WPA3 IS HERE

Pedro Lourenço, Systems Engineer
Agenda

- What’s wrong with WPA2?
- WPA3 is Here
  - Enhanced Open - Oportunistic Wireless Encryption (OWE)
  - WPA3-Personal - Simultaneous Authentication of Equals (SAE)
  - WPA3-Enterprise - Commercial National Security Algorithm (Suite B/CNSA)
  - Current WPA3 support - Client Devices & Aruba Devices
- WPA3 adoption

What’s wrong with WPA2

WPA2 is past retirement (first introduced in 2004)
- WPA2-personal was ‘broken on arrival’
  - Every couple of years someone “rediscovers” offline dictionary attacks
- WPA2-enterprise is still secure, but can be used in ways that lessen its overall security
  - Makes it more complicated to provision
For example, use cases with ill-suited security:
- Stadiums, Airports, Guest Captive Portals, BYOD Onboarding use Open SSIDs
- Coffee shops use WPA2-PSK with a shared and public PSK
- Enterprises, banks, schools, hospitals use WPA2-PSK for IoT (or people!)
- Hotspots have no way of offering server-side (infrastructure) only authentication
WPA3 is Coming Here

“WPA3 closes these gaps and evolves Wi-Fi security for the next decade!”
Dan Harkins

Aruba Supports for OWE and WPA3

- Aruba was directly involved in the development of WPA3
- Supported from InstantOS and ArubaOS 8.4
- Supported on all Aruba 802.11ac wave2 and 802.11ax APs:
- Not yet Supported on Aruba 802.11ac wave1 APs:
  - AP-2xx
- Will not be supported in earlier Aruba AP hardware platforms:
  - AP-1xx and AP-9x
- OWE/WPA3 + PMF supported in Tunnel mode ONLY for CAP, RAP
What is WPA3? New WFA Certifications for wireless security

1. Enhanced Open - OWE (Opportunistic Wireless Encryption) replaces Open
   - Problem: all wireless traffic passed in the clear
   - Solution: all wireless traffic gets encrypted
   - Not part of WiFi Alliance WPA3 Cert

2. WPA3-Personal: SAE (Simultaneous Authentication of Equals) replaces WPA2-PSK
   - Problem: passive attack results in off-line dictionary attack to discover session key
   - Solution: protocol is resistant to active, passive, and dictionary attack

3. WPA3-Enterprise: Suite B/Commercial National Security Algorithms ciphers
   Enhances WPA2-Enterprise
   - Problem: mix-and-match nature of WPA2-Enterprise can result in less-than-optimal security
   - Solution: create a cipher suite and a set of rules to ensure consistent primitive security
   - WFA requires basic (similar to WPA2 with enforced Protected Mgmt Frame settings)
   - Optional Mode for 256-bit + security protocols

Discrete Logarithm Problem
DLP – Discrete Logarithm Problem

The DLP is present in DL Cryptosystems which can be described in the context of Elliptic Curve Cryptography

Elliptic Curve Function plotting

A set of point which satisfies the equation:

\[ Y^2 = x^3 + a \cdot x + b \pmod{p} \]

Is called the elliptic curve group

DLC – Discrete Logarithm Problem

There are rules for adding a point to itself on the curve to arrive at the resultant point on the curve

If \( R \) is a known value, it is easy to define \( 2.R, 3.R, m.R, \) etc

Discrete Logarithm Problem:

“Given \( R \) and \( S \) what is \( m? \)”

If you know \( R \) and \( S \) (where \( S = m \cdot R \)), it is not possible to discover \( m \) (\( R \) and \( S \) are 256 bit or larger variables)

This problem is Computationally Intractable for large numbers
Enhanced Open
Oportunistic Wireless Encryption

Open Networks

- What is the problem with open networks?
  Open => No Encryption/Authentication/Security

- So why do we use them?
  Easy to provide service with no client configuration

- What is a more secure and equally simple alternative?
  Enhanced Open
Enhanced Open: No more Cleartext

- Based on Opportunistic Wireless Encryption (OWE) – RFC 8110
- Provides unauthenticated data encryption to Open Wi-Fi Networks
- Transparent to users & admins – no provisioning required
- Backward compatible to OPEN via “Transition Mode”
- Supports PMK caching, and PMF is required (OWE clients)

Not Mandatory for WPA3 Certification

---

How does OWE Transition Mode work?

- Advertisement and Discovery
  1. Administrator configures a single Open SSID and virtual AP
  2. AP automatically creates two BSSes with separate beacons
     i. BSS1 = Normal ‘Open’ network for non-OWE (legacy) stations. New IE to indicate BSS2
     ii. BSS2 = Hidden OWE with AKM type 18 (OWE). Ignored by legacy clients.
  3. OWE STA does active or passive scanning to discover OWE-capable AP

- Authentication and Association
  1. Normal 802.11 “Open” Authentication
  2. Diffie-Hellman Parameter element added to Association Request/Response

One additional SSID is advertised for every OWE SSID that needs to be accounted for
How does OWE Encrypt Open Traffic?

- OWE performs an **unauthenticated** Diffie-Hellman at association time
- It is based on the **Discrete Logarithm Problem** of **DLC**

1. **Association Request and Response** exchanging ephemeral public keys via Diffie-Hellman
2. **STA and AP** derive a **unique Pairwise Master Key (PMK)**
   - truly pairwise and unknowable by a third party
3. **PMK** is used in 4-way handshake post association to generate traffic encryption keys

---

Mobility Master **Enhanced Open Configuration**

**Create a new SSID profile**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SSID Name</td>
<td>[Step1]</td>
</tr>
<tr>
<td>2</td>
<td>Profile</td>
<td>[Step2]</td>
</tr>
<tr>
<td>3</td>
<td>Encryption</td>
<td>[Step3]</td>
</tr>
</tbody>
</table>

**SSID Profile: New Profile**

- **Profile name**: [Step1]
- **SSID**: [Step2]
- **WPA Passphrase**: [Step3]
- **Encryption**: [Step3]
- **Open system**
- **WPA**
- **WPA2**
Tasks -> Create a new WLAN

New WLAN

Step 1

Step 2

New WLAN

Step 3

Step 4

WPA3-Personal Simultaneous Authentication of Equals
WPA2-PSK Networks

• What is the problem with WPA2-PSK?
  • Same password to generate all encryption keys
  • Susceptible off-line dictionary attack when 4-way handshake is captured, which is trivial to get via “deauth” attacks
  • Security level dependent on password size and complexity

• So why do we use them?
  • “dumb” IoT devices
  • Best wifi security option available in non enterprise environment

• Is there a similar more secure alternative?

WPA3-Personal: Strong Security from Weak passwords

• WPA2-PSK is replaced by Simultaneous Authentication of Equals (SAE) (802.11-2016, section 12.4)
  • Originally intended for mesh security (802.11s)
  • Password-based authentication based on Dragonfly key exchange (RFC 7664)
  • Resistant to active, passive, and dictionary attack

• Supports PMK caching
• Mixed (Transition) mode
• PMF is required (SAE clients)
**SAE – Dragonfly Key Exchange**

Dragonfly Key Exchange is based on a zero knowledge proof

“The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.”

“Dragonfly uses discrete logarithm cryptography to achieve authentication and key agreement. Each party to the exchange derives ephemeral keys with respect to a particular set of domain parameters (referred to here as a “group”). A group can be based on Finite Field Cryptography (FFC) or Elliptic Curve Cryptography (ECC).” from IRTF RFC 7664

---

**HOW DOES SAE WORK – SAE Authentication**

- **password**
  - Known Transformation
  - Point R on elliptic curve
  - random: u
    - Key Generation: K = u.v.R
    - u and v are computationally interactable according to the Discrete Logarithm Problem
    - Hash of K
  - Eliptic curve parameters agreed according to the standard

- **password**
  - Known Transformation
  - Point R on elliptic curve
  - random: v
    - Key Generation: K = v.u.R
    - Mutual Authentication
    - Hash of K

**SPEKE PROTOCOL** (simple password exponential key exchange)
How Does SAE Work – Dragonfly Exchange in SAE Authentication

1. **Password**
   - **Known Transformation**
   - **Point R on elliptic curve**
   - **Random:** u₁, u₂
     - u = u₁ + u₂

2. **Key Generation:**
   - K = u₁.(v.R - v₂.R) = u₁.v₁.R
   - **Hash of K**

3. **Mutual Authentication**
   - **Password**
   - **Known Transformation**
   - **Point R on elliptic curve**
   - **Random:** v₁, v₂
     - v = v₁ + v₂

   - **u and v are computationally interactable according to the Discrete Logarithm Problem**

   - **Key Generation:**
     - K = v₁.(u₁.R - u₂.R) = v₁.u₁.R
   - **Hash of K**

---

How Does SAE Work – Offline Dictionary Attack Resistance

1. **Password**
   - **Known Transformation**
   - **Point R on elliptic curve**
   - **Random:** u
     - k = u.R

2. **Key Generation:**
   - K = u₁.v₁.R
   - **Hash of K**

3. **Mutual Authentication**
   - **Password**
   - **Known Transformation**
   - **Point R on elliptic curve**
   - **Random:** v
     - k = v₁.R

   - **Attacker sniffs and stores key handshake**

4. **Even if password guess is correct**
   - **Knowing R and u₁.R, finding u is intractable**
   - **Computing K is impossible**

   - **Can’t compare with hash of K**
   - **Don’t know if password is correct or not**
HOW DOES SAE WORK – SAE Flow

- **Passively observing SAE reveals nothing – Secure under CDH assumption**
  - By using a zero knowledge proof, an attacker is no longer able to witness a single exchange and go off-line to crack the PSK.

- **Active attack reveals whether a single guess of the password was correct or not**
  - Adversarial advantage grows from interaction and not computation
  - Only way to guess the password is through repeated active attack which can be detected
  - As soon as an AP notices too many SAE connection requests from a device, it will use tokens to limit the amount of simultaneous attempts and thus makes it harder to bruteforce or DoS.

- **Strong protocol allows for “weaker” passwords to be used**
  - As long as password is not trivial, size and complexity doesn’t matter
  - Probability of guess being correct is n/D where D is the number of possible password with n guesses
  - For example to guess a number between 1 and 1M, the probability of a single guess is 1/1M and it would take 500k active attacks to get a 0.5% probability of success
**WPA3-Personal: Strong Security from Weak passwords**

- **SAE provisioning is identical to WPA2-PSK**
  - User enters password just like always but gets improved security behind the scene
  - Allows more natural passwords to be used securely

- **Mixed (Transition) mode:**
  - WPA3 capable client connects using wpa3-sae
  - Legacy clients connect using wpa2-aes-psk

- **SAE transition mode - SAE AKM and PSK AKM on a single SSID**
  - same password used for both
  - This makes the SSID only PMF optional and not PMF required and a hacker could still gain access on your network via WPA2 attacks.
  - Even with a known password SAE provides Perfect Forward Secrecy (PFS) and is still better than just PSK

**Mobility Master SAE Configuration**

1. **Step 1:** Create a new WLAN
2. **Step 2:** Configure the WLAN settings
3. **Step 3:** Set the key management to WPA3-Hermetic
4. **Step 4:** Review and apply the settings
WPA3-Enterprise
Suite-B / Commercial National Security Algorithm

• What is the problem with WPA2-Enterprise?
  • Complex configuration
  • Too many options for WPA2-Enterprise with 802.1x/EAP
    • Diffie-Hellman or RSA key exchange? 1024-bit authenticating 2048-bit? TLS1.0? SHA1?
    • This can result in deployments that are not secure as expected
    • Clients can connect with varying degrees of security; security of the network depends on the weakest link
  • Falible Certificate Verification

• Is there a similar more secure alternative?
WPA3-Enterprise

- ArubaOS 8.4 supports two WPA3-Enterprise modes:
  - WPA3-Enterprise Basic
  - WPA3-Enterprise CNSA

WPA3-Enterprise: Basic

- Opmode is essentially the same as WPA2-Enterprise with enforced PMF settings (MFPR=0, MFPC=1)
- Both Enterprise client supporting 11w [PMF Capable] and legacy Enterprise Client (not supporting 11w) can connect to same SSID
- Transition knob does not apply
- Only tunnel mode is supported on CAP and RAP
### WPA3-Enterprise: Suite-B/CNSA

<table>
<thead>
<tr>
<th><strong>“top secret” security standards for Enterprise WiFi are enforced:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Deriving at least 384-bit PMK/MSK using Suite-B compatible EAP-TLS</td>
</tr>
<tr>
<td>• Securing pairwise data between STA and Authenticator using AES-GCM-256</td>
</tr>
<tr>
<td>• Securing group addressed data between STA and Authenticator using AES-GCM-256</td>
</tr>
<tr>
<td>• Securing group addressed Management frames using BIP-GMAC-256</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Suite-B TLS cipher suites used in EAP-TLS are required:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 using p384 (for Diffie-Hellman and signing)</td>
</tr>
<tr>
<td>• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 using p384 (for DH and RSA public key &gt; 3k for signing)</td>
</tr>
<tr>
<td>• TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (for DH and RSA prime and public key &gt; 3k for signing)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Policy enforced by CPPM based on new Radius attributes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Authenticator (Controller) indicates the Suite-B AKM was negotiated</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Suite-B compatible 802.1x happens between STA and CPPM</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 4-way Handshake and Key Derivation Function (KDF) use SHA384 with Suite-B AKM</td>
</tr>
</tbody>
</table>

### WPA3-Enterprise: Suite-B/CNSA

<table>
<thead>
<tr>
<th><strong>Suite-B capabilities advertised/negotiated in:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Beacons, Probe Responses, Association Requests</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Certificate chain improved testing and mandatory validation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Many WPA2-certificated devices did not properly check a certificate chain</td>
</tr>
<tr>
<td>• Results in insecurities</td>
</tr>
</tbody>
</table>

| **PMF is mandatory** |

| **OKC is supported** |

| **Only tunnel mode is supported on CAP and RAP** |
# Aruba Agora Tech 19

## Mobility Master WPA3-Enterprise Configuration

**Step 1:**
- Name (SSID): [Enter Name]
- Primary Usage: [Enter Usage]
- Broadcast: [Enable/Disable]
- Routing Mode: [Enter Mode]

**Step 2:**
- New WLAN:
  - General:
    - VLAN: [Enter VLAN]
- VL ANs:
  - Show VLAN Details

**Step 3:**
- Security:
  - Key Management:
    - 802.1x
  - Use VLAN:

**Step 4:**
- New WLAN:
  - General:
  - VLANs:
  - Security:
  - More Secure:

---

**What’s Next?**
Client Devices adoption of WPA3

Expected Transition time of ~2 years for critical mass adoption of WPA3 certified clients within Enterprises

• Very few WPA3 certified chipsets / clients today, increasing numbers expected from 2019
• Broadcom claims support for 11ax and WPA3 with their BCM4375 chipset powering Samsung S10
• Qualcomm with Snapdragon 855 chipset claims support for 11ax and WPA3
• Windows 10 19H1 update with tentative release in Spring 2019 might support WPA3
• Apple iOS ?? No info, TBD, could be new phones next year
• Linux supplicant code today (version 2.6) includes WPA3 support

WHAT DOES WPA3 MEAN TO YOU?

• 100% Encryption by default
  – Privacy before identity credentials
  – Encrypted walled gardens, coffee shops/bars

• New opportunities and longer lifespan for PSK
  – Combine with strong profiling
  – Basic IoT, Guest, BYOD, home

• Quantum-resistant enterprise SSID
  – Leverage strong SuiteB ciphers
  – If modern devices support it, leverage it

• Protected Management Frames

• Better security with no added complexity!
Obrigado