Network security: WLAN Security

Tuomas Aura, Microsoft Research, UK

Outline

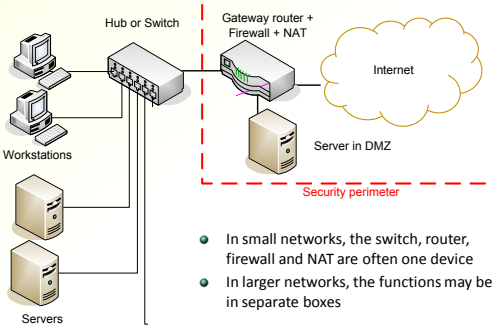
- Wireless LAN technology
- Threats against WLANs
- Weak security mechanisms and WEP
- 802.1X, WPA, 802.11i

Wireless LAN technology

Wireless LAN (WLAN) standards

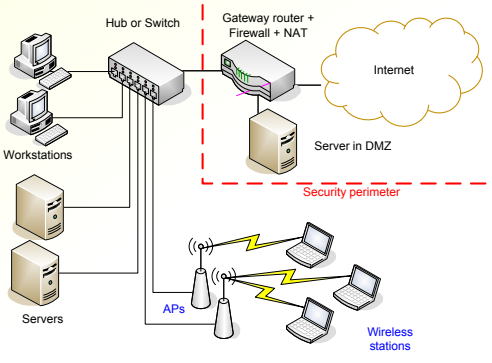
- IEEE 802.11 standard defines physical and link layers for wireless Ethernet LANs
- Wi-Fi is an industry alliance to promote 802.11 interoperability
- Original 802.11 – 1 and 2 Mbps at 2.4 GHz
  802.11b – 5.5 and 11 Mbps at 2.4 GHz
  802.11a – up to 54 Mbps at 5 GHz
  802.11g – up to 54 Mbps at 2.4 GHz
- Stations identified by 48-bit MAC addresses
  - Globally unique MAC address assigned to each NIC by the manufacturer

Small-business LAN



- In small networks, the switch, router, firewall and NAT are often one device
- In larger networks, the functions may be in separate boxes

Small-business WLAN



Wireless LAN components

- Access point (AP) = bridge between wireless (802.11) and wired (802.3) networks
- Wireless station (STA) = PC or other device with a wireless network interface card (NIC)
- Infrastructure mode = wireless stations communicate only with AP
- Ad-hoc mode = no AP; wireless stations communicate directly with each other
- We will focus on infrastructure-mode WLANs

8

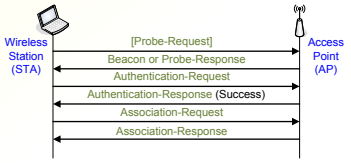
Wireless LAN structure

- Basic service set (BSS) = one WLAN cell (one AP + wireless stations)
- The basic service set is identified by the AP MAC address (BSSID)
- Extended service set (ESS) = multiple cells, APs have the same service set identifier (SSID)
- APs in the same ESS can belong to the same IP network segment, or to different ones

9

Joining a wireless LAN

- AP sends beacons, usually every 50-100 ms
- Beacons usually include the SSID but the SSID broadcast can be turned off
- STA must specify SSID to the AP in association request

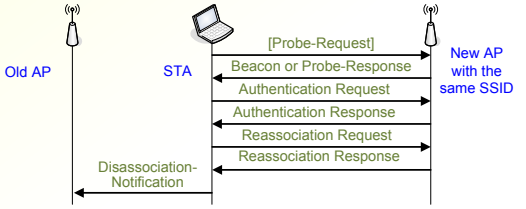


- Open System authentication = no security, empty messages

10

Wireless LAN roaming

- STA chooses AP by signal strength and quality; STA can reassociate with another AP in the ESS



- If APs are connected to same IP network segment, roaming between APs is transparent to the IP layer

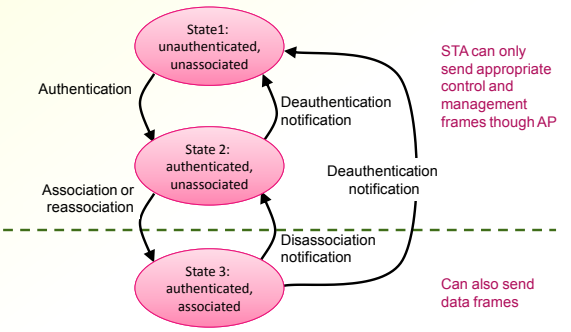
11

Leaving a wireless LAN

- Both STA and AP can send a Disassociation Notification or Deauthentication Notification

12

802.11 association state machine



13

Threats against WLANs

Exercise: WLAN threat analysis

- List as many threats against wireless LANs as you can think of. What kind of unwanted things can happen?
  - Consider home, small-business, corporate and university networks, Internet cafes and commercial hotspot operators
- Prioritize the threats roughly by how serious they are. Which threats can be ignored and which not?

15

Wireless LAN threats

- Signal interception — sniffing
- Unauthorized network access — access to intranet or Internet access without payment
- Access-point misconfiguration
- Unauthorized APs — unauthorized ingress routes may bypass firewall
- Denial of service — logical attacks with spoofed signaling, signal jamming
- AP spoofing — stronger signal attracts STAs

16

Signal interception

- The radio signal is not confined to a physical building → Attacker can sniff traffic outside the building, e.g. in the parking lot
- Directional high-gain antenna can intercept WLAN signal from hundreds of meters away

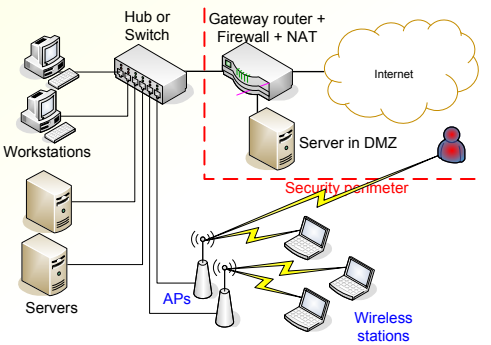
17

Unauthorized network access

- Discussion:
  - Would you mind your neighbors accessing your home AP?
  - Would a university, a company or a commercial WLAN AP operator want to control access?
- Wardriving:
  - Hobbyists drive around the city looking for open hotspots and create maps of open WLANs that can be used for Internet access
  - Tools: http://www.wardrive.net/wardriving/tools/

18

Attacker in a small-business WLAN



19

AP configuration

- Many different ways to configure access points:
  - Web page (home equipment)
  - SNMP (professional equipment)
  - serial cable
  - Telnet
- Default passwords — hackers can change the configuration or replace firmware
- Hub broadcasts — AP connected to a hub leaks wired-to-wired traffic

20

Unauthorized access points

- Unauthorized access points installed by employees are often badly administered:
  - No access control enabled; anyone can connect
  - Direct access to the intranet behind firewall

→ Attacker can use unauthorized APs as an ingress route

- Solutions:
  - Sweeps: walk or drive around premises and look for AP beacons — now a standard corporate practice
  - Scan for AP SNMP and web interfaces
- Similar to unauthorized modems

21

Denial of service

- Logical attacks:
  - Spoofed deauthentication or disassociation message causes the AP or STA to lose state
- AP capacity exhaustion:
  - Typical AP handles data fast but association and authentication slower → flood AP with false authentications to prevent honest nodes from associating
- Radio jamming:
  - Either jam the who radio channel or selectively break some frames

22

AP spoofing

- Clients are configured to associate automatically with APs that advertise specific SSIDs
- Attack: fake AP broadcasts cyclically all known hotspot, hotel, airport and big-company SSIDs

  → clients will associate with it automatically thinking they are at the hotspot
  → easy MitM attack on all IP packets

23

WLAN security goals

- Wireless LAN security protocols have following goals:
  - Data confidentiality and integrity — prevent sniffing and spoofing of data on the wireless link
  - Access control — allow access only for authorized wireless stations
  - Accounting — hotspot operators may want to meter network usage
  - Authentication — access control and accounting usually depend on knowing the identity of the wireless station or user
  - Availability — do not make denial-of-service attacks easy (radio jamming is always possible)
- Not all problems have been solved

24

Weak security mechanisms and WEP

Discussion: common recommendations

- The following security measures are often recommended to WLAN administrators:
  - Disable the SSID broadcast
  - Maintain a list of authorized MAC addresses and block unauthorized ones from the network
  - Select AP locations in the middle of the building (not close to windows), use directional antennas and line walls and windows with metal foil to minimize the signal leakage to the outside of the building
- How much security do these measures bring?
- How expensive are they?

26

Weak WLAN security mechanisms

- Disabling the SSID broadcast — attacker can sniff the SSID when other clients associate
- ACL of authorized MAC addresses — attacker can sniff and spoof another client's MAC address
- AP locations, directional antennas and metal foil to keep signal inside a building — attacker can use a directional antenna with high gain

→ Weak mechanisms are rarely worth the trouble

27

WEP encryption

- WEP = Wired Equivalent Privacy; goal was security equivalent to a wired LAN
- Encryption and integrity check for data frames; management frames unprotected
- RC4 stream cipher with a static 40-bit pre-shared key and 24-bit initialization vector (128-bit WAP = 104-bit key + 24-bit IV)
- Integrity check value (ICV) = CRC checksum encrypted with RC4
- Multiple cryptographic weaknesses make WEP vulnerable to serious attacks

28

WEP keys

- WEP keys are configured manually; no other mechanism specified in 802.11
- STA can store 4 keys simultaneously; every frame header contains a 2-bit key id
- AP and all stations may share the same key, or AP may have a different key for each client STA (per-station keys)
  - No effect on client STA implementation
  - AP implementation much more complex with per-station keys → rarely implemented before WPA

32

WEP security weaknesses

- 40-bit keys → brute-force cracking
- Static keys → cannot change keys often
- 24-bit IV → IV reuse; dictionary attack; all IV values exhausted in 5 hours or less on a busy AP
- IV generation not specified → reuse possible even earlier
- CRC+RC4 for ICV → possible to modify data
- No protection for management frames → disassociation and deauthentication attacks
- Authentication not bound to the session → man-in-the-middle and replay attacks
- Authentication based on RC4 → attacker learns key stream and can spoof responses
- Weak IV attacker against RC4 → cracking of 104-bit WEP keys

34

Need for Link-Layer Security?

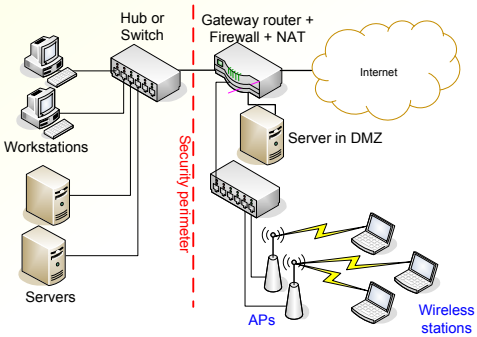
- WEP and 802.11i/WPA provide link-layer security only; not end-to-end protection

  → Good for corporate APs

  → Irrelevant for road warriors at wireless hotspots and other untrusted networks
- Alternative: treat WLAN as insecure and use end-to-end security, such as IPSec or VPN

36

Alternative Architecture



37

Need for WLAN Access Control?

- Arguments for controlling access:
  - Open WLAN allows hackers to access the corporate or home LAN; firewall protection bypassed; "like having an Ethernet socket in the parking lot"
  - Unauthorized users consume network resources without paying
  - Contract with ISP may not allow open APs
  - Liability issues if the unauthorized users send spam or access illegal content
- Arguments for open access:
  - Good service for customers and visitors
  - End-to-end security needed anyway
  - Little lost by giving away excess bandwidth; authorized users can be given better QoS
- New access points and virtual LANs (VLAN) allow combination of the two on the same equipment

38

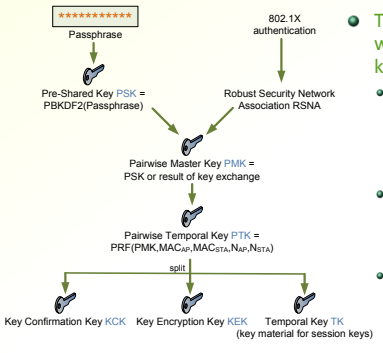
802.1x, WPA, 802.11i

Real WLAN security mechanisms

- 802.11i robust security network (RSN)
  - IEEE standard; Wi-Fi alliance name WPA2
  - 802.1X for access control
  - EAP-TLS authentication and key exchange
  - New confidentiality and integrity protocols TKIP and AES-CCMP
  - Requires new hardware for AES
- Wireless Protected Access (WPA)
  - Defined by Wi-Fi alliance; available before the standard
  - 802.1X; EAP-TLS
  - Supports only TKIP, RC4 with frequently changing keys and other enhancements
  - Firmware update to AP or NIC often sufficient

40

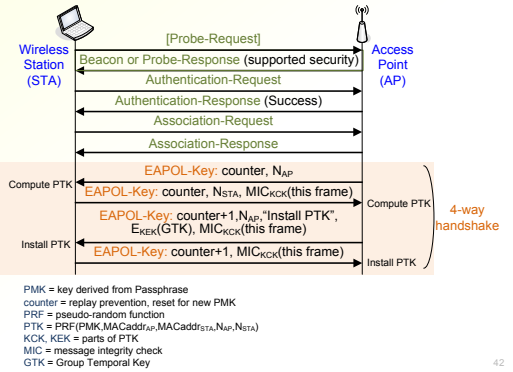
802.11i key hierarchy



- Two alternative ways of obtaining keys:
  - Preshared key (PSK) authentication= WPA2-PSK = WPA2-Personal
  - 802.1x authentication= WPA2-EAP = WPA2-Enterprise
  - Difference to WPA-* only in details and algorithms

41

WPA2-PSK and 4-way handshake



PMK = key derived from Passphrase
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,MACaddr$_{AP}$,MACaddr$_{STA}$,N$_{AP}$,N$_{STA}$)
KCK, KEK = parts of PTK
MIC = message integrity check
GTK = Group Temporal Key

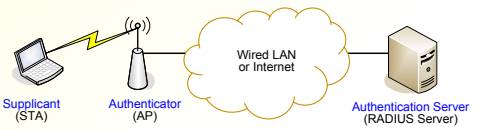
42

IEEE 802.1X

- Port-based access control — originally intended for enabling and disabling physical ports on switches and modem banks
- Conceptual controlled port at AP
- Uses Extensible Authentication Protocol (EAP) to support many authentication methods; usually EAP-TLS
- Starting to be used in Ethernet switches, as well

43

802.11/802.1X architecture



- Supplicant (STA) wants to access the wired network via the AP
- Authentication Server (RADIUS server) authenticates the supplicant
- Authenticator (AP) enables network access for the supplicant after successful authentication

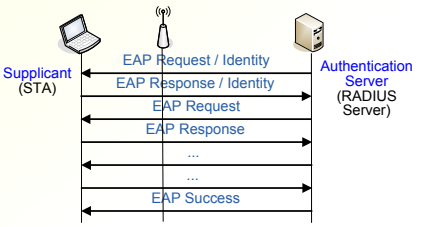
44

EAP

- Extensible authentication protocol (EAP) defines generic authentication message formats: Request, Response, Success, Failure
- Originally designed for authenticating dial-up users with multiple methods
- Security is provided by the authentication protocol carried by EAP, not by EAP itself
- EAP supports many authentication protocols: EAP-TLS, LEAP, PEAP, EAP-SIM, ...
- Used in 802.1x between supplicant (STA) and authentication server

45

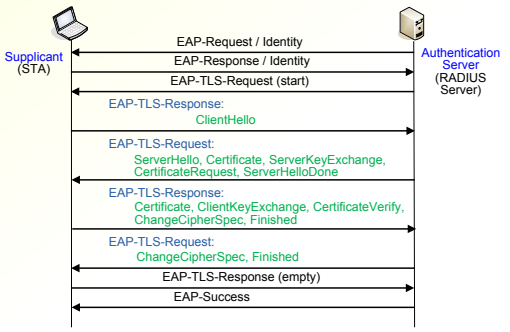
EAP protocol



- Request-response pairs
- User identified by network access identifier (NAI): username@realm

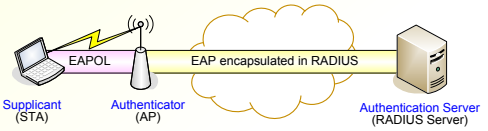
46

EAP-TLS Protocol



47

EAP encapsulation in EAPOL and RADIUS



- On the wire network, EAP is encapsulated in RADIUS attributes
- On the 802.11 link, EAP is encapsulated in EAP over LAN (EAPOL)
- AP is a pass-through device: it copies EAP messages without reading them

48

RADIUS

- Remote access dial-in user service (RADIUS)
  - Originally for centralized authentication of dial-in users in distributed modem pools
- Defines messages between the network access server (NAS) and authentication server:
  - NAS sends Access-Request
  - Authentication server responds with Access-Challenge, Access-Accept or Access-Reject
- In WLAN, AP is the NAS
- EAP is encapsulated in RADIUS Access-Request and Access-Challenge; as many rounds as necessary

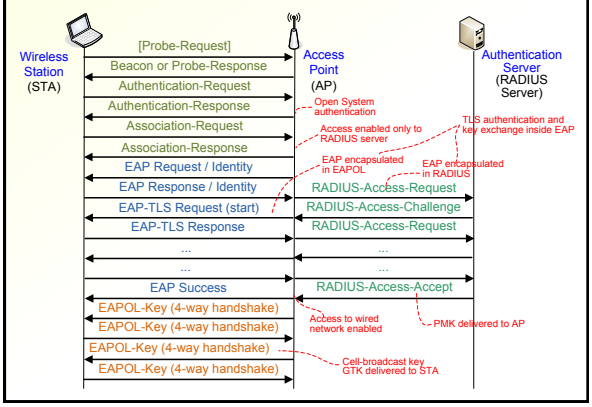
49

RADIUS security

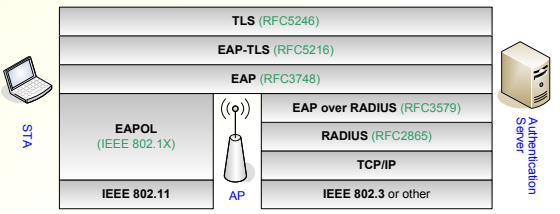
- AP and authentication server share a secret
- Responses from authentication server contain an authenticator; requests from AP are not authenticated
- Authenticator = MD5 hash of the message, AP's nonce and the shared secret
- Per-station key material is sent to the AP encrypted with the shared secret
- Radius uses a non-standard encryption algorithms but no problems found so far (rare!)

50

EAP protocol in context



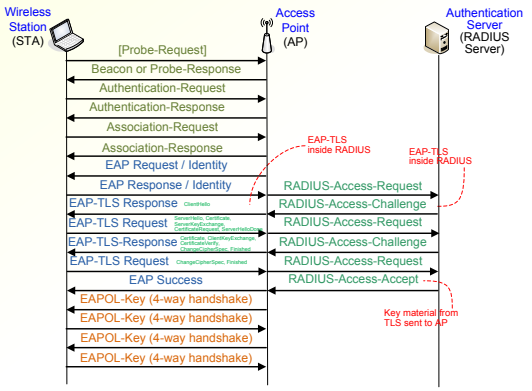
802.1X protocol stack



- Excessive layering?

52

Full WPA/802.11i Authentication



Authentication Latency

- Minimum 7–8 round trips between AP and STA
  - 7 roundtrips when TLS session reused (cf. 4 with PSK)
  - Probe-Request / Probe-Response alternative to Beacon → 1 more round trip, actually may be faster
  - Messages with many long certificates may need to be fragmented → more round trips
- 3–4 round trips between AP and authentication server
  - 3 roundtrips when TLS session reused
- Typical authentication latency >1 second every time STA roams between APs
- Preauthentication and other handover optimizations

54

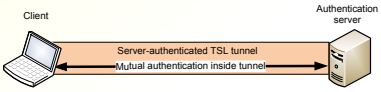
LEAP, PEAP, EAP-TTLS

- Idea: authenticate the server with TLS, then the client inside the encrypted tunnel
- Lightweight Extensible Authentication Protocol (LEAP) by Cisco — insecure and no longer used
- Protected EAP (PEAP) by Microsoft
  - Round 1: EAP-TLS with server-only authentication
  - Do not send EAP-Success; instead, start encryption and move to round 2
  - Round 2: any EAP authentication method (e.g. MSCHAPv2) with mutual authentication
- Inner authentication could be any EAP method. In practice, WPA stations support EAP-PEAP-MSCHAPv2
- Password authentication inside encrypted tunnel
- EAP-Success message is also authenticated
- Some identity protection:
  - PEAP encrypts the EAP-Request-Identity message
    → user identity in round 2 is hidden
  - Client may send machine identity in round 1
- Another similar proposal: EAP-TTLS

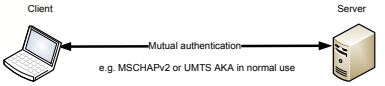
55

Tunnelled authentication problem (1)

- PEAP and EAP-TTLS clients authenticate the server with TLS
- Server authenticates the client inside the TLS tunnel with MSCHAPv2, TLS, UMTS AKA, or any other protocol — authentication may be mutual



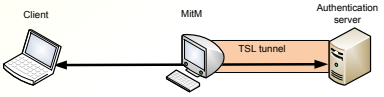
- Session key is provided by the TLS tunnel — session keys from the inner authentication are not used
- BUT… the same inner authentication methods are used also without TLS tunnelling



56

Tunnelled authentication problem (2)

- Attacker can pretend to be a server in the no-tunnel version and forward his authentication inside a tunnel [Asokan, Niemi, Nyberg 2003]
- Easy for UMTS AKA — attacker can pretend to be a 3G base station
- More difficult for MSCHAPv2 — attacker needs to be a server on the intranet to which the client connects



57

WPA/RSN key Hierarchy

- WPA and RSN define a complex key hierarchy
- Pairwise keys between AP and STA:
  - Pairwise master key (PMK)
  - 4 temporal keys derived from PMK
    → data encryption and integrity keys
    → EAPOL-Key encryption and integrity keys
- 4-message protocol of EAPOL-Key messages is used to refresh temporal keys from PMK, nonces and MAC addresses
- Group keys for group and broadcast communication

58

TKIP

- Temporal Key Integrity Protocol (TKIP) can be implemented with pre-WPA2 hardware and a firmware update
- Still RC4 but WEP vulnerabilities fixed:
  - New message integrity algorithm — Michael
  - New encryption key for each frame
  - 48-bit IV constructed to avoid RC4 weak keys
  - IV used as sequence counter to prevent replays
- Recent attacks against WPA!
- Key hierarchy → pairwise keys

59

AES-CCMP

- AES Counter Mode-CBC MAC Protocol is used for encryption and integrity in 802.11i/RSN
- Advanced Encryption Standard (AES)
- CCM = Counter Mode + CBC MAC
  → AES counter mode encryption
  → CBC MAC for integrity protection
- Key hierarchy → pairwise keys
- Requires new hardware

60

Exercises

- How could the network attachment and access control protocols be optimized to reduce latency?
- Is WLAN security alternative or complementary to end-to-end security such as TLS?
- Explain how each of the security weaknesses in WEP arises from the protocol and algorithm details

62