Advanced Network Security

WiFi security

Joeri de Ruiter
Agenda

- WiFi security
- WPA(2)
  - Personal
  - Enterprise
- WPA3
- Key reinstallation attacks
WiFi

• IEEE 802.11 standard
• Some terminology:
  • Station (STA) is a device with WiFi capability
  • Access Point (AP) is a station that other stations can connect to to get access to a network, also referred to as authenticator
  • Supplicant, used to indicate the client when authenticating
  • SSID (Service Set Identifier) is the name of the network
  • MIC: Message Integrity Check
    – Prevents confusion with MAC (Media Access Control) addresses
WiFi security

• Open networks
• Wireless Equivalent Privacy (WEP)
• WiFi Protected Access (WPA)
  • Personal
  • Enterprise
• Hidden networks and MAC address whitelists
  • Does not provide real security
WiFi security

- WPA, 7.37%
- WEP, 2.66%
- OPEN, 21.96%
- WPA2, 68.02%

© 2016 Kaspersky Lab. All Rights Reserved.
Open network security

• No encryption on the traffic
  • Also used for public hotspots with captive portal
  • Possible for an attacker to eavesdrop on all network traffic
• Typically anyone can connect to the network
  • Possible to filter based on MAC address, but can easily be spoofed
• Evil twin attacks: a malicious access point pretend to be a preferred network of the user
  • User will connect to the attacker’s network, putting the attacker in a man-in-the-middle position
• KARMA: special case of the evil twin attack
  • Observe probe requests by clients and pretend to be that network
WEP security

- Cryptographic algorithm based on RC4 used to protect data traffic
- Broken since a long time
- Easy to crack and about as good as an open network
- Stop using it!
WPA(2) security

• Data confidentiality algorithms
  • Temporary Key Integrity Protocol (TKIP)
    - Uses same hardware as WEP
    - Also included in WPA2 for backwards compatibility
  • Counter Mode with CBC-MAC Protocol (CCMP)
    - Based on AES

• Authentication methods
  • Pre-shared key (PSK)
  • IEEE 802.1x authentication
    - Uses Extensible Authentication Protocol (EAP)

<table>
<thead>
<tr>
<th></th>
<th>Encryption</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA Personal</td>
<td>TKIP</td>
<td>PSK</td>
</tr>
<tr>
<td>WPA Enterprise</td>
<td>TKIP</td>
<td>802.1x</td>
</tr>
<tr>
<td>WPA2 Personal</td>
<td>CCMP</td>
<td>PSK</td>
</tr>
<tr>
<td>WPA2 Enterprise</td>
<td>CCMP</td>
<td>802.1x</td>
</tr>
</tbody>
</table>
TKIP security

- Deprecated in the IEEE 802.11 standard
- Based on the RC4 stream cipher
  - Known to have biases that can be exploited to break it
- Possible to inject and decrypt packets
  - Only takes about an hour to perform the attack
  - Relies on the generation of identical packets

---

1 All Your Biases Belong To Us: Breaking RC4 in WPA-TKIP and TLS by Mathy Vanhoef and Frank Piessens, Usenix Security 2015
Key hierarchy

- Pairwise master key (PMK): secret key shared between the client and access point
  - Pairwise transient key (PTK): a concatenation of the following session keys
    - Key Confirmation Key (KCK): used for message authentication in 4-way handshake
    - Key Encryption Key (KEK): used for encryption of keys
    - Temporal Key (TK): key used for confidentiality and integrity of the data
- Group master key (GMK): optional key used to derive GTK
- Group temporal key (GTK): key shared between all connected clients and the access point
  - Used for broadcast and multicast traffic
WiFi connection phases

- **Discovery**
  - Find nearby networks
  - Networks announce capabilities
- **Authentication**
  - Typically “Open”
- **(Re)Association**
  - Agreement on security algorithms
- **Optional: 802.1x authentication**
- **Optional: 4-way handshake**
- **Data exchange**

![Diagram of WiFi connection phases]

- Probe request
  - Probe response (security parameters)
  - Authentication request
  - Authentication response
  - Association request (security parameters)
  - Association response
  - 802.1x authentication
  - 4-way handshake
  - Data
4-way handshake

- Based on a shared secret PMK
  - Can be the pre-shared key or the output of the 802.1x authentication
- Mutual authentication of user and access point
  - Verify whether both know PMK
- Also used for negotiation of fresh keys
- Negotiation of Pairwise Transient Key (PTK)
  - If a MIC (Message Integrity Code) is included, it is computed using the Key Confirmation Key (KCK)
  - If a key is included, it is encrypted using the Key Encryption Key (KEK)
4-way handshake (simplified)

Supplicant

ANonce

Derive PTK

SNonce, MIC

Install PTK and GTK

ANonce, MIC, Enc_{KEK}(GTK)

Install PTK

MIC

Encrypted data frames

Authenticator
Key derivation

- PRF (pseudo-random function) is typically a SHA-based HMAC
- PTK is split into the KCK, the KEK and the TK
WPA(2) Personal

- Uses pre-shared key (PSK) for authentication
  - Can be derived from an ASCII password using a key derivation function (KDF):
    \[ PSK = KDF(password, SSID) \]
- “Open” method used in the authentication phase
  - Actual authentication takes place in the 4-way handshake
- PSK used directly as PMK in the 4-way handshake
WPA(2) Personal – Key derivation

Key derivation for authentication based on password
WPA(2) Personal - Attacks

- Which information is available to a passive attacker that observes a successful connection including the 4-way handshake?
  - SSID, MAC addresses, nonces
- Enough information to perform offline brute-force attacks
  - For example, dictionary attacks or rainbow table attacks
  - What is the problem with rainbow tables?
- What can an attacker do once the PSK is known?
  - Connect to the network
  - Eavesdrop on other users
    - If 4-way handshake is observed, which might be possible to force by sending a deauthentication message to the client and access point
- Often WPA password is shared, for example, in coffee bars or restaurants...
WPA(2) Enterprise

- Not always convenient (or secure) to share one key/password with all users
- Re-use existing credentials
  - Usernames and passwords
  - Certificates
- Authentication using IEEE 802.1x
- For example, used in eduroam
IEEE 802.1x

- Extensible Authentication Protocol (EAP) over LAN (EAPOL)
- Actual authentication done by authentication server
  - Typically a RADIUS server (Remote Authentication Dial-In User Service)
  - Anonymous identity used to select RADIUS server
- Common EAP methods used
  - TLS
  - PEAP
  - TTLS
- Key provided by the authentication server to the client and access point
EAP: TLS

- Mutual authentication between user and authentication server via TLS using certificates
- Key management difficult
  - All users need a public key pair and corresponding certificate
- Important to properly check certificates
EAP: PEAP

- Protected Extensible Authentication Protocol (PEAP)
- Provides a protection layer for legacy EAP methods (inner authentication method)
  - In particular MS-CHAPv2
- TLS tunnel between user and authentication server
  - Typically only server authentication
- MS-CHAPv2 can be used to authenticate using username/password combination
- Again, important to check certificate
EAP: TTLS

- Tunnelled TLS (TTLS)
- Similar to PEAP: provide a TLS tunnel to use legacy authentication methods (inner authentication method)
- More flexible and allows for more authentication methods
  - Not only ones that have EAP support
- Once again, important to verify certificates
EAP-PEAP

Supplicant

802.11 Association
EAP: request identity
EAP: identity
EAP: Start EAP-PEAP
Authentication and key exchange inside TLS tunnel
EAP: Success
4-way handshake

Authenticator

Anonymous identity (if configured)

RADIUS: Access request, identity
RADIUS: Start EAP-PEAP
RADIUS: Access accepted, key material

Authentication server (RADIUS)
eduroam

- Allows users from one institute to use the wireless network at another institute
- Uses 801.2x authentication
- Explained in RFC 7593
- Federated authentication: authentication delegated to home institution
  - Routing based on domain (e.g. ru.nl in anonymous@ru.nl)
- EAP messages forwarded to home institution’s RADIUS server
- Similar system for governments: govroam
eduroam hierarchy

- Confederation top-level RADIUS Server (TLR)
  - E.g. Europe or Asia and Pacific region
- Federation-Level RADIUS servers (FLRs)
  - E.g. SURF for .nl
- Identity provider (IdP)
  - E.g. Radboud University for ru.nl
Eduroam

Source: https://www.bsc.es/marenostrum/access-to-eduroam
Issues with PEAP and TTLS

- Who uses eduroam?
- Who configured an anonymous identity?
- Who configured a CA?
- Who configured a hostname for the RADIUS server?
Issues with PEAP and TTLS

- If no anonymous identity is configured, you are sending your real username in plaintext
- Most inner authentication methods are broken
  - MSCHAPv2 can easily be cracked
  - PAP (Password Authentication Protocol): plaintext username/password
- But this inner authentication is protected using a TLS tunnel, right?
  - How do you check the certificate?
Issues with PEAP and TTLS

- Which CA certificate do you configure on the clients?
  - None → anyone can impersonate your network
  - Public CA → anyone can impersonate your network, as long as you do not configure the RADIUS hostnames
  - Dedicated/private CA → impersonation is not possible (assuming no keys are compromised)
  - Trust on first use: accept a certificate on first connection and store it

- What happens if verification is not done properly?
  - Evil twin attacks are possible
  - Attacker gets access to the inner authentication
  - Potentially worse than no encryption!

- All depends on the configuration by the users
WPA3

- Announced in January 2018 by Wi-Fi alliance
- Several new security features
- Individualised data encryption in open networks
  - Using Opportunistic Wireless Encryption (OWE)
- Resilient password-based authentication
  - Use of Simultaneous Authentication of Equals (SAE)
- Stronger cryptographic algorithm (192 bits security)
Opportunistic Wireless Encryption (OWE)

- Specified in RFC8110
- Intended to make eavesdropping a bit harder in public networks (open or with publicly known pre-shared key)
- Based on Diffie-Hellman
- Part of the association step
  - Client adds public Diffie-Hellman value to association request
  - Access point add public Diffie-Hellman value to association response
- PMK derived from the result of the Diffie-Hellman key exchange
- PMK then used as input for the 4-way handshake
Simultaneous Authentication of Equals (SAE)

- Improve security of PSK method when using a password
- Password-authenticated key exchange method based on Diffie-Hellman
  - Based on zero-knowledge proof
  - Prevents dictionary attacks
  - One guess per session
  - Forward secrecy
- Takes place in authentication phase
- Originally intended to provide authentication between peers in a mesh networks
Simultaneous Authentication of Equals (SAE)

- Two message exchanges
  - Commitment exchange
  - Confirmation exchange
- PWE (Password Element): group element derived from password and MAC addresses of both parties involved
- The protocol results in a PMK shared between the two parties
  - Subsequently used in the 4-way handshake to establish session keys
Simultaneous Authentication of Equals (SAE)

Generate random scalars randS and maskS
Derive $\text{PWE}$
commitScalarS = \((\text{randS} + \text{maskS}) \mod r\)
commitElementS = $\text{PWE}^{-\text{maskS}}$

commitScalarS, commitElementS

Compute shared secret
$K = (\text{PWE}^{\text{commitScalarS}} \cdot \text{commitElementS})^{\text{randS}}$
Derive KCK and PMK

HMAC\(_{\text{KCK}}\)(commitScalarS, commitElementS, commitScalarA, commitElementA)

Authentication accepted

Generate random scalars randA and maskA
Derive $\text{PWE}$
commitScalarA = \((\text{randA} + \text{maskA}) \mod r\)
commitElementA = $\text{PWE}^{-\text{maskA}}$

commitScalarA, commitElementA

Compute shared secret
$K = (\text{PWE}^{\text{commitScalarA}} \cdot \text{commitElementA})^{\text{randA}}$
Derive KCK and PMK

HMAC\(_{\text{KCK}}\)(commitScalarA, commitElementA, commitScalarS, commitElementS)
Key Reinstallation Attacks

• Discovered by Mathy Vanhoef in 2017
• Force nonce reuse for the data confidentiality algorithm
  • Impact depends on algorithm
• Independent from authentication method
  • Targets 4-way handshake
• Problems in both the specifications and implementations
• WiFi designed to cope with packet loss
Recap: 4-way handshake

- **Msg1(r, ANonce)**
- **Msg2(r, SNonce, MIC)**
- **Msg3(r+1, ANonce, MIC, Enc_{KEK}(GTK))**
- **Msg4(r+1, MIC)**

Derive PTK

Install PTK and GTK

Install PTK

Encrypted data frames
Frame encryption (simplified)

Nonce reuse implies keystream reuse!

Based on slide by Mathy Vanhoef
Recap: 4-way handshake

Msg1(r, ANonce)

Msg2(r, SNonce, MIC)

Nonce set to zero

Msg4(r+1, MIC)

Install PTK and GTK

Install PTK

Encrypted data frames
Reinstallation attack

Install PTK and GTK

Key reinstalled and nonce set to zero!
Reinstallation attack

Msg1(r, ANonce)
Msg2(r, SNonce)
Msg3(r+1, ANonce, MIC, Enc_{KEK}(GTK))
Msg4(r+1, MIC)

Install PTK and GTK

Install PTK and GTK

Same nonce is used!

Enc_{PTK}(1, Data(...))
Enc_{PTK}(1, Data(...))
Reinstallation attack

Install PTK and GTK

Install PTK and GTK

Keystream

Decrypted data!
Impact

• Messages can be replayed and decrypted
  • Replay towards victim
  • Decrypted from victim
• Access points can be attacked if IEEE 802.11r is supported
  • Used for roaming within corporate networks
• Data confidentiality algorithm specific
  • CCMP: no practical forging attacks
  • TKIP: recover MIC key from plaintext → forge/inject frames from victim
  • GCMP: recover authentication key → forge/inject frames from and to victim
• Particular version of Android and wpa_supplicant reinstalled all zero keys
Countermeasures

- Do not reset nonces and replay counter when reinstalling the current key
- Only install one key per 4-way handshake
WiFi risks

• Broadcasts medium → everyone can listen and send traffic
• Client can easily be tracked → privacy risks
  • MAC address
  • Broadcasted SSIDs by client
  • 802.1x identity
• Security relies heavily on correct configuration of clients
  • Wrong configuration can lead to compromise of network access and credentials
WiFi advantages

- WiFi authenticates all users
  - As opposed to network sockets
- Encrypts all traffic on link layer
- Can control access to resources based on user identity
Further activities

• Read the following paper:

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2
M. Vanhoef and F. Piessens