Differentiate These Roaming Technologies: Part 2

PMK Caching vs OKC

PMK Caching saves PMKIDs on known APs

- Client associates to an AP. The AP saves the PMKID from the session

- If the client roams back to the same AP, the client moves straight to 4-Way handshake.

- This differs from "preauthentication" where the a new PMK is created on a target AP for roaming.

How do I know if I'm using PMK Caching ?

Check for your vendor's documentation on defaults per SSID type and how to set these parameters.

For example, Meraki enables PMK Caching by default for a "secure SSID (OWE, WPA3-Personal, and WPA2/3 Enterprise)"

OKC is Opportunistic Key Caching

-Builds on PMK Caching. One PMK is saved per-client across all APs in the ESS

-Other APs then use the PMK to calculate the PMKIDs for subsequent roams.

-Support varies based on client vendor.

How do I know
if I'm using OKC?

Likewise with PMK Caching, check for your vendor's documentation on default settings or how to configure OKC.

Mist for exmple uses PMK caching as default, but **not** OKC.

The methods for fast roaming are, Default, Opportunistic Key Caching (OKC) and .11r. For both these methods, there is no need to send access request packets to the RADIUS server.

The fast roaming option becomes available when you select WPA3 or WPA2 as your security type.

Default

- Mist APs locally cache the client Pairwise Master Key (PMK) ID obtained during the initial authorization and use it for subsequent re-associations on the same AP. This is also known as "fast secure roam back," and is suitable for use cases where scale is not a factor because clients must fully re-authenticate at each new AP in the network until all the APs have their own local copy of the client's PMKID.

Caveats with PMK Caching and OKC

- When troubleshooting, keep in mind OKC and PMK Caching are often enabled at the same time as 802.11r

-Vendors often do not enable PMK Caching or OKC on WPA2-PSK SSIDs. This is due to potential vulnerabilities and it not really needed for security type with low-processing time.

Recap

PMK Caching saves the client PMKID for previously 802.1x authetncated APs only. OKC allows other APs in the ESS to generate new PMKIDs with the same PMK.

Sources/Credits

-Certified Wireless Analysis Professional 2nd Edition, Certitrek Publishing

-Roaming Technologies, Cisco Meraki Documentation

-Opportunistic Key Caching, Cisco Whitepaper

-RSSI, Roaming, and Fast Roaming, Juniper Mist Documentation

This post has been designed using resources from Flaticon.com (Artist: Flat Icon, Afian Rochmah Afif)