UNIT-5

→ Wireless Network Security:

* Threats to wireless networks:

↳ unauthorized access; tampering, eavedropping; man in the middle, denial of service.

*→ Security measures:

① WPA2 Encryption: (WiFi Protected Access 2)
↳ uses AES to encrypt data transmitted over wireless network.

② TKIP: (Temporal Key Integrity Protocol)
↳ provides per packet key mixing & a message integrity check to prevent tampering

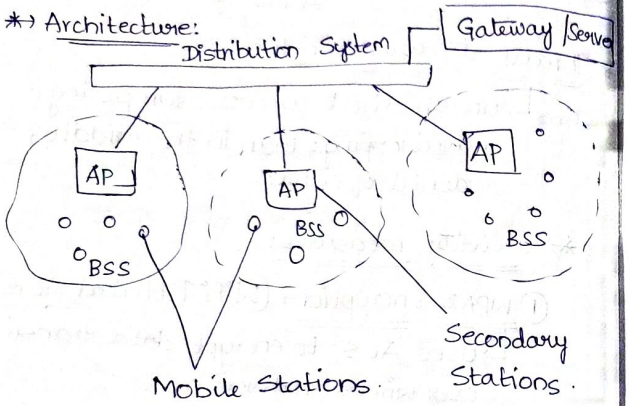
③ CCMP: (Counter Mode CBC-MAC protocol)
↳ provides data encryption and integrity using AES in counter mode.

④ Secure authentication protocols:
↳ Protocols such as 802.1X and EAP-TLS provide authentication & authorization

* IEEE 802.11 Wireless LAN:

↳ set of standards of wireless LANs.

*→ Architecture:



ESS: Extended Service Set

STA: device that connects to a WLAN.

Access Point (AP): device that provides access to WLAN.

Distribution System: connects multiple APs together.

*→ Protocols:

① MAC (Media Access Control):

↳ defines how devices access the wireless medium & transmit data.

② PHY (Physical Protocol):

↳ defines the physical layer of the wireless communication; including modulation, & trasmission frequency.

→ IEEE 802.11i Wireless LAN:

↳ amendment to IEEE 802.11 that provides security enhancements.

Security:

- → WPA2
- → TKIP
- → CCMP
- → Secure Authentication protocols.

* IP Security:

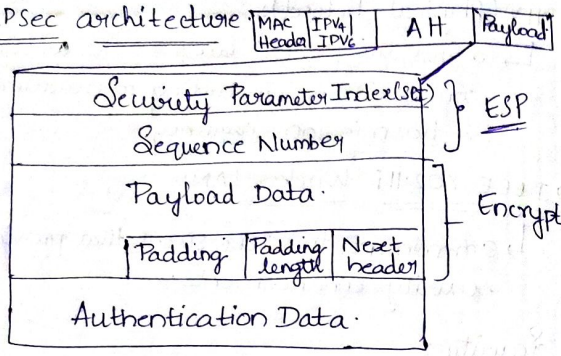
↳ suite of protocols that provides security for IP communications.

↳ IPsec is designed to ensure confidentiality, integrity, authenticity for IP packets.

*→ Features:

↳ Encryption, Authentication, Key Exchange.

* IPSec architecture



*→ Protocols:
- → Internet Key Exchange: (IKE)
  - ↳ used to establish secure keys for encryption & authentication
- → Encapsulating Security Payload (ESP):
  - ↳ Encryption & authentication for IP packets.

*→ Authentication Header.
- ↳ AH ensures that IP packets are not tampered (or) altered during trasmission.

* Intrusion Detection System
- → monitors network traffic for signs of unauthorized access (or) malicious activity.
- → Types:
  - ↳ network-based IDS, host-based IDS, distributed IDS.
- → Techniques:
  - ↳ Signature-based, anomaly-based stateful protocol analysis.

*→ Signature-based:
- → uses predefined signatures of known attacks to identify malicious activity.
- → Advantages
  - → effective against known attacks
  - ↳ implemented using string matching algo.
- ↳ Disadvantages:
  - → not efficient for unknown attacks.
  - ↳ frequent signature updates.

* → Anomaly-based:

- uses ML algos to identify unusual patterns of activity that may indicate an attack.
- Advantages:
  - can detect unknown attacks.
  - does not require sign updates.
- Disadvantages:
  - generate false +ves
  - requires training data.