Network Security: WLAN Security

Tuomas Aura
T-110.5240 Network security
Aalto University, Nov-Dec 2010
Outline

- Wireless LAN technology
- Threats against WLANs
- Weak security mechanisms and WEP
  - 802.1X, WPA, 802.11i, WPA2
- WLAN mobility
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 802.11-1997, 802.11-2007, 802.11n
- Stations identified by **48-bit MAC addresses**
  - Globally unique MAC address assigned to each NIC by the manufacturer
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

- Workstations
- Servers
- Hub or Switch
- Gateway router + Firewall + NAT
- Internet
- Server in DMZ
- Security perimeter
- APs
- Wireless stations
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
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
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 authentication, empty messages
Leaving a wireless LAN

Both STA and AP can send a Disassociation Notification or Deauthentication Notification.
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?
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
WLAN security goals

Wireless LAN security protocols have the 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
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?
In original 802.11-1997 standard, no longer is use

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 attacks; now gives no security
802.11 shared-key authentication

- Alternative to open-system authentication in 802.11-1997, never really used
- AP authenticates STA: STA encrypts a challenge with the WEP algorithm and preshared key

Unidirectional entity authentication only; no connection to message authentication

AP may require WEP encryption and authentication or only one of them
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
Need for Link-Layer Security?

Wireless LAN security protocols provide link-layer security only; not end-to-end protection
→ Good for corporate APs: access control to LAN
→ Good for commercial WLAN operators: access control for paying customers
→ Irrelevant for road warriors at wireless hotspots and at other untrusted networks

Alternative: treat WLAN as insecure and use end-to-end security, such as IPSec or VPN
e.g. Aalto vs. Aalto Open
Alternative Architecture

- Workstations
- Gateway router + Firewall + NAT
- Hub or Switch
- Wireless stations
- Servers
- Server in DMZ
- APs
- Security perimeter
- Internet
- Wireless stations
802.1X, WPA, WPA2
Real WLAN security mechanisms

Wireless Protected Access 2 (WPA2)
- WPA2 is the Wi-Fi alliance name for the 802.11i amendment to the IEEE standard, now part of 802.11-2007
- 802.11i defines robust security network (RSN)
- 802.1X for access control
- EAP authentication and key exchange, eg. EAP-TLS
- 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 11i standard
- 802.1X; EAP-TLS
- Supports only TKIP encryption = RC4 with frequently changing keys and other enhancements
- Firmware update to older AP or NIC often sufficient
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
- WPA-* differs from WPA2-* only in minor details and algorithms
**WPA2-PSK and 4-way handshake**

<table>
<thead>
<tr>
<th>Wireless Station (STA)</th>
<th>Access Point (AP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Probe-Request]</td>
<td>Beacon or Probe-Response (supported security)</td>
</tr>
<tr>
<td>Authentication-Request</td>
<td>Authentication-Response (Success)</td>
</tr>
<tr>
<td>Association-Response</td>
<td>Association-Request</td>
</tr>
<tr>
<td>Association-Request</td>
<td>Association-Response</td>
</tr>
</tbody>
</table>

- **EAPOL-Key**: counter, $N_{AP}$
- **EAPOL-Key**: counter, $N_{STA}$, $MIC_{KCK}(\text{this frame})$
- **EAPOL-Key**: counter+1,$N_{AP}$, “Install PTK”, $E_{KEK}(\text{GTK})$, $MIC_{KCK}(\text{this frame})$
- **EAPOL-Key**: counter+1, $MIC_{KCK}(\text{this frame})$

**4-way handshake**

- **PMK**: key derived from Passphrase
- **counter**: replay prevention, reset for new PMK
- **PRF**: pseudo-random function
- **PTK**: $PRF(\text{PMK, MACaddr}_{AP}, \text{MACaddr}_{STA}, N_{AP}, N_{STA})$
- **KCK, KEK**: parts of PTK
- **MIC**: message integrity check, a MAC
- **GTK**: Group Temporal Key
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
Suppliant wants to access the wired network via the AP  
Authentication Server (AS) authenticates the supplicant  
Authenticator enables network access for the supplicant after successful authentication
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 and authentication server
- EAP term for supplicant is peer, reflecting the original idea that EAP could be used for mutual authentication between equal entities
Request-response pairs

User identified by network access identifier (NAI): username@realm

Allows multiple rounds of request–response, e.g. for mistyped passwords
EAP-TLS Protocol

Peer

EAP-Request / Identity

EAP-Response / Identity

EAP-TLS-Request (start)

EAP-TLS-Response:
ClientHello

EAP-TLS-Request:
ServerHello, Certificate, ServerKeyExchange, CertificateRequest, ServerHelloDone

EAP-TLS-Response:
Certificate, ClientKeyExchange, CertificateVerify, ChangeCipherSpec, Finished

EAP-TLS-Request:
ChangeCipherSpec, Finished

EAP-TLS-Response (empty)

EAP-Success

EAP Server
On the wire network, EAP is encapsulated in RADIUS attributes.

On the 802.11 link, EAP is encapsulated in EAP over LAN (EAPOL).

In 802.1X, AP is a pass-through device: it copies (most) EAP messages without reading them.
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
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 (surprising!)
**EAP protocol in context**

Wireless Station (STA)

[Probe-Request]
- Beacon or Probe-Response
- Authentication-Request
- Authentication-Response
- Association-Request
- Association-Response
- EAP Request / Identity
- EAP Response / Identity
- EAP-TLS Request (start)
- EAP-TLS Response
- ...
- ...
- EAP Success
  - EAPOL-Key (4-way handshake)
  - EAPOL-Key (4-way handshake)
  - EAPOL-Key (4-way handshake)
  - EAPOL-Key (4-way handshake)

Access Point (AP)

- Access enabled only to RADIUS server
- Open System authentication
- EAP encapsulated in EAPOL
- EAP encapsulated in RADIUS
- RADIUS-Access-Request
- RADIUS-Access-Challenge
- RADIUS-Access-Request
- ...
- ...
- RADIUS-Access-Accept

Authentication Server (RADIUS Server)

- TLS mutual authentication and key exchange inside EAP
- PMK delivered to AP
- Temporal keys created from PMK, cell-broadcast key GTK delivered to STA
- Access to wired network enabled
### 802.1X Protocol Stack

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
<th>RFC/Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IEEE 802.11</strong></td>
<td>STA (Station)</td>
<td></td>
</tr>
<tr>
<td><strong>IEEE 802.11</strong></td>
<td>AP (Access Point)</td>
<td></td>
</tr>
<tr>
<td><strong>IEEE 802.3 or other</strong></td>
<td>Authentication Server</td>
<td></td>
</tr>
<tr>
<td><strong>EAPOL</strong> (IEEE 802.1X)</td>
<td>EAP (Extensible Authentication Protocol)</td>
<td>RFC3748, 5248</td>
</tr>
<tr>
<td><strong>EAP over RADIUS</strong></td>
<td>EAP over RADIUS</td>
<td>RFC3579</td>
</tr>
<tr>
<td><strong>RADIUS</strong> (RFC2865)</td>
<td>TCP/IP</td>
<td></td>
</tr>
<tr>
<td><strong>TLS</strong> (RFC5246)</td>
<td>EAP-TLS (Extensible Authentication Protocol over TLS)</td>
<td>RFC5216</td>
</tr>
<tr>
<td><strong>EAP-TLS</strong> (RFC5216)</td>
<td>EAP-TLS (Extensible Authentication Protocol over TLS)</td>
<td>RFC5216</td>
</tr>
<tr>
<td><strong>EAP</strong> (RFC3748, 5248)</td>
<td>EAP-TLS (Extensible Authentication Protocol over TLS)</td>
<td>RFC5216</td>
</tr>
</tbody>
</table>

**Excessive layering?**
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Type</th>
<th>Role</th>
<th>Role Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS</td>
<td>Client</td>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>EAP/AAA</td>
<td>Peer</td>
<td>Authenticator</td>
<td>EAP server / Backend authentication server</td>
</tr>
<tr>
<td></td>
<td>Suppliant</td>
<td>Authenticator</td>
<td>Authentication server (AS)</td>
</tr>
<tr>
<td>802.1X</td>
<td>Network access server (NAS)</td>
<td>RADIUS server</td>
<td></td>
</tr>
<tr>
<td>802.11</td>
<td>STA</td>
<td>Access point (AP)</td>
<td></td>
</tr>
</tbody>
</table>
Full WPA/802.11i Authentication

- [Probe-Request]
  - Beacon or Probe-Response
  - Authentication-Request
  - Authentication-Response
  - Association-Request
  - Association-Response
  - EAP Request / Identity
  - EAP Response / Identity
  - EAP-TLS Request (start)
  - EAP-TLS Response
  - EAP-TLS Request
  - EAP-TLS-Response
  - EAP-TLS Request
  - EAP-TLS-Response (empty)
  - EAP Success
  - EAPOL-Key (4-way handshake)
  - EAPOL-Key (4-way handshake)
  - EAPOL-Key (4-way handshake)
  - EAPOL-Key (4-way handshake)

- Access Point (AP)

- Authentication Server (RADIUS Server)

- EAP-TLS inside RADIUS

- Key material from TLS sent to AP
Authentication Latency

- 7-8 round trips between AP and STA for EAP-TLS
  - 7 roundtrips when TLS session reused (cf. 4 with PSK)
  - Probe-Request / Probe-Response alternative to Beacon → 1 more round trip
  - 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 → we need optimizations
Session protocol: AES-CCMP

- AES Counter Mode-CBC MAC Protocol is used for encryption and integrity in 802.11i/RSN
- Advanced Encryption Standard (AES)
- CCMP = Counter Mode + CBC MAC
  → AES counter mode encryption
  → CBC MAC for integrity protection
- Requires new hardware
Session protocol: 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 cryptographic attacks against TKIP! Time to start using only WPA2.
WPA/802.11i security - goals and reality

- Authentication and access control prevents unauthorized network access
- Mutual authentication prevents association with rogue access points
- CCMP encryption prevents data interception on wireless link
- Strong integrity check prevents data spoofing on wireless link
- Deauthentication and disassociation attacks still possible
  - Difficult to fix because of the layering
Link-layer mobility in WLAN
Wireless LAN roaming

Moving between APs is slow
- Many roundtrips to a remote authentication server
- Many messages between STA and AP, channel acquisition time for each message can be long on a busy WLAN
- Complex protocol layering leads to unnecessary messages

How to speed up the handover?
PMK caching

- AP and STA may cache previous pair-wise master keys (PMK) and reuse them if the same client returns to the same AP.

- Only a 4-way handshake between STA and AP needed after (re)association to create new session keys from the PMK.

- Key identifiers to identify PMK.

- STA may send a list of key identifiers in (re)association request; AP selects one in Message 1 of the 4-way handshake.

- Standardized in 802.11i, now in 802.11-2007/WPA2.
Wireless switch

- Proprietary roaming solution from equipment manufacturers
- Moving parts of the authenticator to a switch
- Client STA assumes AP has cached PMK even if it has never authenticated to that AP
  - called “opportunistic PMK caching”
- Switch pushes PMK to all APs, or AP pulls key on demand
802.1X preauthentication

1. Association & open port at AP
2. Scan for potential new APs
3. Preauthentication over the LAN with the other APs

Current AP

Potential next AP

Intranet

Authentication server

EAP over RADIUS

Distribution system, usually a switched wire LAN

STA
Even local handoffs require connection to the AS, which may be far away.
Amendment 802.11r adds mechanisms for fast handover

- With PSK or cached MSK, piggyback the 4-way handshake on 802.11 authentication and association messages → only 2 roundtrips between STA and AP
- **Mobility domain** = group of APs close to each other + local “server” that helps in local handoffs
- AP advertises capability for fast BSS transition, and a mobility domain identifier
- **Key hierarchy** within the mobility domain: local server (R0KH) holds first-level key (PMK-R0), which is used to derive second-level keys (PMK-R1) for APs (R1KH) in the same domain → avoid contacting a remote authentication server
- In practice:
  - R0KH = wireless switch, R1KH = AP
- Also, prerereservation of resources for QoS (see 802.11e) done in parallel with the 4-way handshake
802.11r key hierarchy

**Passphrase**

- **Pre-Shared Key PSK** = PBKDF2(Passphrase)

**Master Session Key MSK**

- **Pairwise Master Key, first level PMK-R0** = R0-Key-Data = KDF(PSK/MSK, "FT-R0", SSID, MDID, R0KH-ID, MAC\textsubscript{STA})

- **Pairwise Master Key, second level PMK-R1** = PMK-R1 = KDF(PMK-R0, “FT-R1”, BSSID, MAC\textsubscript{STA})

**Pairwise Temporal Key PTK** = PTK = KDF(PMK-R1, "FT-PTK", N\textsubscript{STA}, N\textsubscript{AP}, BSSID, MAC\textsubscript{STA})

- **Key Confirmation Key KCK**
- **Key Encryption Key KEK**
- **Temporal Key TK** (key material for session keys)

- **802.1X authentication**

**PMK-R0** = key shared by STA and the mobility domain (wireless switch); derived from PSK or EAP MSK

**PMK-R1** = key shared by STA and AP; derived locally from PMK-R0

AP only knows PMK-R1, STA knows PMK-R0 and can compute PMK-R1 for each new AP
Handoff within a mobility domain is supported by the local R0KH EAP with AS only when moving between mobility domains. 802.11r specifies the key hierarchy and communication between STA and AP; the protocol between APs and the R0KH is not standardized.
Password authentication for WLAN
Universal access method (UAM)

- Web-based authentication
- Used mostly in wireless hotspots for credit-card payment or for password-based access
- Redirect new users to authentication web page when they open a web browser

Methods of redirection:
- Spoofed HTTP redirection
- DNS spoofing
- Redirection of IP packets at switch

Authenticated users’ MAC addresses added to a whitelist
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
    \[ \rightarrow \text{ user identity in round 2 is hidden} \]
  - Client may send machine identity in round 1

Another similar proposal: EAP-TTLS
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

![Diagram showing client and server with mutual authentication inside a TLS tunnel]

- 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

![Diagram showing client and server with mutual authentication without a TLS tunnel, e.g. MSCHAPv2 or UMTS AKA in normal use]
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
Exercises

- Why is WPA-Enterprise not widely used in home wireless networks, wireless hotspots or Internet cafes?
- Why are password-based methods needed for authorizing WLAN access?
- UAM has to intercept the first web page that user tries to access. What problems can the different methods for doing this cause?
- If a cellular network operator wants to offer wireless hotspot access to its customers, how could the SIM card be used for authorizing WLAN access from the phones?

- How could the network attachment and access control protocols be further optimized to reduce latency? Which standards bodies would need to be involved?
- Is WLAN security alternative or complementary to end-to-end security such as TLS?