WPA3: Improve your Wi-Fi security

Security Challenges

WPA2 since 2004

- ❑WPA2-PSK : already broken on arrival
- ❑WPA2-Enterprise : Still secure but not so easy to implement

ill-suited security uses cases :

- ❑OPEN : Stadiums, Airports, Hotels, Guest portals
- ❑PSK : Coffee shops, restaurants, etc with a shared and public PSK

WPA3   **WPA2**

What’s new ?

- 1- **Enhanced Open – OWE** (Opportunistic Wireless Encryption) replaces Open
  - Problem: all wireless traffic is passed in clear
  - Solution: all wireless traffic gets encrypted

- 2a- **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
  - Optional Suite B /CNSA encryption improve the security level for WPA2-Enterprise

- Other improvements (EasyConnect, MPF …)

Enhanced Open

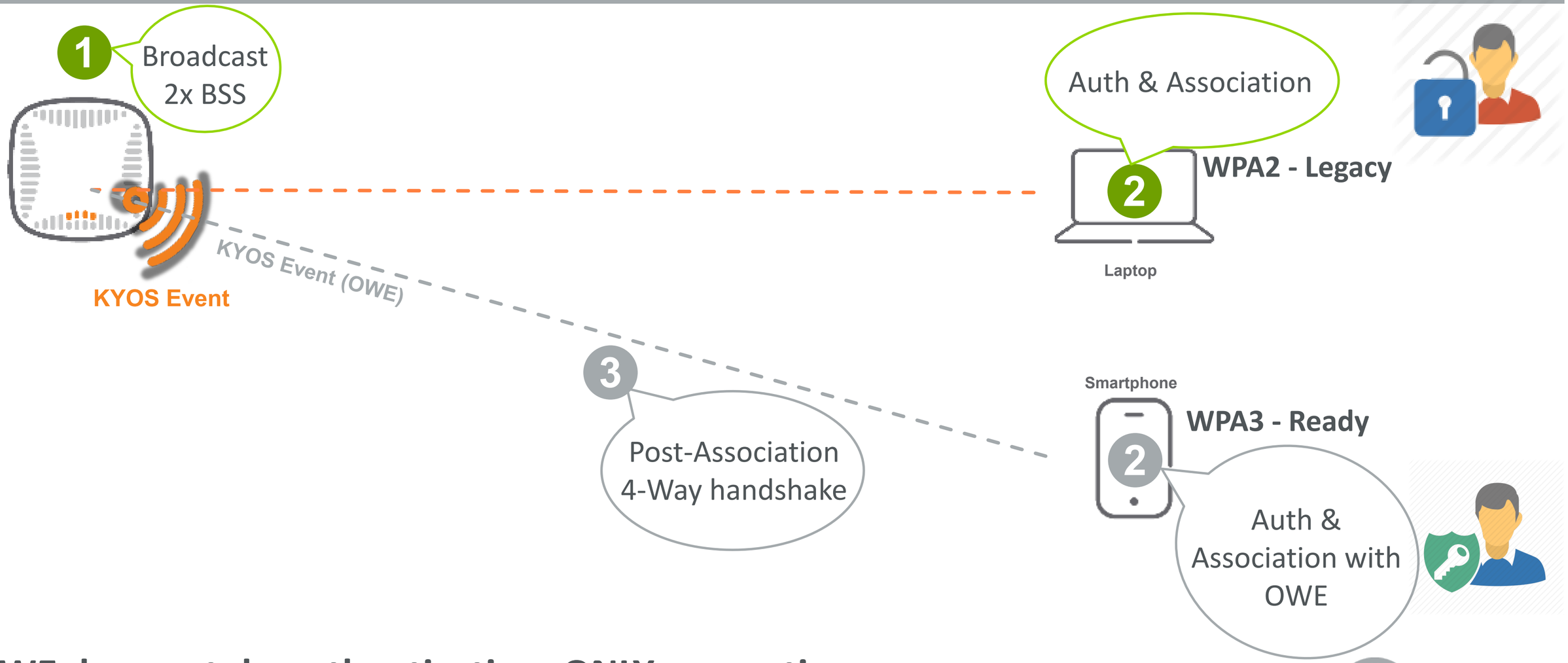
NO MORE CLEARTEXT !

- Based on Opportunistic Wireless Encryption (OWE) – RFC 8110
- Provides unauthenticated data encryption to Open Wi-Fi
- Transparent to users & admins
- Backward compatible to OPEN via Transition Mode

USE CASES :

- Coffee shops, schools, enterprises, airports, stadium
- Captive portal which throw away keys from HTTPS and then do Open 802.11

OWE Transition Mode



OWE does not do authentication, ONLY encryption

WPA3-Personal : **Strong Security from Weak passwords**

- WPA2-PSK is replaced by Simultaneous Authentication of Equals (SAE)
  - Password-based authentication based on Dragonfly key exchange (RFC 7664)
  - Resistant to active, passive, and dictionary attack
- SAE uses 802.11 authentication frames
  - Authentication generates a PMK, association indicates the PMKID
  - Post-association 4-way handshake generates traffic encryption keys
- SAE provisionning is identical to WPA2-PSK
  - User enters password just like always but gets improved security behind the scene

WPA3-Enterprise

- Opmode is essentially the same as WPA2-Enterprise with enforced PMF settings
- Enterprise client supporting 802.11w (PMF Capable) and legacy Enterprise client can connect to the same SSID
- ArubaOS 8.4 supports two WPA3-Enterprise modes:
  - WPA3-Enterprise Basic
  - WPA3-Enterprise Suite-B = Quantum-resistant
  - Only tunnel mode is supported on CAP and RAP

Devices compatibility

- ❑ Windows 10 in Spring 2019 (19H1 update)
- ❑ Linux supplicant code today (version 2.6)
- ❑ Apple IOS, no news… Maybe announced for the next Keynote
- ❑ Android Q (v10)

/!\ Samsung S10 support 802.11ax but not WPA3 for the moment (will be released in the next Android version)

Transition time estimated at ~ 2 years in Enterprises.

Aruba Support for WPA3

aruba
a Hewlett Packard Enterprise company

- Available with Aruba OS 8.4
- Compatible with Aruba AP-3xx series not on AP-1xx and AP-2xx

Wi Fi WPA3

NEW

Aruba 5xx series

kyos embedded security

To remember : **Better security with no added complexity**

- ❑ 100 % Encryption by default
  - Privacy before identity credentials
  - Encrypted walled gardens, coffee shops, airports, shops..
- ❑ Closing down known attack vectors
  - Dictionary attack no longer possible. Rainbow table attack tools also
  - Passive attack agains Hostpot not possible : passwords are now manageable
  - Mandatory PMF security prevents de-auth attacks
- ❑ Upgrade Enterprise SSID
  - Leverage strong SuiteB/CNSA ciphers – 256bits encryption
  - Robust approach

Contact us

Kyos SARL

Chemin Frank Thomas, 32
1208 Genève

Tel. : +41 22 566 76 30
Fax : +41 22 734 79 03

www.kyos.ch

info@kyos.ch

Suivre @KyosCH

Thanks

Camil KOUCHAD

kyos embedded security