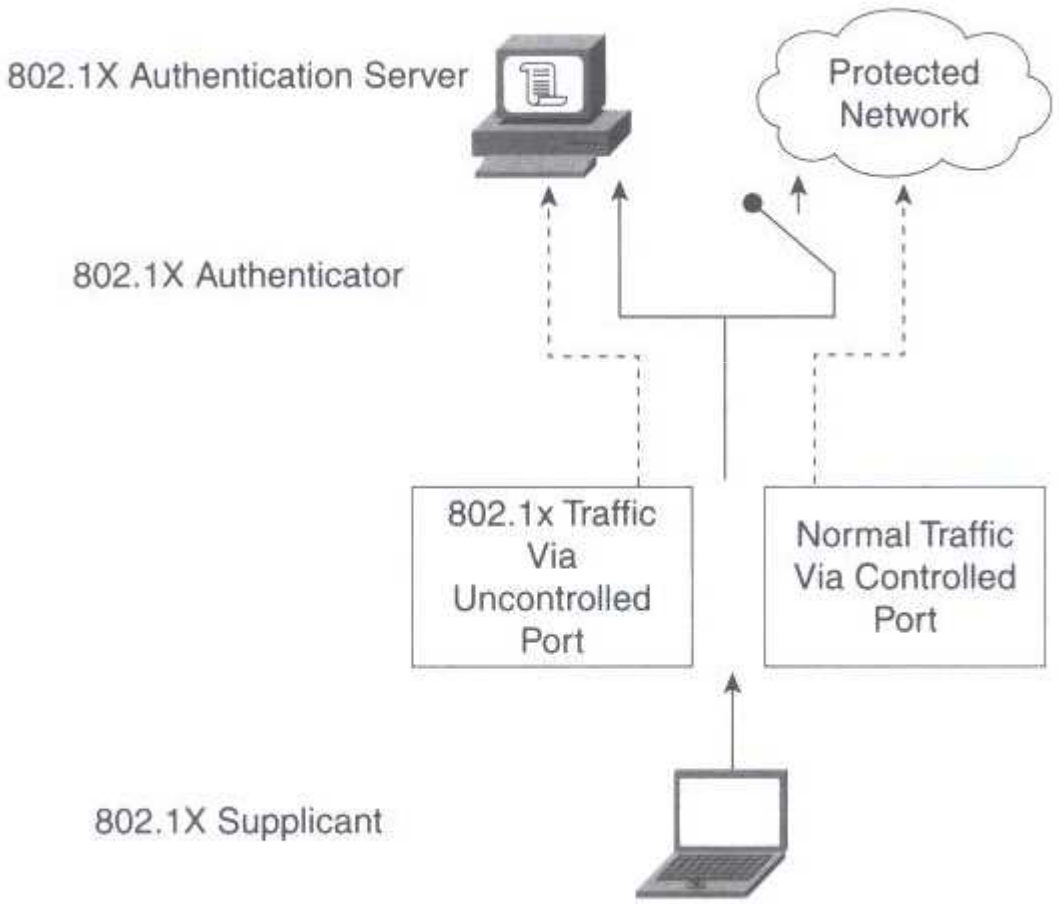
- Extensible Authentication Protocol (EAP).
- 802.1X encapsulates EAP messages for use at Layer 2
- 802.11i incorporates the 802.1X authentication framework (user-based auth.)



- 802.1X and EAP do not mandate the use of any specific authentication algorithm.
- Only requirement: both client and authentication server support the same authentication algorithm. Examples:
  - EAP-Transport Layer Security(EAP-TLS,PEAP): similar to SSL, Mutual authentication by digital certificates used to create a SSL tunnel
  - EAP- Message Digest 5 (EAP-MD5): similar to Challenge Handshake Authentication Protocol (CHAP). Password based one-way authentication mechanism
  - EAP-Cisco (LEAP): Password based mutually authenticating algorithm

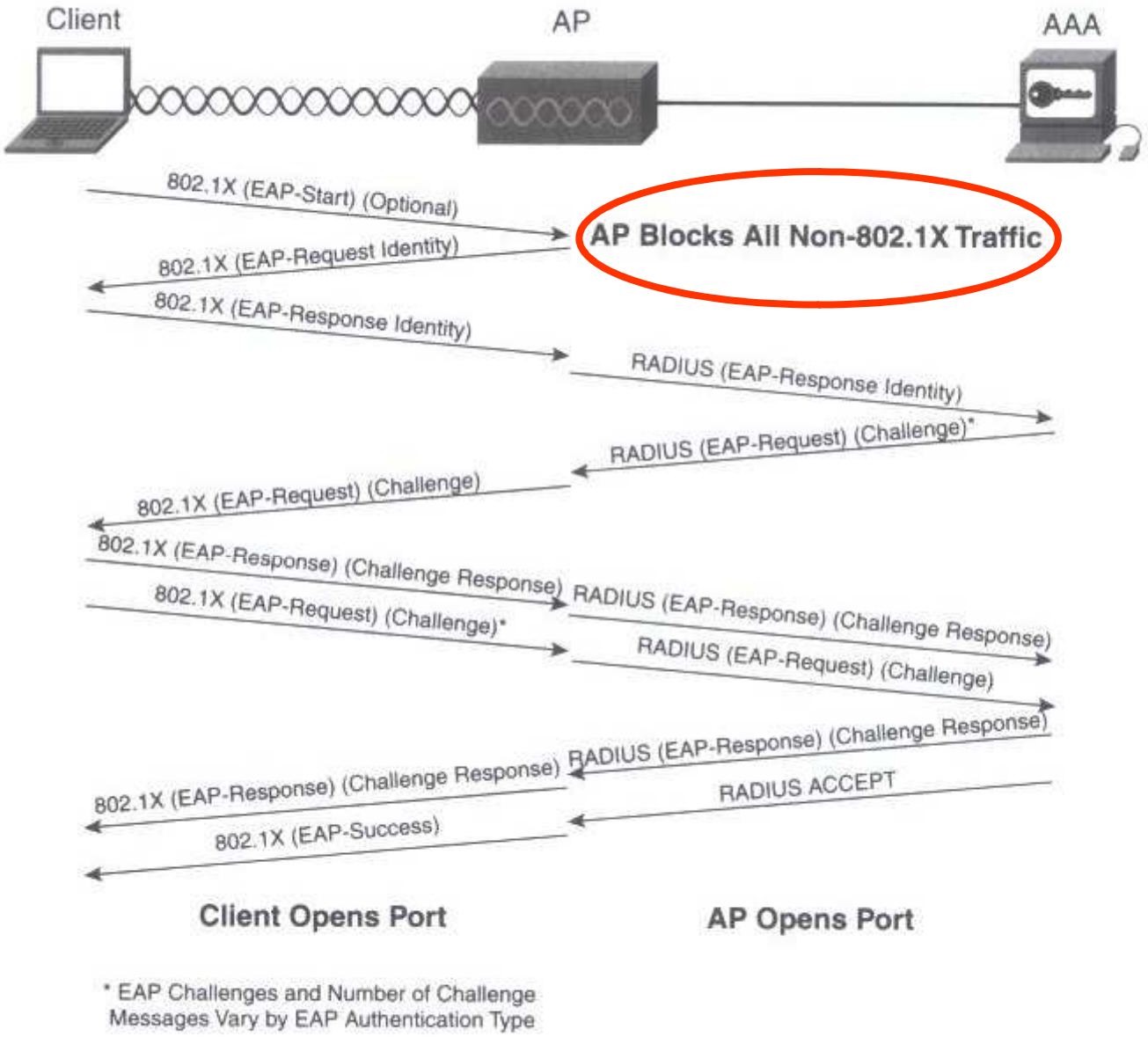
802.1X authentication

- 802.1X authentication requires 3 entities:
  - The supplicant: resides on the WLAN client
  - The authenticator: resides on the AP
  - The authentication server: resides on the RADIUS server



One logical port (AID), two paths (Controlled and Uncontrolled)

The 802.1X Message Exchange

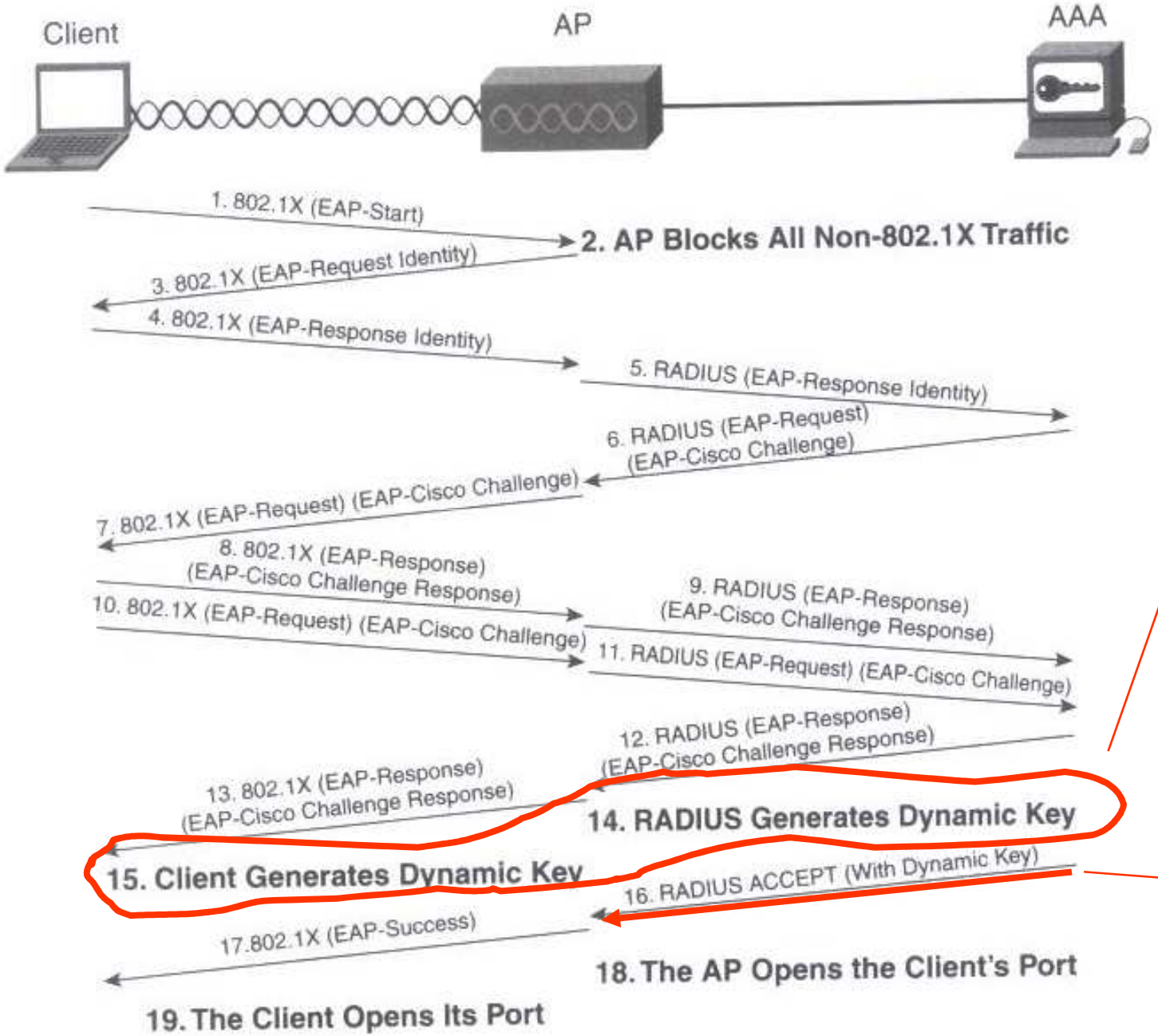


802.1X does not specify nor mandate any particular EAP authentication algorithm.

The Authentication algorithm

- 802.11i and WPA provide a mechanism for authentication algorithms to communicate between client, AP, and authentication server via 802.1X authentication framework
- 802.11i and WPA do not mandate the use of a specific authentication algorithm
- Next Slide (EAP – Cisco). EAP Cisco is proprietary → no details

EAP-Cisco Authentication



Client and AAA server generate a dynamic encryption key based on common information (user identity)

The AAA server sends the key to the AP

Data Privacy

- Wep is vulnerable
- How can you fix 802.11 encryption without requiring a complete replacement of AP hardware or client NIC?
- The answer is the Temporary Key Integrity Protocol (TKIP)
- TKIP uses many key functions of Wep, but:
  - The Wep key is quickly changed on a per-frame basis
  - Message Integrity Check (MIC) prevents frame tampering and frame replay.

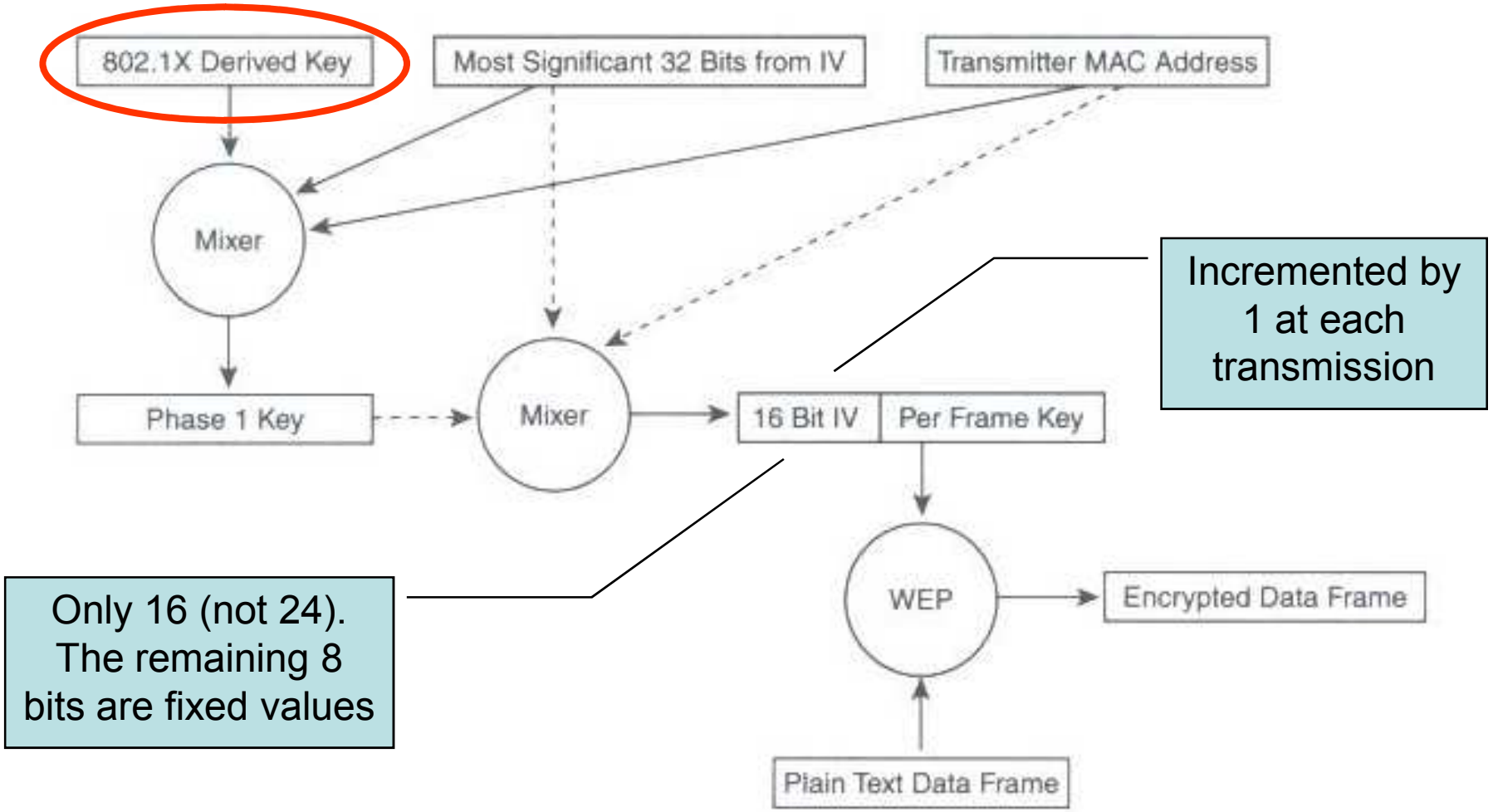
Per-frame keying

- Fluhrer, Martin and Shamir paper describes vulnerability of RC4 as it is implemented in Wep.
- Attack rely on collecting several data frames with encrypted data using weak IVs
- Solution: change the Wep key before attacker can collect enough frames to derive key bytes → per-frame keying

Per-frame keying

- Premise: IV, transmitter MAC and WEP key are processed together via two phase mixing function.
- The output of this function matches standard 104-bit Wep key and 24-bit IV.
- IEEE is proposing the 24-bit IV be increased to 48-bit IV.

The Per-Frame Keying Operation



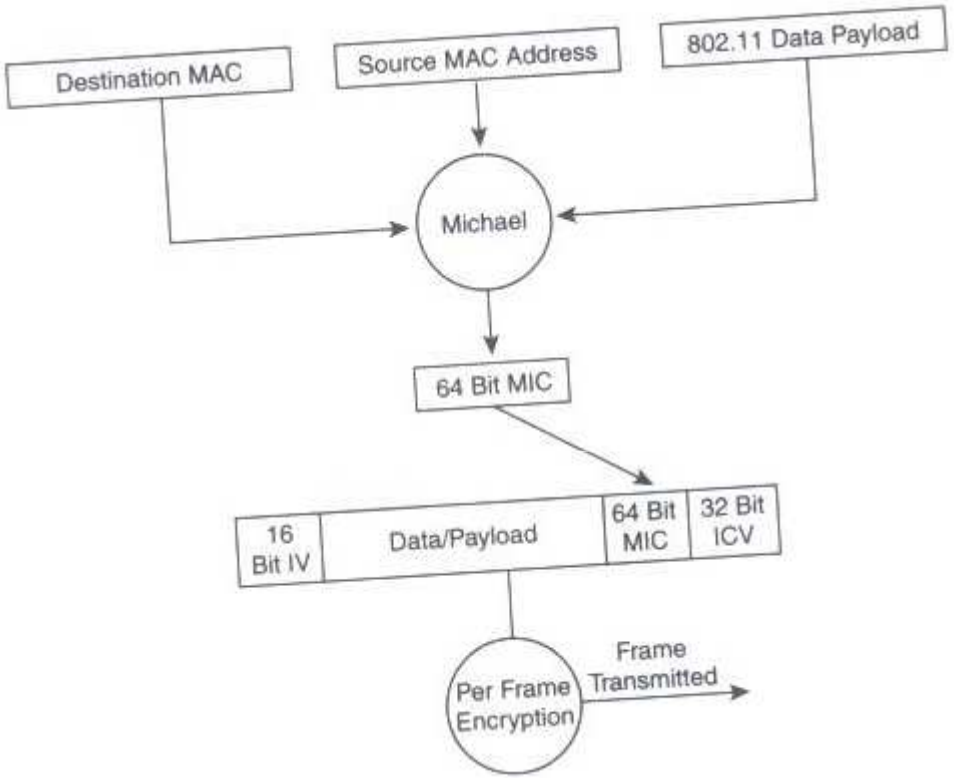
The per-frame key is only valid when the 16-bit IV values have not been used → no collision. To avoid IV collision, the phase 1 key is recalculated by incrementing the most significant 32 bits of the IV by 1 and recalculating the per-frame key

Collisions

- Will this mechanism ever cause an IV collision?
- 802.11b roughly 1000frames/sec
- 16-bit frame IV exhausts after 65 seconds (2^16 frames/1000)
- There are 2^32 possible phase I IVs
- 65*2^32 →8852 years
- Remember TKPI is designed to patch the holes in 802.11 (weak algorithms in lieu of hardware replacement)

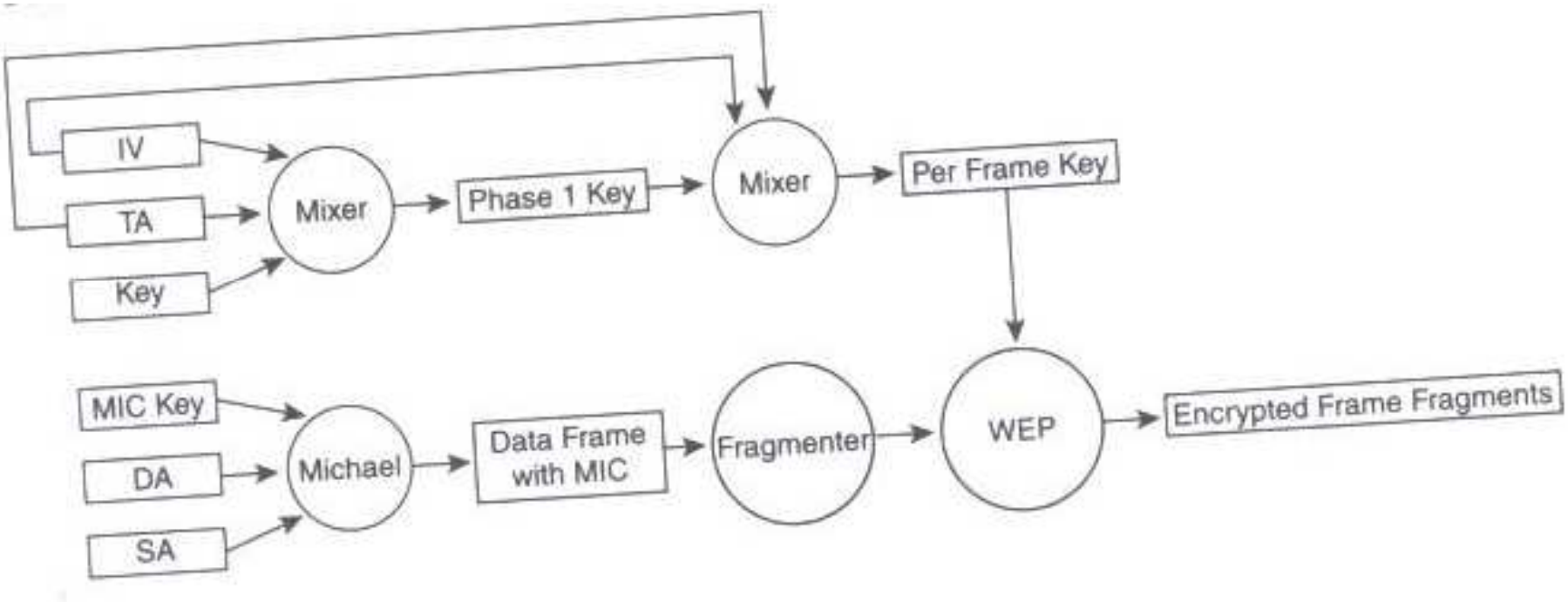
Data Integrity

- Message Integrity Check (MIC) is a feature used to augment the ineffective ICV
- MIC solves the frame tampering/bit flipping attacks
- The MIC has a unique key that differs from the key used to encrypt data frames
- This unique key is mixed with the destination MAC address, the source MAC address and the data payload

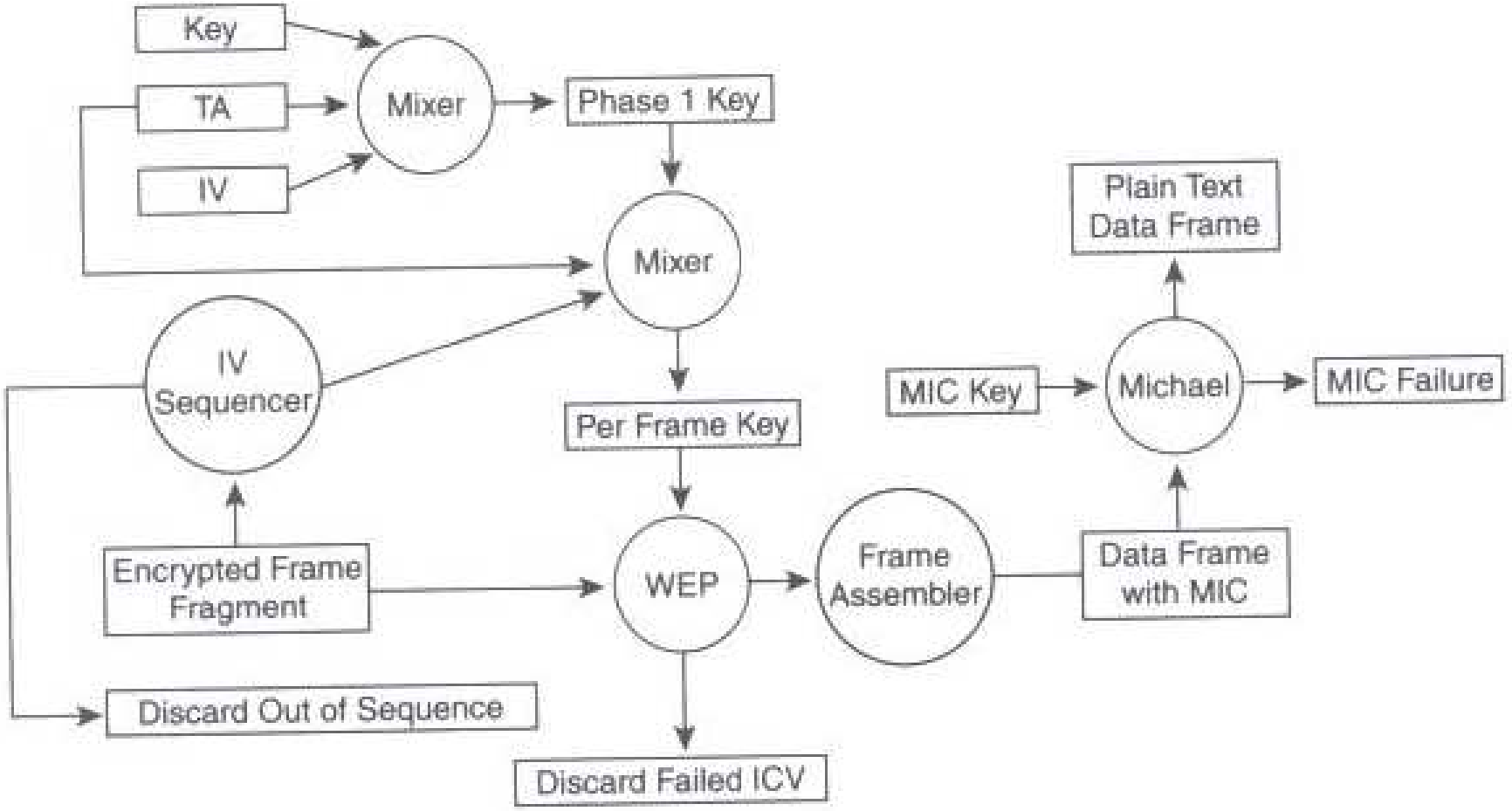


The Michael MIC algorithm

TKPI Encryption process



TKPI decryption process



MIC countermeasures

- The receiver deletes the existing keys for the association
- The receiver logs the issue as a security-relevant matter
- The associated client from which the faulty frame was received cannot associate and authenticate for a period of 60 seconds to slow down the attacker
- If the client received the faulty frame, the client drops any non-802.1X frames
- The client also request a new key

Enhanced Key Management

- No discussion covered how the encryption key and the MIC key are managed
- 802.1X and EAP can provide the RADIUS server and client with dynamic, user-based keys.
- The key used for authentication is not the same used for frame encryption or message integrity.
- It is a MASTER Key used to derive the other keys.

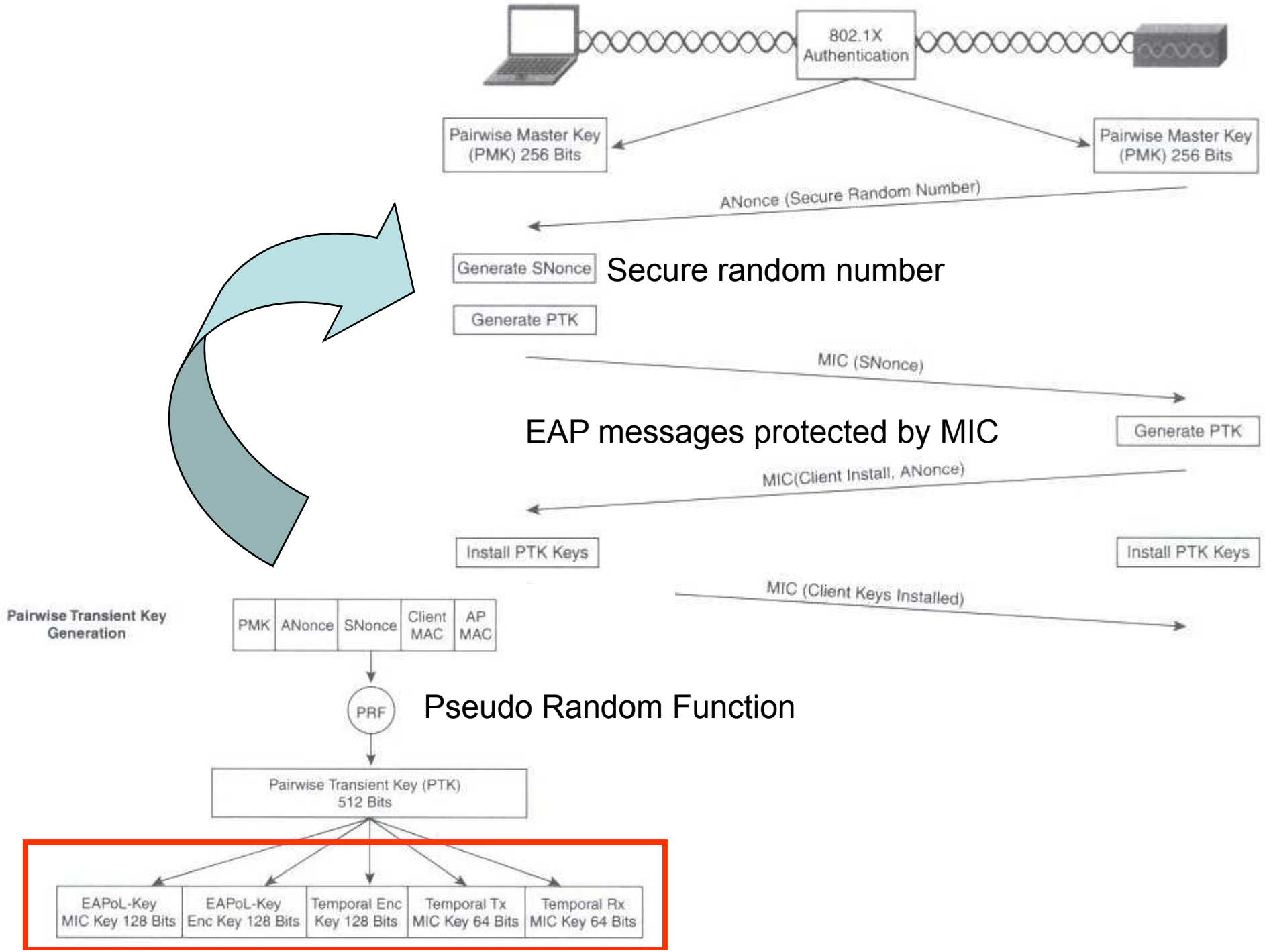
Implementing WPA

To upgrade your wireless security to WPA, you must have three critical components:

- an access point (AP) or wireless router that supports WPA
- a wireless network card that has WPA drivers available
- a client (called a supplicant) that supports WPA and your operating system

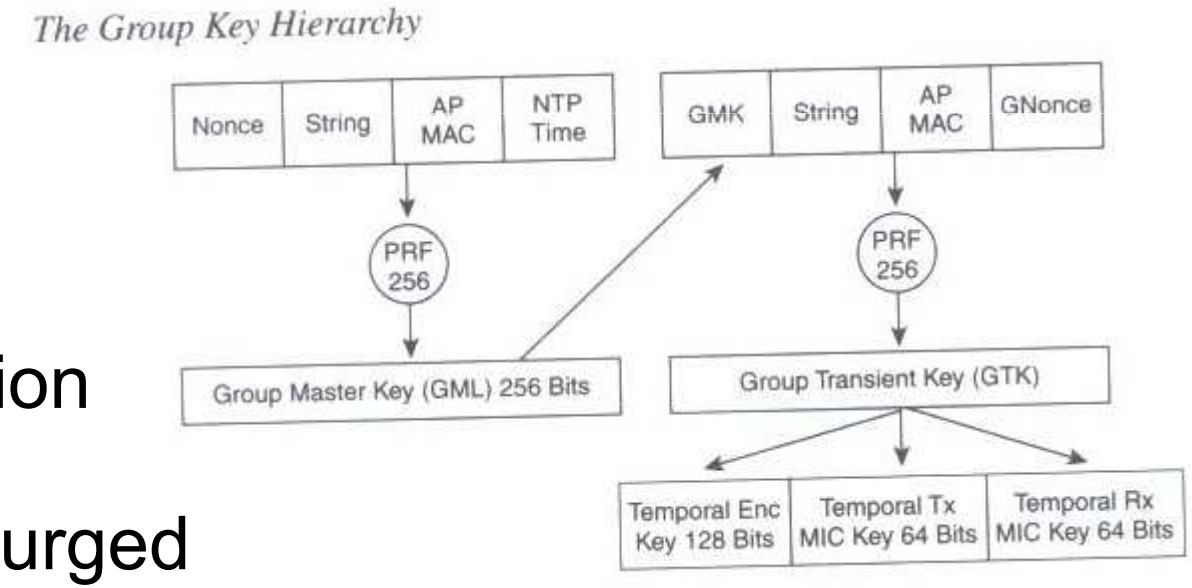
Implementing WPA

- From a hardware standpoint, this means only that your wireless access points and your wireless NICs must recognize the WPA standard. Unfortunately, most hardware manufacturers won't support WPA through a firmware upgrade, so you may find yourself forced to buy new wireless hardware if you want to use WPA.
- Adding WPA support to your OS is the easiest part of the process is. Microsoft provides a free WPA upgrade, but it only works with Windows XP. If you are running an OS other than Win XP, you'll need third-party client software, called a supplicant.


802.1X
Authentication
Pairwise Master Key
(PMK) 256 Bits
Pairwise Master Key
(PMK) 256 Bits
ANonce (Secure Random Number)
Generate SNonce
Secure random number
Generate PTK
MIC (SNonce)
EAP messages protected by MIC
Generate PTK
MIC(Client Install, ANonce)
Install PTK Keys
Install PTK Keys
MIC (Client Keys Installed)
Pairwise Transient Key
Generation
PMK
ANonce
SNonce
Client
MAC
AP
MAC
PRF
Pseudo Random Function
Pairwise Transient Key (PTK)
512 Bits
EAPoL-Key
MIC Key 128 Bits
EAPoL-Key
Enc Key 128 Bits
Temporal Enc
Key 128 Bits
Temporal Tx
MIC Key 64 Bits
Temporal Rx
MIC Key 64 Bits

Broadcast

- PMK and PTK keys are unicast in nature
- The AP is the only entity in a BSS that can send broadcast or multicast traffic
- Broadcast and multicast frames use the group key hierarchy
- The AP sends the GMK encrypted with the client unicast encryption key
- The GMK are purged each time a client disassociate or MIC failure



AES encryption

- The IEEEhas adopted the **Advanced Encryption Standard** (AES) to the data-privacy section of the proposed 802.11i standard (alg. from Rijndael)
- AES requires a feedback mode to avoid ECB