05 - WLAN Encryption and Data Integrity Protocols

WIRELESS LAN SECURITY

Key Management

- One of the big problems in 802.11 is the distribution of keys
- 802.11i introduces key management schemes that allow for a separate authentication process to enable the distribution of keys:
  - Master key establishment
  - Key exchange

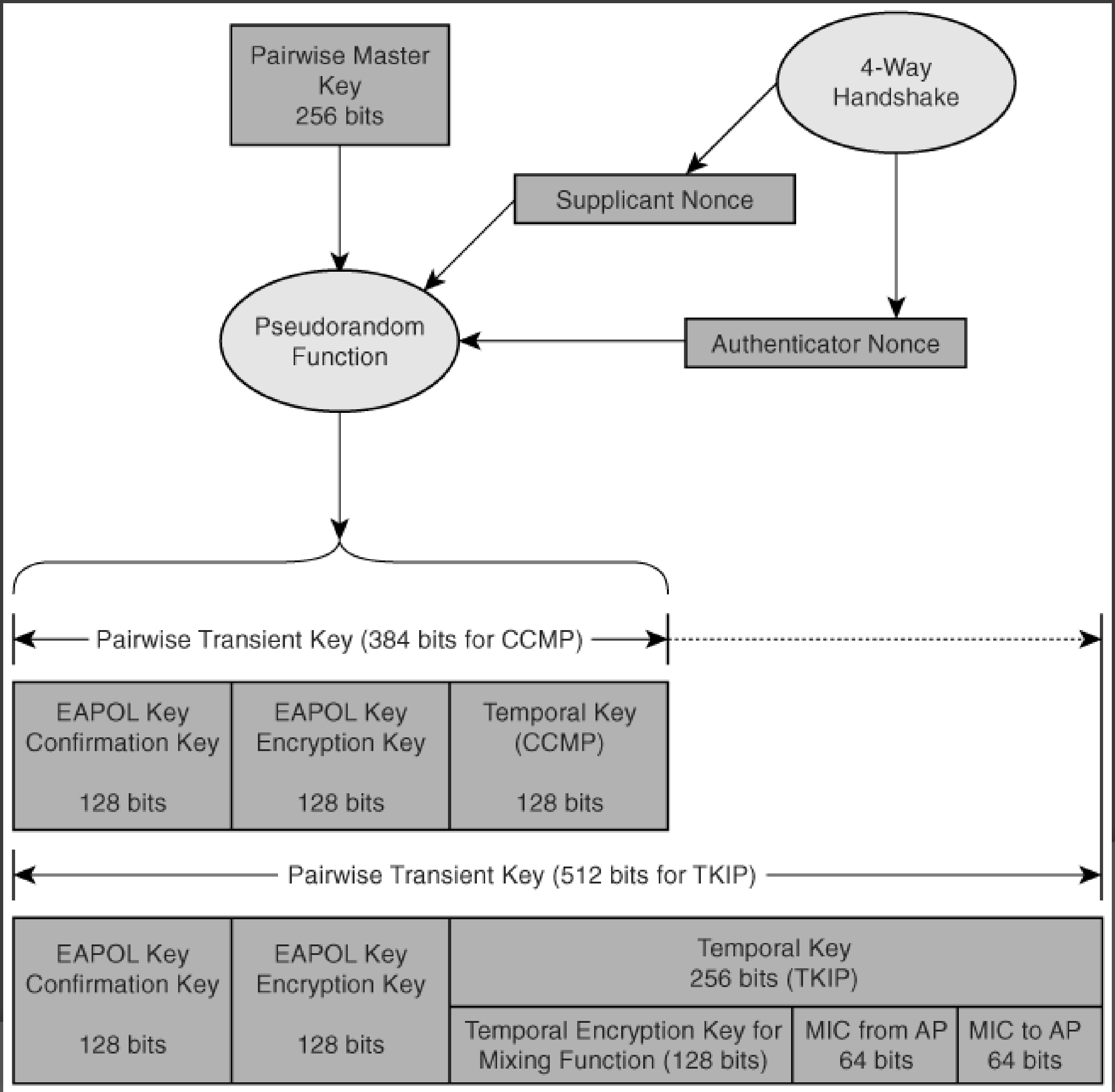
Master Key Establishment

- occurs either manually via configuration (Preshared Key PSK) or dynamically via the 802.1x protocol using EAP:
  - A station authenticates using open system authentication
  - The station and AP then conduct mutual authentication, generating a shared key (Pairwise Master Key PMK) between the AS and the station.
  - The AS transfers this key to the AP via RADIUS

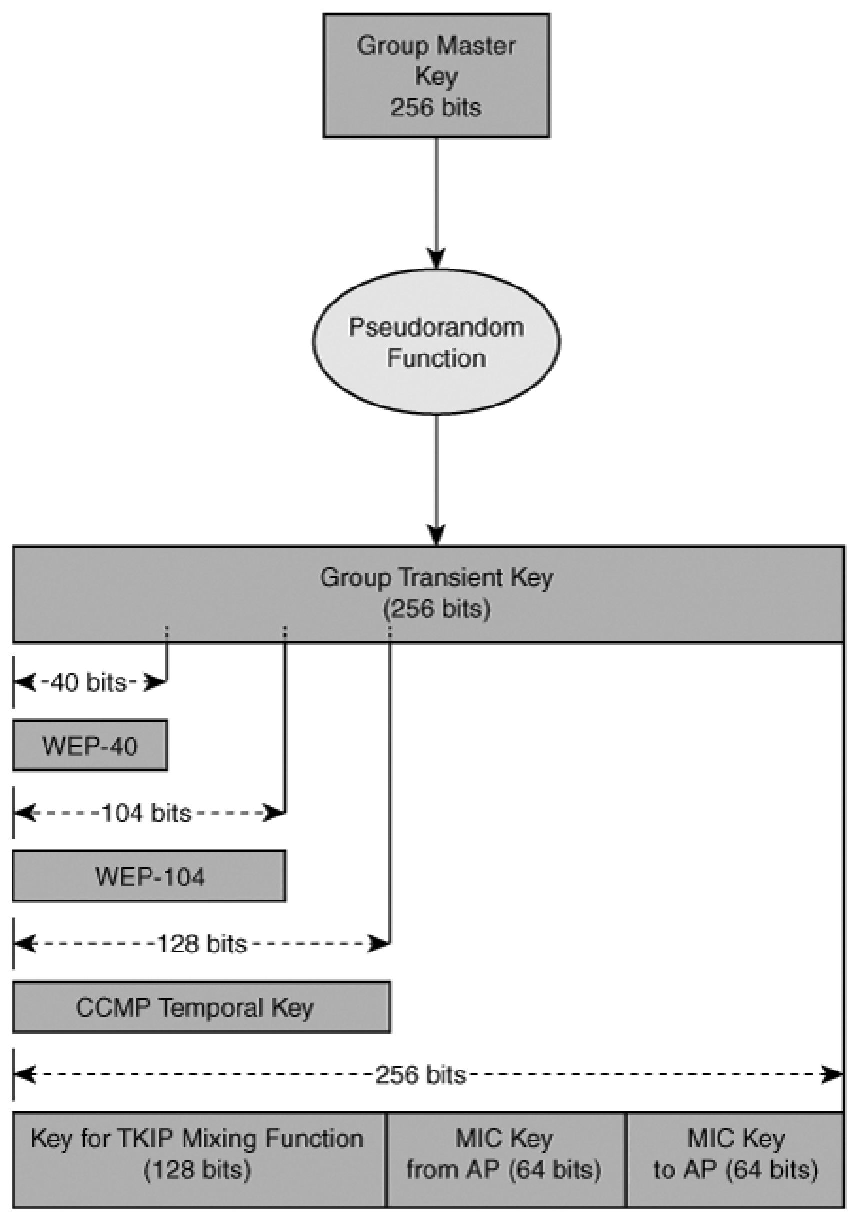
Key Hierarchy

- There are two types of keys in 802.11i:
  - Pairwise for unicast traffic
  - Group for multicast traffic
- The main root pairwise key is the PMK, and the main multicast key is the Group Master Key (GMK).
- The PMK can have a long lifetime and last through multiple associations to an AP.
- The GMK can be configured to be changed every time a station is disassociated or at a regular interval.

Pairwise Key Hierarchy


Pairwise Master Key 256 bits
4-Way Handshake
Supplicant Nonce
Pseudorandom Function
Authenticator Nonce
Pairwise Transient Key (384 bits for CCMP)
EAPOL Key Confirmation Key 128 bits
EAPOL Key Encryption Key 128 bits
Temporal Key (CCMP) 128 bits
Pairwise Transient Key (512 bits for TKIP)
EAPOL Key Confirmation Key 128 bits
EAPOL Key Encryption Key 128 bits
Temporal Key 256 bits (TKIP)
Temporal Encryption Key for Mixing Function (128 bits)
MIC from AP 64 bits
MIC to AP 64 bits

Group Key Hierarchy


Group Master Key 256 bits
Pseudorandom Function
Group Transient Key (256 bits)
-40 bits-
WEP-40
104 bits
WEP-104
128 bits
CCMP Temporal Key
256 bits
Key for TKIP Mixing Function (128 bits)
MIC Key from AP (64 bits)
MIC Key to AP (64 bits)

Group Key Hierarchy (cont.)

- In contrast to the PMK, which is mutually derived, the AP generates the GMK.
- The AP uses the GMK to generate the GTK.
- The GTK can be used with WEP, TKIP, or CCMP. Depending on the encryption protocol used for group communication, its length differs.

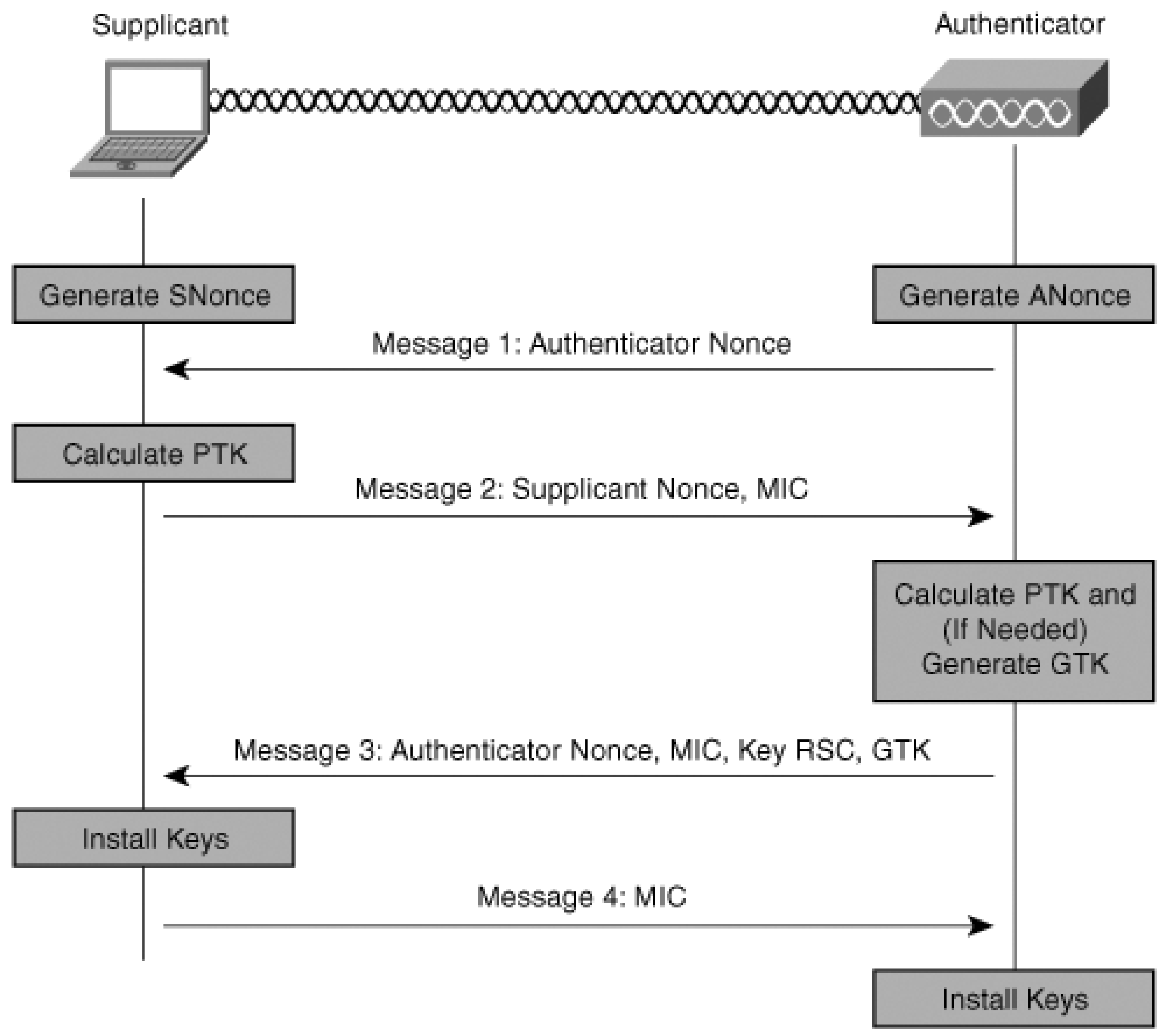
Key Exchange

- After master key establishment, both sides share a PMK and are ready to negotiate the transient keys.
- They do this via the 4-way handshake and the group key handshake.
- After either of these handshakes occurs, the keys derived are stored and used for pairwise or group communication.

The 4-Way Handshake

- After a successful EAP authentication and establishment of the PMKs, a station must use the 4-way handshake to establish the transient keys with the AP.
- The 4-way handshake ensures that both sides still share a current PMK to exchange nonces to be used in building the key hierarchy and to exchange the GTK.

4-Way Handshake


Supplicant
Authenticator
Generate SNonce
Generate ANonce
Message 1: Authenticator Nonce
Calculate PTK
Message 2: Supplicant Nonce, MIC
Calculate PTK and (If Needed) Generate GTK
Message 3: Authenticator Nonce, MIC, Key RSC, GTK
Install Keys
Message 4: MIC
Install Keys

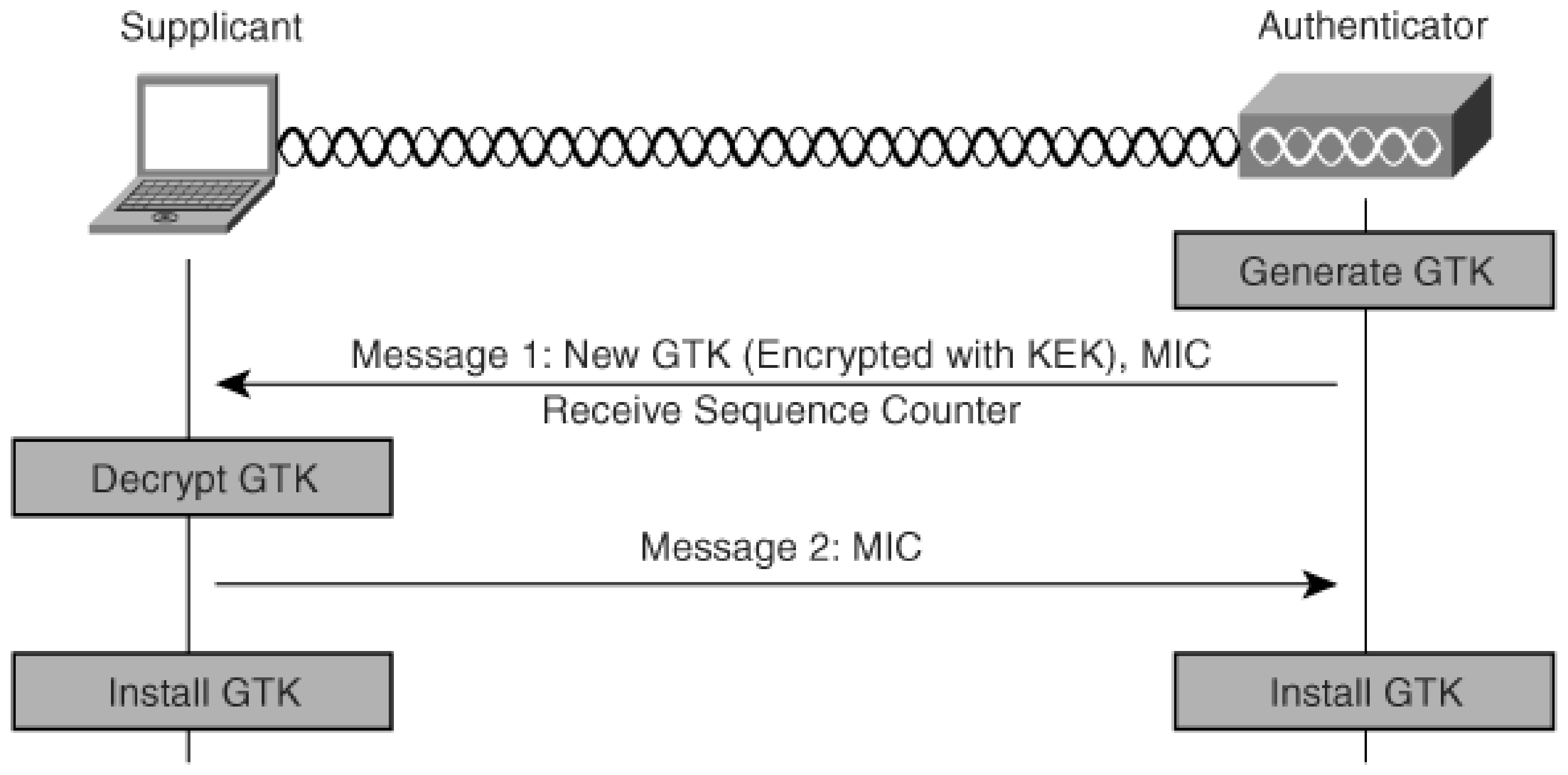
The 4-Way Handshake (cont.)

- The nonce serves as replay protection and must be a value not used before with the PMK.
- The supplicant replies with a proof of its PMK by including a MIC in Message 2.
- Message 3 includes the receive sequence counter (RSC) and allows the station to detect replayed broadcast messages.

The Group Key Handshake

- The authenticator uses this handshake if only the GTK needs changing.
- The authenticator initiates the group key handshake in the event of a Michael MIC failure in either direction, upon deauthentication or disassociation of a station, or at a specified interval.
- In addition, a station can request a renegotiation of the GTK, which the authenticator then initiates.

Group Key Handshake



Supplicant

Authenticator

Generate GTK

Message 1: New GTK (Encrypted with KEK), MIC

Receive Sequence Counter

Decrypt GTK

Message 2: MIC

Install GTK

Install GTK

Security Problems Addressed - Reconnaissance

- 802.11i does nothing to address reconnaissance.
- The improvements in encryption, integrity, and authentication significantly strengthen the security of the networks behind them.
- Attacks on them will be much less likely to succeed.

Security Problems Addressed - DoS Attacks

- 802.11i does nothing to prevent the disassociation and deauthentication attacks .
- These attacks will not be stopped until there is authentication of management and control frames.
- It is important to remember that because nothing can be done about radio frequency jamming or interference attacks, there will never be a complete solution to DoS attacks.

Security Problems Addressed - Shared-Key Authentication Attacks

- 802.11i solves the attacks on the flawed shared-key authentication by obsoleting this authentication method.

Security Problems Addressed - MAC Address Spoofing

- prevents MAC address spoofing by including portions of the MAC address in the MIC calculation
- TKIP does this with the padded MSDU that goes into the Michael algorithm.
- CCMP does this with the additional authentication data included in its MIC calculation.

Security Problems Addressed - Message Modification and Replay

- The MIC, which includes a key, allows a recipient to detect any modification of messages.
- Also, because it is a hash, the attacker cannot make appropriate modifications to it by flipping bits in the MIC.
- Messages cannot be replayed because of the increasing packet counters (TSC in TKIP, PN in CCMP).

Security Problems Addressed - Dictionary-Based WEP Key Recovery

- WEP keys are no longer based on dictionary words, so attackers cannot guess.
- However, WPA includes a standard for the creation of Preshared Master Keys based on ASCII characters.
- The passphrase should be long and includes nonalphanumeric characters. It should be possible to generate it by machine.

Security Problems Addressed - WEP Keystream Recovery

- CCMP uses a block-based cipher, so there is no keystream to recover.
- TKIP's key mixing algorithm ensures that each key, and thus each keystream, will be used only once.
- Although there are still chosen plaintext attacks in which an attacker might be able to recover the keystream, the keystream will not be useful for anything.

Security Problems Addressed - Fluhrer-Mantin-Shamir Weak Key Attack

- The FMS attack relies on receiving a large number of packets encrypted with the same WEP key.
- CCMP does not use WEP, and TKIP changes the WEP key with each packet.

Security Problems Addressed - Rogue APs

- 802.11i does nothing to prevent rogue APs.
- Some of the 802.1x EAP methods address this by providing for certificates to prove the AP’s identity to the client.