7 : Wireless Network Security

IT6406 - Network Security and Audit

Level III - Semester 6

Overview

7.1. Wireless Security

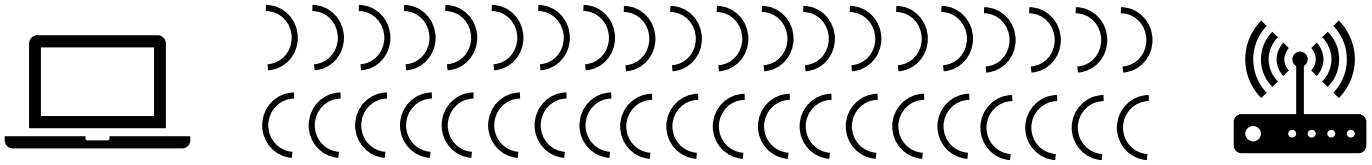
7.2. Mobile Device Security

7.3. IEEE 802.11 Wireless LAN Overview

7.4. IEEE 802.11i Wireless LAN Security

7.1. Wireless Security

- Factors contributing to the higher security risk of wireless networks compared to wired networks,
  - Channel
  - Mobility
  - Resources
  - Accessibility



Endpoint Wireless medium Access point

Read more: Ref 1: Pg. (582-584)

7.1. Wireless Security…(2)

- Wireless Network Threats
  - Accidental association
  - Malicious association
  - Ad hoc networks
  - Nontraditional networks
  - Identity theft (MAC spoofing)
  - Man-in-the middle attacks
  - Denial of service (DoS)
  - Network injection

Read more: Ref 1: Pg. (582-584)

7.1. Wireless Security…(3)

- Wireless Security Measures
  - Securing wireless transmission
    - Signal-hiding techniques
    - Encryption
  - Securing wireless access points
  - Securing wireless networks
    - Use encryption
    - Use antivirus and anti-spyware software, and a firewall
    - Allow only specific computers to access your wireless network

Read more: Ref 1: Pg. (582-584)

7.2. Mobile Device Security

- Security threats
  - Lack of physical security control
  - Use of untrusted mobile devices
  - Use of untrusted networks
  - Use of applications created by unknown parties
  - Use of untrusted content
  - Use of location service

Read more: Ref 1: Pg. (585-588)

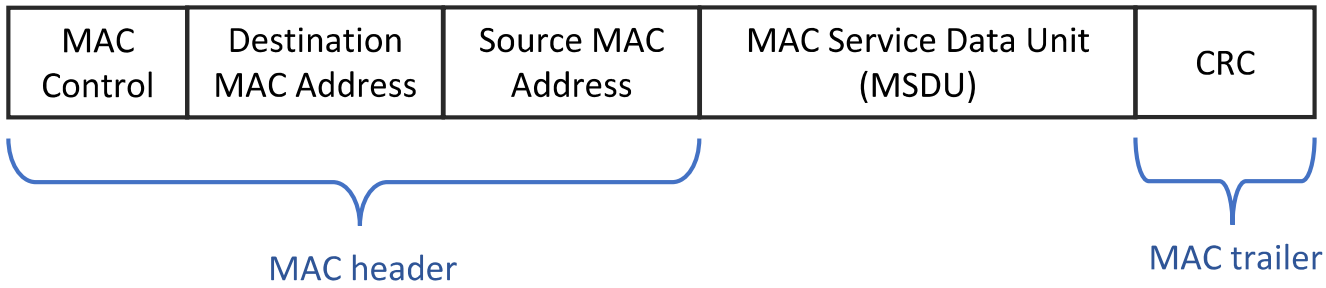
7.2. Mobile Device Security…(2)

- Mobile Device Security Strategy
  - Device security
    - Enable auto-lock
    - Enable password or PIN protection
    - Avoid using auto-complete features that remember user names or passwords.
    - Enable remote wipe
    - Keep operating system and softwares up to date
    - Either sensitive data should be prohibited from storage on the mobile device or it should be encrypted.
  - Traffic security - encryption and authentication
  - Barrier security - protect network from unauthorised access

Read more: Ref 1: Pg. (585-588)

7.3. IEEE 802.11 Wireless LAN Overview

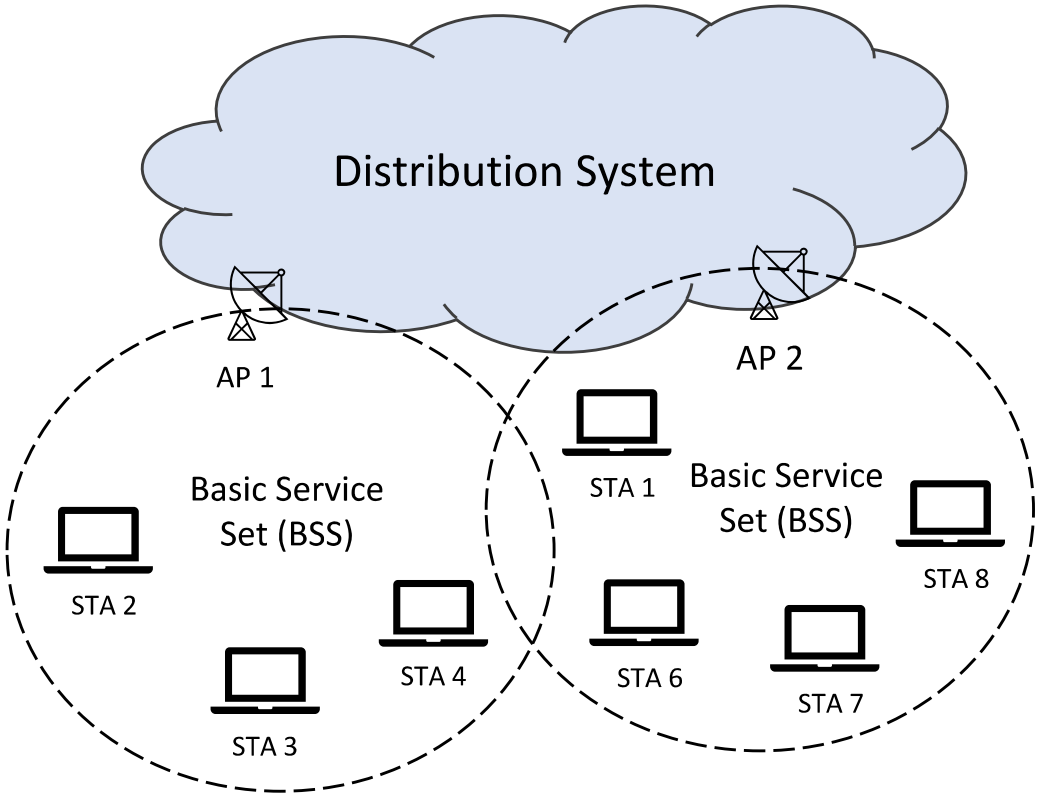
- IEEE 802 Protocol Architecture
  - Physical layer - IEEE 802.11 defines frequency bands and antenna characteristics.
  - Media access control (MAC) - MAC layer receives data from a higher-layer protocol.
    - On transmission MAC, assemble data into a frame, with address and error-detection fields.
    - On reception, disassemble frame, and perform address recognition and error detection.



Read more: Ref 1: Pg. (589-594)

7.3. IEEE 802.11 Wireless LAN Overview...(2)

- IEEE 802.11 Network Components and Architectural Model



Read more: Ref 1: Pg. (589-594)

7.3. IEEE 802.11 Wireless LAN Overview…(3)

- IEEE 802.11 Services
  - Association
  - Authentication
  - De-authentication
  - Disassociation
  - Distribution
  - Integration
  - MSDU delivery
  - Privacy
  - Re-association

Read more: Ref 1: Pg. (589-594)

7.4. IEEE 802.11i Wireless LAN Security

- Security protocols available in IEEE 802
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - Robust Security Network (RSN)

Read more: Ref 1: Pg. (595-609)

7.4. IEEE 802.11i Wireless LAN Security…(2)

- 802.11i RSN security specification defines the following services,
  - Authentication
  - Access control
  - Privacy with message integrity

Read more: Ref 1: Pg. (595-609)

7.4. IEEE 802.11i Wireless LAN Security…(3)

- IEEE 802.11i Phases of Operation
  - Discovery - access points use messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy.
  - Authentication - Wireless stations and authentication server prove their identities to each other.
  - Key generation and distribution - Wireless stations and access points negotiate cryptographic keys.
  - Protected data transfer - exchange data frames through the access point securely.
  - Connection termination - secure connection is torn down and restore to the original state.

Read more: Ref 1: Pg. (595-609)

Reference

- Ref1: Cryptography and Network Security, Principles and Practice, 7th Edition, William Stallings.