Wireless Network Security
IEEE 802.11

Wireless Local Area Network

- A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires to communicate between network-enabled devices.

Wireless Network Modes

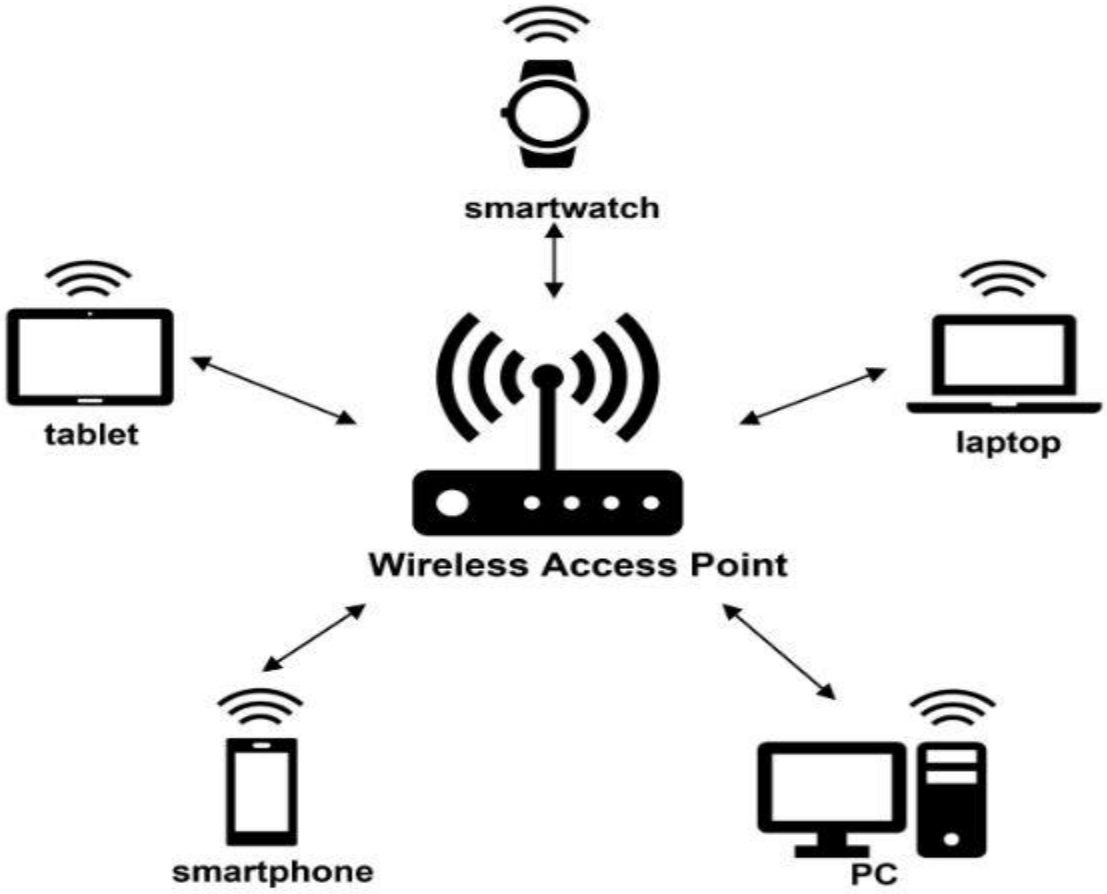
- The 802.11 wireless networks operate in two basic modes:
  - Infrastructure mode
  - Ad-hoc mode

- Infrastructure mode
  - Each wireless client connects directly to a central device called Access Point (AP)
  - No direct connection between wireless clients
  - AP acts as a wireless hub that performs the connections and handles them between wireless clients

Wireless Network Modes (Contd…)

- Ad-hoc mode:
  - Each wireless client connects directly with each other
  - No central device managing the connections.
  - Rapid deployment of a temporal network where no infrastructures exist (advantage in case of disaster…)
  - Each node must maintain its proper authentication list.

Wireless LAN



Access Point

- A wireless access point (AP) is a hardware device that allows wireless communication devices, such as PDA (Personal Digital Assistant) and mobile computers, to connect to a wireless network.

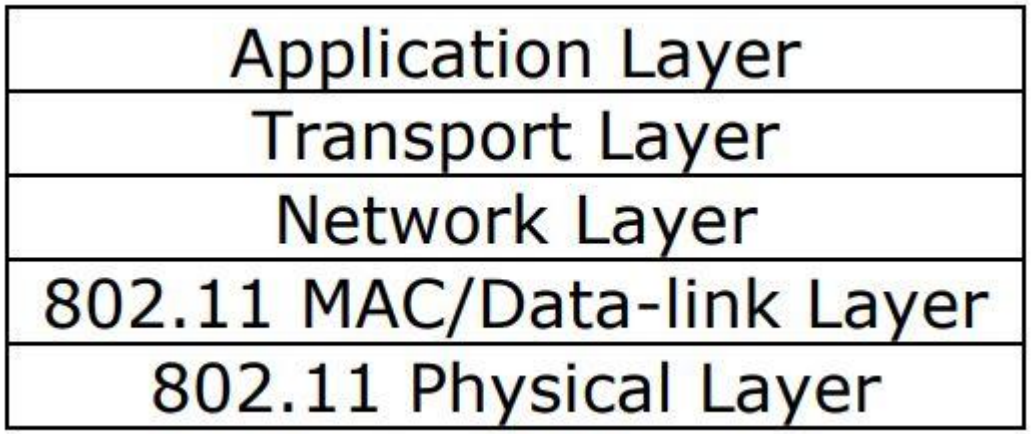
- Usually, an AP connects into to a wired network, and provides a bridge for data communication between wireless and wired devices.

Service Set Identifier (SSID)

- It is a configurable identification that allows wireless clients to communicate with an appropriate access point.
- With proper configuration, only clients with correct SSID can communicate with the access points.
- In effect, the SSID acts as a single shared password between access point and clients.

Protocol Stack

- The protocol stack for WLANs was designed such that existing applications can use them with minor modifications.
- The top three layers of the stack are same as the other networks.



Physical Layer

- The 802.11 physical layers modulate the data and send it over the air.
- Three popular standards: 802.11a, 802.11b, 802.11g

Parameter	802.11a	802.11b	802.11g
Speed	54 Mbps	11Mbps	54Mbps
Frequency Band	5 GHz	2.4 GHz	2.4 GHz
Modulation	OFDM	DSSS	OFDM
Distance(Indoor)	18 mts	30 mts	30 mts
Distance(Outdoor)	30 mts	120 mts	120 mts
No. of simultaneous networks	12	3	3

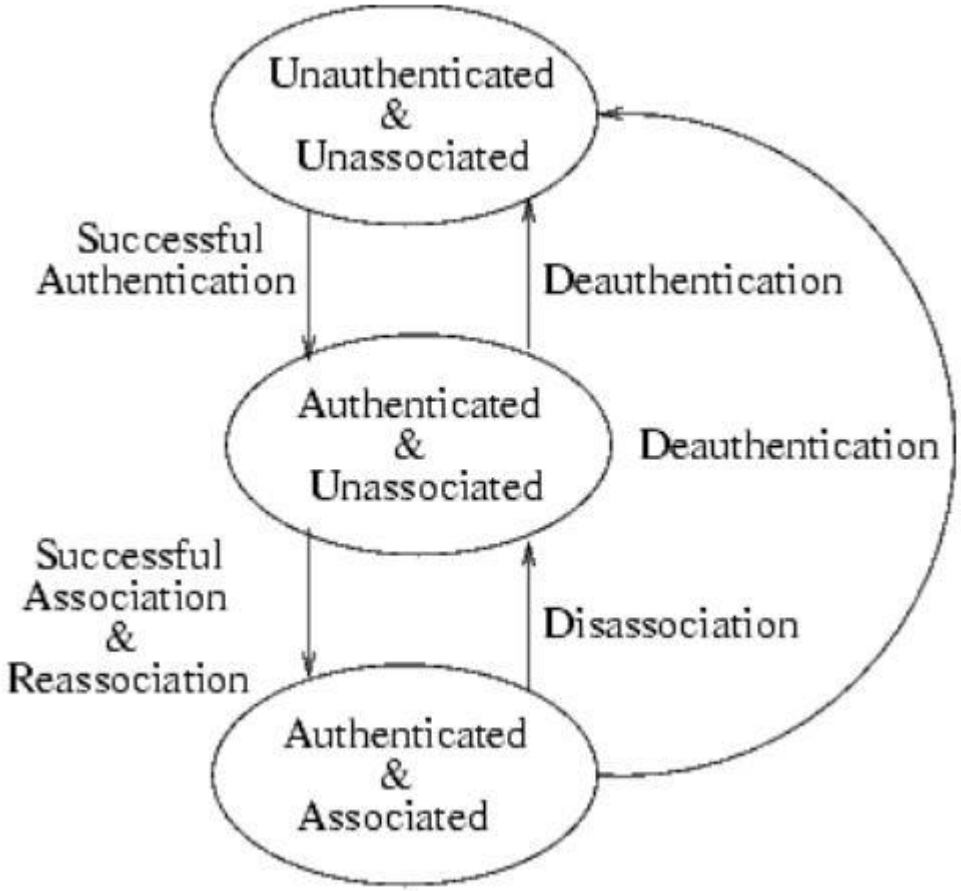
MAC Layer

- The MAC / data link layer of 802.11 specifies the following features:
  - CRC checksum
  - Fragmentations
  - Auto-Roaming
  - Authentication and Association
  - WEP, WPA1,WPA2,WPA3 protocols

Authentication and Association

- The need of a client to be mobile brought in the separation of authentication and association processes.
- Since a client frequently changes AP boundaries, he can be authenticated to various AP at a given point, yet remains associated to his chosen one.
- Before a client gets associated to other, he must be first authenticated.

Authentication and Association



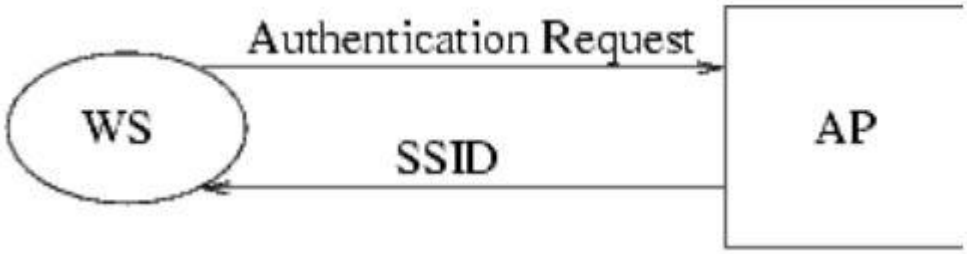
Types of Authentication

- Two types of authentications:
  - Open system authentication
  - Shared key authentication
  - Extended Authentication Protocol

Open system authentication

- Open system authentication is the default and simplest authentication algorithm.
- Provides authentication without performing any type of client verification.
- It is considered a null authentication because no exchange or verification of identity takes place between the devices.
- A client just needs an SSID for successful Association.

.



Shared system authentication

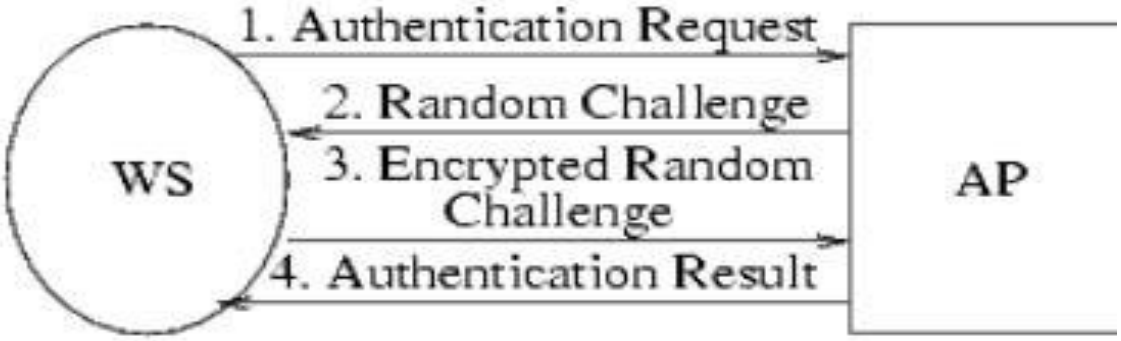
- Shared key authentication uses a Pre-Shared key (PSK) for the AP and client to complete authentication.

- Shared key authentication uses the following process:
  1. The client sends an authentication request to the AP.
  2. The AP randomly generates a challenge text and sends it to the client.
  3. The client uses the WEP key to encrypt the challenge text and sends it to the AP.

Shared system authentication

4.The AP uses the WEP key to decrypt the challenge text and compares the decrypted challenge text with the original challenge text.

- If they are identical, the client passes the authentication. If they are not, the authentication fails.



Extended Authentication Protocol (EAP)

- It provides the framework within which the various authentication methods work.

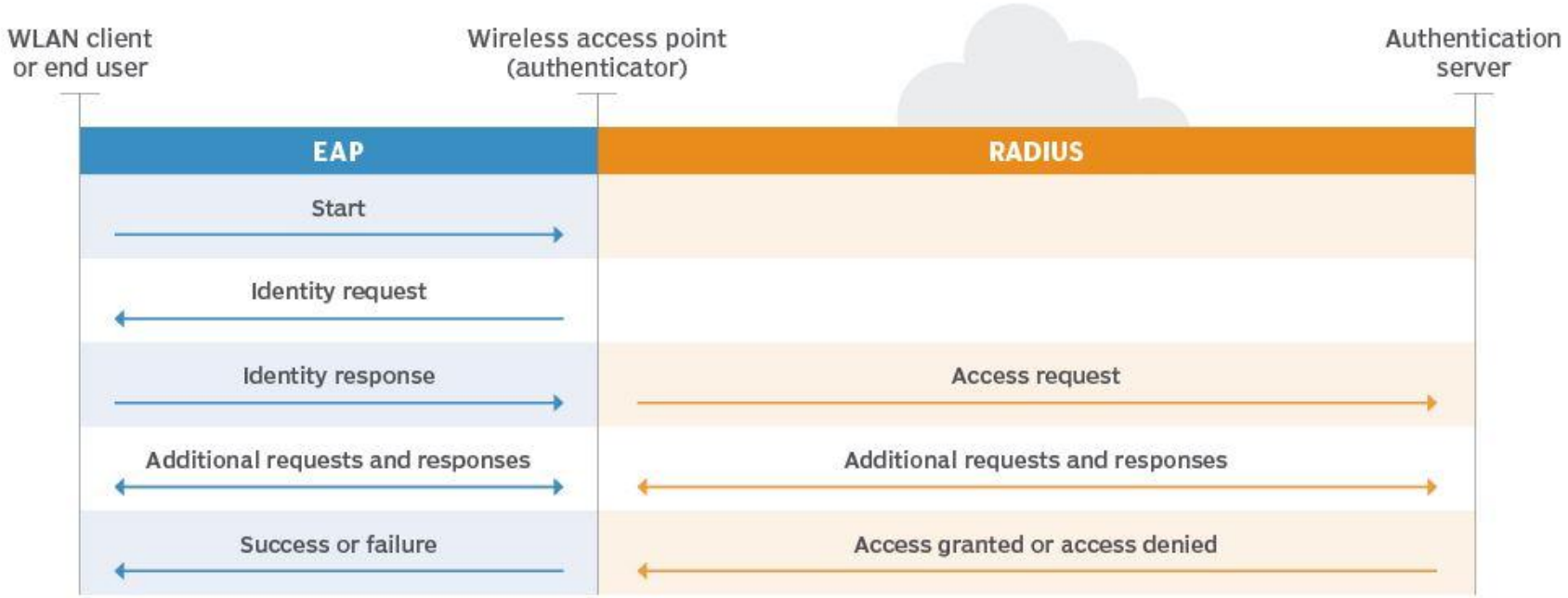
- It supports various authentication methods, including as token cards, smart cards, certificates, one-time passwords and public key encryption etc.

- Component of 802.1x authentication are:
  - The user's wireless device.
  - The wireless access point (AP).
  - The authenticator server/database.

EAP (Contd..)

- The EAP process works as follows:
  1. A user requests connection to a wireless network through an AP.
  2. The AP requests identification data from the user and transmits that data to an authentication server.
  3. The authentication server asks the AP for proof of the validity of the identification information.
  4. The AP obtains verification from the user and sends it back to the authentication server.
  5. The user is connected to the network as requested.

EAP (Contd..)


WLAN client or end user
Wireless access point (authenticator)
Authentication server
EAP
RADIUS
Start
Identity request
Identity response
Access request
Additional requests and responses
Additional requests and responses
Success or failure
Access granted or access denied

Association

- To start the actual communication.
- Association only occurs on wireless infrastructure networks, not in peer-peer mode.
- Mobile device authenticates to an AP/router and then sends an Association Request.
- AP/router processes the Association Request.
- AP/router vendors may have different implementations for deciding if a client request should be allowed.
  - When an AP/router grants association, it responds with a status code of 0 (successful) and the Association ID (AID).
  - Failed Association Requests include only a status code

Wireless Security Overview

- Concerns for wireless security are similar to those found in a wired environment

- Security requirements are the same:
  - Confidentiality, integrity, availability, authenticity, accountability
  - Most significant source of risk is the underlying communications medium

Key Factors Contributing to Risks

- Channel: broadcast communication (more susceptible to eavesdropping and jamming)
- Mobility: additional risks (later)
- Resources: advanced OS (iPhone, Android), but limited resources (memory, processing)
- Accessibility: Certain devices may be left unattended

Mobile Device Security Challenges

- No more tight control over computing devices
- Growing use of mobile (endpoint) devices
- Cloud-based applications readily available (Box, Dropbox, Skype, …)
- De-perimeterization: static network perimeter is gone
- External business requirements (guests, third-party contractors, …)
- Bring Your Own Device (BYOD)

Mobile Device Security Threats

- Lack of physical security control
- Use of untrusted mobile devices
- Use of untrusted networks
- Use of apps created by unknown parties
- Interaction with other systems (e.g., cloud-based data sync)
- Use of untrusted contents.

Securing Wireless Networks

- Use encryption
- Use and enable anti-virus, anti-spyware, firewall
- Turn off SSID broadcasting
- Change default identifier on router
- Change router’s preset password
- Apply MAC-filtering

Mobile Device Security Strategy

- Device security (next slide)
- Traffic security (e.g., SSL, VPNs)
- Barrier security (e.g., firewalls, IDS/IPS)

Mobile Device Security

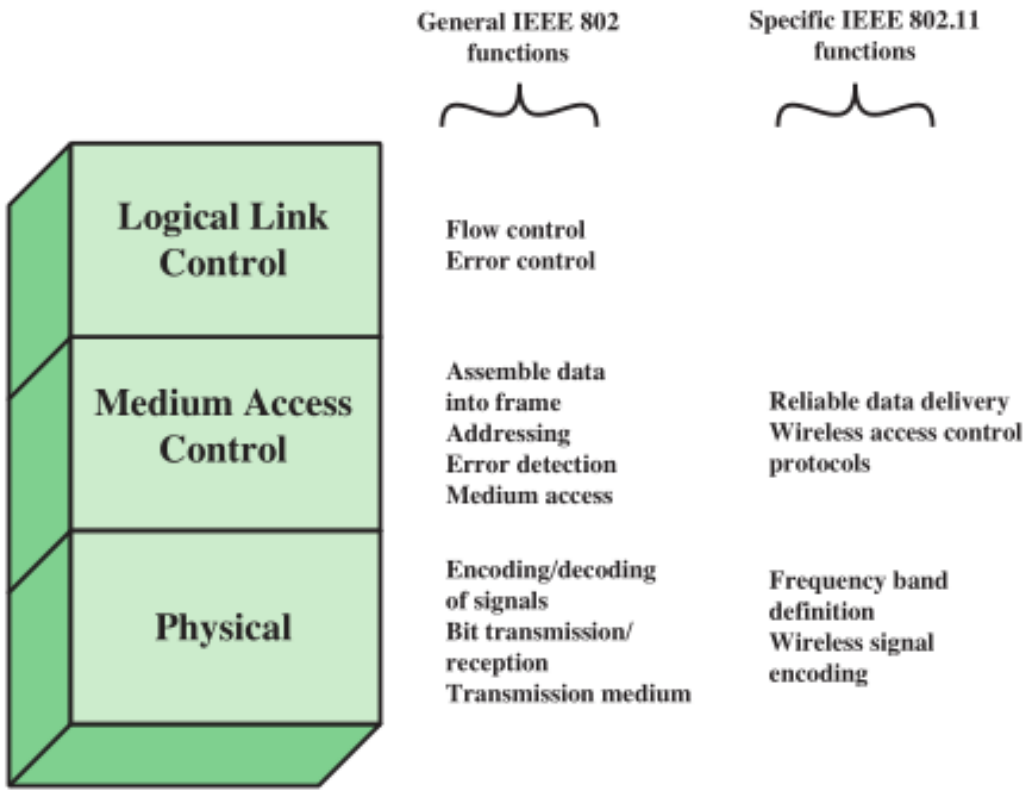
- Configure (enable) auto-lock
- Configure/enable SSL
- Enable password/PIN protection
- Configure (disable/discourage) auto-completion (for passwords)
- Up-to-date OS/software
- Install anti-virus software
- Encrypt sensitive data on mobile devices
- Prohibit installation of third-party apps

IEEE 802.11 Wireless LAN

- IEEE 802: a committee responsible for LANs
- IEEE 802.11: responsible for developing wireless protocols
  - Many standards are developed
  - WEP was introduced.
- The Wi-Fi alliance: became popular with 802.11b
  - Wi-Fi Protected Access (WPA, WPA2)

IEEE 802.11 Protocol Stack

- **Physical layer** (encode/decode signals)
- **MAC layer**: assembles MAC frame, disassembles frames and performs address recognition
- **LLC**: keeps track of frame transmission

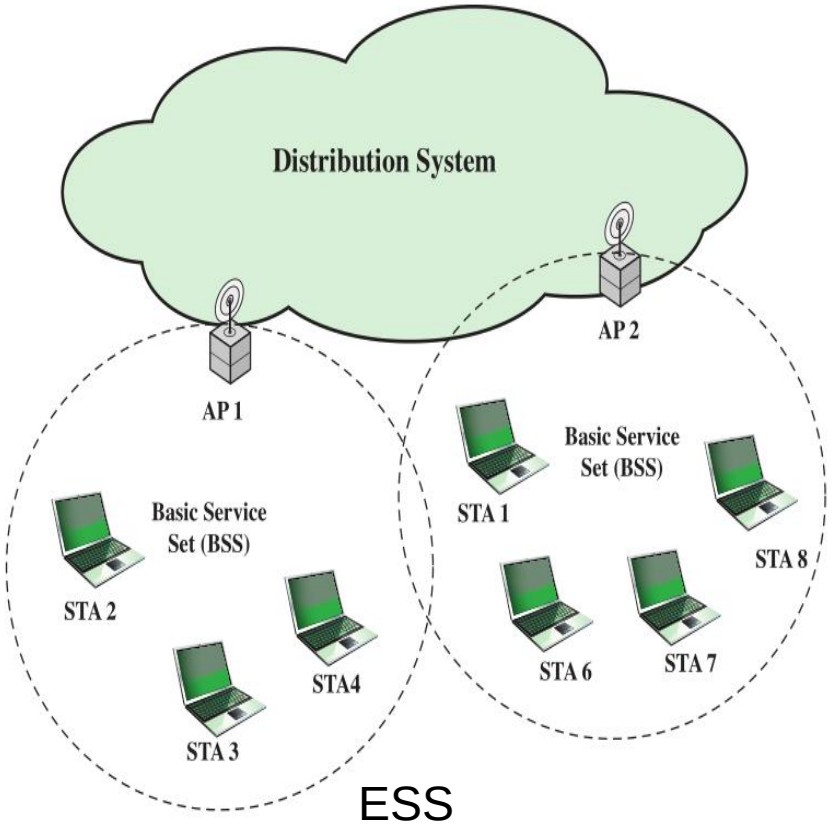


A MAC Frame (MPUD)

- MAC protocol data unit (MPUD)

IEEE 802.11 Extended Service Set

- **BSS**: Basic Service Set the smallest building block
- **BSSs** contains Access Points (**APs**) and Stations (**STA**).
- **ESS**: Extended Service Set, two or more BSSs.
- **DS:** Distribution System



IEEE 802.11: Wireless Security Protocols

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
  - WPA1
  - WPA2
  - WPA3

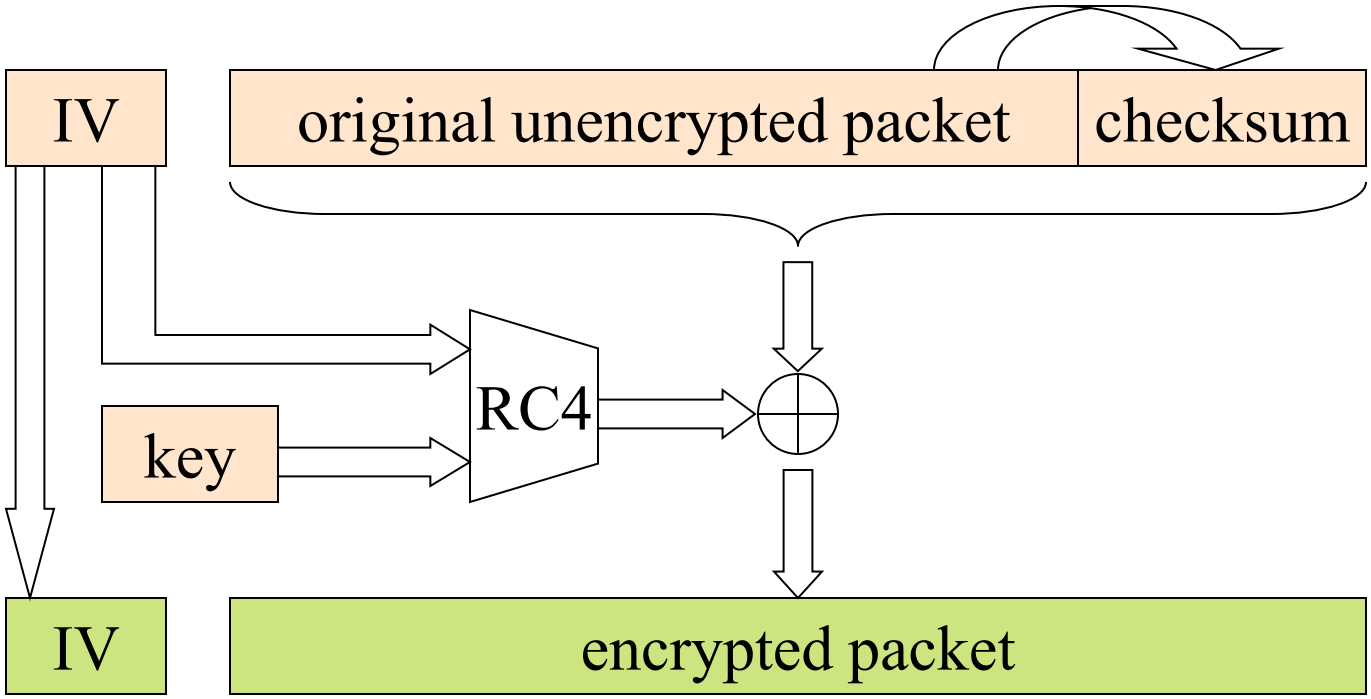
WEP : Wired Equivalent Protocol

- WEP (Wired Equivalent Protocol) is a wireless security protocol introduced and ratified by the IEEE.
- Both IEEE 802.11 and IEEE 802.11i standards contain a description of this protocol.
- Used to protect wireless communication from eavesdropping (confidentiality)
- Prevent unauthorized access to a wireless network (access control)
- Prevent tampering with transmitted messages (Integrity).

WEP

- Authentications: It can use both Open System authentication and shared key authentication.
- Encryption: The encryption algorithm used in this protocol is RC4 (Rivest Cipher 4) stream cipher.
- CRC checksum is used for data integrity.
- Single key is used with 40, 104 or 232 bit keys can be used.

How WEP works



WEP Weaknesses

- High degree of data manipulation and data loss so integrity is not guaranteed.
- The size of the key is small, which provides a lack of security to the data packets.
- Initialization Vector, is reused and is small in size. Attacker can use this to crack the encryption.
- It is now considered as unsecured because a WEP key can be cracked in a few minutes with the aid of automated tools. (So it should not be used).

Known attacks on WEP

- Passive Attacks
  - Dictionary based attacks
  - Cracking the WEP Key
- Active attacks
  - Authentication spoofing
  - Message Injection
  - Message Modification
  - Message Decryption
  - Man in the middle attack

WPA : Wifi Protected Access

- Wi-Fi Protected Access (WPA) is a wireless security protocol designed to address and fix the known security issues in WEP.

- This protocol is a subset of 802.11i, and it is designed to provide security to all versions of 802.11 devices, including 802.11a, 802.11b, and 802.11g.

- WPA uses the basic principle of WEP however, it rectifies its security problems by providing improvements in security problems of authentication and data integrity.

WPA

- Encryption: It uses Temporal Key Integrity Protocol for encryption(TKIP).
  - TKIP include per packet key, integrity check, re-keying mechanism.

- Authentication: Pre Shared Key (PSK) is used for personal use and Extensible Authentication Protocol (EAP) is used for Enterprise.
  - Remote Authentication Dial In User Service (RADIUS) allow central server to authenticate user.

Temporal Key Integrity Protocol (TKIP)

- TKIP algorithm acts as a wrapper to the old WEP algorithm, providing extra layer security without modifying WEP.

- TKIP is a cipher suite. It includes
  - 64 bit MIC (Message Integrity Check)
  - Packet sequencing control.
  - Per packet key mixing function.

TKIP

Process:

- The mixing function uses a pairwise transient key, the sender's MAC address, and the packet's 48-bit serial number.
- It is combined with the IV (initialization vector) to generate 128 bit key.
- The key is then used with RC4 cipher.

- It provides two services:
  - Message Integrity: Add MAC code after data field
  - Data Confidentiality: Symmetric encryption using generated key.

WPA Strength

- Prevents forgeries by using the cryptographic Message Integrity Code (MIC).
- Using the Message Integrity Code, the wireless network will be secured from the man in the middle attack and DoS attacks.
- Replay attacks are removed using a new Initialization Vector (IV).
- Key relaying mechanism is used to provide a new and fresh key for data encryption.
  - Making it difficult to break the key.

WPA2

- Enhancement for WPA.
- For Encryption Advanced Encryption Standard (AES) and Counter/Mode/CBC-MAC protocol (CCMP) is used.
- Key Size used is 128 bit.
- EAP for enterprise and PSK for personal authentication is used.
  - The Personal mode uses a PSK (Pre-shared key) & does not require a separate authentication of users
  - The enterprise mode requires the users to be separately authenticated by using the EAP protocol

CCMP

- CCMP is an abbreviation of **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol**.
- CCMP is the encryption protocol used in the WPA2 and WPA3.
- Counter Mode (CTR): CCMP uses Counter Mode (CTR) encryption, which involves encrypting individual data blocks with a unique encryption key.
  - This ensures that even if an attacker manages to decrypt one block, they cannot decrypt the entire message.
- Cipher Block Chaining (CBC): CCMP also utilizes Cipher Block Chaining (CBC), which involves chaining the encrypted blocks together.
  - This adds an additional layer of security and prevents patterns from emerging in the encrypted data.

WPA2

- WPA2 has immunity against many types of hacker attacks
  - ✓ Man-in-the middle
  - ✓ Authentication forging
  - ✓ Replay
  - ✓ Key collision
  - ✓ Weak keys
  - ✓ Packet forging
  - ✓ Dictionary attacks

WPA3

- It is an enhancement for WPA2 released in 2018.
- The Encryption method used is AES-CCMP/ AES- GCMP(Galois Counter Mode Protocol).
  - It use 128 bit or 256 bit keys.
- It uses SAE (Simultaneous Authentication of Equal) protocol.

GCMP

- Galois Counter Mode Protocol (GCMP) is protocol suite used to provide data confidentiality, integrity and authentication.
- It uses Galois/Counter Mode (GCM) similar to CCMP used to encrypt individual blocks.
- It uses Galois Message Authentication Code (GMAC) as a cryptographic hash function.
- GMAC provides message integrity and authentication.

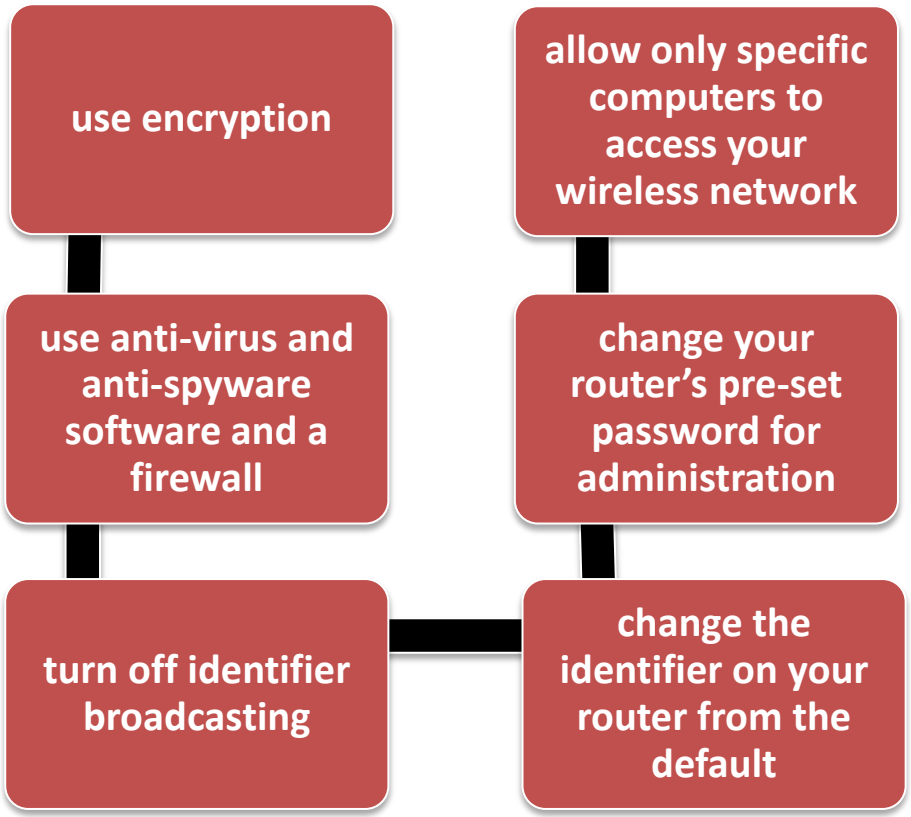
Comparison of different protocols

	WEP	WPA	WPA2	WPA3
ENCRYPTION	RC4	RC4-TKIP	AES-CCMP	AES-GCMP
KEY ROTATION	NONE	Dynamic Session Keys	Dynamic Session Keys	Dynamic Session Keys
SESSION KEY SIZE	40 bits	64/128 bits	128 bits	128 bits/256bits
AUTHENTICATION	PSK	PSK and EAP	PSK and EAP	EAP and SAE

Procedures to Improve Wireless Security

- Use wireless intrusion prevention system (WIPS)
- Enable WPA-PSK
- Use a good passphrase/password
- Use WPA2 where possible.
- AES is more secure, use TKIP for better performance
- Change your SSID every so often.
- Wireless network users should use or upgrade their devices to the latest security standard released.

Securing Wireless Networks



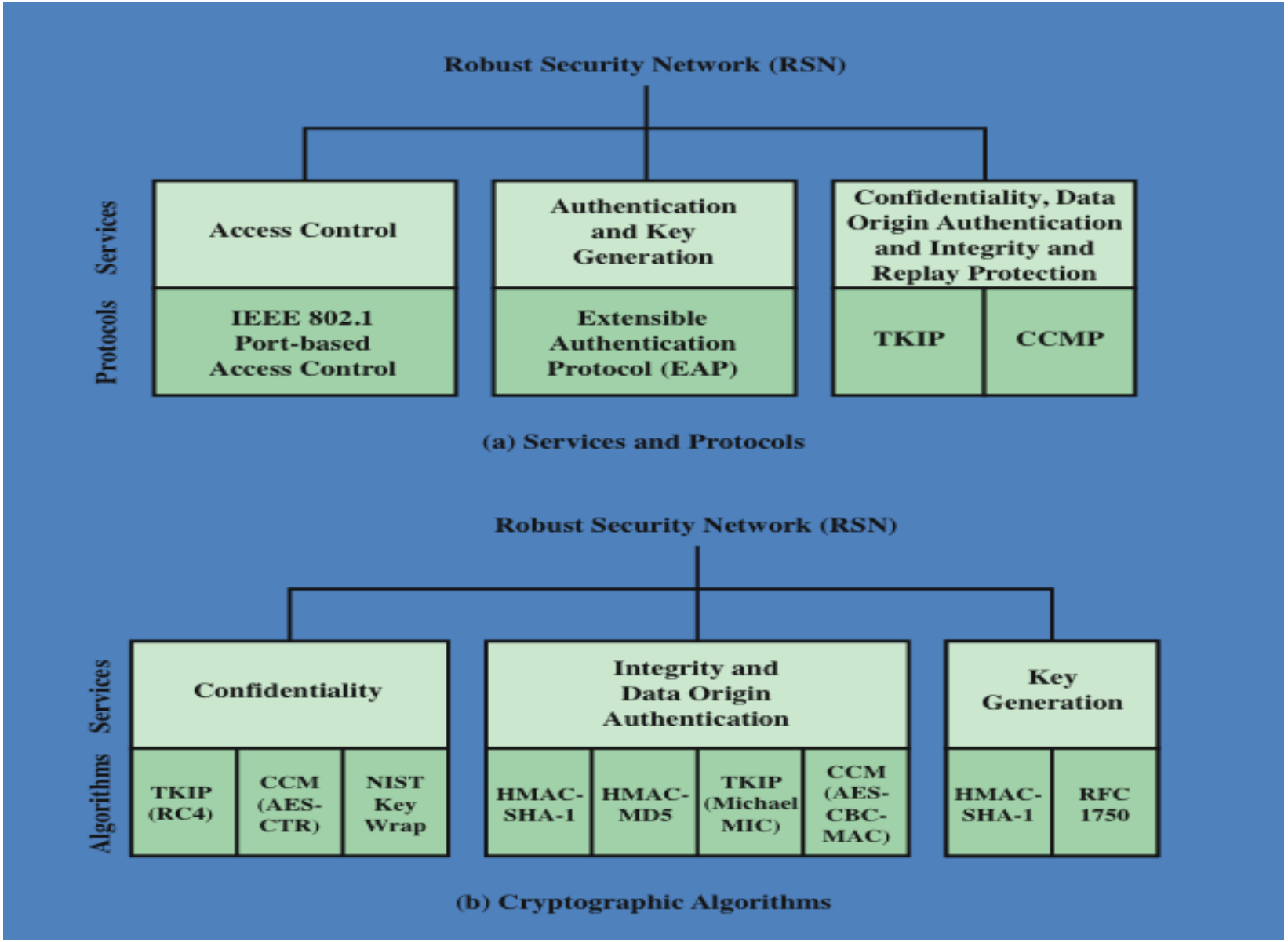
IEEE 802.11i Services

- **Robust Security Network (RSN):** Robust Security Network is a term used in WiFi networks to describe the security enhancements encompassed in the IEEE 802.11i i.e. WEP, WPA,WPA2 and WPA3.

Services:

- **Authentication**: the exchange between a user and an authentication server (AS); temporary keys are generated
- **Access control**: routes messages properly, facilitates key exchange
- **Privacy**: MAC level data are encrypted (GMAC, MIC)

Elements of IEEE 802.11i



Packet sniffing

- A great deal of traffic is sent through wireless networks, such as **RTP**, **SNMP** or **HTTP**.
- The common feature of these is the fact that they are in **plain text**.
- Someone with **malicious intentions** can simply steal your passwords and similar sensitive information.

- Packet sniffing can be evaded using encryption solutions.

Parking Lot Attack

- Access points emit radio signals in a circular pattern. Signal Exceed the intended physical boundaries.
- Signals can be intercepted outside buildings, or even through the floors in multi-storey buildings.
- As a result, attackers can implement a "parking lot" attack, where they actually sit in the organisation's parking lot and try to access internal hosts via the wireless network.

- Prevention can be radio frequency shielding applied.

Rogue Access Point

- **Rouge access point** refers to any unauthorized access point (AP) on a network. It can be created by an attacker or even a misinformed employee. Moreover, rouge APs make the entire network vulnerable to **DoS attacks**, packet captures, **ARP poisoning** and more.

- You can use **network access controls** and **network access protocols** or introduce **authentication processes** to protect your organization.

Evil Twin Attack

- An evil twin attack takes place when an attacker sets up a fake Wi-Fi access point hoping that users will connect to it instead of a legitimate one.

- When users connect to this access point, all the data they share with the network passes through a server controlled by the attacker.

- Avoid Unsecured wifi hotspot
- Disable auto connect.
- Avoid logging into private accounts on public Wi-Fi.
- Use VPN in public wifi .

Network Jamming

- Jamming (also known as network interference) aims to disrupt the network.
- Due to the wireless features, interference is almost unavoidable.
- Most of the time, ill intended intruders combine **jamming techniques** with other methods like **evil twinning**.
- **Spectrum analyser** an be used to boost the signal or use different frequencies than the attacker.

Wireless Network Tools

- MAC Spoofing
  - ✓ http://aspoof.sourceforge.net/
  - ✓ http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp
  - ✓ http://www.klcconsulting.net/smac/
- WEP Cracking tools
  - ✓ http://www.backtrack-linux.org/
  - ✓ http://www.remote-exploit.org/articles/backtrack/index.html
  - ✓ http://wepattack.sourceforge.net/
  - ✓ http://wepcrack.sourceforge.net/
- Wireless Analysers
  - ✓ http://www.kismetwireless.net/
  - ✓ http://www.netstumbler.com/