How Arista's UPSK Overcomes the Challenges of WPA3 and MAC Randomization

UPSK - An Innovative Approach

Arista has designed a solution where client MAC addresses are not the primary key. Rather, AGNI uses a user's SSO identity as the primary key. This approach eliminates the need for users to keep track of the MAC addresses of their devices. Additionally, this method works for hardware MAC addresses or random MAC addresses.

Segmentation with MSS-G UPSK

As mentioned above, AGNI is required for MSS-G UPSK. MSS-G UPSK effectively creates private networks for each user (using their own UPSK) that share a single SSID and a single VLAN. When MSS-G UPSK is enabled, clients connecting with the same UPSK can talk to each other regardless of which APs the clients are associated to, while clients that do not share a UPSK cannot talk to each other. All user devices can access clients that are in the Shared Client Group (e.g. shared printers), as depicted in the Fig. 1 on page 2.

PSK implementation challenges with WPA3 and MAC Randomization

Alphabet Pre Shared Key (PSK) implementations (e.g. M/D/I/P-PSK) typically require that per user PSKs be tied to a MAC address when the end user registers a new client. These implementations use a technique called 'WPA2 PSK Cracking' where the server can deduce the PSK based on MAC and few other parameters sent by the AP, and the per user PSKs is tied to a MAC address. With WPA3, it is no longer possible to tie the PSK to a MAC address hence breaking existing implementations. Additionally, with many clients exhibiting MAC randomization behavior, any technique that ties PSK to MAC address breaks, requiring new ways of solving this problem.

UPSK Overview

Unique Pre Shared Keys (UPSK) provide a simplified and secure client authentication process. UPSK allows users to connect to the same SSID using a unique / user specific PSK. Arista's UPSK solution provides added security over single PSK deployments because single PSKs use the same PSK for all connected devices. PSKs are more easily compromised, and the fallout is greater than if a UPSK is compromised.

UPSK can be implemented with Arista Guardian Network Identity (AGNI) or a third party NAC. Using AGNI with UPSK also provides an option for UPSK-to-UPSK based segmentation where wireless Macro Segmentation Service - Groups UPSK (MSS-G UPSK) are created. Third party NACs do NOT support MSS-G UPSK segmentation.

UPSK with WPA2

There has been a solution for registering new clients using WPA2 for some time. Various vendors have been using a well known cracking method that occurs during the 4-way handshake to derive the user's PSK. When a user connects a new client, or a client that is using a new random MAC address, the new MAC address can be automatically registered to the user's UPSK Group and the new client will be automatically authenticated using the user's UPSK. AGNI supports this methodology for on-boarding clients using WPA2.

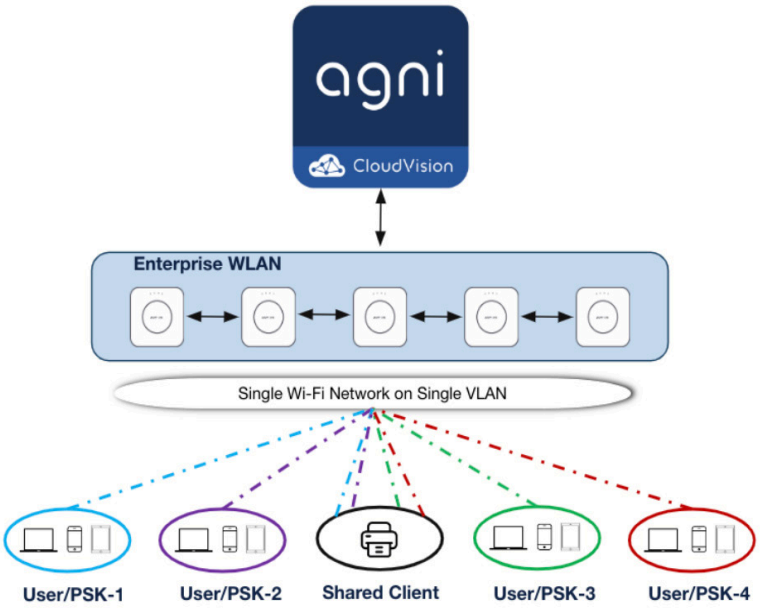

Figure 1.

UPSK with WPA3 Challenges

The cracking solution used for WPA2 outlined above will not work for WPA3 as WPA3 relies on Simultaneous Authentication of Equals (SAE). SAE is not susceptible to the WPA2 cracking method. One work around to this challenge might be to register MAC addresses manually but that method is too laborious, prone to errors, does not scale, and now with the pervasiveness of MAC randomization usage by various client types, manual MAC address registration is impractical.

Arista's UPSK with WPA3 Solution

The Arista solution automatically ties a user's client MAC addresses to a user's UPSK Group by keying on the user's SSO identity. There are a number of methods for adding client devices to a user's UPSK Group.

Option 1: Self Service Portal via Onboarding PSK

1. A user's new device connects via the onboarding PSK.
2. The user then gets redirected to the AGNI Self Service Portal where the user enters their SSO credentials. After the user successfully enters their credentials the user will be presented with their UPSK and a QR code.
3. The user then configures their device to use their UPSK, or for iOS and Android devices, the user can scan the QR code to have their UPSK automatically configured on the provisioned device.
4. Now the new device, or a device that was previously registered but with a different random MAC address, automatically gets added to the user's UPSK Group and gets authenticated using their UPSK.

Option 2: Self Service Portal via QR Code Scan

1. A new device scans QR code and connects to the UPSK SSID with the onboarding passphrase.
2. The user then gets directed to the AGNI Self Service Portal where the user enters their SSO credentials. After the user successfully enters their credentials the user will be presented with their UPSK and a QR code.
3. The user then configures their device to use their UPSK, or for iOS and Android devices, the user can scan the QR code to have their UPSK automatically configured on the Provisioned device.
4. Now the new device, or a device that was previously registered but with a different random MAC address, automatically gets added to the user's UPSK Group and gets authenticated using their UPSK.

Option 3: Client Groups for Headless / IoT Devices

1. The Admin logs into AGNI to create a Client Group and enters a UPSK for that Client Group.
2. Admin can directly import or add client MAC addresses to the Client Group. Admin can also enable delegated management, to allow end users (such as technicians) to import / manage MAC addresses in the Client Group via AGNI Self Service Portal without requiring admin involvement.
3. The admin or technician then configures the headless / IoT devices to use the UPSK created for the Client Group.
4. The user connects the headless device (printers, IoT device) to the network using their Client Group UPSK.
5. Devices using the UPSK for the Client Group will now be tied to the Client Group.
6. successfully enters their credentials the user will be presented with their UPSK and a QR code.
7. The user then configures their device to use their UPSK, or for iOS and Android devices, the user can scan the QR code to have their UPSK automatically configured on the Provisioned device.
8. Now the new device, or a device that was previously registered but with a different random MAC address, automatically gets added to the user's UPSK Group and gets authenticated using their UPSK.

Client MAC Randomization

For options 1 - 3 with WPA3, as well as with WPA2, new MAC addresses are automatically added to a user's identity and their UPSK group during SSO authentication. Again, the main key is the SSO identity. It is during SSO authentication that new MAC addresses (random or hardware) are added to a user's UPSK Group. Old MAC addresses (e.g. a random MAC that is no longer being used) will age out of the database after 7 days of non-use.

Conclusion

SSO identity is the primary key in the UPSK solution, rather than relying on client MAC addresses. Therefore there is no need for users to keep track of the MAC addresses used by their devices. In addition to increased security over PSK, Arista's UPSK solution works for both WPA2 and WPA3 with hardware or random client MAC addresses.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062