Overview

♦ Security problems with 802.11
  – Not strong access control and authentication
♦ RSN-Robust Security Network
  – Long term security for 802.11
  – Recent IEEE 802.1X for
    • Access control
    • Authentication
    • Key management
Overview (Cont)

- Two security problems:
  - Session hijacking
  - Man-in-the-middle attack

- Result:
  - Combination of 802.11 and 802.1X
    - No sufficient level of security

The IEEE 802.11 Network

- Goal:
  - Wired equivalent wireless network
    - Wired equivalent Privacy (WEP)

- Two modes:

  - **ad-hoc** (Independent Basic Service Set)
  - **Infrastructure** (Basic Service Set)

C: Client  AP: Access Point (central entity)
The IEEE 802.11 Network (Cont)

- Here only infrastructure mode security
  - Association = Wireless clients establish a relation with an Access Point (AP)
- States for complete association:
  - unauthenticated & unassociated
  - authenticated & unassociated
  - authenticated & associated
- Frames for the client transitions within the states:
  - Management frame
  - Data frame
- Authentication & access control methods
  - Open-system
  - Shared-key
  - MAC-address based access control list

The Classic 802.11 state machine

[Diagram showing the state machine with states and transitions]
802.1X Standard

♦ Provides an architectural method for authentications methods (i.e. certificate-based authentication, smartcards, one-time passwords)

♦ Provides port-based network access control for hybrid networking technologies (i.e. token ring, 802.3, 802.5 and 802.11 local area networks).

♦ Network port: an association between a station and an AP

Robust Security Network (RSN)

♦ Used by 802.1X to provide security
  – Authentication
  – Access control
  – Key management

♦ Provides mechanisms to restrict network connectivity at MAC layer to authorized entities

♦ Network connectivity through network port (association)
Robust Security Network (RSN)

- Three entities to provide security framework:
  - **Suppliant**
    - Entity desires to use a server offered by a port on **authenticator**
  - **Authenticator**(network port)
    - Switch, AP
    - Many ports for a single network which supplicant can authenticate the service
  - **Authentication server**
    - Supplicant authenticates via authenticator to authentication server
    - Central system
    - Directs authenticator to provide service after successful authentication

---

IEEE 802.1X Setup

The three different roles in IEEE 802.1X: Supplicant, Authenticator and the Authentication Server.
Extensible Authentication Protocol (EAP)

- Used by IEEE 802.1X standard
- permit a wide variety of authentication mechanisms
- challenge/response communication mechanism
- Message types
  - **EAP request**: sent to supplicant to indicate a challenge
  - **EAP Response**: supplicant reply message
  - **EAP Success**: to notify the supplicant for success
  - **EAP Failure**: to notify the supplicant for failure
EAP (Cont.)

♦ The protocol is
  – Extensible: any authentication mechanism can be encapsulated within EAP request/response messages

  – Gains flexibility by operating at a network layer rather than link layer
    • Can route messages to a centralized server rather than have each network port (AP) make the authentication decisions
      – Central service: An EAP server (RADIUS)

EAP (Cont.)

♦ Before the authentication succeeds, AP must permit EAP traffic. The models used for this:
  – Dual-port model
    • Uncontrolled port
      – Filters all network traffic
      – Allows only EAP packets to pass
      – Enables backward capability for clients incapable of supporting RSN
    • Controlled port
The EAP Over Lan (EAPOL)

♦ EAP Messages are themselves encapsulated
♦ EAPOL protocol
  – carries the packets between authenticator and supplicant
  – Provides EAP-encapsulation
  – Notifications
    • Session start
    • Session logoff
  – A key message provides a communication way to a higher layer (TLS) negotiated session key
♦ EAP & EAPOL protocol do not contain integrity and privacy protection

Remote Authentication Dial-in User Service (RADIUS)

♦ Used for the communication between authentication server and authenticator
♦ Carries EAP messages as an attribute
♦ Provides mechanism for
  – per-packet authenticity and
  – integrity verification
  between AP and RADIUS server
A complete 802.1X authentication session

![Diagram of 802.1X authentication session]

Goals of 802.11

- Access control and mutual authentication
- Flexibility
- Ubiquitous Security
- Strong Confidentiality
- Scalability
Goals of 802.1X (RSN Provides)

- Per packet authenticity & integrity between the RADIUS server and AP
- Scalability & Flexibility
- Access control
- One-way authentication

Attacks

- Man-In-Middle Attack
- Session Hijacking
Man-In-Middle Attack

- An attacker acts as an AP to supplicant and as client to the AP (authenticator)
- Absence of Mutual Authentication
- One way authentication of the supplicant to AP
- An attacker can get all network traffic from supplicant to pass through it.

Session Hijacking

- Lack of clear communication between RSN and 802.1X state machines and message authenticity. The messages are:
  - 1-2-3: Supplicant authenticates itself
  - 4: An attacker sends a 802.11 MAC disassociate management frame using AP’s MAC address that causes supplicant to get disassociated: RSN state Machine Unassociated while 802.11 state machine’s authenticator still authenticated
  - 5: Attacker gains network access using MAC address of authenticated supplicant because it’s state is still authenticated
Solutions

♦ Per-packet authenticity
  – Authenticity and integrity of EAPOL messages

♦ Peer-to-peer authentication
  – Symmetric authentication
  – Scalable Authentication