Wireless Fundamentals: Encryption and Authentication

This article gives insight on wireless encryption and authentication to help users make an educated decision on what type of security to implement into their wireless network. Cisco Meraki equipment supports several types of encryption and authentication:

- WEP
- WPA
- WPA2 - PSK (Pre Shared Key)
- WPA2 - Enterprise
- Splash Page
- Hidden SSID

**WEP**

Wired Equivalent Privacy, now depreciated, was part of the original 802.11 standard. WEP utilized a 40-128 bit key that was a combination of a key (string of hexadecimal characters) and an initialization vector. Cisco Meraki Access Points support pre-shared key WEP authentication. WEP was deemed insecure due to how easy it could be decoded but is still available in Cisco Meraki equipment for legacy devices.

**WPA**

Wi-Fi Protected Access, WPA, was created to “patch” the issues with WEP, allowing users to update their equipment with a firmware update as opposed to buying brand new hardware. WPA included a new type of key system called TKIP (Temporal Key Integrity Protocol.) TKIP develops a unique encryption key for each wireless frame facilitating a more secure connection. However, TKIP is susceptible to wireless attacks and is no longer considered the Enterprise standard.

**WPA2 – Personal**

WPA2 is currently the most secure standard utilizing AES (Advanced Encryption Standard) and a pre-shared key for authentication. WPA2 is backwards compatible with TKIP to allow interoperability with legacy devices. AES uses CCMP encryption protocol which is a stronger algorithm for message integrity and confidentiality. By default, SSIDs on Cisco Meraki access points that are configured as WPA2 utilize a combination of both TKIP and AES encryption.

**WPA2 – Enterprise**

WPA2 Enterprise utilizes authentication on a user level, using the 802.1x standard, along with the features of WPA2 such as AES. Cisco Meraki fully supports WPA2 Enterprise association with RADIUS and PEAP/MSCHAPv2, or Meraki Authentication, to provide a secure wireless network for enterprise use. Users log in with a valid username and password to authenticate instead of a pre-shared key susceptible to social engineering.

**Splash Page**

Cisco Meraki provides a variety of splash pages that can be utilized for additional security.
• Sign on with Authentication - Forces users to authentication through a sign on page using various types of Authentication including RADIUS, LDAP, and Meraki Authentication.
• Sign on with SMS Authentication - Forces users to authenticate with an SMS code that they would receive on their phone.
• Systems Manager Sentry - Utilizes Cisco Meraki Systems Manager, users will need to install the manager client on their computer, their device can then be viewed on a Systems Manager network.

Splash Pages can be used with or without a WPA/WEP solution as well.

**Hidden SSID**

A hidden SSID can prevent public visibility of your corporate SSID. Hidden SSID's require a manual creation of a wireless profile in order for the wireless client to initiate association. Although packet sniffers can detect SSID names from other probe requests and association frames, disabling SSID broadcasts can dissuade many would-be attackers from trying to gain access.

Shown below Figure 1 is a standard non hidden SSID beacon frame, the AP will send this out for each of the SSIDs that it is broadcasting out.

**Figure 1**

<table>
<thead>
<tr>
<th>IEEE 802.11 Beacon frame, Flags: ........</th>
<th>IEEE 802.11 wireless LAN management frame</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type/Subtype:</strong> Beacon frame (0x08)</td>
<td><strong>Fixed parameters (12 bytes)</strong></td>
</tr>
<tr>
<td><strong>Frame Control:</strong> 0x0080 (Normal)</td>
<td><strong>Tagged parameters (184 bytes)</strong></td>
</tr>
<tr>
<td>Version: 0</td>
<td>Tag: SSID parameter set: MOTOROLA-BC7E0</td>
</tr>
<tr>
<td>Type: Management frame (0)</td>
<td>Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]</td>
</tr>
<tr>
<td>Subtype: 8</td>
<td>Tag: DS Parameter set : Current Channel: 1</td>
</tr>
<tr>
<td>Flags: 0x0</td>
<td>Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap</td>
</tr>
<tr>
<td>Duration: 0</td>
<td>Tag: ERP Information</td>
</tr>
</tbody>
</table>

A hidden SSID will not broadcast the beacon frames - clients will have to know the SSID name to associate. Figure 2 is an iPhone broadcasting a request to see if the SSID "Test" is available in the area.

**Figure 2**
IEEE 802.11 Probe Request, Flags: .......
Type/Subtype: Probe Request (0x04)
Frame control: 0x0040 (Normal)
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
Fragment number: 0
Sequence number: 28

IEEE 802.11 wireless LAN management frame
Tagged parameters (96 bytes)
- Tag: SSID parameter set: Test
- Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
- Tag: HT Capabilities (802.11n D1.10)
- Tag: Vendor Specific: Broadcom
- Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
- Tag: Vendor Specific: Microsoft: Unknown 8

For more information on Wireless Security, please review the Wireless LAN Security Overview document.