IMAGINE THE POSSIBILITIES...
Wi-Fi Passwords (WPA2-Personal)

• **They’re great!** Simple to define, simple to share.

• **BUT:**
  • One device can observe another device’s traffic
  • Once a password is shared, it can’t be “unshared”.
  • Changing the Wi-Fi password on networks becomes a larger problem as more devices are added to the network
  • With IoT devices (smart speakers, smart plugs, smart bulbs, smart thermostats, etc.) the issue of changing Wi-Fi passwords has moved from “inconvenient” to “highly disruptive”/”virtually impossible”
    • IoT devices are notorious for having inconsistent means of provisioning Wi-Fi credentials
    • Workflows are geared for initial “quick start” setup, not reprovisioning
    • Many devices even require a complete factory reset to be provisioned – leading to a cascade of issues with lost device configurations, app, and reassociating devices with their various cloud services.
WPA2 Personal Authentication

How it works...

Each station can have its own PMK, but in WPA-2 Personal, the AP and all stations derive the PMK from the same password. So everyone has the same PMK.
WPA2/3 4-Way Handshake

How it works...

- Each Station has an associated PTK that’s calculated independently by the AP and Station using a shared secret: The PMK
- There are multiple ways that the PMK is established on the AP and Station.
  - WPA2 Personal: Shared password
  - WPA2/3 Enterprise: Various forms of EAP
  - WPA3 Personal: Shared password (SAE)
  - DPP/Easy Connect: Connectors
**WPA2/3 Enterprise Authentication**

**How it works…**

- The Station is allowed to communicate using special packets (EAPOL) with an EAP server before authentication.

- The Station and Auth Server can use a number of methods to authenticate the user (e.g., TLS authentication using X.509 cert).

- Station calculates a PMK and shares it with the Authenticator—which is communicated to the AP.

- The Station and AP perform 4-way handshake with the now-shared PMK.
WPA3 Personal SAE

How it works...

- Each station uses a Simultaneous Authentication of Equals (SAE) to derive a high-entropy key from a low entropy-password
- Key is formed in a way that enables forward secrecy
- The shared, derived key is used as the PMK
Some hybrid multi-password solutions

How it works…

• Each Station - or multiple Stations - is/are assigned its own password

• During association of Station A, the AP uses the MAC address of A to determine the password/PMK to use and uses PMK_A in the 4-way handshake

• Issues:
  - Provisioning passwords via MAC is cumbersome
  - TOFU is tricky (first Station presenting PW is associated)
  - MAC can be copied from one device to another
  - MAC randomization can foul this up
Issues with provisioning WPA 2/3 devices today…

- **WPA-2 Personal**
  - Need to be manually entered on every device
  - No revocation (without complete reprovisioning of the network)
  - Not secure (no PFS, any Station can see all AP traffic)

- **WPA-3 Personal**
  - More secure, but with the same issues as WPA2

- **WPA-2/3 Enterprise**
  - Enables separated, revocable credentials
  - Integrates with Enterprise user authentication systems
  - BUT devices don’t necessarily map to users
  - Complex infrastructure and no easy provisioning mechanism for enterprise credentials

- **None provide provisioning, reprovisioning, bulk provisioning, or a secure device identity**
DP P/Eas yCo n n e c t Direc t Pro visio n in g

How it works…

• DPP/Easy Connect device advertises a URI which can be provided via a preprinted QR code, a display, or BT/NFC advertisements

• The URI contains the Wi-Fi channel the device is tuned to, a public “bootstrap” key, and other metadata

• A “Configurator” app—which has a trust relationship with the AP(s)—securely connects to the device and provisions network credentials

• STA_A presents Conn_A to the AP and the AP presents Conn_AP to STA_A

• The AP and STA_A authenticate each other using Csk_CF
DPP/Easy Connect AP-Based Provisioning

How it works...

- The AP performs the communication with the device instead of the configuration app.
- The AP configuration app can communicate with the AP via cloud and non-DPP credentials, as is typically done.
- Credentials (including the private credential-signing key, csk_{CF}) stay on the AP.
  - No issue with csk_{CF} getting "lost" or securely backing it up.
  - May be easier to secure csk_{CF} on the AP.

DPP/Easy Connect

WFA DPP/Easy Connect

Access Network (AP)

AP Configuration App

Configurator creates Conn_{AP} for STA_{AP}, signing it with csk_{AP}.

1

Quick Start

User scans QR code using Configurator application (Public Key + MAC + Frequency/ Chan).

2

Configurator passes URI to the AP.

Configurator configures Station using Easy Connect Auth/Config messages (SSID, Conn_{AP}, Csk_{AP}):

3a

STA_{AP} authenticates using Conn_{AP} establishing PTK_{X}/GTK_{X}.

3b

© 2020 SCTE•ISBE, CableLabs & NCTA. All rights reserved. | scte.org • isbe.org
**DPP Connectors**

- Must contain a `netAccessKey` and `groups` – but can contain other information the Configurator wants to associate with the Station

- Signed using the Configurator’s private key (the `"c-sign-key"`)

- Can be identified by the signature or hash of the signature

---

```json
{
"groups": [
{
"groupId": "home",
"netRole": "sta"
},
{
"groupId": "cottage",
"netRole": "sta"
}
],
"expiry": "2019-01-31T22:00:00+02:00",
"netAccessKey": {
"kty": "EC",
"y": "LUsDBmn7tv-LCnn6fBoXkSfPgLJiiPv_yknTcKggsgeU",
"x": "Xj-zV2iEiH8XwyA9i3psL6xyLvDiIBthrHO8ZVxwmpA",
"crv": "P-256"
}
}
```

---

**Header data**

**The encoded connector JSON**

**Signature**
Connector-based Authentication

How it works...

- The AP and the Station provide each other their Connectors and each authenticates the other
  - AP establishes trust in the Station
  - Station establishes trust in the AP
- They each use both Connector’s Network Access Key to derive a common PMK
- Using the derived PMK, the AP and Station perform the 4-way handshake to determine session keys
- Note that the MAC of each party can be established after mutual authentication (useful if/when MACs are randomized)
Benefits of DPP/Easy Connect

- Easy to deploy shared password, per-Station Connector credentials, and enterprise credentials to devices
- Onboarding workflow provides an opportunity to interact with the user
- Supports mutual authentication (via Connectors)
- Enables reconfiguration of devices (updated credentials, policy groups, SSID name, etc.)
- Can be implemented/deployed in a number of ways (direct provisioning, AP-based, bulk provisioning)
- Connectors provide identity, with extensible metadata
  - Can remove the dependency on static MAC addresses for advanced features
  - Can enable advanced network and device policies/features
AP/Gateway Virtual Network Segmentation

1. AP/gateway segments network into trust domains
2. User/app/cloud policy/AI map devices into trust domains
3. SDN enforces and controls switching, routing, and access control rules
4. User has control to move, remove, or quarantine unwanted/questionable devices
AP/Gateway Segmentation

- Enables the separation of devices by risk category and/or function
  - e.g. Home automation/security devices can be allowed to connect to the Internet but cannot initiate connections to devices in other segments
  - e.g. Interactive devices such as smart phones and tablets can initiate connections with home automation/security devices but those HA/security devices cannot access non-HA/security devices
- Devices that are suspected of being compromised can be “quarantined” – either explicitly via user direction or automatically, based on behavior/AI or external threat notifications
- Can enable the application of segment-level policies – such as data usage and time quotas
- Requires an attestable non-transferrable identifier and a reliable way to determine the MAC address of a station
Thank You!

Craig Pratt
Lead Software Engineer
CableLabs
c.pratt@cablelabs.com