

Evolution of WLAN Security



David Coleman

Director of Product Marketing

Extreme Networks

Who is this guy?

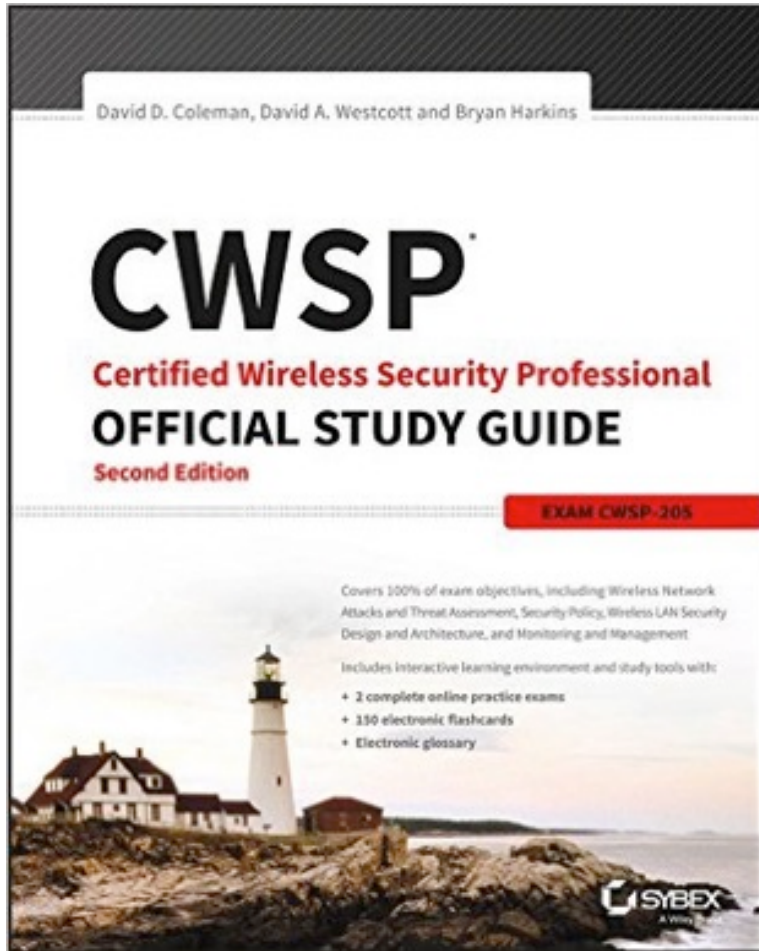
Extreme Networks
Director of Product Marketing

 [@mistermultipath](https://twitter.com/mistermultipath)



FEATURING
DAVID COLEMAN
CWNE #4

Co-Author - Sybex CWSP Security Guide – 2nd edition



Amazon: <http://bit.ly/CWSPv2>

Topics

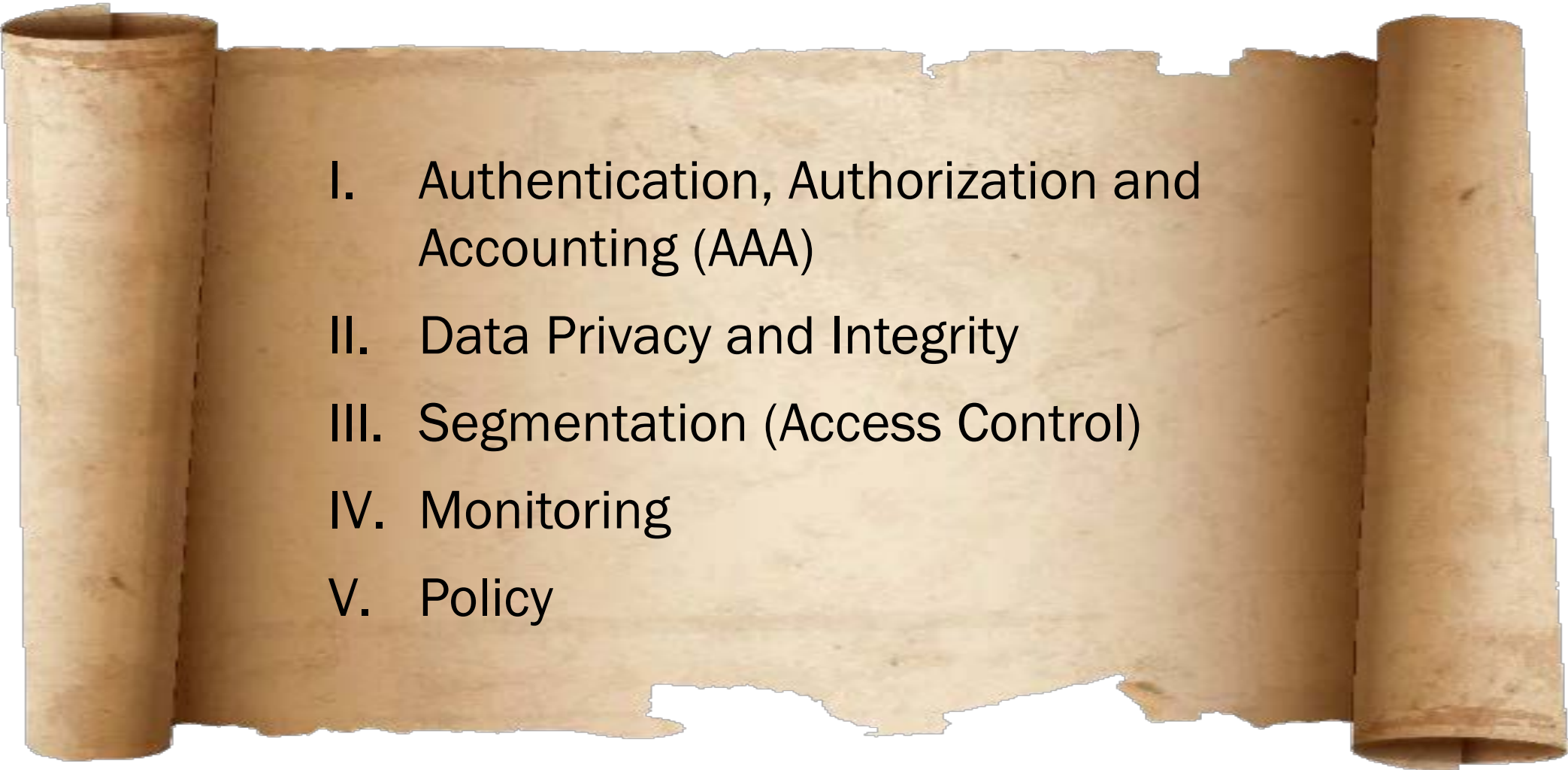
- History of Wi-Fi security
- Five Tenets of WLAN security
- Real-world caveats of Wi-Fi security
- WPA3
- Challenges and Future of WLAN security

802.11 security standards and certifications

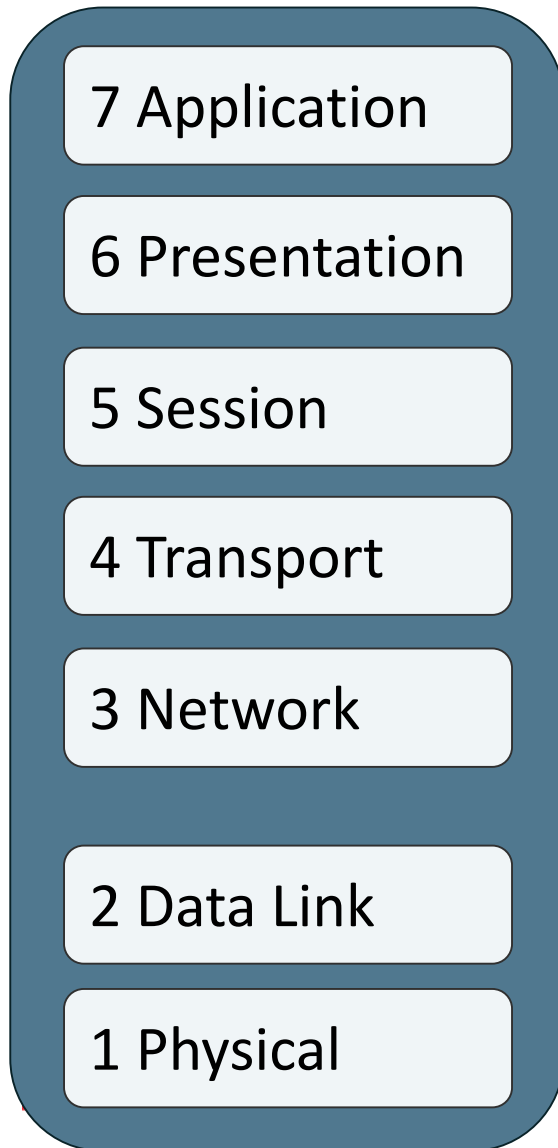
IEEE	IEEE	Wi-Fi Alliance	Encryption Method	Cipher	Key Generation
Legacy		Open	WEP	ARC4	Static
Pre-802.11i	WPA- Personal	PSK	TKIP	ARC4	Dynamic
Post-802.11i	WPA- Enterprise	802.1X	TKIP	ARC4	Dynamic
Post-802.11i	WPA-2 Personal	PSK	CCMP	AES	Dynamic
Post-802.11i	WPA-2 Enterprise	802.1X	CCMP	AES	Dynamic



Five tenets of WLAN security

- 
- I. Authentication, Authorization and Accounting (AAA)
 - II. Data Privacy and Integrity
 - III. Segmentation (Access Control)
 - IV. Monitoring
 - V. Policy

Wi-Fi security and the OSI model



- OSI Model
- Remember that Wi-Fi operates at Layer 1 and the MAC sublayer of Layer 2
- **Robust Security Network (RSN)** security mechanisms operate at the MAC sublayer

← **WLAN Security**

AAA

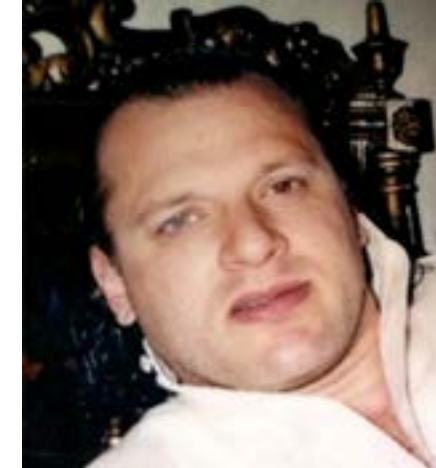
- **Authentication:** Validate user/device identity
- **Authorization:** Authorize user/device identity
- **Accounting:** Paper trail

- Wi-Fi is a wireless portal into corporate networks

Validating identity is important!

David Coleman

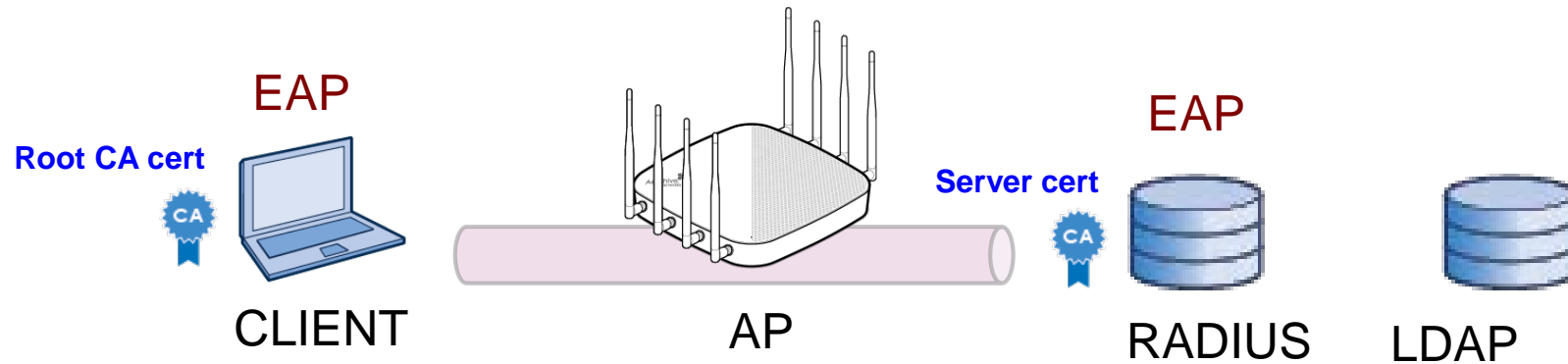
- Wi-Fi Geek
- Born February 1960



David Coleman Headley

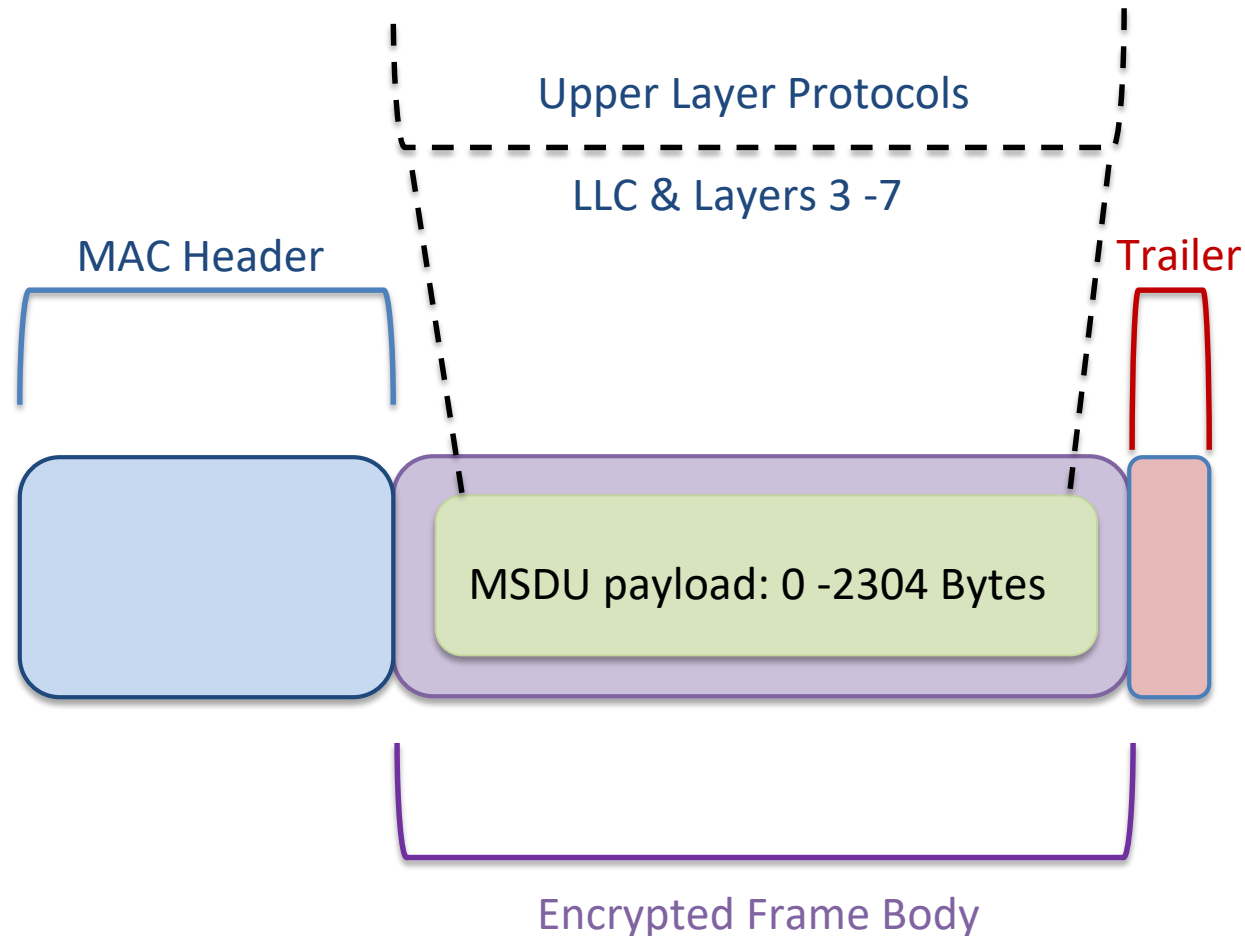
- Convicted terrorist
- Born June 1960

Authentication – 802.1X/EAP



- 802.1X: Port based access control
- Authorization Framework
 - Supplicant
 - Authenticator
 - Authentication Server
- Integrates with LDAP
- Extensible Authentication Protocol (EAP)
 - Server certificate and Root CA certificate
 - Tunneled authentication using SSL/TLS

Encryption

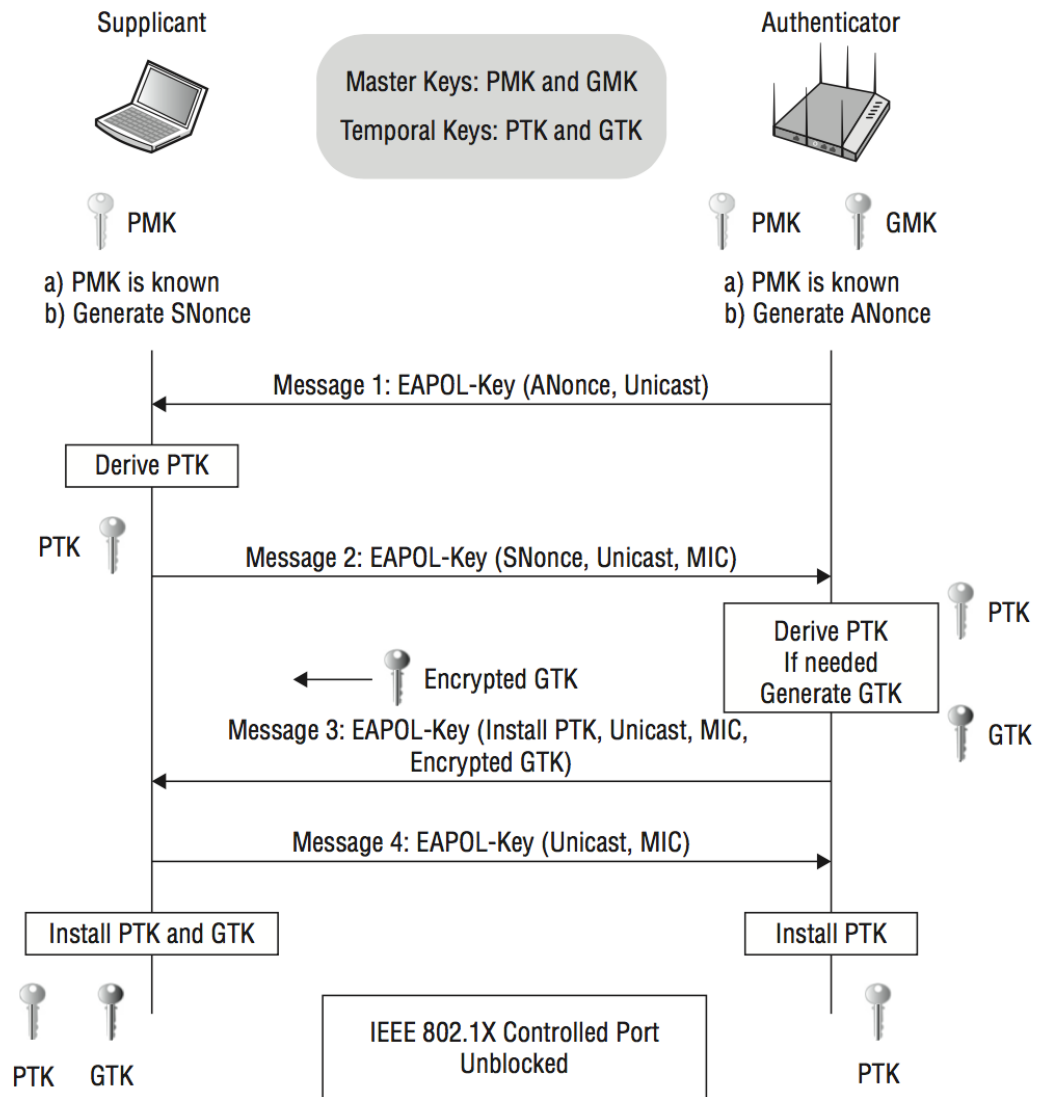


- Encapsulated inside the frame body of an 802.11 data frame is an upper-layer payload called the **MAC service data unit (MSDU)**.
- The MSDU contains data from the Logical Link Control (LLC) and layers 3–7.
- When encryption is enabled, the MSDU payload within an 802.11 data frame is encrypted.

Dynamic Key Encryption Generation

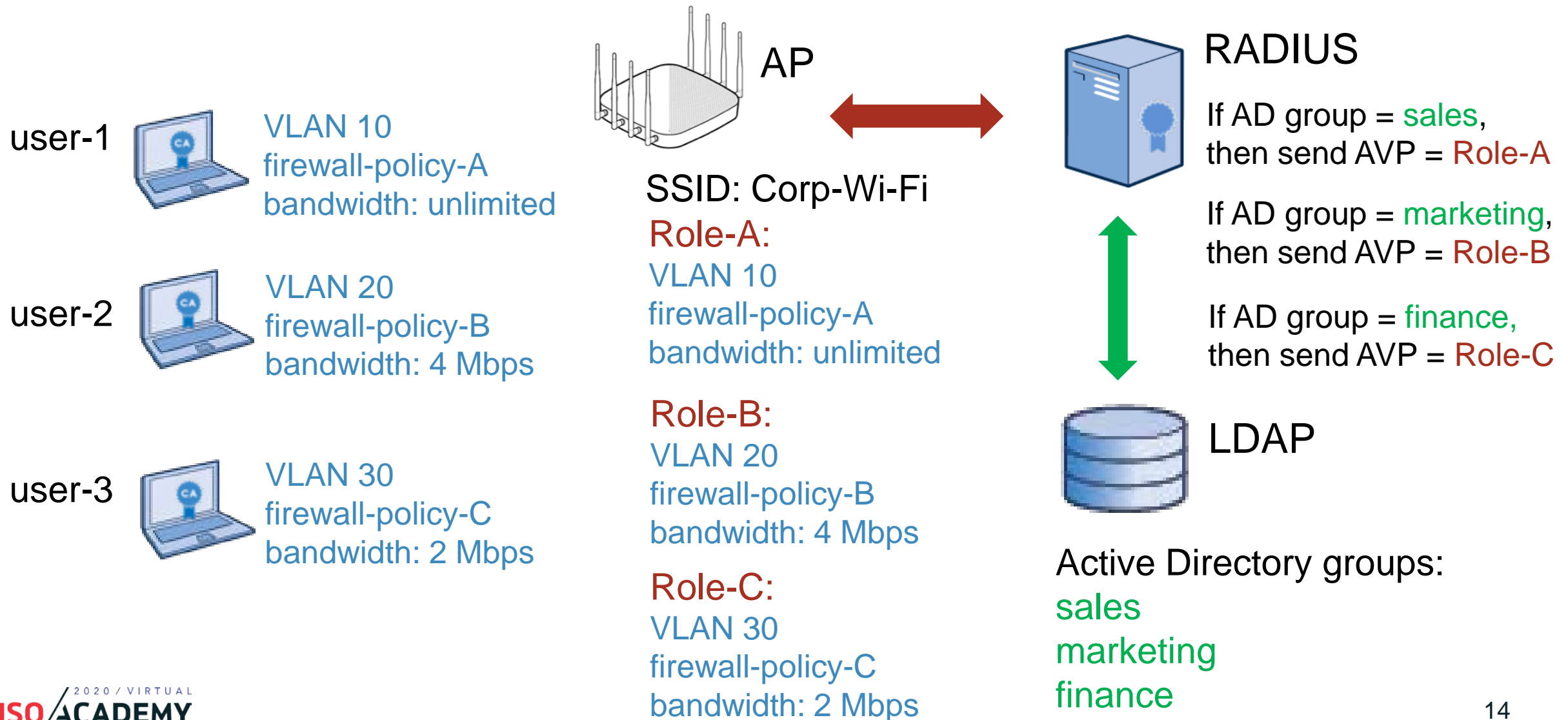
- There is a **symbiotic relationship** between **PSK/802.1X authentication** and the generation of dynamic encryption keys.
- An outstanding by-product of **802.1X/EAP** can be the generation and distribution of dynamic encryption keys.
- Dynamic encryption keys can also be generated as a by-product of **PSK authentication**.
- Encryption and authentication are tied to each other in a **Robust Secure Network Association (RSNA)**.

4-Way Handshake

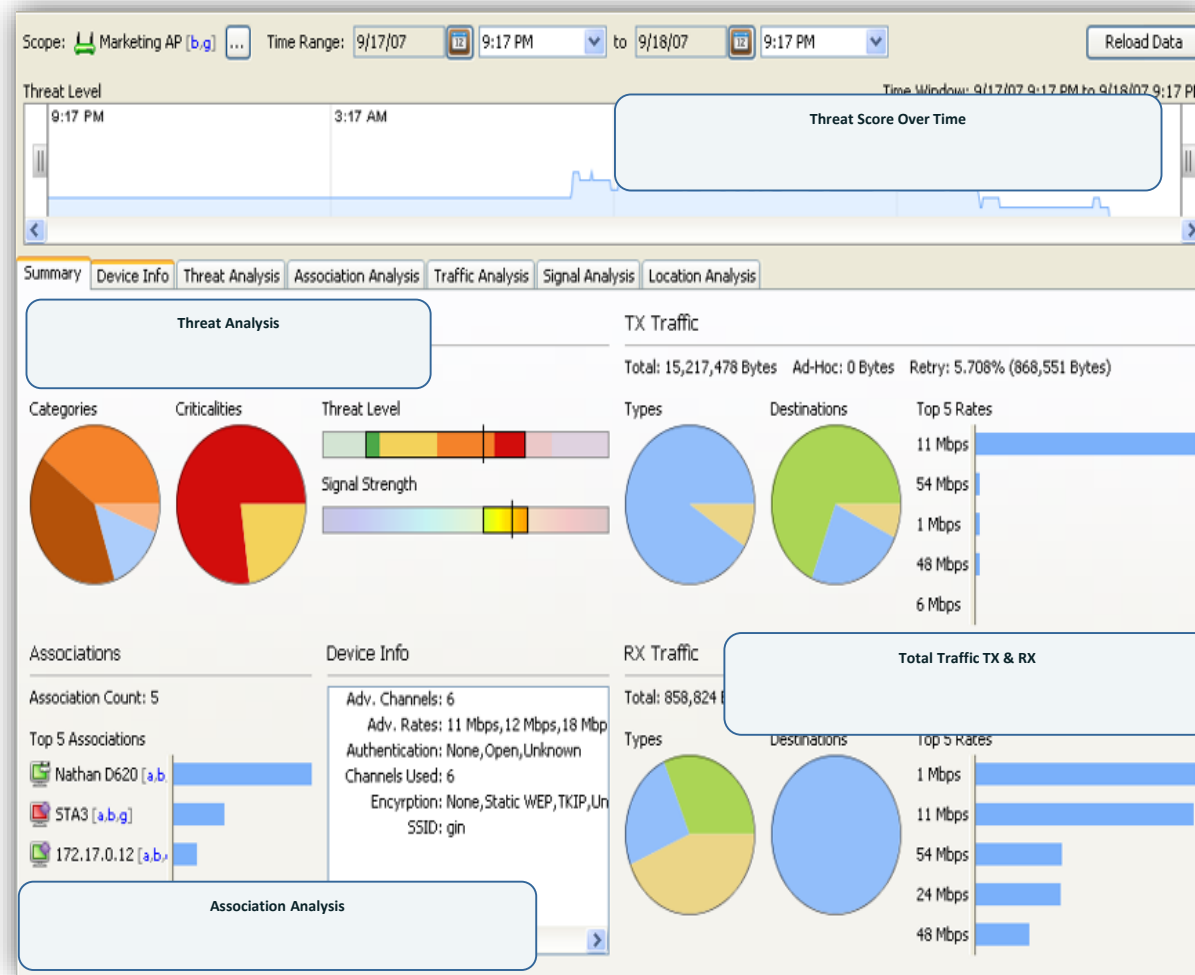


- EAP protocols that utilize mutual authentication provide “seeding material” that can be used to generate encryption keys dynamically.
- To create the pairwise **transient key (PTK)**, the **4-Way Handshake** uses a pseudo-random function that combines the following:
 - Pairwise Master Key (PMK)
 - Numerical authenticator nonce
 - Numerical supplicant nonce
 - Authenticator’s MAC address (AA)
 - Supplicant’s MAC address (SPA)

Role -based access control (RBAC)



Monitoring - WIPS



- Very often, the WLAN vendors' WIPS solution was just enough to “check-a-box” in a request-for-proposal (RFP).
- Sadly, in many cases, WIPS security is now just an after-thought.

Extreme AirDefense: <https://www.extremenetworks.com/extreme-networks-blog/extreme-networks-wireless-security-jewel-airdefense/>

Policy

- General policy
 - Statement of Authority
 - Audience
 - Violation reporting procedures
 - Risk assessment & threat analysis
 - Security auditing
- Functional policy
 - Baseline practices
 - Monitoring and response



Human beings are always the weakest link

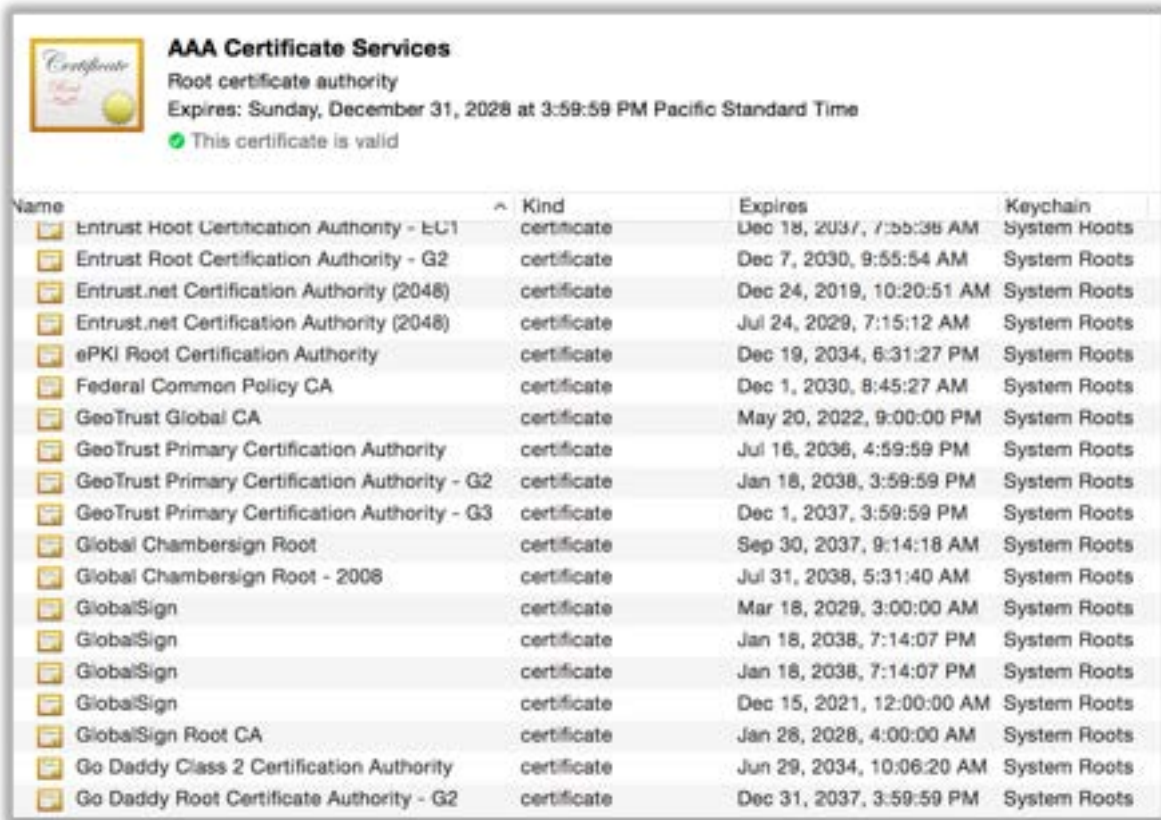
Policy – Penetration Testing



www.wifipineapple.com

- A popular WLAN auditing tool is **Wi-Fi Pineapple** from Hak5.
- Wi-Fi Pineapple consists of custom, purpose-built hardware and software, enabling its users to quickly and easily deploy advanced attacks using an intuitive web interface.

Real-World Caveats – 802.1X – Server certificate

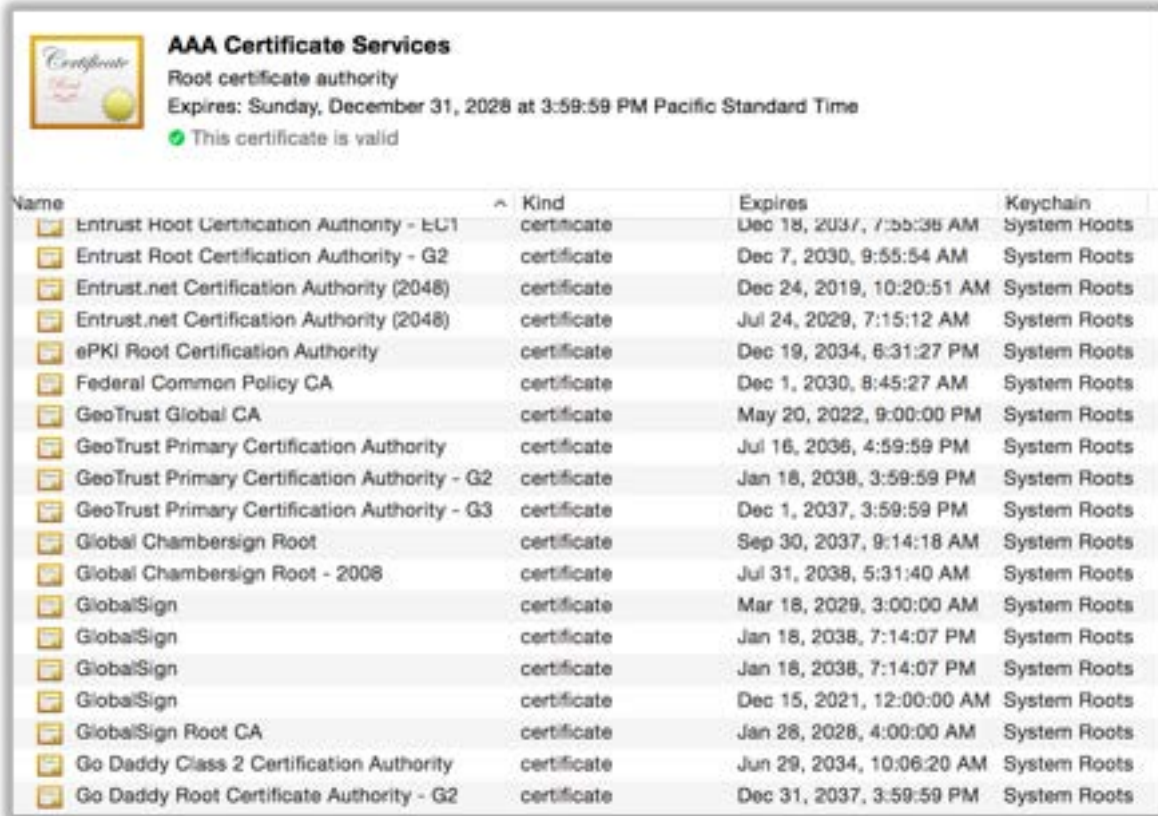


AAA Certificate Services
Root certificate authority
Expires: Sunday, December 31, 2028 at 3:59:59 PM Pacific Standard Time
This certificate is valid

Name	Kind	Expires	Keychain
Entrust Root Certification Authority - EC1	certificate	Dec 18, 2037, 7:55:38 AM	System Roots
Entrust Root Certification Authority - G2	certificate	Dec 7, 2030, 9:55:54 AM	System Roots
Entrust.net Certification Authority (2048)	certificate	Dec 24, 2019, 10:20:51 AM	System Roots
Entrust.net Certification Authority (2048)	certificate	Jul 24, 2029, 7:15:12 AM	System Roots
ePKI Root Certification Authority	certificate	Dec 19, 2034, 6:31:27 PM	System Roots
Federal Common Policy CA	certificate	Dec 1, 2030, 8:45:27 AM	System Roots
GeoTrust Global CA	certificate	May 20, 2022, 9:00:00 PM	System Roots
GeoTrust Primary Certification Authority	certificate	Jul 16, 2036, 4:59:59 PM	System Roots
GeoTrust Primary Certification Authority - G2	certificate	Jan 18, 2038, 3:59:59 PM	System Roots
GeoTrust Primary Certification Authority - G3	certificate	Dec 1, 2037, 3:59:59 PM	System Roots
Global Chambersign Root	certificate	Sep 30, 2037, 9:14:18 AM	System Roots
Global Chambersign Root - 2008	certificate	Jul 31, 2038, 5:31:40 AM	System Roots
GlobalSign	certificate	Mar 18, 2029, 3:00:00 AM	System Roots
GlobalSign	certificate	Jan 18, 2038, 7:14:07 PM	System Roots
GlobalSign	certificate	Jan 18, 2038, 7:14:07 PM	System Roots
GlobalSign	certificate	Dec 15, 2021, 12:00:00 AM	System Roots
GlobalSign Root CA	certificate	Jan 28, 2028, 4:00:00 AM	System Roots
Go Daddy Class 2 Certification Authority	certificate	Jun 29, 2034, 10:06:20 AM	System Roots
Go Daddy Root Certificate Authority - G2	certificate	Dec 31, 2037, 3:59:59 PM	System Roots

- 802.1X requires a server cert signed by a CA
- The simple method is to purchase a server certificate from a **trusted root Certificate Authority (CA)** such as GoDaddy (www.godaddy.com) or Verisign (www.verisign.com)

Real-World Caveats – 802.1X

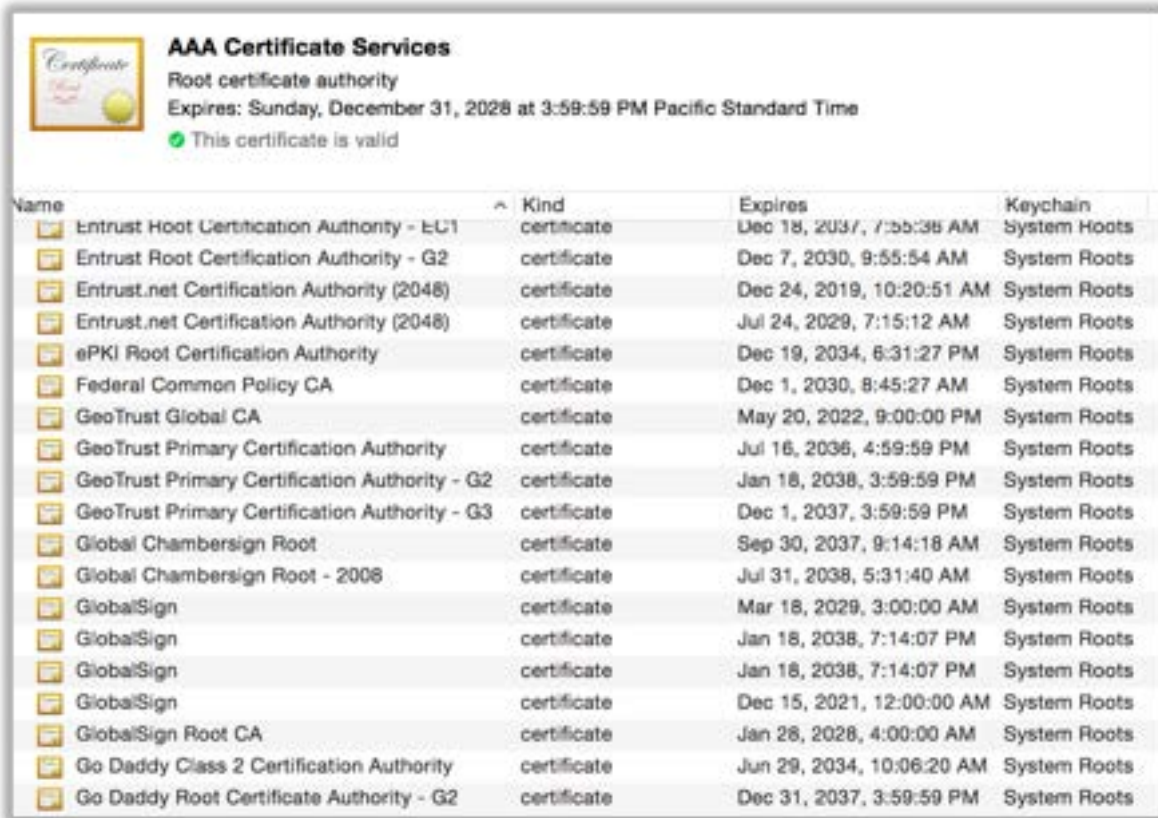


AAA Certificate Services
Root certificate authority
Expires: Sunday, December 31, 2028 at 3:59:59 PM Pacific Standard Time
This certificate is valid

Name	Kind	Expires	Keychain
Entrust Root Certification Authority - EC1	certificate	Dec 18, 2037, 7:55:38 AM	System Roots
Entrust Root Certification Authority - G2	certificate	Dec 7, 2030, 9:55:54 AM	System Roots
Entrust.net Certification Authority (2048)	certificate	Dec 24, 2019, 10:20:51 AM	System Roots
Entrust.net Certification Authority (2048)	certificate	Jul 24, 2029, 7:15:12 AM	System Roots
ePKI Root Certification Authority	certificate	Dec 19, 2034, 8:31:27 PM	System Roots
Federal Common Policy CA	certificate	Dec 1, 2030, 8:45:27 AM	System Roots
GeoTrust Global CA	certificate	May 20, 2022, 9:00:00 PM	System Roots
GeoTrust Primary Certification Authority	certificate	Jul 16, 2036, 4:59:59 PM	System Roots
GeoTrust Primary Certification Authority - G2	certificate	Jan 18, 2038, 3:59:59 PM	System Roots
GeoTrust Primary Certification Authority - G3	certificate	Dec 1, 2037, 3:59:59 PM	System Roots
Global Chambersign Root	certificate	Sep 30, 2037, 9:14:18 AM	System Roots
Global Chambersign Root - 2008	certificate	Jul 31, 2038, 5:31:40 AM	System Roots
GlobalSign	certificate	Mar 18, 2029, 3:00:00 AM	System Roots
GlobalSign	certificate	Jan 18, 2038, 7:14:07 PM	System Roots
GlobalSign	certificate	Jan 18, 2038, 7:14:07 PM	System Roots
GlobalSign	certificate	Dec 15, 2021, 12:00:00 AM	System Roots
GlobalSign Root CA	certificate	Jan 28, 2028, 4:00:00 AM	System Roots
Go Daddy Class 2 Certification Authority	certificate	Jun 29, 2034, 10:06:20 AM	System Roots
Go Daddy Root Certificate Authority - G2	certificate	Dec 31, 2037, 3:59:59 PM	System Roots

- The major trusted Certificate Authorities pay a lot of money to have their public root certificates accessible within the various operating systems.
- The main advantage of purchasing a server certificate from a trusted CA is that there is no need to distribute and install root certificates on WLAN clients because they already are there.

Real-World Caveats – 802.1X



AAA Certificate Services
Root certificate authority
Expires: Sunday, December 31, 2028 at 3:59:59 PM Pacific Standard Time
This certificate is valid

Name	Kind	Expires	Keychain
Entrust Root Certification Authority - EC1	certificate	Dec 18, 2037, 7:55:38 AM	System Roots
Entrust Root Certification Authority - G2	certificate	Dec 7, 2030, 9:55:54 AM	System Roots
Entrust.net Certification Authority (2048)	certificate	Dec 24, 2019, 10:20:51 AM	System Roots
Entrust.net Certification Authority (2048)	certificate	Jul 24, 2029, 7:15:12 AM	System Roots
ePKI Root Certification Authority	certificate	Dec 19, 2034, 8:31:27 PM	System Roots
Federal Common Policy CA	certificate	Dec 1, 2030, 8:45:27 AM	System Roots
GeoTrust Global CA	certificate	May 20, 2022, 9:00:00 PM	System Roots
GeoTrust Primary Certification Authority	certificate	Jul 16, 2036, 4:59:59 PM	System Roots
GeoTrust Primary Certification Authority - G2	certificate	Jan 18, 2038, 3:59:59 PM	System Roots
GeoTrust Primary Certification Authority - G3	certificate	Dec 1, 2037, 3:59:59 PM	System Roots
Global Chambersign Root	certificate	Sep 30, 2037, 9:14:18 AM	System Roots
Global Chambersign Root - 2008	certificate	Jul 31, 2038, 5:31:40 AM	System Roots
GlobalSign	certificate	Mar 18, 2029, 3:00:00 AM	System Roots
GlobalSign	certificate	Jan 18, 2038, 7:14:07 PM	System Roots
GlobalSign	certificate	Jan 18, 2038, 7:14:07 PM	System Roots
GlobalSign	certificate	Dec 15, 2021, 12:00:00 AM	System Roots
GlobalSign Root CA	certificate	Jan 28, 2028, 4:00:00 AM	System Roots
Go Daddy Class 2 Certification Authority	certificate	Jun 29, 2034, 10:06:20 AM	System Roots
Go Daddy Root Certificate Authority - G2	certificate	Dec 31, 2037, 3:59:59 PM	System Roots

- The downside of using a public CA with 802.1X/EAP is that an attacker can possibly perform a **man-in-the-middle** attack.
- An attacker can use a rogue AP along with rogue RADIUS server and a server certificate that was also created from the same public CA.

Real-World Caveats – 802.1X

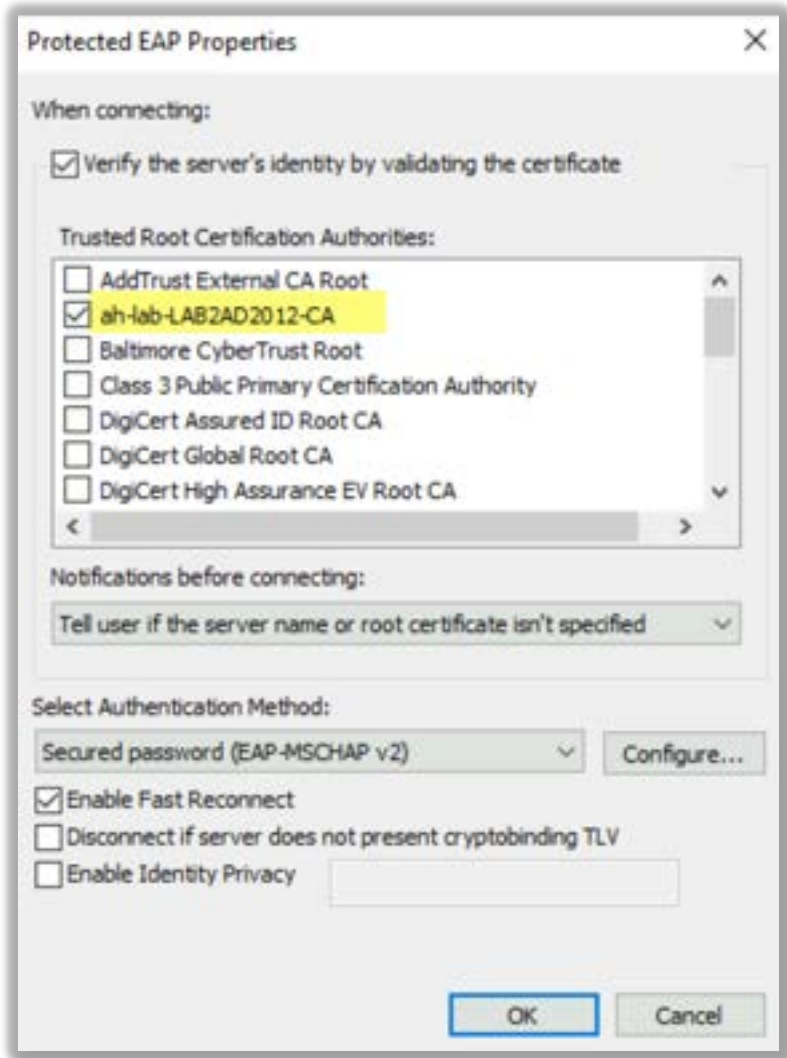


AAA Certificate Services
Root certificate authority
Expires: Sunday, December 31, 2028 at 3:59:59 PM Pacific Standard Time
This certificate is valid

Name	Kind	Expires	Keychain
Entrust Root Certification Authority - E-C1	certificate	Dec 18, 2037, 7:55:38 AM	System Roots
Entrust Root Certification Authority - G2	certificate	Dec 7, 2030, 9:55:54 AM	System Roots
Entrust.net Certification Authority (2048)	certificate	Dec 24, 2019, 10:20:51 AM	System Roots
Entrust.net Certification Authority (2048)	certificate	Jul 24, 2029, 7:15:12 AM	System Roots
ePKI Root Certification Authority	certificate	Dec 19, 2034, 6:31:27 PM	System Roots
Federal Common Policy CA	certificate	Dec 1, 2030, 8:45:27 AM	System Roots
GeoTrust Global CA	certificate	May 20, 2022, 9:00:00 PM	System Roots
GeoTrust Primary Certification Authority	certificate	Jul 16, 2036, 4:59:59 PM	System Roots
GeoTrust Primary Certification Authority - G2	certificate	Jan 18, 2038, 3:59:59 PM	System Roots
GeoTrust Primary Certification Authority - G3	certificate	Dec 1, 2037, 3:59:59 PM	System Roots
Global Chambersign Root	certificate	Sep 30, 2037, 9:14:18 AM	System Roots
Global Chambersign Root - 2008	certificate	Jul 31, 2038, 5:31:40 AM	System Roots
GlobalSign	certificate	Mar 18, 2029, 3:00:00 AM	System Roots
GlobalSign	certificate	Jan 18, 2038, 7:14:07 PM	System Roots
GlobalSign	certificate	Jan 18, 2038, 7:14:07 PM	System Roots
GlobalSign	certificate	Dec 15, 2021, 12:00:00 AM	System Roots
GlobalSign Root CA	certificate	Jan 28, 2028, 4:00:00 AM	System Roots
Go Daddy Class 2 Certification Authority	certificate	Jun 29, 2034, 10:06:20 AM	System Roots
Go Daddy Root Certificate Authority - G2	certificate	Dec 31, 2037, 3:59:59 PM	System Roots

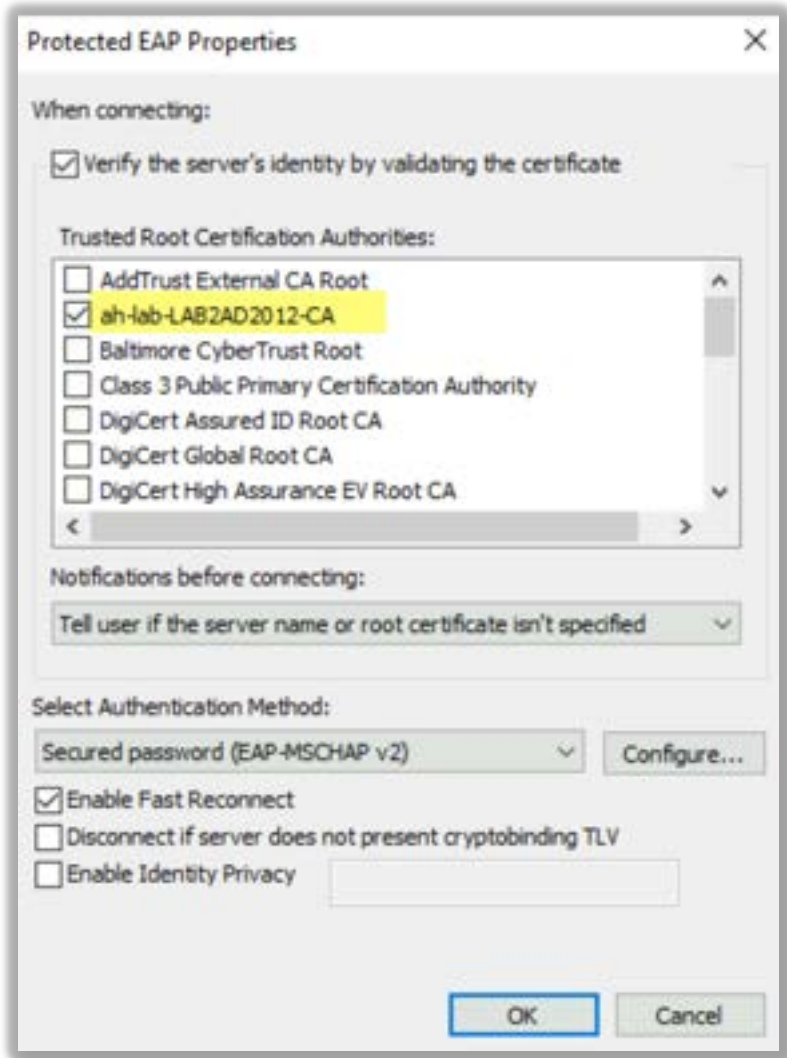
- This attack is complex and has many moving parts.
- But because the chain of trust might be compromised, most organizations instead choose to install a server certificate signed by an **internal CA** on the RADIUS server.

Real-World Caveats – 802.1X



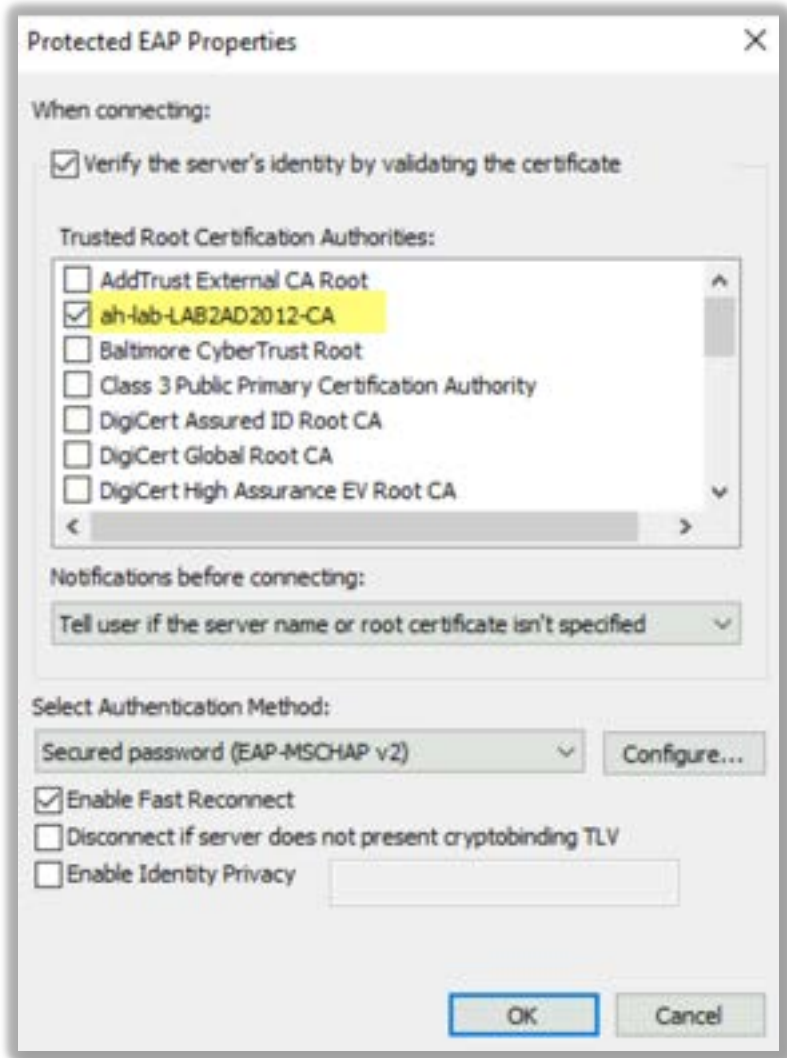
- The other option is to create a server certificate signed by an **internal private CA** such as Microsoft Certificate Services.
- Much like a public CA, a private CA establishes an internal company trust chain using separate certificates for the root and the servers.
- Many companies choose this method because they prefer to keep all the security in-house.

Real-World Caveats – 802.1X



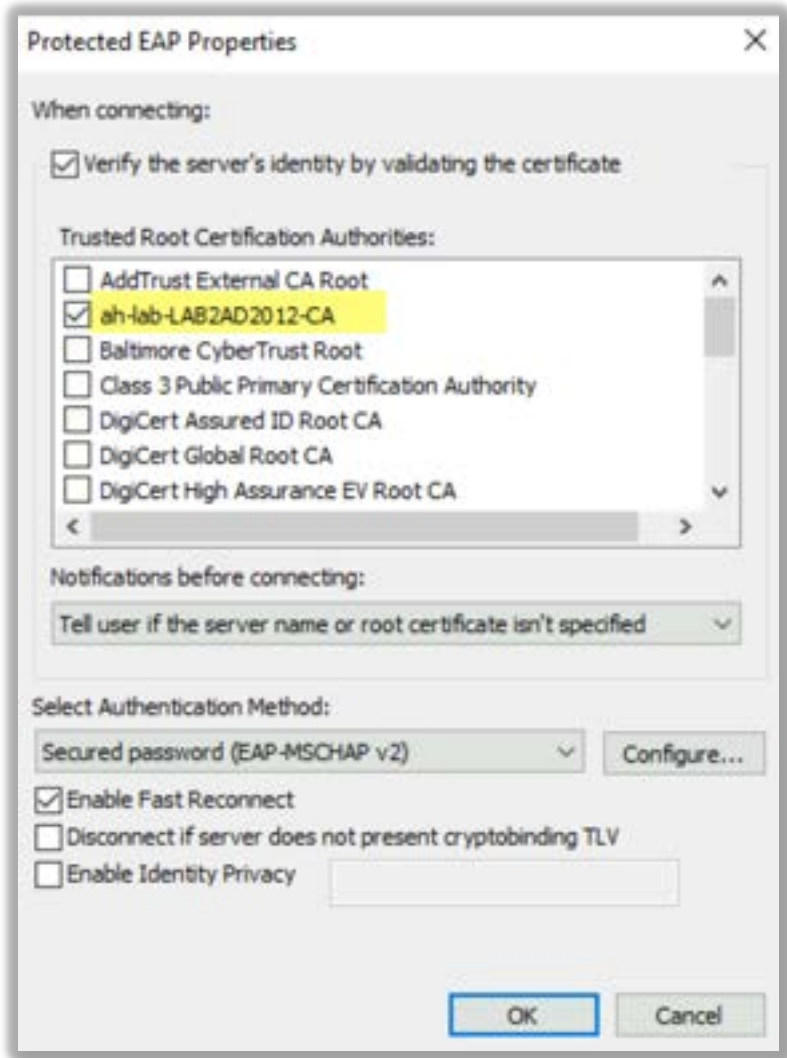
- There must be a means in which to distribute and install the root certificate to all of the WLAN supplicants.
- For example, the root certificate must be installed in the **Trusted Root Certification Authorities Store** of a Windows machine.
- Installing the root certificate onto Windows laptops can be easily automated using a **group policy object (GPO)**.

Real-World Caveats – 802.1X



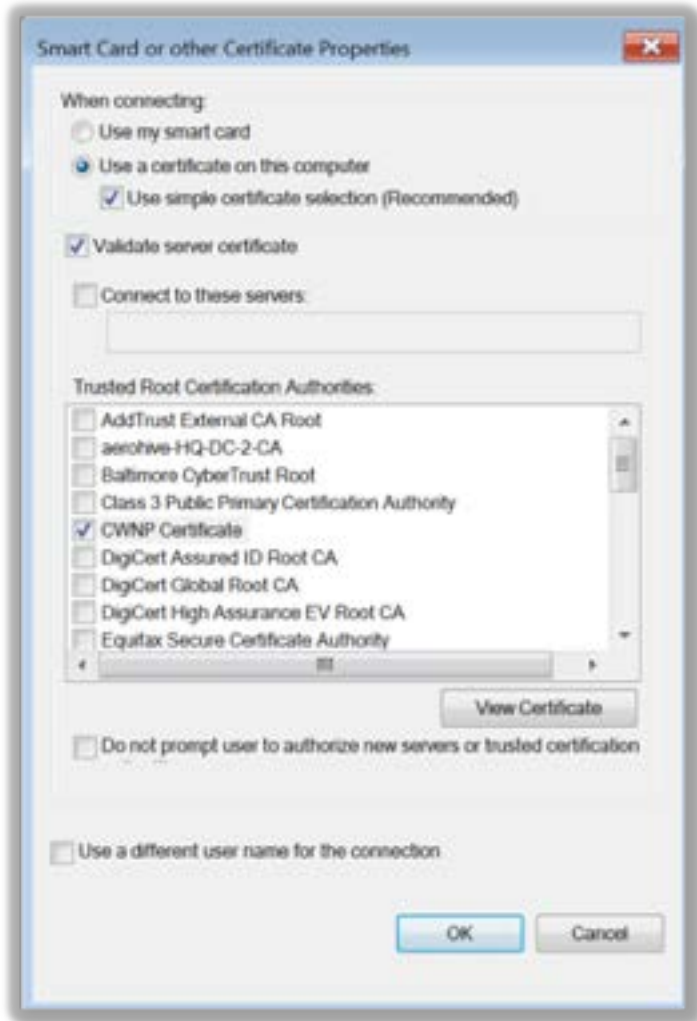
- However, a GPO cannot be used for MacOS, iOS, or Android mobile devices, or for personal Windows BYOD device that are not joined to the AD domain.
- Manually installing certificates on mobile devices and employee-owned devices is an administrative nightmare.
- For this reason, mobile device management (MDM) solutions are often deployed.

Real-World Caveats – 802.1X



- Instead of a full-blown MDM solution, another option is a **self-service device onboarding solution**.
- Several WLAN vendors offer self-service solutions so employees can easily self-install security credentials such as an 802.1X /EAP root CA certificate.
- Third-party self-service onboarding solutions such as SecureW2 (www.securew2.com) are also available.

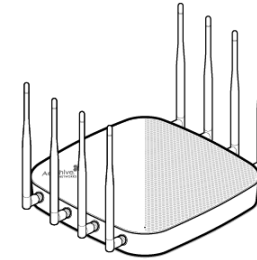
Real-World Caveats – 802.1X



- Most secure 802.1X protocol is EAP-TLS which make use of client-side certificates.
- A client certificate is an entirely different animal within a PKI infrastructure.
- Distribution of client certificates adds a whole new layer of complexity

Real World Caveats – static PSK

- 8-63 character shared passphrase
- Never intended for use in the enterprise
- Often used for **BYOD, Guest Access and IoT** devices in the enterprise
- Susceptible to offline dictionary attacks
- Wi-Fi Alliance recommends 20 strong characters or more
- Biggest weakness is that the PSK credential is “**static**”

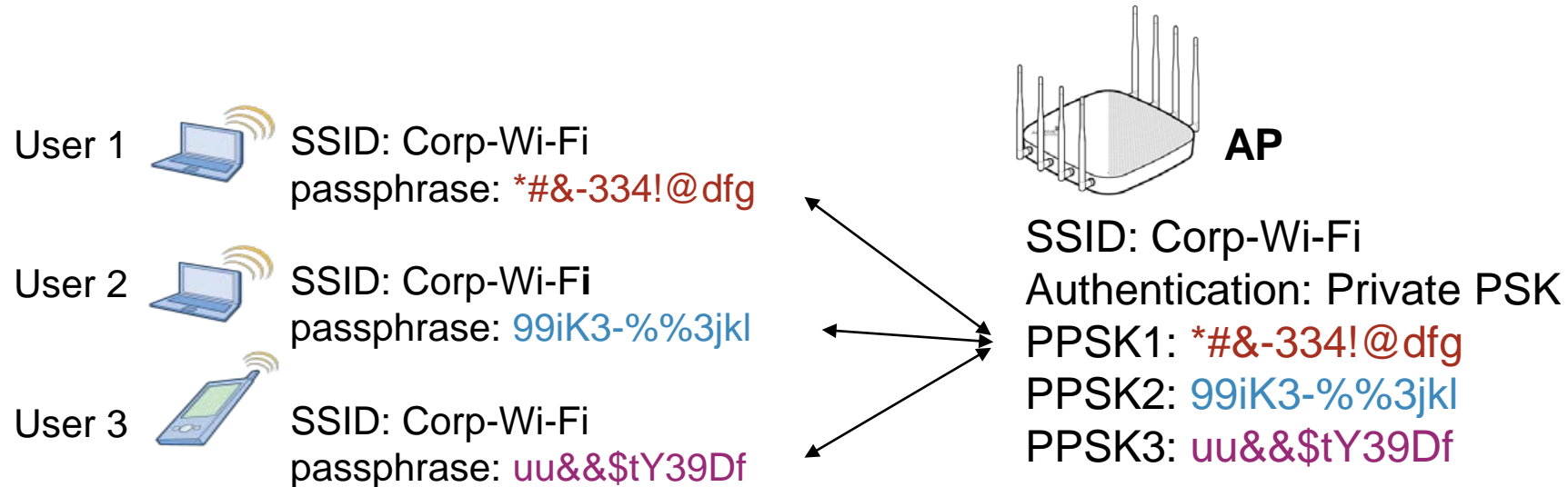


PSK = passphrase123!



PSK = passphrase123!

Private PreShared Key (PPSK)



- All users and devices have **unique credentials**
- If a user leaves or device is lost, the **PPSK credential** is simply changed for that one user or device

Private PreShared Key (PPSK)

- Multiple per-user and per-device PSKs assigned to a single SSID
- Easy to deploy
- No need for PKI, certificates or RADIUS servers
- Can be time-based credentials
- Solves the “static” PSK problem

<input type="checkbox"/>	Coleman-iMac	Private PSK-Manual	ZTe079<'&gHo669)?%OI
<input type="checkbox"/>	Coleman - MacBook	Private PSK-Manual	QLS655:>-IQC929#_[PK
<input type="checkbox"/>	Donnie - iPhone	Private PSK-Manual	wPf004[^TJe188`%)BE
<input type="checkbox"/>	Coleman - iPhone	Private PSK-Manual	Vns938#}?eiB396:_&Jh
<input type="checkbox"/>	Coleman-Kindle	Private PSK-Manual	bDx635?;;Pus901_\;kD
<input type="checkbox"/>	Coleman-Surface-Pro3	Private PSK-Manual	fUx564.>}QhJ650I"_an

Private PreShared Key (PPSK) – Use Cases

- **IoT Devices:** Provide unique and secure credentials for IoT devices. Many IoT devices and/or devices only support WPA2 Personal (PSK)
- **BYOD:** Onboarding personal and/or company issued mobile devices with unique and secure credentials
- **Guest Access:** Provide guest users with unique and **secure credentials**

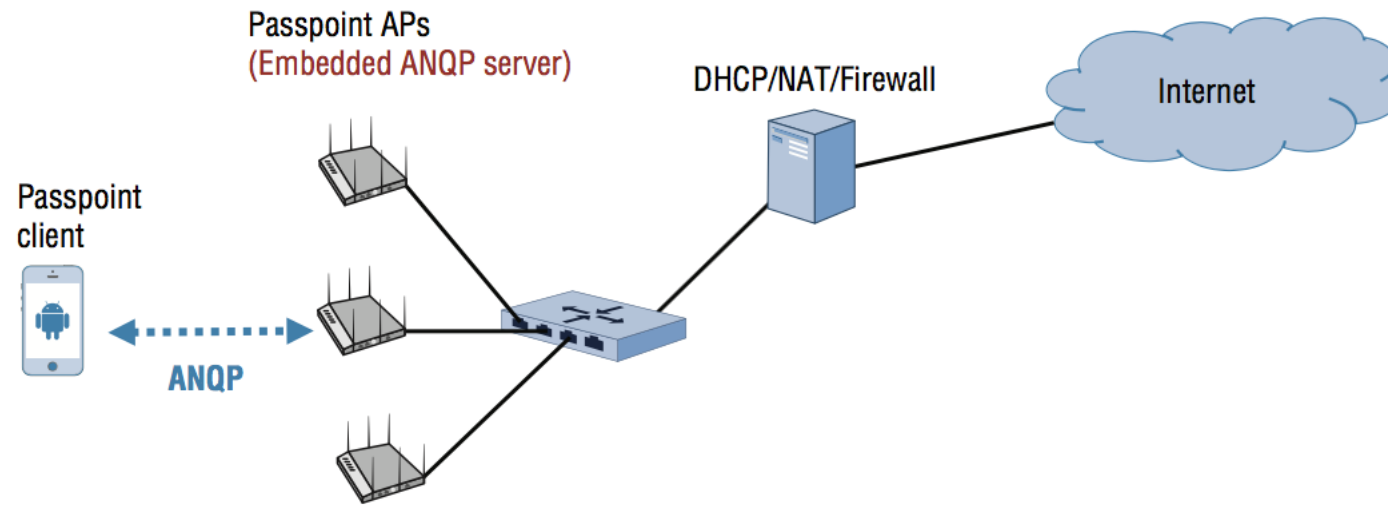


Real-World Caveats – Hotspot Wi-Fi Access



- The bad guys are lurking at public access Wi-Fi hotspots
- Corporate **Guest SSID** are using open and unsecure
- Growing trend to provide **encrypted guest access**

Encrypted Hotspot Security– Passpoint devices



- Another growing trend with public access networks is the use of 802.1X/EAP with **Hotspot 2.0**.
- Hotspot 2.0 is a Wi-Fi Alliance technical specification that is supported by the **Passpoint** certification program.
- Implementation in USA hotspots is sporadic and requires client-side support

Encrypted Guest access – Enterprise



- PPSK credentials have gained popularity for private company guest access
- Provides unique security credentials and **encrypted guest access**
- Value-added security for guest Wi-Fi users
- Another option is OWE

Real-World Caveats: Corporate Guest Access

Guest user traffic should always be segmented from employee user traffic.

Source IP	Destination IP	Service	Action
Any	Any	DHCP-Server	PERMIT
Any	Any	DNS	PERMIT
Any	10.0.0.0/255.0.0.0	Any	DENY
Any	172.16.0.0/255.240.0.0	Any	DENY
Any	192.168.0.0/255.255.0.0	Any	DENY
Any	Any	Any	PERMIT

- **Guest SSID:** Wireless guest users should always connect to a separate guest SSID because it will have different security policies than a corporate or employee SSID.
- **Guest VLAN:** Guest user traffic should be segmented into a unique VLAN tied to an IP subnet that does not mix with the employee user VLANs.
- **Captive Web Portal:** A captive web portal can be used to accept guest login credentials. More importantly, the captive web portal should have a legal disclaimer.
- **Guest Firewall Policy:** An ingress guest firewall policy is the most important component of WLAN guest management.

WPA History

Security Enhancements have typically taken a reactive approach:

WEP – first exploits 2001

WPA (2003)

attempted to bridge security gap from WEP to 802.11i

2008 – Beck-Tews attacks shows vulnerabilities in TKIP (compromises confidentiality)

WPA-PSK brute force attacks (compromises network access and confidentiality)

WPA2 (2004) - IS NOT BROKE

Integrated security enhancements from 802.11i (added AES)

WPA2-PSK: brute force attacks still exist

Still maintains a TKIP only mode of operation

Inconsistent cryptography strength (SHA-1 <80 bits of security)

WPA3 (2018)

Disallows WEP & TKIP protocols

Requires the use of Protected Management Frames

Replaces PSK with SAE (Simultaneous Authentication of Equals)

WPA3 Enterprise



- 802.1X security has not changed
- Disallows WEP & TKIP protocols
- Requires the use of **Protected Management Frames**
- Optional **Suite B Security** certification, provides greater security
 - Based on U.S. Government cryptographic tools for sensitive networks
 - 192-bit Security suite of protocols includes:
 - AES-GCM-256 for authenticated encryption
 - HMAC-SHA384 for key derivation and key confirmation
 - ECDHE and ECDSA using a 384-bit elliptic curve
 - RSA key lengths of 3k-bits or greater
 - BIP-GMAC-256 for robust management frame protection

WPA3 Personal



- Disallows WEP & TKIP protocols
- Requires the use of **Protected Management Frames**
- Replaces PSK with **Simultaneous Authentication of Equals (SAE)**
 - Password is never shared during the key exchange protocol
 - Uses 'Zero knowledge proof'
 - Resistant to dictionary attacks, you only get to guess the password once

SAE

Select passphrase



Select passphrase



- WPA3 Personal replacement for PSK authentication
- **Secure Authentication of Equals (SAE)**
- SAE is a variant of **Dragonfly**, a password authentication key exchange based on a zero-knowledge proof

SAE

Select passphrase



Select passphrase



- Prove you know the credentials without compromising the credentials
- No forging, modification or replay attacks
- No offline dictionary attacks

Real-World Caveats – WPA3



- Although WPA3 security has been around since 2018, mandatory support just became a requirement this year
- 95% of current client population does not support
- Tactical deployments of WPA3 are rare but growing

Enhanced Open

- Optional certification for Wi-Fi CERTIFIED devices
 - Separate certification for open networks, not a component of WPA3
 - Does not require WPA2 or WPA3 certification
- Enhanced Open = Opportunistic Wireless Encryption (OWE) protocol
 - No user intervention required & no passwords to enter
 - Encryption without authentication
 - No authentication means no unique identity
- Enhanced Open mode provides basic protection against snooping, or eavesdropping over open networks
- Requires use of Protected Management Frames (PMF)



Real-World Caveats – OWE (Enhanced Open)

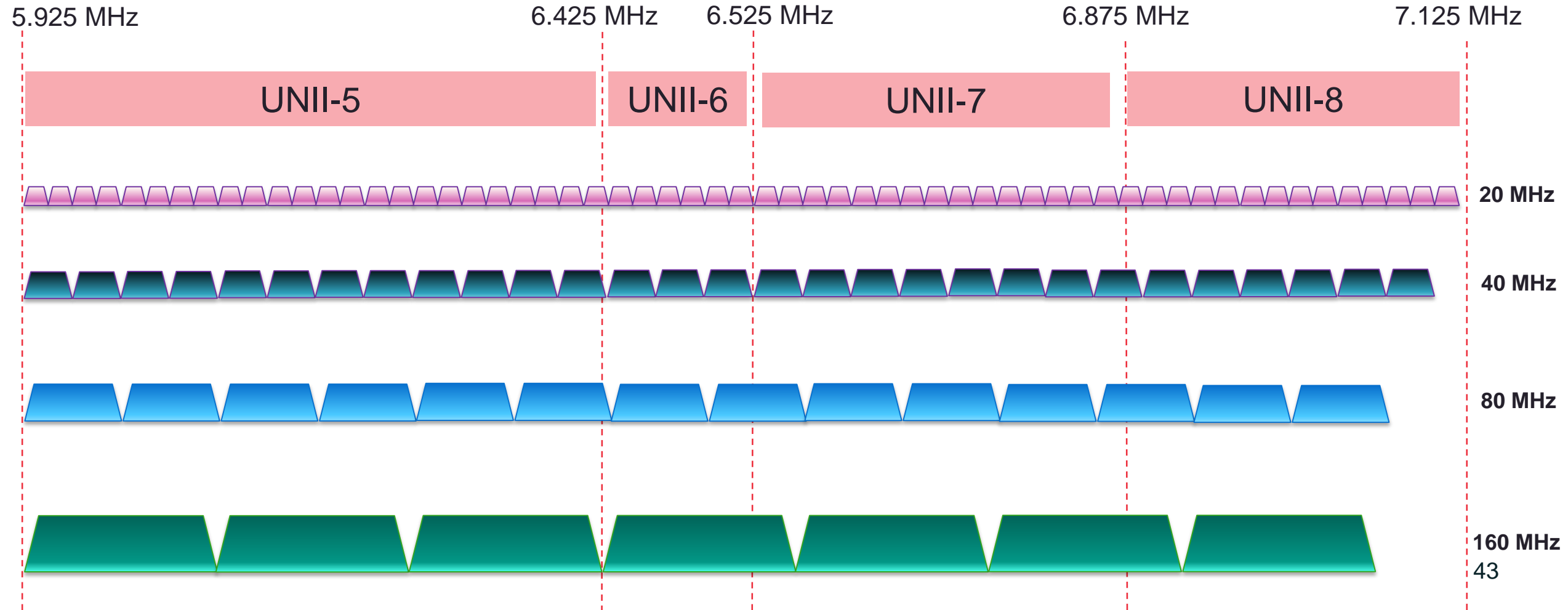
- Will not work with legacy clients
- OWE support on new clients is also rare because it is *optional*
- Encryption *without* authentication
- However support will most likely be mandated for the upcoming 6 GHz frequency band





- (59) 20 MHz channels
- (29) 40 MHz channels
- (14) 80 MHz channels
- (7) 160 MHz channels

1200 MHz of new frequency spectrum

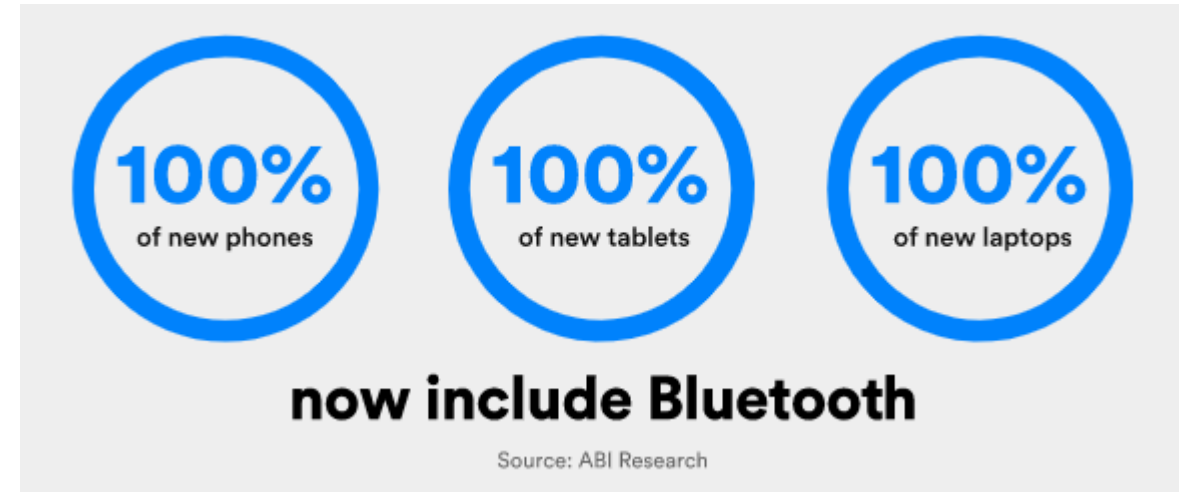


Concerns and Future of Wi-Fi Security



- Lack of proper implementation
- IoT Devices - low-hanging fruit
- BLE attacks and hacks

Bluetooth Proliferation



2.1 BILLION
annual shipments of Bluetooth® phones, tablets
& PCs by 2024

Source: ABI Research

Questions



Wi-Fi 6 for Dummies

Download your free copy today!

<http://bit.ly/WiFi6forDummies>

