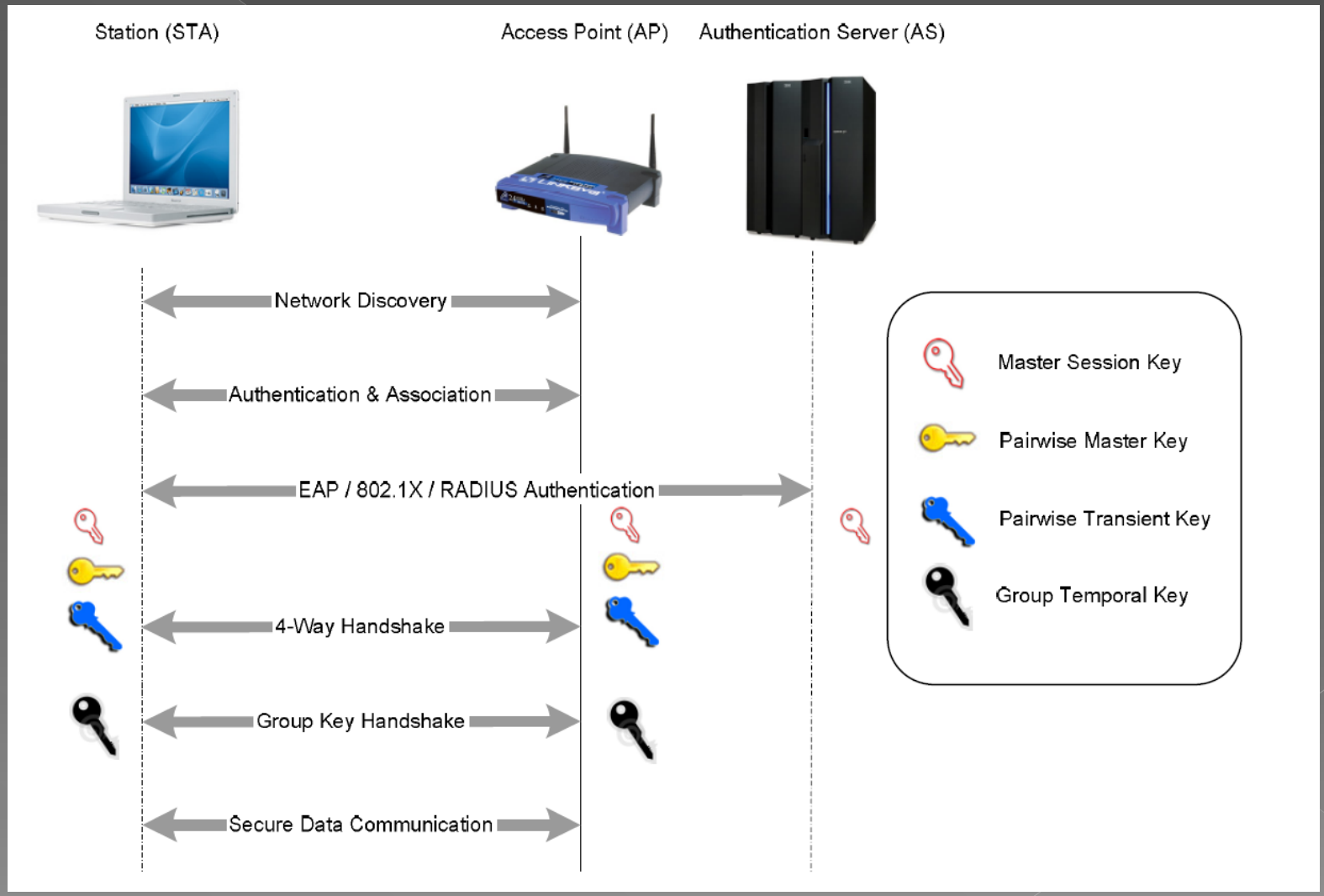
802.11i Security Analysis

802.11i Authentication Process

1. discovery phase
2. authentication and association phase
3. EAP/802.1x/RADIUS authentication
4. 4-way handshake
5. group key handshake
6. secure data communication.

802.11i Authentication Procedures



Discovery Phase

- The access point periodically advertise its IEEE 802.11i security policy in a certain channel through the Beacon frame.
- Station passively monitors the Beacon frame and uses the frame to identify the access point.

Authentication and association phase

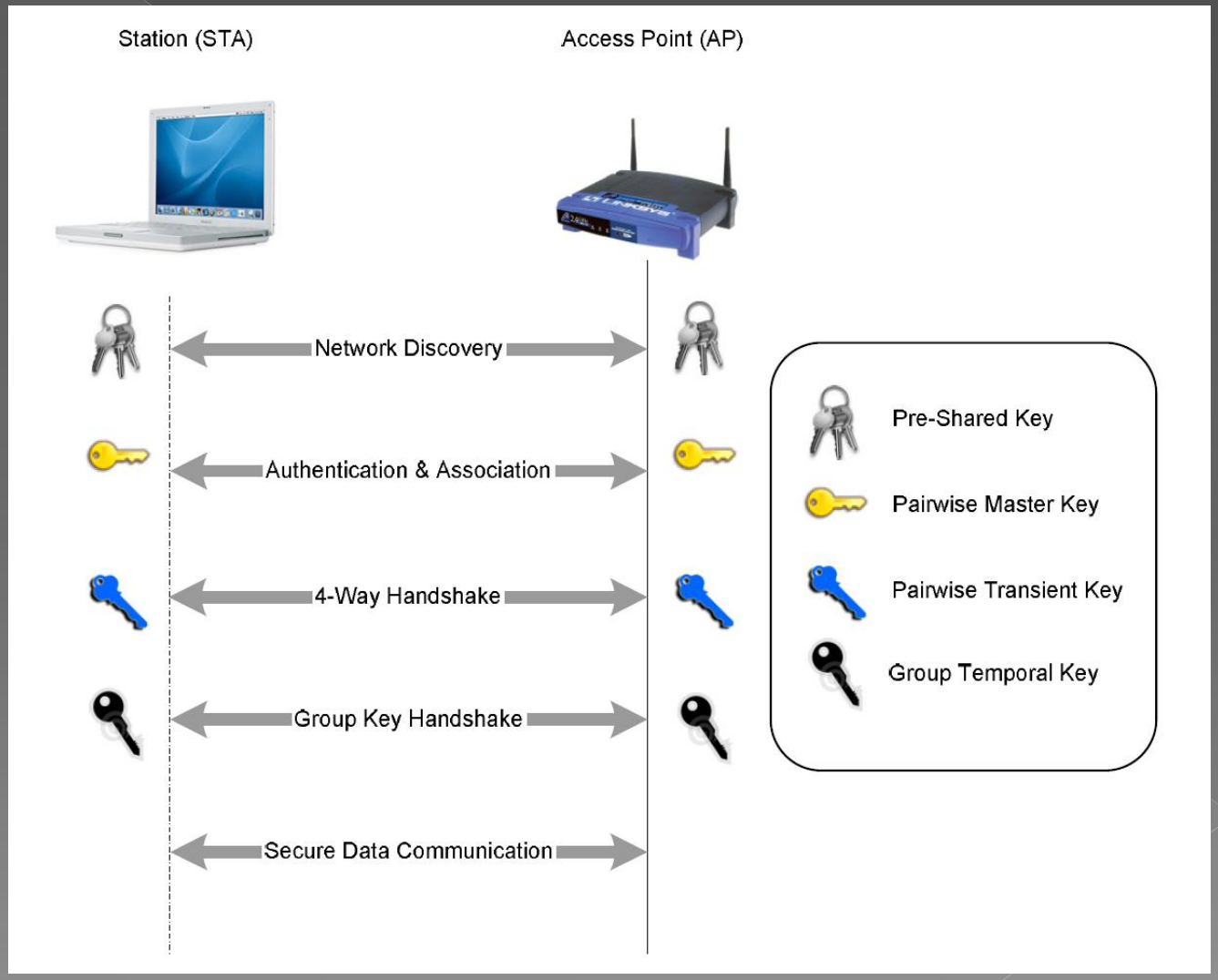
- The station selects one access point from the list of available access points and attempts to authentication and associate with that access point.

- However, this authentication requires to be supplemented by further mutual authentication.

EAP/802.1x/RADIUS authentication

- The station and the authentication server perform mutual authentication and thus some common secret (i.e. PMK) is generated between the station and the authentication server.
- This step does not exist if a static PSK is preinstalled over the station and the access point.

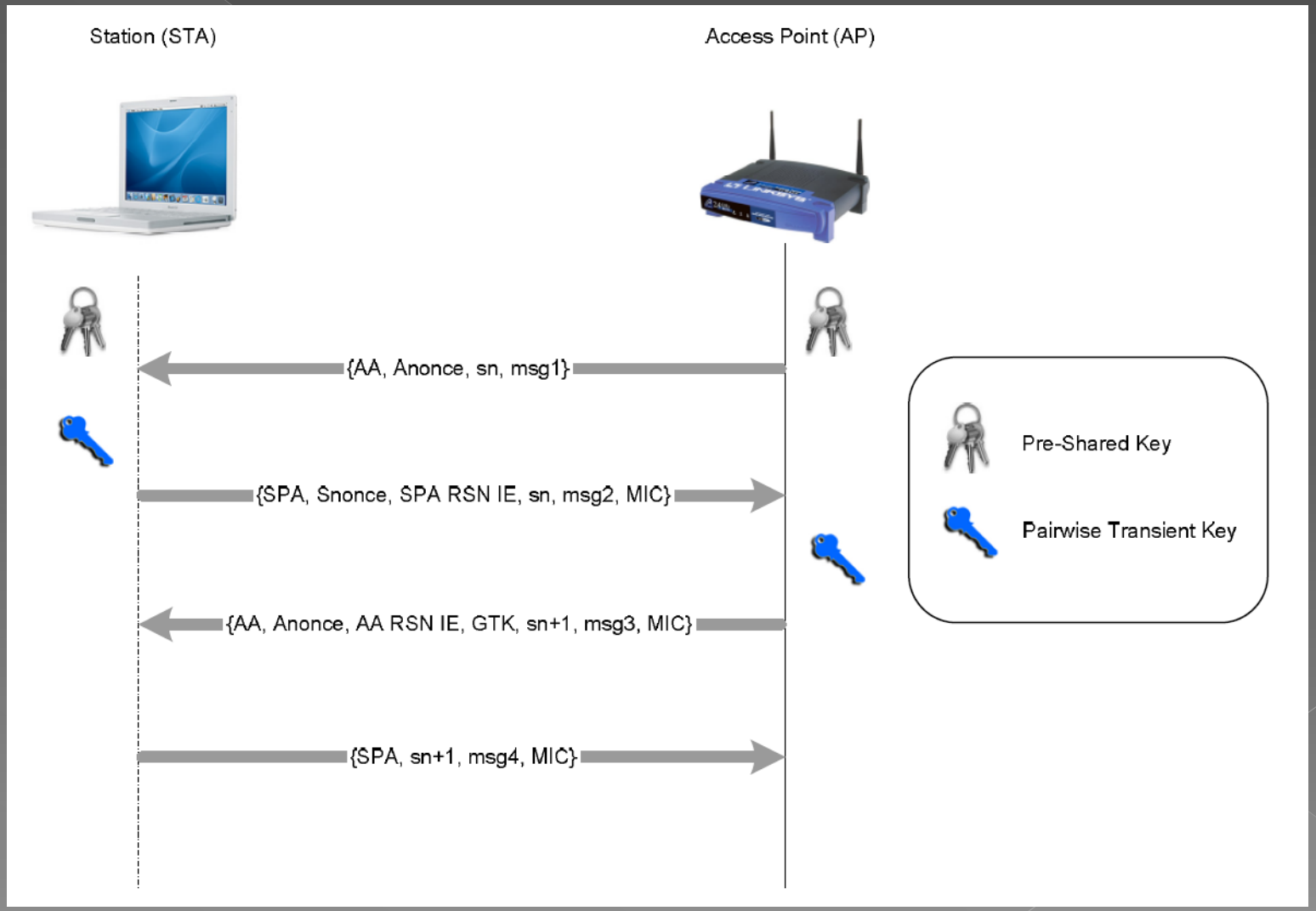
The IEEE 802.11i authentication procedures with PSK



4-way Handshake

- The station and the access point utilize a handshake scheme to confirm the existence of the PMK verify the selection of the cipher suite and derive a Fresh PTK.
- PTK is shared between the station and the access point.

4-way Handshake Scheme



Group Key Handshake

- Due to the requirement of multicast applications, the access point is able to generate and distribute a fresh GTK to the stations.

Secure Data Communication

- By using PTK or GTK, the station and the access point construct a secret transmission channel and thus accomplish robust data confidentiality.

Vulnerabilities

1. Vulnerability to Insider Attack
2. Vulnerability to Offline Guessing Attack
3. No Protection for Management Frames
4. No Protection for Null Data Frames
5. No Protection for EAPOL Frames
6. Denial-of-Service Attack

Vulnerability to Insider Attack

- A great number of vendors adopt a single PSK for every station.
- An insider adversary is able to easily sniff and store all the messages generated at the 4-way-handshake stage.
- The adversary can use the shared PSK and first two handshake messages, including the MAC address and the nonces of the station and access point, through a Pseudo Random Function to derive the fresh PTK.

Vulnerability to Offline Guessing Attack

- An adversary is capable to guess the PSK by capturing and analyzing 4-way-handshake messages.
- The adversary extracts MAC addresses, nonce, the MIC, SN and payload (msg1,2,3,4).
- Due to the fact that MIC is calculated by using PTK to encrypt nonce, SN and message payload, the attacker is able to use authentication message copies, guess and verify the PTK in an offline environment.

No Protection for Management Frames

- 802.11 management frames are always transmitted in an unsecured manner.
- Based on this drawback, a prodigious amount of attacks are launched such as DoS attack, masquerading attack and MitM attack, etc.
- An adversary can simply conduct a DoS attack either by flooding abundant management frames or transmitting forged management frames (such as deauthentication and
- disassociation) to deny service to legitimate users.

No Protection for Null Data Frames

- contains an empty frame body, to carry special control information to another station.
- An adversary can send forged null data frames to steal buffered frames.
- Furthermore, an adversary can update the NAV field in a null data frame and thus mislead stations cannot gain access to the channel.

No Protection for EAPOL Frames

- During the authentication procdure, all the EAPOL frames are out of protection since a RSNA has not been established.
- An adversary can passively eavesdrop and cache sensitive traffic (eg. access account).
- An adversary injects either a forged EAPOL-logoff frame to force a legitimate station out of service, or a forged EAPOL-failure frame to disconnect a station from an existing session.
- In addition, adversaries are able to spoof a station to disconnect from an authentication session by sending a premature EAPOL-success frame

Denial-of-Service Attack

- There is another potential security issue at the 4-way-handshake stage.
- The first handshake message does not involve MIC filed to accomplish integrity protection.
- Therefore, an adversary can flood forged initialized messages and thus derive inconsistent keys between the station and access point.