WI-FI SECURITY: THE DETAILS MATTER

Tom Carpenter
CTO
CWNP
@carpentertom | @CWNP
Why Does Wi-Fi Security Matter?

<table>
<thead>
<tr>
<th>541.6 million hotspots by 2021</th>
<th>500 million new mobile workforce professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi is entering new areas every month</td>
<td>Cloud-managed WLAN market to grow to $3.3 billion by 2020</td>
</tr>
</tbody>
</table>
Wi-Fi Security Landscape

Application Layer
Use of secure applications assists in network security

Network (IP) Layer
Secure infrastructure and protocols should be used

Data Link (MAC) Layer
Data encryption and authentication should be used

Physical Layer
Monitoring and alert systems should be used
Focus Points

- Authentication
- Encryption
- Monitoring
802.11 Authentication Methods

- Open System
- Pre-Shared Key
- 802.1X/EAP
- Shared Key is deprecated as of 802.11i-2004
Open System Authentication

A null authentication method

<table>
<thead>
<tr>
<th>No</th>
<th>M</th>
<th>Time</th>
<th>Delle</th>
<th>Length</th>
<th>Source</th>
<th>Destination</th>
<th>BSSID</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>25161</td>
<td>1/28 13:54:06.549052</td>
<td>123375...</td>
<td>153</td>
<td>31</td>
<td>00:1A:1E:14:F3:30</td>
<td>00:1A:1E:14:F3:30</td>
<td>001A:1E:14:F3:30</td>
<td>802.11 authentication</td>
</tr>
<tr>
<td>25163</td>
<td>1/28 13:54:06.549708</td>
<td>123375...</td>
<td>153</td>
<td>100</td>
<td>00:21:5C:50:16:B1</td>
<td>00:21:5C:50:16:B1</td>
<td>001A:1E:14:F3:30</td>
<td>802.11 association request</td>
</tr>
<tr>
<td>25165</td>
<td>1/28 13:54:06.556312</td>
<td>123375...</td>
<td>153</td>
<td>113</td>
<td>00:1A:1E:14:F3:30</td>
<td>00:1A:1E:14:F3:30</td>
<td>001A:1E:14:F3:30</td>
<td>802.11 association response</td>
</tr>
<tr>
<td>25167</td>
<td>1/28 13:54:06.557749</td>
<td>123375...</td>
<td>153</td>
<td>155</td>
<td>00:1A:1E:14:F3:30</td>
<td>00:1A:1E:14:F3:30</td>
<td>001A:1E:14:F3:30</td>
<td>802.11 EAPOL-key</td>
</tr>
</tbody>
</table>

Note that Open System authentication occurs as the first step after network discovery and does not imply a secure “authentication.”
Pre-Shared Key (PSK)

The association request frame of a PSK-based authentication will show the AKM Suite type as 00-0F-AC:02.
WPA2-Personal is also known commonly as WPA2-PSK
How PSK Authenticates

- Authentication occurs during the 4-way handshake
- Frames 2-4 are MIC-protected
- The MIC calculation includes the KCK, which is part of the PTK, as an input
- Mismatched MIC calculations between the supplicant and authenticator result in termination of the 4-way handshake
An entity at one end of a point-to-point LAN segment that is being authenticated by an Authenticator attached to the other end of that link.

An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.

An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the Authenticator.
802.1X Port Functions
For RSN compliance, mutual authentication must be performed between the supplicant and AS.
Mutual authentication prevents man-in-the-middle attacks and ensures that the EAP peer and EAP server are valid.
The strength of subsequent cipher suite negotiation depends upon mutual authentication.
802.1X/EAP Architecture

Suppliant → Authenticator

Authenticator Requests Identity
Supplicant Responds with Identity
Authenticator Forwards Authentication Info Request
Supplicant Responds Authentication Info
Authenticator Forwards Authentication Info
Authenticator Forwards Identity to Authentication Server
Authentication Server Requests Needed Authentication Info
Authentication Server Validated or Invalidates the Client
Authenticator Switches the Controlled Port to Authorized (if the client is validated)
Several components are involved in the flow for WPA/WPA2 Enterprise implementations. A single device is not typically used for all services.
802.11 Encryption Methods

- Authentication and Key Management suites
  - Temporal Key Integrity Protocol (TKIP) – Deprecated
  - Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)

- Encryption algorithms
  - Rivest Cipher 4 (RC4) - Deprecated
  - Advanced Encryption Standard (AES)

- Modern Wi-Fi generates encryption keys during the 4-way handshake
4-Way Handshake

Message 1: Authenticator → Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,DataKD_M1)
where DataKD_M1 = 0 or PMKID for PTK generation, or PMKID KDE (for sending SMKID) for STK generation

Message 2: Supplicant → Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,DataKD_M2)
where DataKD_M2 = RSNE for creating PTK generation or peer RSNE, Lifetime KDE, SMKID KDE (for sending SMKID) for STK generation

Message 3: Authenticator → Supplicant:
EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,DataKD_M3)
where DataKD_M3 = RSNE,GTK[N] for creating PTK generation or initiator RSNE, Lifetime KDE for STK generation

Message 4: Supplicant → Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,DataKD_M4)
where DataKD_M4 = 0.
Message 1: Authenticator → Supplicant: EAPOL-Key\(0,0,1,0,P,0,0\), DataKD_M1

\[\text{where DataKD_M1 = 0 or PMKID for PTK generation, or PMKID KDE (for sending SMKID) for STK generation}\]

1 when initial key exchange is complete
1 when MIC is in the message
1 when a response is required
Install bit – 1 means install the keys
Key Type – P is Pairwise and G is Group

Key RSC (Receive Sequence Counter) for GTK

Used only in PeerKey operations (1 is PeerKey)

Elements defining the key

MIC
Message 2: Supplicant → Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,DataKD_M2) where DataKD_M2 = RSNE for creating PTK generation or peer RSNE, Lifetime KDE, SMKID KDE (for sending SMKID) for STK generation

The client now sends its NONCE (SNONCE) to the AP/Controller

At this point the client and the AP both have all that’s required to generate the Pairwise Transient Key (PTK)
Message 3: Authenticator → Supplicant:
EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,DataKD_M3)
where DataKD_M3 = RSNE,GTK[N] for creating PTK generation or initiator RSNE, Lifetime KDE for STK generation

The AP/Controller can now send the GTK to the client and the install bit (bit 4) is set to 1

This is the point at which KRACK operates
Message 4: Supplicant → Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,DataKD_M4) where DataKD_M4 = 0.

This is really just the “all is good” message so the AP/Controller knows the client has the PTK and GTK installed
KRACK Operation

Client → AP

Initiate

Jam Channel 1, Offer Channel 6

Channel 1

Client → AP

Attack

Channel 1

Client → Channel 6

Channel 1

Client → AP

Attack
Who is to blame for KRACK?

- Great question; Complex answer

- Some say the IEEE because of closed processes and lack of availability of the standard early after release
  - Tom’s take: the 802.11i amendment has been easily available for 13 years with no fee most of that time, if someone noted the problem, the IEEE could have easily included a fix in 11n, 11ac, or any other amendment since then – not sure this is the real problem

- Some say the vendors because they should have implemented the flexible state machine more securely
  - Tom’s take: this is a hard one, the standard leaves a lot of flexibility, so each vendor would do it differently and if they make it too complex they could introduce compatibility problems

- Tom’s opinion: Time
  - Tom’s take: time is to blame; nearly every security solution degrades over time as the most brilliant minds may create it, but other brilliant minds want to thwart it – time is usually on the side of the attackers

- End result: Security is a process not an event
802.11 Key Hierarchy

- **Encryption Keys**
  - Key Encryption Key (KEK)
  - Key Confirmation Key (KCK)
  - Temporal MIC Keys
  - Temporal Encryption Key (TEK)

- **Temporal Keys**
  - Group Temporal Key (GTK)
  - Pairwise Transient Key (PTK)

- **Pairwise Master Key (PMK)**
- Is derived from 802.1X/EAP authentication or is the equivalent of the passphrase

- **Group Master Key (PMK)**
- Highest order 802.11 key. Derived from MSK (802.1X) or PSK

- **Master Session Key (MSK)**
- Authenticator uses separate derivation process to produce the GMK.

- **Encryption and MIC keys**
Pairwise Transient Key (PTK)

The PTK is comprised of three keys: KCK, KEK and TK

KCK used for key integrity

KEK used to encrypt and send keys (GTK)

The TK is used to encrypt data payloads
Wi-Fi Monitoring Methods

- Infrastructure solutions
- Overlay solutions
- Mobile solutions
Where do I go from here?

- **Immediately**
  - Validate the proper security of your existing Wi-Fi gear
    - Verify patches
    - Verify configuration

- **In the next 2-3 months**
  - Ensure all newly acquired equipment supports WPA2 (amended) or WPA3
    - Anything certified after November 2017 is tested for KRACK patching

- **In the next six months**
  - Consider a dedicated Wi-Fi security monitoring solution
    - Monitor configurations, new RF devices, anomalies
  - Many performance tools integrate security metrics, such as 7signal
THANK YOU