4.4 Wireless Network Security

Wireless Security

Some of the key factors contributing to higher security risk of wireless networks include

- Channel
- Mobility
- Resources
- Accessibility

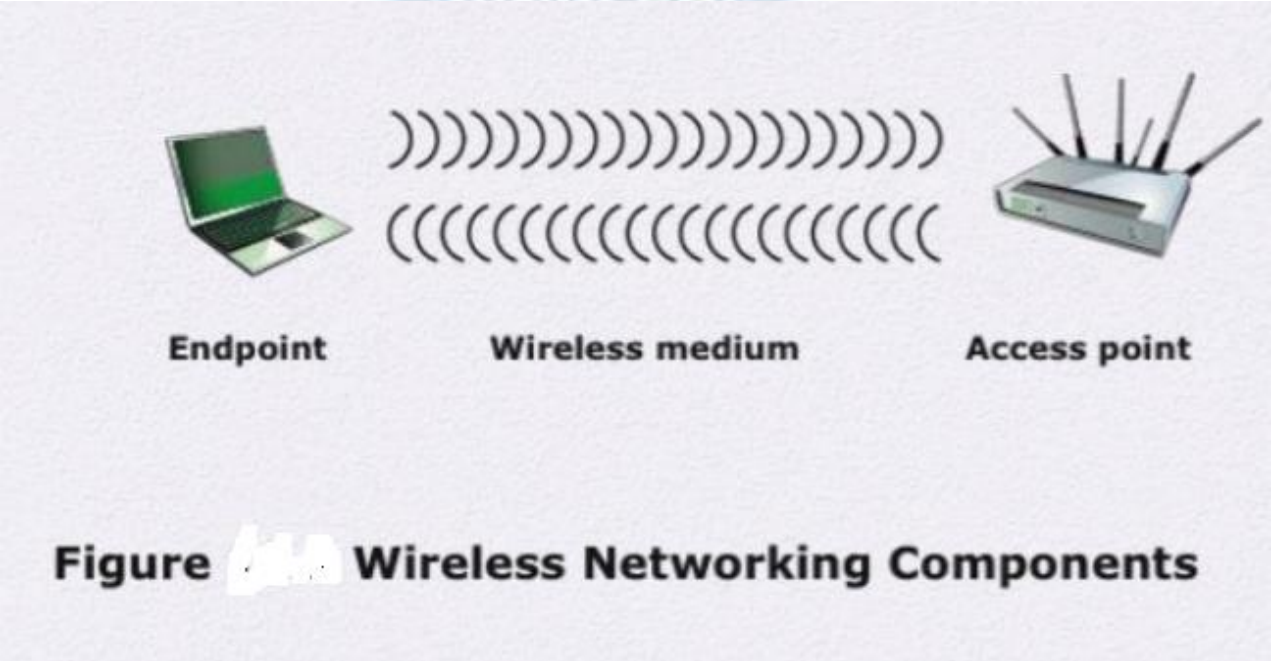


Figure 4.4 Wireless Networking Components

Wireless Network Threats

- Accidental association
- Malicious Association
- Man in the middle attack
- DoS
- Identity theft

SECURITY MEASURES

Securing Wireless transmissions from Eavesdropping

- Signal hiding techniques
- Encryption

Securing Wireless Access Points

- Unauthorized Access to the network

Solutions

IEEE 802.1x standard for port based network access control

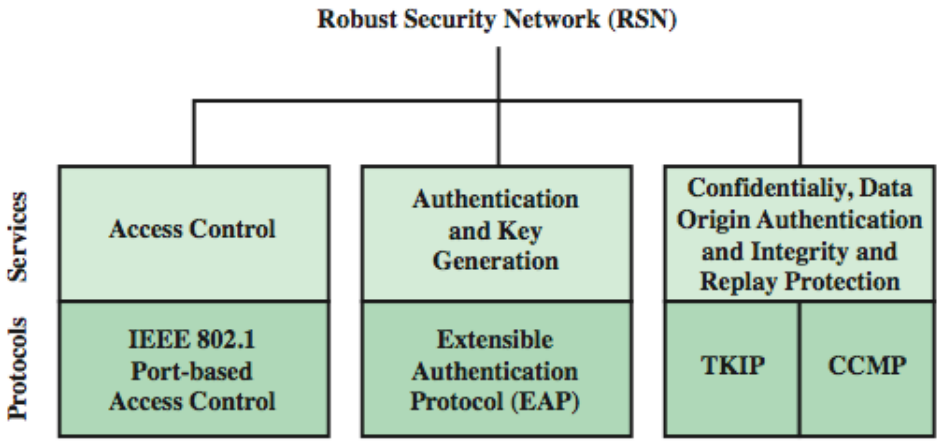
Securing wireless networks

- Use encryption
- Use antivirus, antispyware software and firewall
- Turnoff Identifier broadcasting
- Allow only specific computers to access your wireless netw

IEEE 802.11i

- The differences between wired and wireless LANs suggest the increased need for robust security services and mechanisms for wireless LANs.
- For privacy, 802.11 defined the **Wired Equivalent Privacy (WEP)** algorithm. The privacy portion of the 802.11 standard contained major weaknesses. In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance circulated **Wi-Fi Protected Access (WPA)** as a Wi-Fi standard. The final form of the 802.11i standard is referred to as **Robust Security Network** (RSN). The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA 2 program.

802.11i RSN Services and Protocols



The 802.11i RSN security specification defines the following services:

- Authentication

- Access control
- Privacy with message integrity

802.11i Phases of Operation

Figure lists the cryptographic algorithms used for the 802.11i RSN security services.

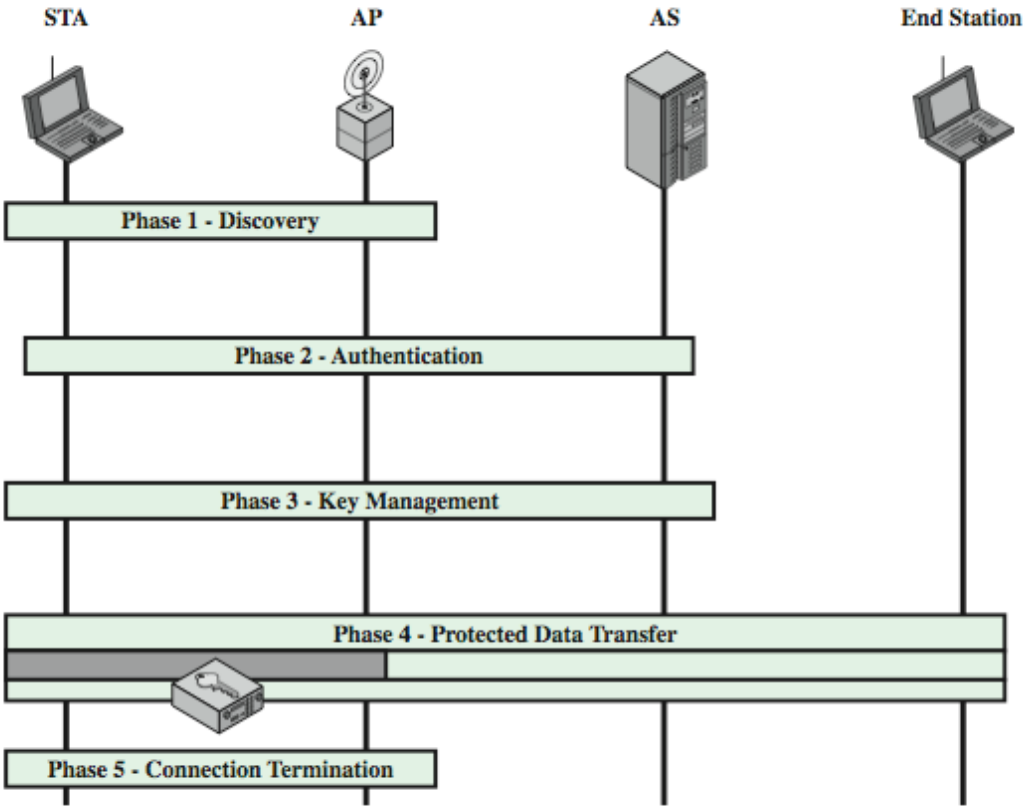
The operation of an IEEE 802.11i RSN can be broken down into five distinct phases of operation, as shown in Figure.

One new component is the authentication server (AS).

The five phase are:

• Discovery: An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.

• Authentication: During this phase, the STA and AS prove their identities to each other. The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.



• Key generation and distribution: The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only

• Protected data transfer: Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.

• Connection termination: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.

802.11i Discovery and Authentication Phases

The discovery phase consists of three exchanges: Network and security capability discovery, Open system authentication, and Association.

802.11i Key Management Phase

This exchange is known as the 4-way handshake. The STA and AP use this handshake to confirm the existence of the PMK, verify the selection of the cipher suite, and derive a fresh PTK for the following data session. For group key distribution, the AP generates a GTK and distributes it to each STA in a multicast group.

802.11i Protected Data Transfer Phase

IEEE 802.11i defines two schemes for protecting 802.11 MPDU data message integrity and confidentiality:

- Temporal Key Integrity Protocol (TKIP)
- Counter Mode-CBC MAC Protocol (CCMP).

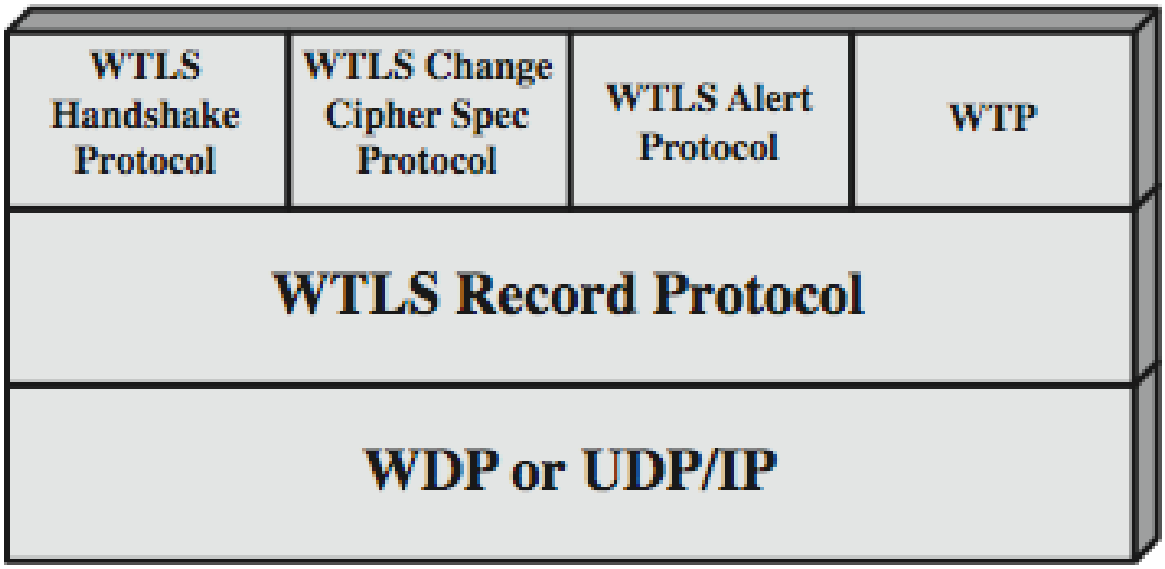
WAP (Wireless Application Protocol)

- a universal, open standard developed to provide mobile wireless users access to telephony and information services

Wireless Transport Layer Security (WTLS)

- provides security services between mobile device (client) and WAP gateway
    - provides data integrity, privacy, authentication, denial-of-service protection
- based on TLS
    - more efficient with fewer message exchanges
    - use WTLS between the client and gateway
    - use TLS between gateway and target server
- WAP gateway translates WTLS / TLS

WTLS Protocol Architecture



WTLS Record Protocol