airheads TECH TALK LIVE

aruba
a Hewlett Packard Enterprise company

Next Gen Wi-Fi Security: WPA3, Enhanced Open, DPP

Dan Harkins, Aruba

#ArubaAirheads

Agenda

- Why We're Here/WPA2 problems
- WPA3 Components
  - Enhanced Open: OWE
  - WPA3-Personal: SAE
  - WPA3-Enterprise and Suite B/CNSA
- Device Provisioning Protocol (DPP)
- Q&A

Wi-Fi Security As of Yesterday: WPA2

- **WPA2 was standardized in 2004**
  - When APs could not do heavy-weight cryptographic work
  - Wi-Fi was a PCMCIA card doing 11g– solely a last hop technology
- **Unforeseen from the horizon of 2004**
  - Captive portals
  - Wi-Fi everywhere! Planes, trains, automobiles, stadiums, the mall, coffee shops…
  - Wi-Fi as an entitlement… and an inducement to sit down, stay, and spend money
  - Rise of app-based services on client devices that rely on Wi-Fi
  - Wi-Fi being used to manage operations of large spaces (cameras, signage, PCI, etc)
- **Tools provided by WPA2 cannot meet current market needs**
  - WPA2-PSK– is flawed, imposes unreasonable requirements on users to address the flaw
  - WPA2-Enterprise– very complicated to provision, fragile, not supported by every device
- **Operators, service providers, enterprises, and users have to "make do"**
  - Tragic results naturally follow


Chermside!
Your WPA2
Secrity is SHIT!
Reagrds,
you will never know
REBEL
Valleygirl


Teplé nápoje - Hot Drinks - Wärme Trinken
0,25 l Čaj - Tea - Tee (dle nabídky/per daily offer) 25 Kč
0,2 l Horká hruška, jahoda, jablko, pomeranč 40 Kč
0,2 l Svařené víno - Mulled wine - Glühwein 55 Kč
0,2 l Grog - 0,4 cl Tuzemského rumu 55 Kč
7 g Turecká káva, espresso 35 Kč
7 g Káva a mléko - dle nabídky Piazza d´Oro 45 Kč
Free WiFi spot
Free Wi-Fi Hotspot
SSID: Hotel_Florenc
Heslo/password: 666F726469


Wi-Fi Access
marko
w3Lc0m3!!IFRE
W PASSWORD *****
s case-sensitive
"Forget" or "Remove"
CBS
THIS
MORNING
SUPER BOWL SECURITY
INSIDE SECRET, FIRST-OF-ITS-KIND COM

WPA3 & Enhanced Open: What Are They?
View from 10,000 meters…

- **Open is replaced by OWE– Opportunistic Wireless Encryption**
  - Problem: all wireless traffic is passed in the clear
  - Solution: all wireless traffic gets encrypted
- **PSK mode is replaced by SAE– Simultaneous Authentication of Equals**
  - Problem: passive attack results in off-line dictionary attack to discover PSK
  - Solution: protocol is resistant to active, passive, and dictionary attack
- **WPA3–Enterprise now provides for Suite B/CNSA grade ciphers**
  - Problem: mix-and-match nature of WPA2-Enterprise can result is less-than-optimal security
  - Solution: create a cipher suite and a set of rules to ensure consistent primitive security
- **Enhancements to certification testing**
  - Too many WPA2-Enterprise certified devices did not properly check certificate chains
  - Management frame protection, optional for WPA2, is mandatory for WPA3

Enhanced Open

aka Opportunistic Wireless Encryption (OWE)

Enhanced Open: No More Cleartext

- **Opportunistic Wireless Encryption (OWE) defined in RFC 8110**
- **OWE performs an unauthenticated Diffie-Hellman at association time**
  - Associate Request and Response exchange Diffie-Hellman public keys
  - STA and AP calculate a PMK as a result of association
  - PMK is used in 4-way handshake post association to generate traffic encryption keys
- **Unauthenticated, isn't that insecure?**
  - Strictly speaking yes, there are no assurances regarding who is connecting to what
  - But it's ***more secure*** than a shared and public PSK in a coffee shop!
  - Shared and public PSK means a passive attack gets traffic encryption keys, with OWE this is not possible
- **Completely transparent to users– looks just like Open, no provisioning**
- **Use cases:**
  - Coffee shops, bars, anywhere that encryption is needed but authentication is not
  - Captive portals which throw away keys from HTTPS and then do Open 802.11

How Does OWE Transition Mode Work?

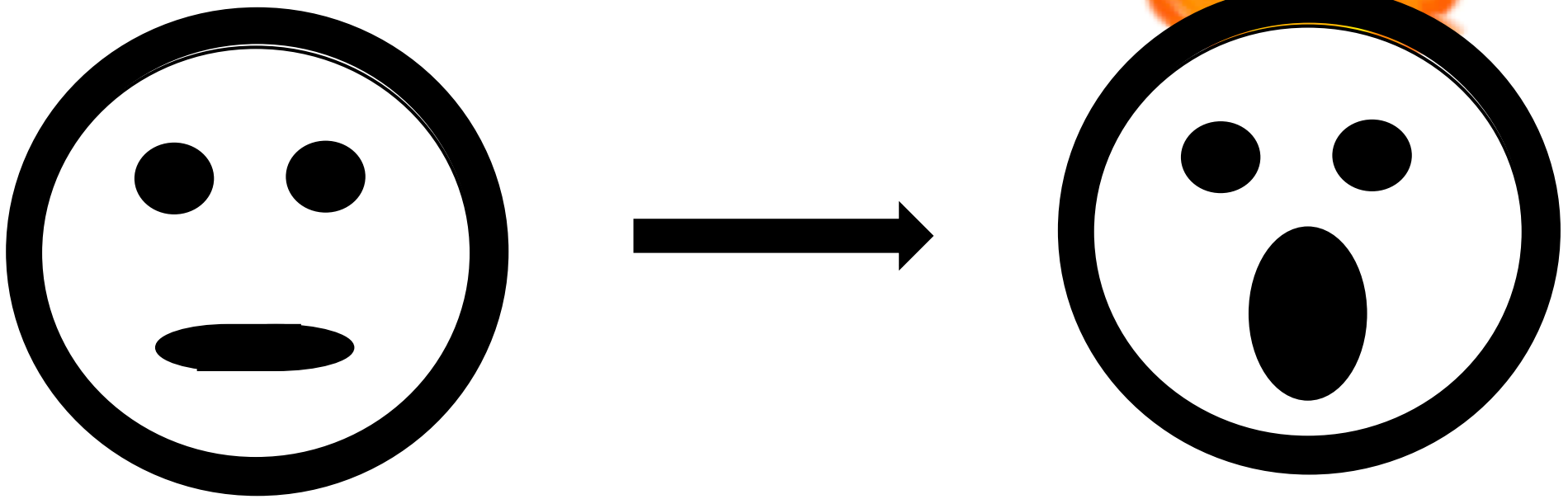
- **Advertisement and Discovery**
  - Administrator configures a single open SSID
  - AP automatically creates two BSSs and transmits two beacons
    - BSS1 = Normal “Open” network for non-OWE stations. New IE to indicate BSS2.
    - BSS2 = Hidden OWE RSN with AKM. New IE to indicate BSS1.
  - OWE STA does active or passive scanning to discover OWE-capable BSS
  - Non-OWE STA does active or passive scanning and connects to Open BSS
  - Yes, it sucks but *It Sucks Less*™ than the alternatives
- **Authentication and Association with OWE**
  - 802.11 “Open” Authentication
  - Diffie-Hellman Parameter element added to Association Request/Response
  - STA and AP derive a PMK (that is truly pairwise, unique, and unknowable by a third party) from ephemeral private key and other party’s public key
- **Post-Association with OWE**
  - STA and AP perform 4-way Handshake to derive Traffic Encryption Keys from PMK

Why Isn't OWE Part of WPA3?

The Natural Progression of Security Awareness

People don't care about security until they are forced to…

complete indifference



total panic

WPA3-Personal– SAE

strong security with passwords

“Passwords are like underwear: don’t let people see ‘em, change ‘em very often, and you shouldn’t share ‘em with strangers.”

- Chris Pirillo, blogger, on-line celebrity

WPA3-Personal: Strong Security from Simple Passwords

- **Problem with WPA2-PSK: off-line dictionary attack**
  - Susceptible to passive attack: adversary records 4-way handshake
  - Runs through all possible passwords– over 200,000 per second– to find right one
- **WPA2-PSK is replaced by SAE (802.11-2016, section 12.4)**
  - Originally intended for mesh security
  - Password-based authentication based on dragonfly key exchange
  - 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 provisioning is identical to WPA2-PSK**
  - User enters password just like always but under the covers gets improved security

How Does SAE Work?

- **Dragonfly Key Exchange is based on a zero knowledge proof**
  - Password indexes into a secret point (PWE) on an elliptic curve
  - Secret point is base of a cryptographic exchange
  - Each side must use the same base to arrive at the same secret
- **Passively observing SAE reveals nothing**
- **Active attack reveals whether a single guess of the password was correct or not**
- **Off-line dictionary attack is not possible**
- **Result of SAE is a key known by only 2 entities in the whole world: the client and the AP**
  - Provides forward secrecy even in the case where an attacker knows the password
- **SAE transition mode**
  - SAE AKM and PSK AKM on a single SSID– same password used for both
  - Cracking the password on PSK mode would enable it to be used with SAE
  - Even with a known password SAE provides forward secrecy so still better than just PSK

Off-line Dictionary Attack

WPA2-PSK versus WPA3-SAE

- **With WPA2-PSK the password is the master key in the 4-way Handshake**
  - If an attacker sees the 4-way handshake he has both nonces and both hashes, only thing missing is the password
  - Attacker runs through possible PSKs, hashing in the nonces, until a hash is verified--> voila! Found the password
- **Discrete logarithm problem: given *G* and $A = G^a$ it is computationally infeasible to determine *a***
  - What if the attacker doesn't know *G* and is just given *A*, he can't figure out either *G* or *a*!
  - With SAE the password is hashed into an elliptic curve to create a secret base (PWE)
- **With SAE, the attacker gets *(r + m)* and PWE^{-m} but knows none of those values**
  - If the prime, q, is 256 bits there are 2^{256} different possibilities of *r* and *m* that produce *(r + m) mod q*
  - Attacker doesn't know *PWE* and even if he did, figuring out *–m* is still computationally infeasible
  - At SAE *commitment* stage the attacker commits to a single value of *PWE* and therefore a single password guess
- **Attacker gets one guess at PWE per active attack, if guess is wrong the attack fails**
  - In other words, the attacker's gains an advantage through *interaction* and not *computation*
- **An off-line dictionary attack is not possible!**

Implication of Resistance to Dictionary Attack

- **Passwords need not be long, random, with special characters**
- **Doesn't mean passwords can be "weak"**
  - If you're password is passw0rd or abc123 you will still be attacked
- **Need to make the *interactions* necessary to attack SAE be massive**
  - Don't make your password a random selection of the 10 most popular passwords
  - Make your password be unguessable
- **Imagine a password that is a number randomly chosen between 1 and 1,000,000**
  - With WPA2-PSK that can be discovered in seconds, a probability of successful attack of 1
  - With WPA3-SAE it will take 500,000 active attacks before the probability even reaches 0.5
- **Password management and use is easier and more natural**
  - Humans have a hard time entering even moderately-sized strings consistently with a low probability of error
  - Unguessibility as a requirement means easily remembered and easily entered passwords can be used
- **The burden of security is not placed on the users anymore (where it never should've been!)**
- **Rainbow tables are completely useless**

Password Identifiers with SAE

- **Typical use of PSKs/passwords with WPA2-PSK and WPA3-SAE is a single PSK for the network…**
  - For APs anyone who knows the PSK gets access to the network
  - Everyone gets the same authorization treatment
- **…or, more rarely, assigning a PSK to each MAC address**
  - Each client has a (possibly unique) PSK, provides authorization but poses scaling difficulties
  - When more clients start randomizing MAC addresses this is not viable
- **This poses some deployment problems**
  - Multiple SSIDs are needed to support user groups, each with their own PSK. This produces beacon bloat and uses airtime.
  - If PSKs are assigned based on MAC address (e.g. MPSK), the AP as well as the device need provisioning which makes adding new devices more time consuming and scales poorly
  - To have a viable authorization solution it is necessary to do 802.1X/EAP which requires a trust root to use properly and not all devices support 802.1X/EAP

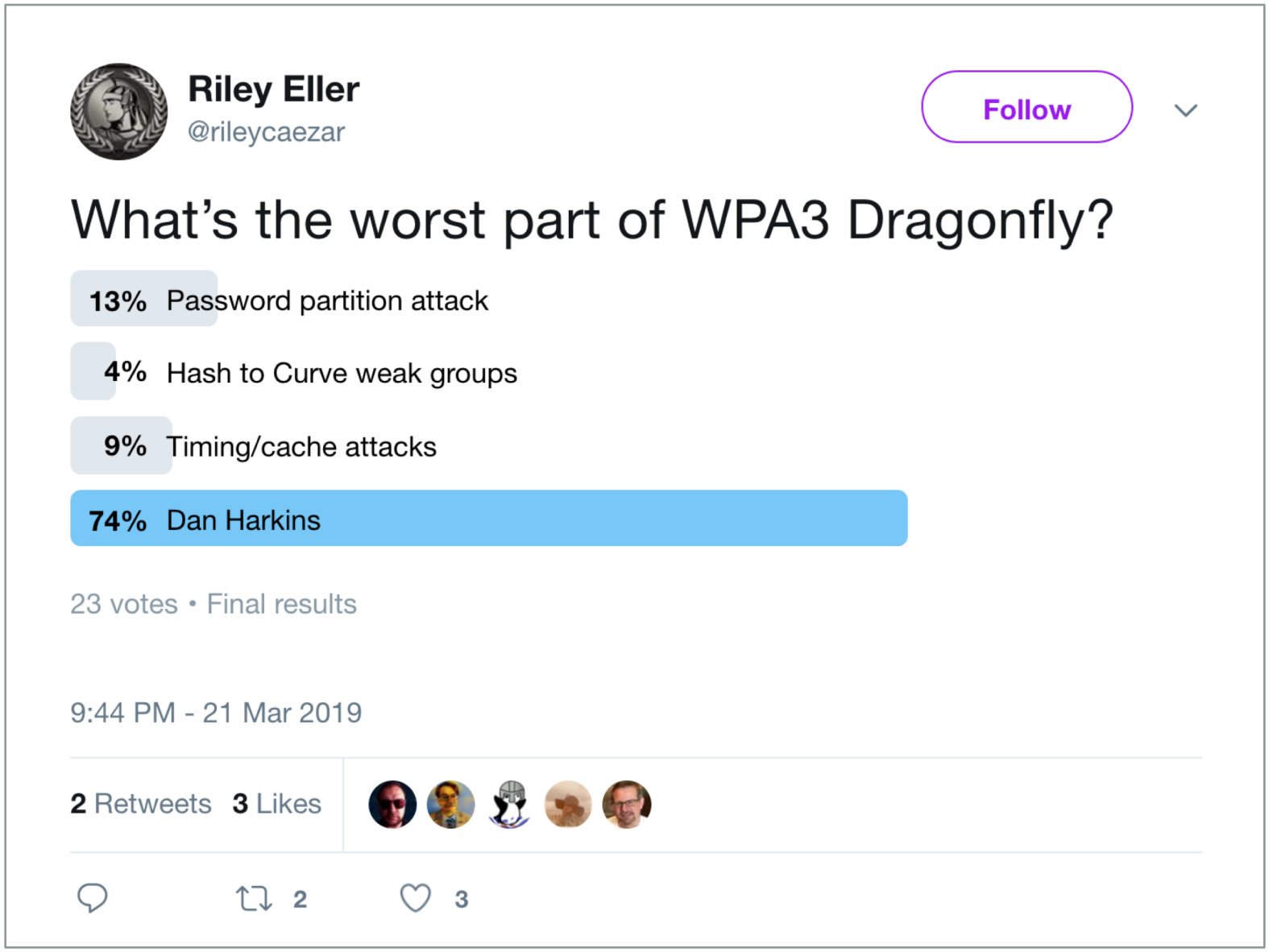
Password Identifiers with SAE

- **Password Identifiers are part of 802.11 today**
  - A password can have an arbitrary string associated with it, sort of like a username. There can still be a “fallback” password analogous to what we have today
  - Each password/identifier can be assigned a VLAN (or any other authorization treatment, like access-control list assignment) all on a single SSID
  - No need to store a PSK for every single device on the AP/controller, just store a PSK per group
  - No need to touch the AP/controller when a new device is added– just give the new device the identifier and password
- **Password Identifiers will be part of WPA3 certification… *Real Soon Now*™**
- **New deployments possible**
  - Multi-tenant building has Wi-Fi provided as a service, one single SSID for the entire complex– e.g. dormitories at a university. Each dorm room gets its own unique password and identifier. Occupants are responsible for provisioning personal devices. Roaming works, devices continue to stay on their network as they roam.
  - Home network segmentation– have one password for the children and guests, another password for the home office (access to the printer, etc), another for sensitive IoT devices like the thermostat, alarm system, cameras, etc.
  - Small office can provide encrypted guest access with a single SSID– one password for workers, a different one for guests– with no 802.1X/EAP necessary

Dragonblood– Analysis of WPA3-SAE

- **DOS protection**– technique provided by SAE is inadequate to deal with DOS attack (anything more sophisticated than simple packet spraying)
  - APs should limit the number of nascent connections it allows and perform SAE operations on “slow” queue
- **Small sub-group attack**– there are 3 known weak MODP groups that are unacceptable for use with SAE (or for anything for that matter)
  - There are actually 20 groups in the IANA registry that should not be used. These 3 are well-known to be weak and are unsuitable for really any purpose
- **Group downgrade**– there is no protection against an attacker rejecting offers until a weak group is offered
  - STAs should only offer groups whose strength is commensurate with the cipher it will be using post authentication
- **Transition mode attack**– since WPA2-PSK and SAE use the same password it is possible to attack the WPA2-PSK side
  - This is not an attack on WPA3 and even with a known password SAE provides forward secrecy
- **Cache attack/password portioning**– the hash-to-curve technique in one implementation did not use constant-time operations to test quadratic residuosity
  - This is a serious attack but it is an attack against an implementation not against the standard. It has already been patched in the code repository of that implementation

WPA3 SAE (dragonfly)… what's the worst part?!



WPA3-Enterprise
and Suite B/CNSA

WPA3-Enterprise vs WPA2-Enterprise

- **Fundamentally the same– 802.1X/EAP-based authentication, authorization, and accounting**
- **What's different for AP/Controller?**
  - Management frame protection is mandatory
  - *Transition Mode* consists of advertising PMF-Capable: WPA3 clients will connect with PMF and WPA2 clients will connect without PMF
- **What's different for Clients?**
  - Management frame protection is mandatory
  - Certificate validation checks and certificate chain validation

- **That's *IF* you're not doing Suite B/CNSA….**

WPA3-Enterprise: Upgrade to SuiteB/CNSA

- **Too many options for WPA2-Enterprise, especially for EAP authentication**
  - Diffie-Hellman or RSA key exchange? 1024-bit signature authenticating 3072-bit Diffie-Hellman? TLS1.0? SHA1?
  - This can result in deployments that are not as secure as might be imagined
  - Clients may connect with varying degrees of security
- **Suite B/CNSA provides for a consistent level of security for the entire network**
- **Requires Suite B TLS ciphersuites (RFC 6460) to be used in EAP-TLS**
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 using p384; or,
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 using p384 and RSA > 3k; or,
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 using RSA > 3k
- **Policy is enforced by EAP server based on new RADIUS attributes**
  - Authenticator indicates the AKM negotiated between client and AP
  - RADIUS server only negotiates Suite B/CNSA TLS when the AKM indicates Suite B/CNSA
- **4-way Handshake and KDF use SHA384, Pairwise cipher is GCM-256 or CCM-256**
- **Requires a flag day in order to deploy– Suite B/CNSA is exclusive to all other AKMs**
- **Brings 256-bit encryption to Enterprise security even without Suite B/CNSA**

WPA3: An Upgrade to Wi-Fi Security

- **More Useful Tools to Provide Security for Today's Wi-Fi Networks**
  - Unauthenticated encryption of the air with *OWE*
  - Password exchange that is resistant to active, passive, and dictionary attack with *SAE*
  - 256-bit encryption (requires support by client devices)
- **Fixes Known Flaws, Closes off Known Attack Vectors**
  - No more unencrypted networks, even open gets encryption
  - PSK exchange is secured, easy-to-remember-and-manage passwords are possible
  - Everything is now protected, even management frames
- **Addresses Modern Use Cases**
  - Captive-portal– encrypt captive portal access, bind encryption keys to authentication
  - Coffee shop/bar/restaurant– no more PSKs written on a menu/chalkboard
  - IoT/CPU-limited devices can securely connect with a simple password
- **Coming soon– Password Identifiers**
  - Lets groups of users share a unique password and get unique authorization treatment
  - Single SSID can support multiple groups of users, all segregated from each other

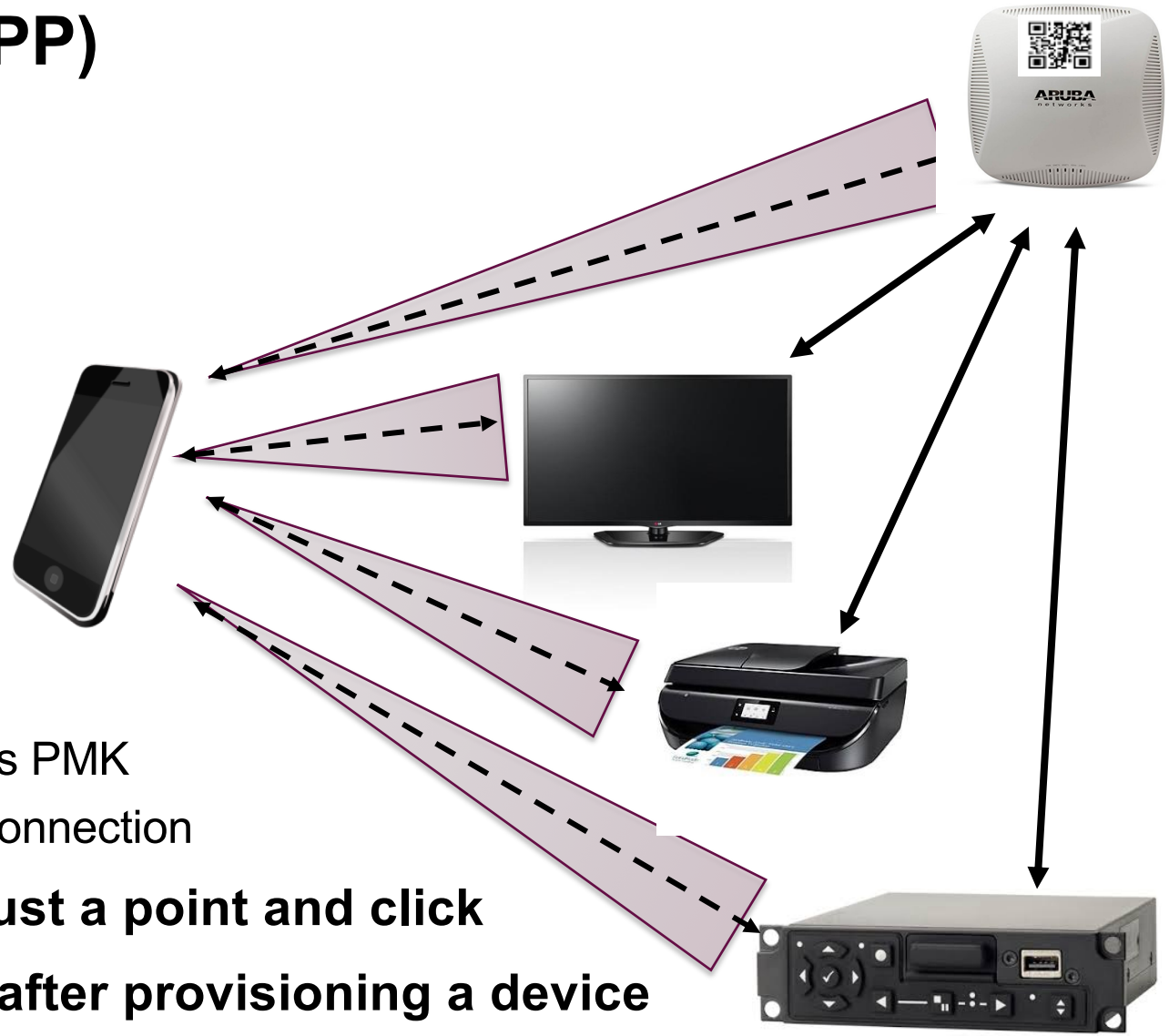
Device Provisioning Protocol

How does DPP Work?

- **Two players– Initiator and Responder– in one of two roles– Configurator or Enrollee**
- **Four phases in DPP: bootstrapping, authentication, provisioning, network connection**
- Bootstrapping– Gaining trust in the public key of an unknown and unauthenticated device
  - Typically a CA does this but in DPP there is no CA
  - Bind a device to its public key such that the public key becomes its identifier and the device proves who it is by using the corresponding private key
  - Different ways to bootstrap: QR codes, PKEX (shared key), NFC (proximity), cloud, …
- Authentication– Using the trusted, bootstrapped, key to ensure the right device is being spoken to
  - Responder proves possession of private analog to bootstrapping public key
  - Allows for mutual authentication and a form of non-mutual authentication that retains a degree of trust
- Provisioning– Authenticated Enrollee requests provisioning, Configurator does provisioning
- Network Access– A DPP-provisioned device communicates with another DPP-provisioned device
  - Each device exchanges a *Connector*– a devices network access key signed by the Configurator
  - Devices do a Diffie-Hellman with each other's *Connectors* to derive a Pairwise Master Key (PMK)

Device Provisoning Protocol (DPP)

- **Configurator defines network (SSID, etc)**
- **Enrollees get configured**
  - Access Point is provisioned as “ap”
  - TV is provisioned as “sta”
  - Printer is provisioned as “sta”
  - DVR is provisioned as “sta”
- **Devices connect to DPP network on AP**
  - AP advertises a new AKM
  - Device exchanges connectors with AP, generates PMK
  - Device associates, 4-way handshake, secured connection
- **Additional devices are provisioned with just a point and click**
- **Configurator not involved in the network after provisioning a device**



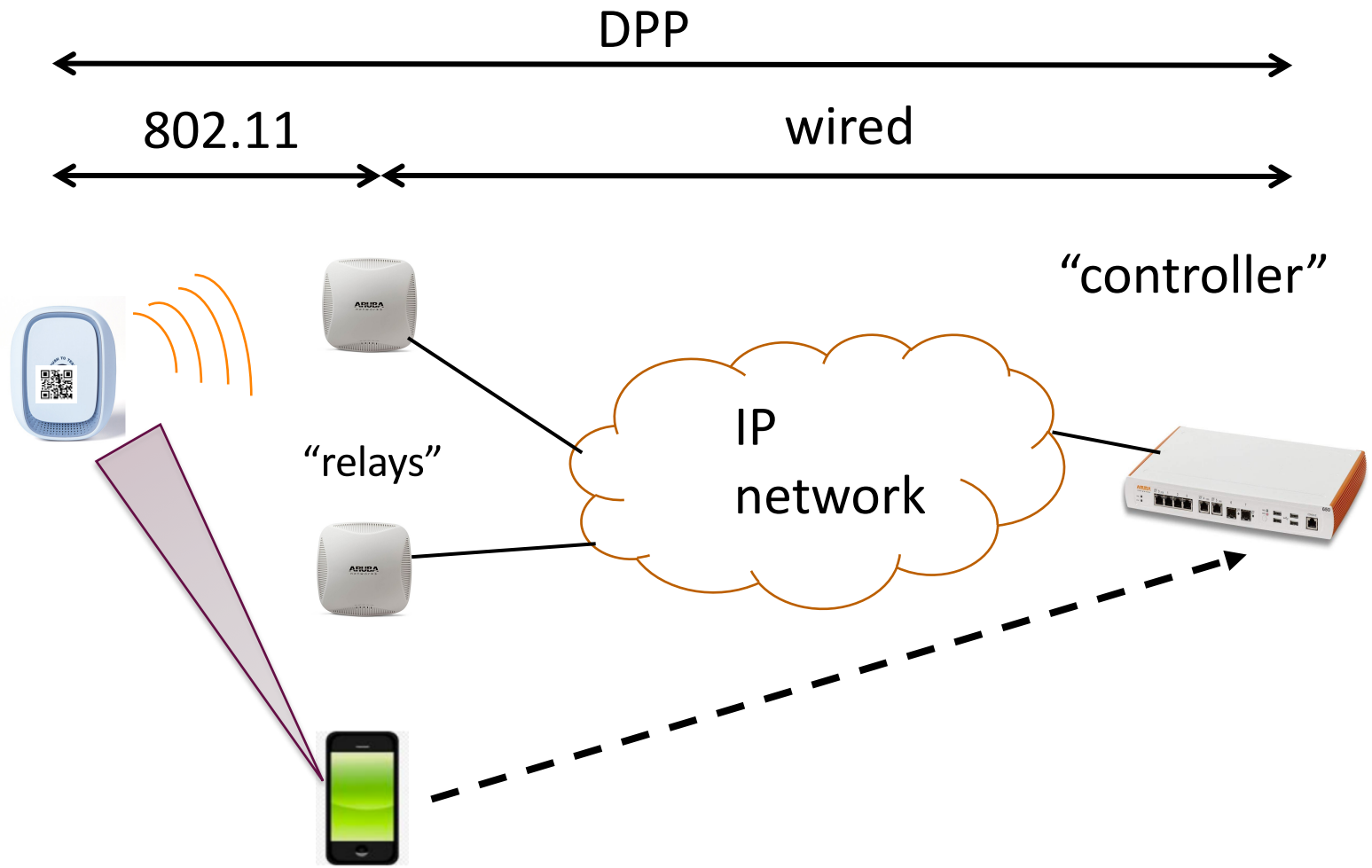
Why is DPP Better than the Alternatives?

- **Misuse-resistant**
  - Pointing a camera at a QR code is hard to get wrong, entering a shared key (PKEX) is either right or wrong and failure is the only result if it's wrong
  - All options are handled in the protocol without user interaction
  - Minimum of user interaction
- **Does not require EAP!**
  - Extraneous layering and abstraction is not necessary
  - Previous solutions, such as WPS, created an EAP method that had issues with integration into existing state machines
- **No insecure and clumsy soft-AP needed**
  - No leap of faith
  - No configuration of security credentials on open soft-AP network
  - All DPP messages are done with pre-association 802.11 Action frames
- **Addresses unique use cases unsupported by alternatives**

Why is DPP Better than the Alternatives?

- **DPP can run over a wired connection**
  - Allows a switch/controller/concentrator to act as a Configurator
  - Allows for entirely non-Wi-Fi DPP conversation (e.g. 4G) to obtain Wi-Fi credentials
  - Adapts to more use cases
- **Role flexibility to match use cases**
  - Initiator can be the Enrollee or the Configurator
  - Adapts to more use cases
- **Support for batch provisioning**
  - Scan a multitude of QR codes, stage devices for provisioning
- **Different bootstrapping methods**
  - No one-sized-fits-all approach
  - Protocol adapts to use, not other way around

How is Aruba Implementing DPP?



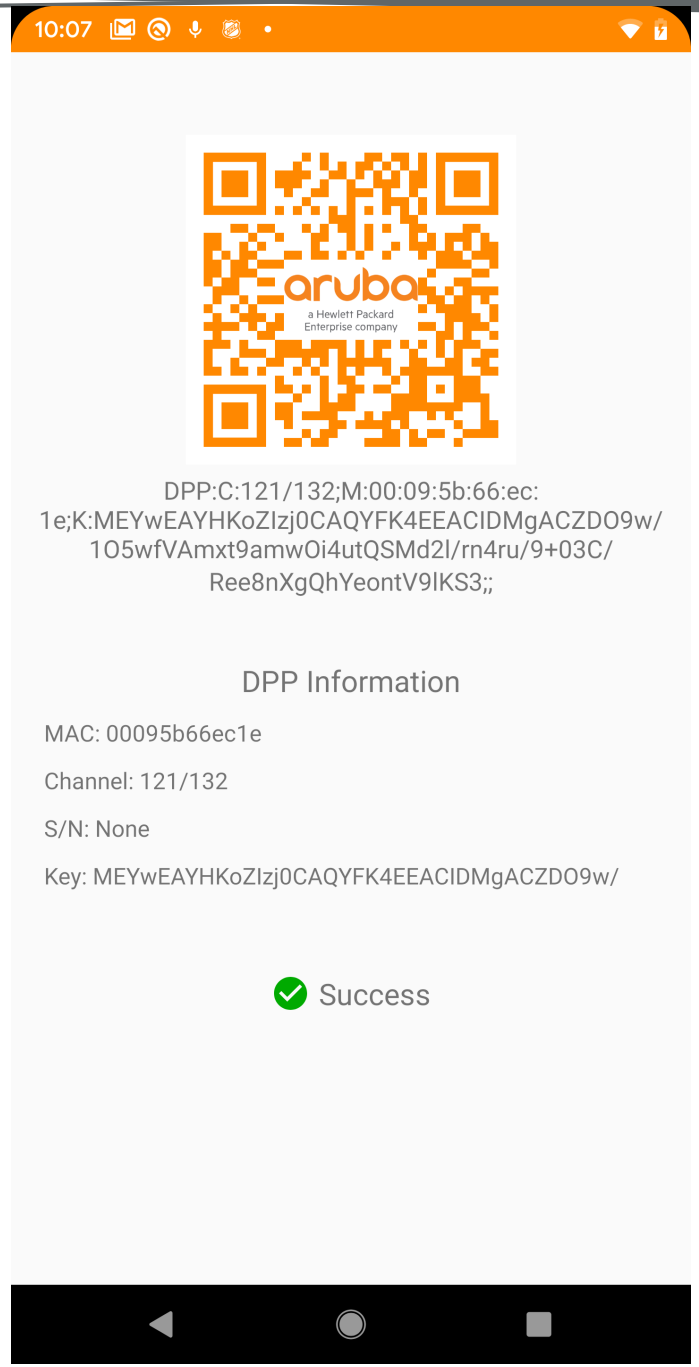
- **Aruba app running on handheld**
  - Scans QR code of IoT device
  - Sends bootstrapping URI info to Controller
- **DPP over wired**
  - Controller acting as Configurator
  - Relays merely encaps/decaps frames to convert between 802.11 and TCP
  - Controller initiates DPP to device
  - Device is provisioned into role, given connector credential
- **IoT device connects to network**
  - Discovers AP advertising DPP network
  - Performs DPP Network Access protocol
  - Derives PMK/PMKID
  - Performs 4way handshake
  - Securely connected!

How Is Aruba Implementing DPP?

Aruba Configurator APP

- User logs in to account
- Scans DPP QR code
- Bootstrapping data uploaded
- Controller provisioned
- DPP initiated

Provisioned device automatically joins DPP network



WPA3 and DPP: An Upgrade to Wi-Fi Security

- **More Useful Tools to Provide Security for Today's Wi-Fi Networks**
  - Unauthenticated encryption of the air with *OWE*
  - Password exchange that is resistant to active, passive, and dictionary attack with *SAE*
  - 256-bit encryption (requires support by client devices)
- **Fixes Known Flaws, Closes off Known Attack Vectors**
  - No more unencrypted networks, even open gets encryption
  - PSK exchange is secured, easy-to-remember-and-manage passwords are possible
  - Everything is now protected, even management frames
- **Addresses Modern Use Cases**
  - Captive-portal– encrypt captive portal access, bind encryption keys to authentication
  - Coffee shop/bar/restaurant– no more PSKs written on a menu/chalkboard
  - IoT/CPU-limited devices can securely connect in a simple, secure, and scalable manner
- **Coming soon– Password Identifiers**
  - Lets groups of users share a unique password and get unique authorization treatment
  - Single SSID can support multiple groups of users, all segregated from each other

Questions?

aruba
a Hewlett Packard Enterprise company

airheads TECH TALK LIVE

Thank You