Evolution of WLAN Security

David Coleman

Aerohive Networks - Senior Mobility Leader

CWNE #4

Co-author of CWNA, CWSP and CWAP Study Guides

IT Professional Wi-Fi Trek 2015

#wifitrek

Certified Wireless Network Professional

cwnp

Evolution of WLAN Security

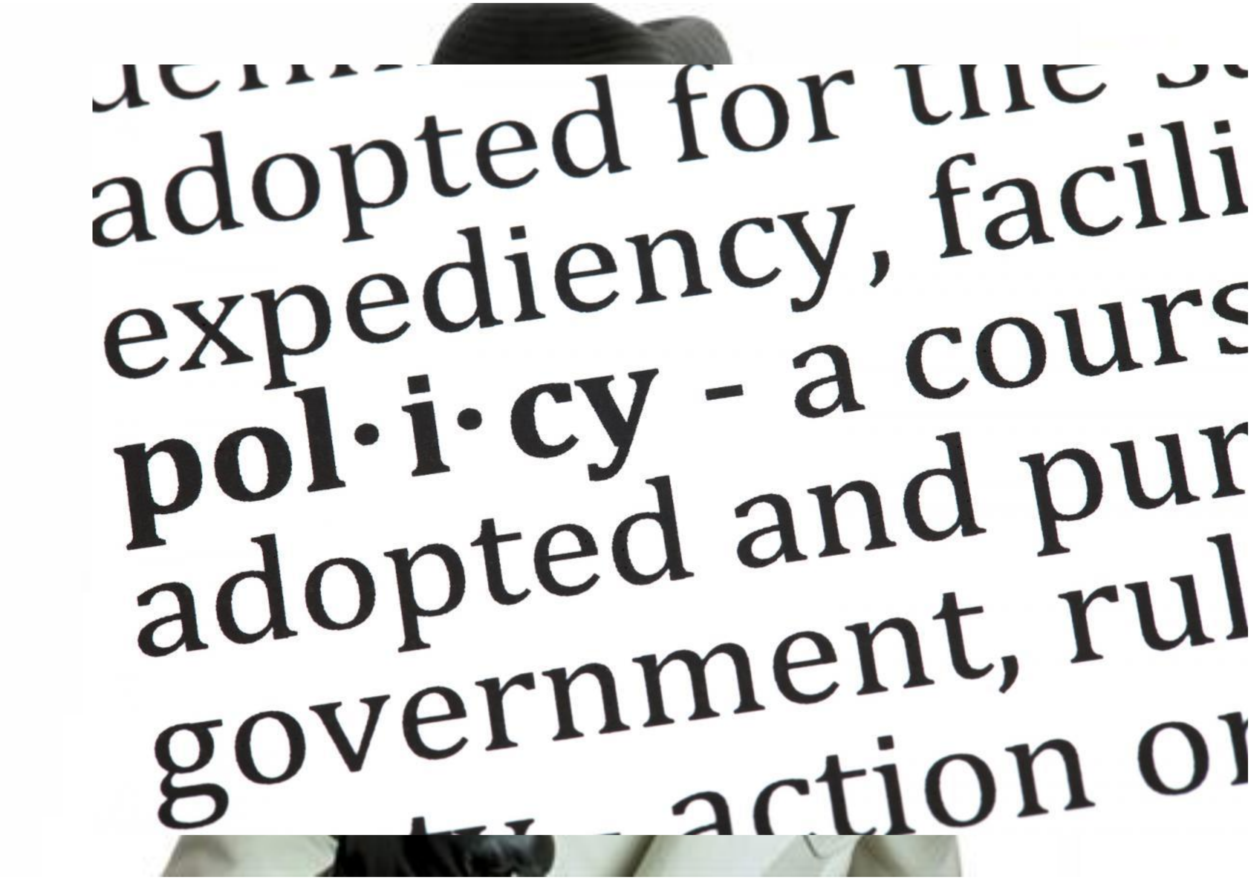
- 802.11 Security Standards and Certifications
- Five Basic Tenets of WLAN Security
- New Tenets of WLAN Security
- Future of WLAN Security

802.11 Security Standards and Certifications:

IEEE	Wi-Fi Alliance	Authentication Method	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 Basic Tenets of Security

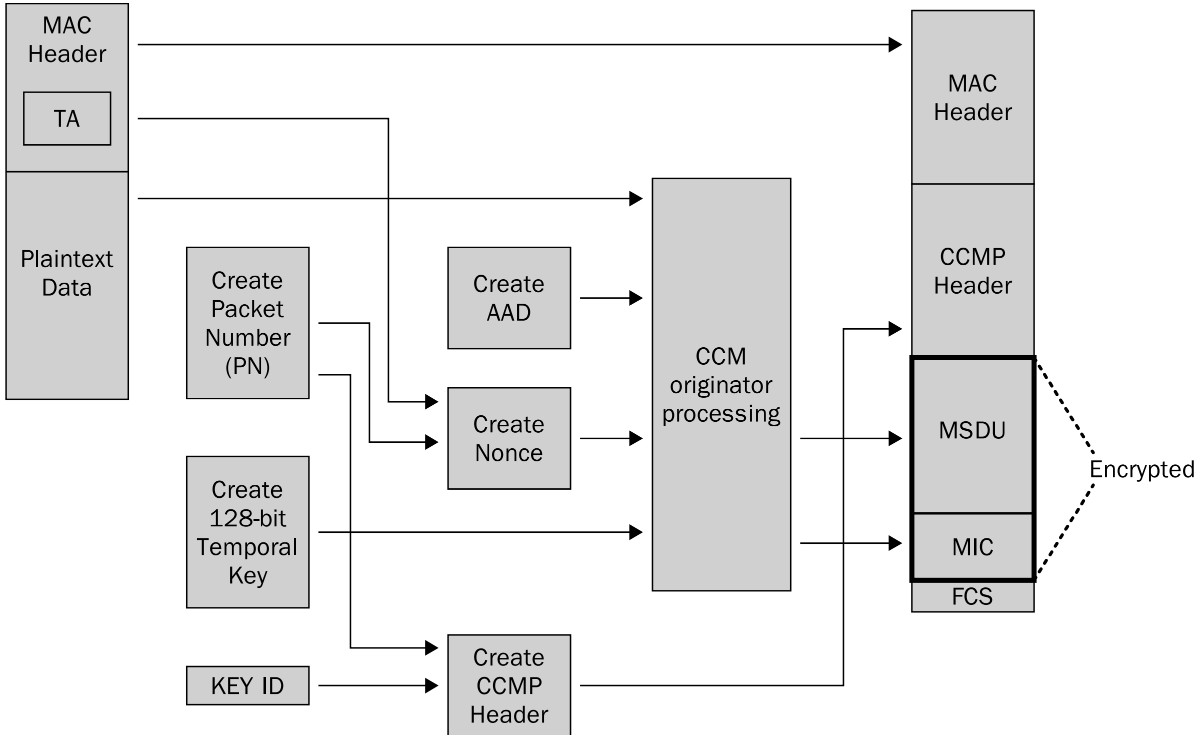
- Data privacy and integrity
- Authentication, authorization accounting (AAA)
- Segmentation
- Monitoring
- Policy



adopted for the s
expediency, facili
pol·i·cy - a cours
adopted and pur
government, rul
action o

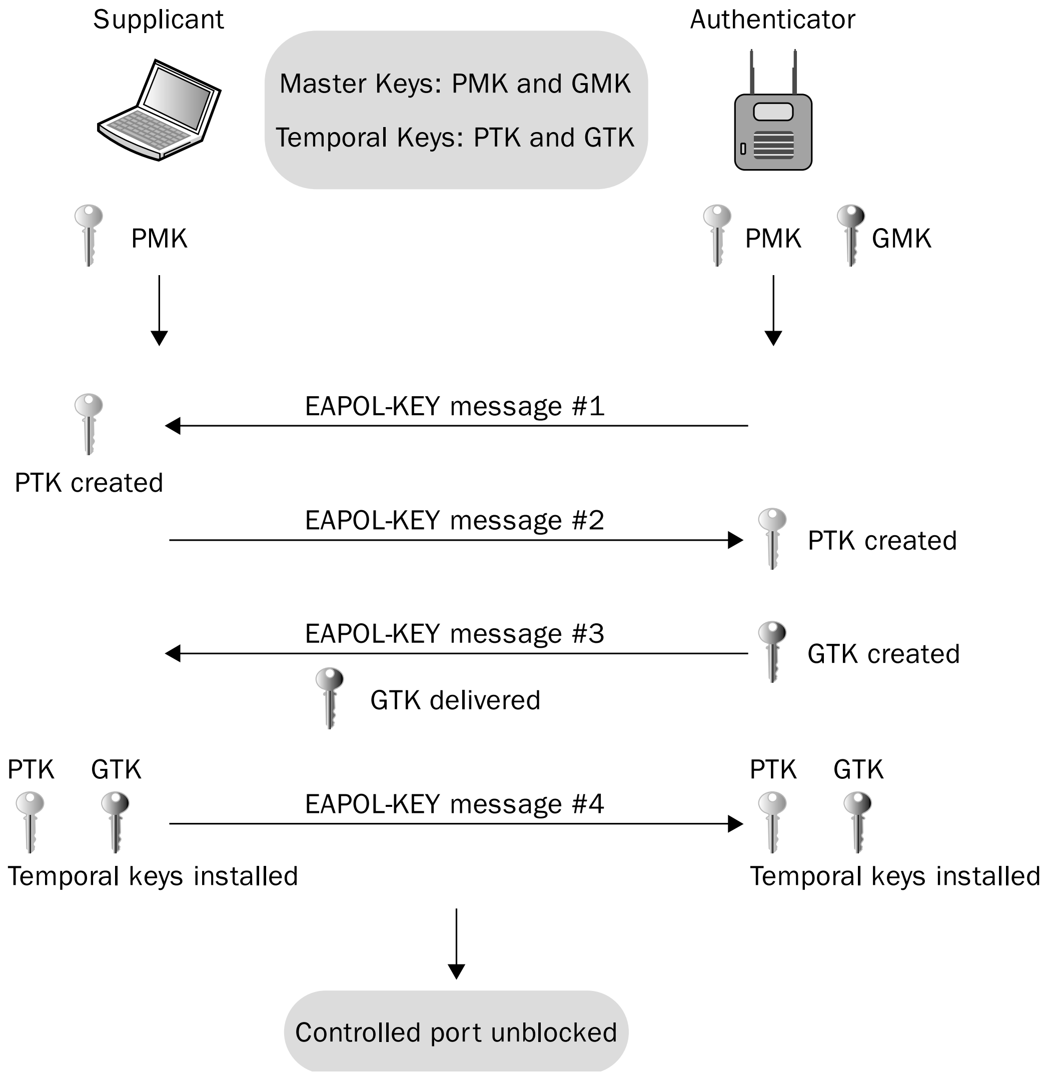
Data Privacy and Integrity:

- WEP is a broken old dinosaur
- TKIP not supported for 802.11n or 802.11ac data rates
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- Advanced Encryption Standard (AES) 128-bit cipher



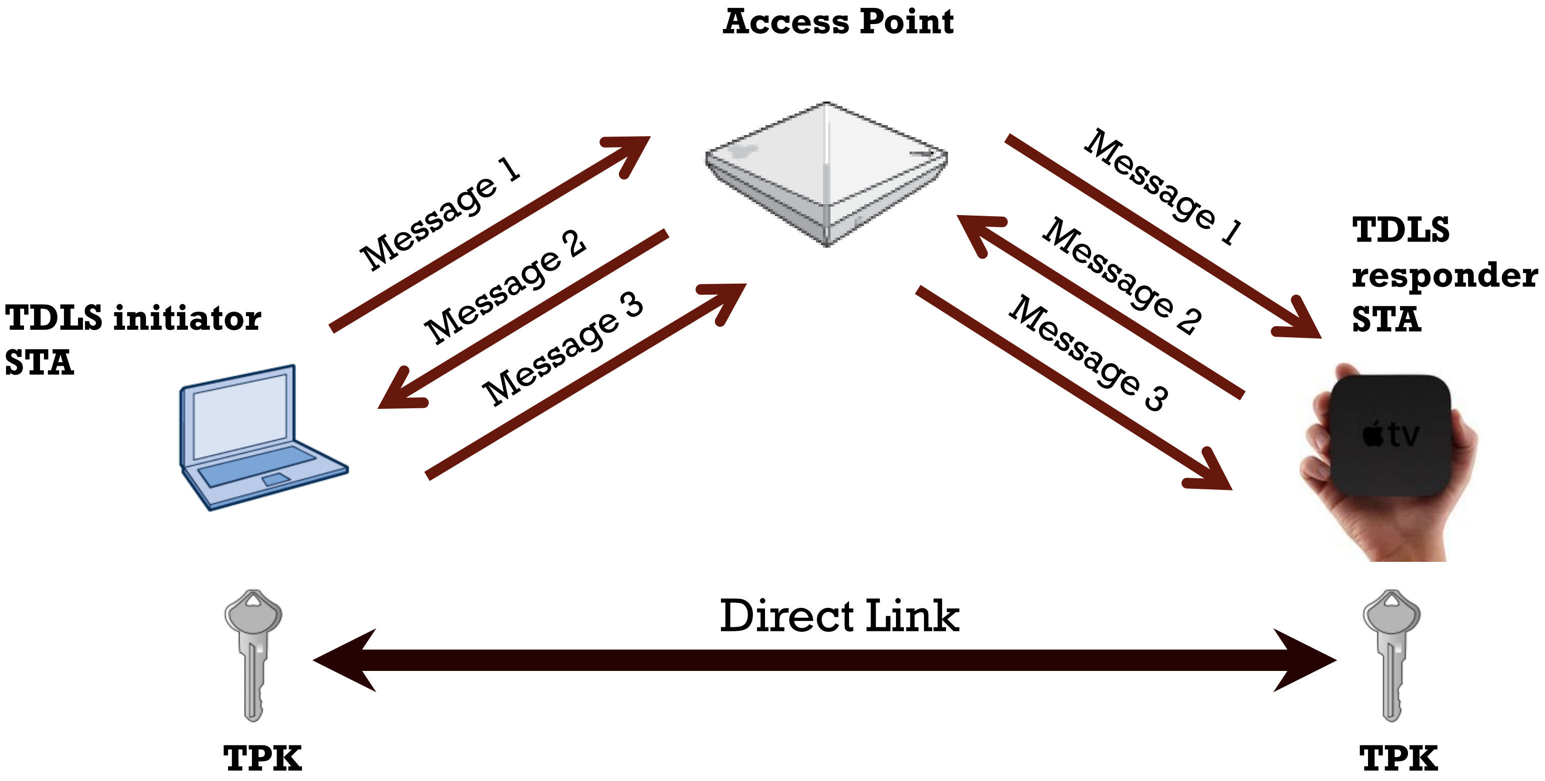
Data Privacy and Integrity:

- The 802.11-2007 standard defines *authentication and key management (AKM)* services.
- Authentication required for key creation
- Robust Security Network (RSN) dynamic encryption
- 4-Way Handshake



Data Privacy and Integrity:

- Tunneled Direct Link Setup
- Examples: AirPlay and Apple TVs
- 3-Way Handshake

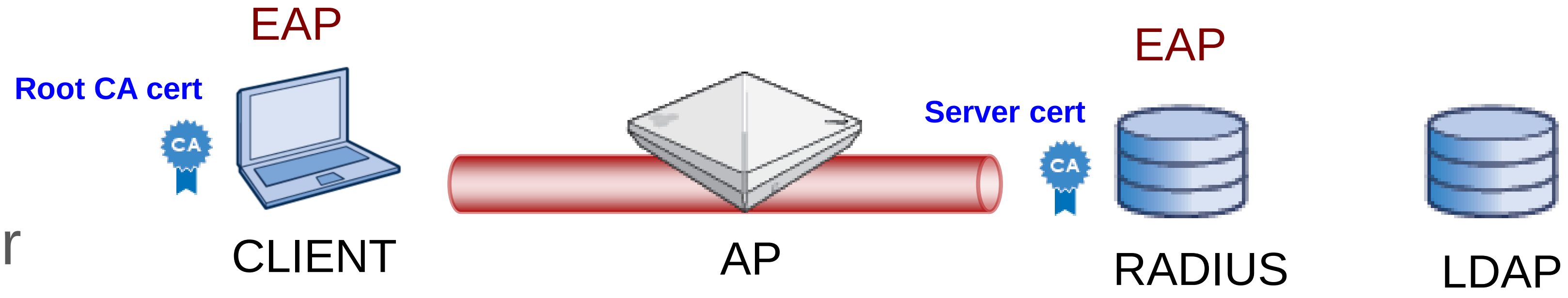


AAA:

- Authentication: Validate user/device identity
- Authorization: Authorize user/device identity
- Accounting: Paper trail
- 802.11 security requires an *authentication and key management protocol (AKMP)* that can be either a preshared key (PSK) or an EAP protocol used during 802.1X authentication.

802.1X/EAP:

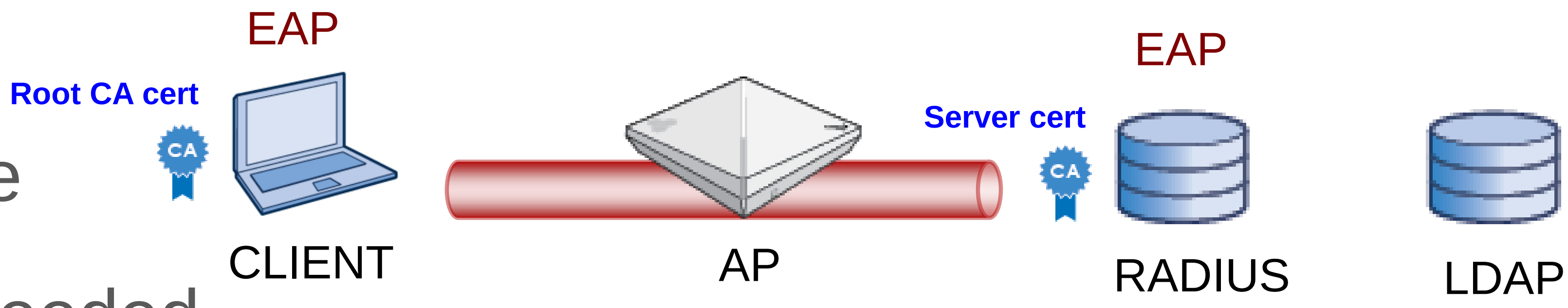
- 802.1X: Port based access control
- Authorization Framework
  - Supplicant
  - Authenticator
  - Authentication Server

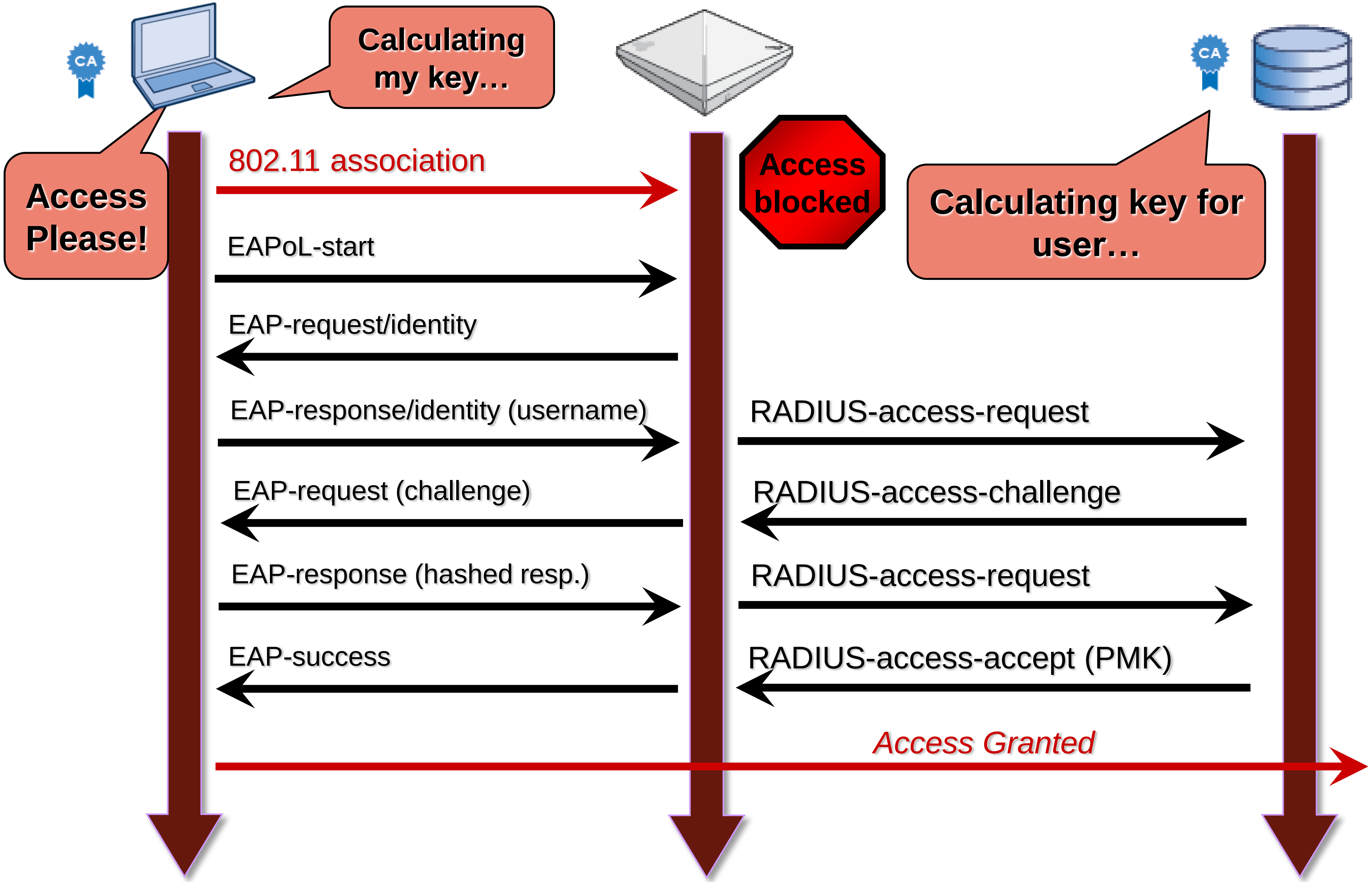


- Extensible Authentication Protocol (EAP) – Layer 2
- Server certificate and Root CA certificate
- Tunneled authentication using SSL/TSL

802.1X/EAP:

- Most secure authentication method
- Ideal for the enterprise
- Certificates and PKI needed
- Can be difficult to deploy
- Can be difficult to troubleshoot





Calculating my key…

Access Please!

802.11 association

Access blocked

Calculating key for user…

EAPoL-start

EAP-request/identity

EAP-response/identity (username)

RADIUS-access-request

EAP-request (challenge)

RADIUS-access-challenge

EAP-response (hashed resp.)

RADIUS-access-request

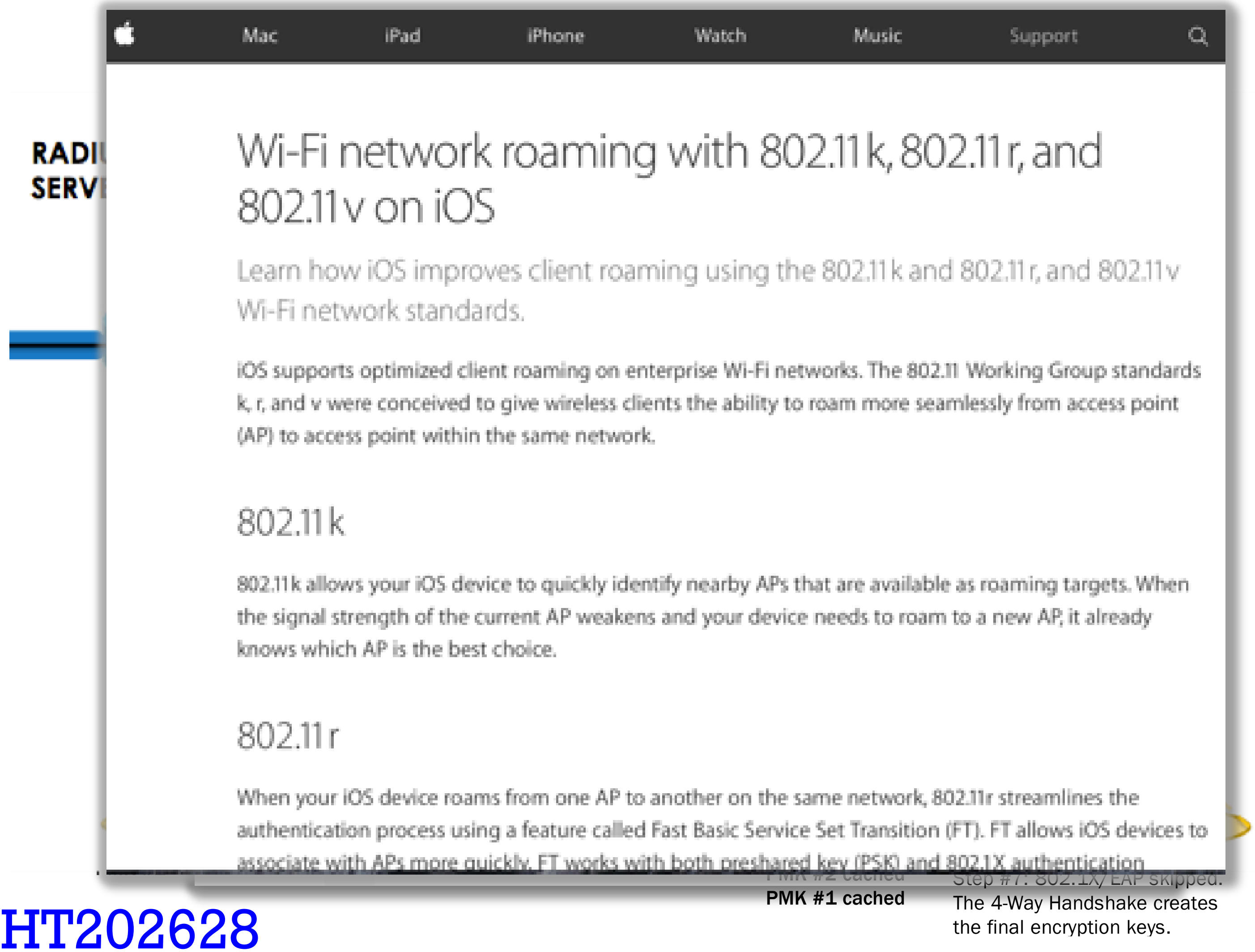
EAP-success

RADIUS-access-accept (PMK)

Access Granted

Fast Secure Roaming

- Opportunistic Key Caching (OKC)
- 802.11r – Fast BSS Transition (FT)
- Voice Enterprise
- Client support growing


Mac
iPad
iPhone
Watch
Music
Support
RADI
SERV
PMK #2 cached
PMK #1 cached
Step #7: 802.1X/ EAP skipped.
The 4-Way Handshake creates
the final encryption keys.

Wi-Fi network roaming with 802.11k, 802.11r, and 802.11v on iOS

Learn how iOS improves client roaming using the 802.11k and 802.11r, and 802.11v Wi-Fi network standards.

iOS supports optimized client roaming on enterprise Wi-Fi networks. The 802.11 Working Group standards k, r, and v were conceived to give wireless clients the ability to roam more seamlessly from access point (AP) to access point within the same network.

802.11k

802.11k allows your iOS device to quickly identify nearby APs that are available as roaming targets. When the signal strength of the current AP weakens and your device needs to roam to a new AP, it already knows which AP is the best choice.

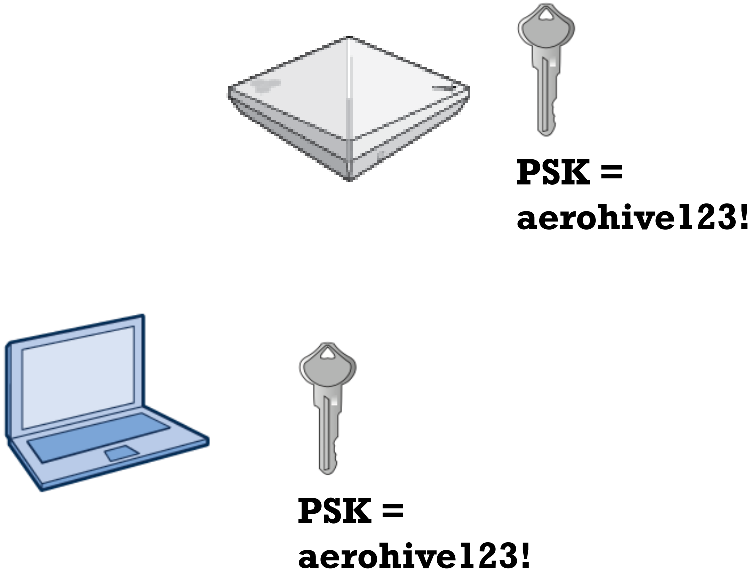
802.11r

When your iOS device roams from one AP to another on the same network, 802.11r streamlines the authentication process using a feature called Fast Basic Service Set Transition (FT). FT allows iOS devices to associate with APs more quickly. FT works with both preshared key (PSK) and 802.1X authentication

https://support.apple.com/en-us/HT202628

PSK:

- 8-63 character shared passphrase
- Never intended for use in the enterprise
- Susceptible to offline dictionary attacks
- Wi-Fi Alliance recommend 20 strong characters or more
- Biggest weakness is that the PSK credential is “static”

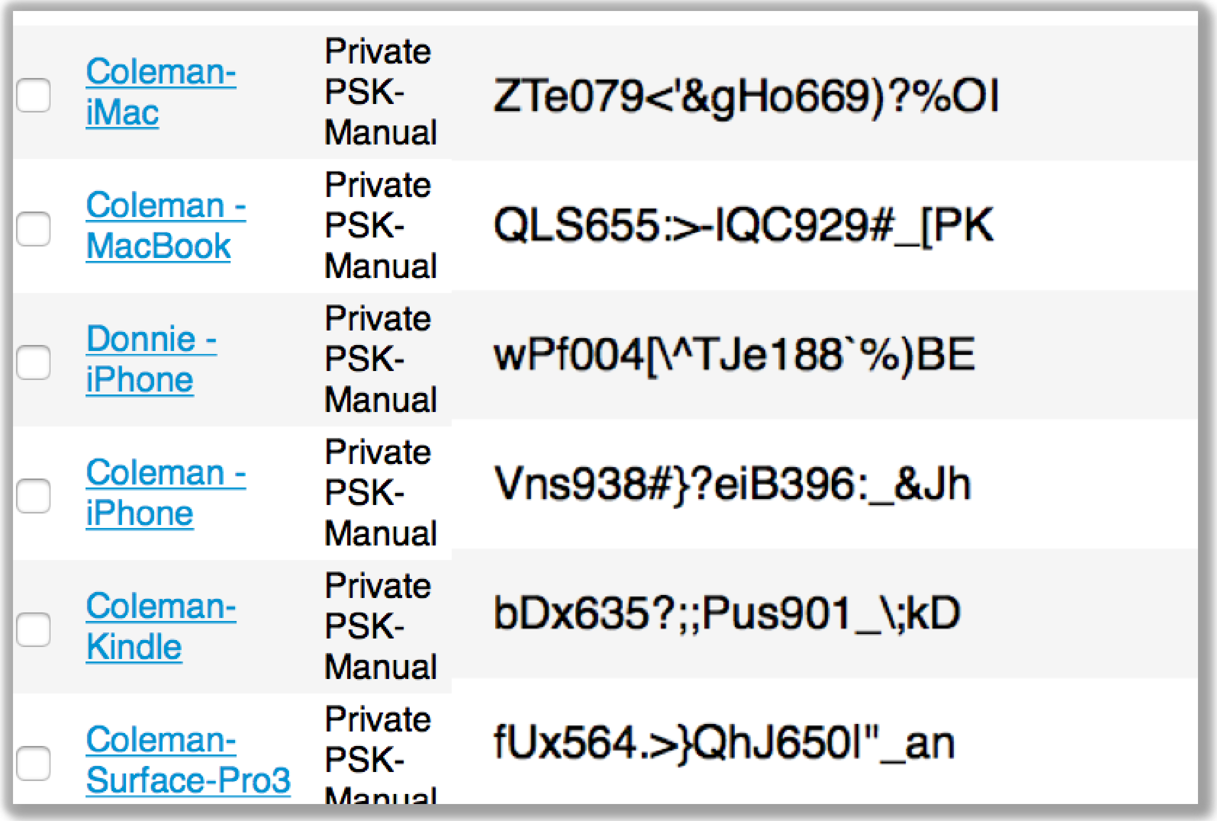


PSK = aerohive123!

PSK = aerohive123!

Per-user and per-device PSK:

- Several vendors offer proprietary PSK solutions
- Multiple per-user and per-device PSKs assigned to a single SSID
- Easy to deploy
- Can be time-based credentials
- Solves the “static” PSK problem



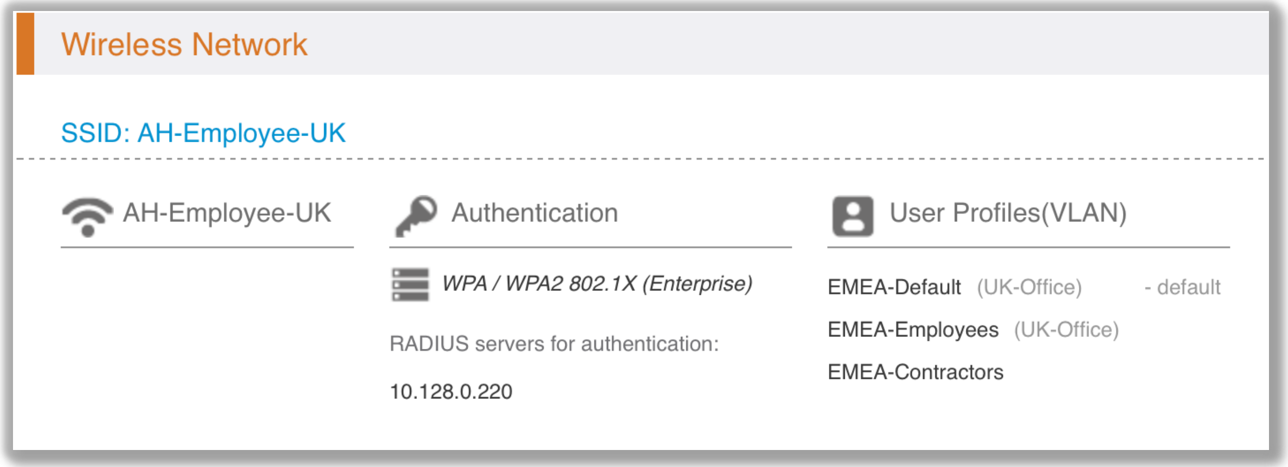
□	Coleman-iMac	Private PSK-Manual	ZTe079<'&gHo669)?%OI
□	Coleman - MacBook	Private PSK-Manual	QLS655:>-IQC929#_[PK
□	Donnie - iPhone	Private PSK-Manual	wPf004[\^TJe188`%)BE
□	Coleman - iPhone	Private PSK-Manual	Vns938#}?eiB396:_&Jh
□	Coleman-Kindle	Private PSK-Manual	bDx635?;;Pus901_\;kD
□	Coleman-Surface-Pro3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

PPSK Enterprise Use Cases:

- Legacy devices
- Supplement to 802.1X/EAP
- Replacement to 802.1X/EAP
- BYOD security
- Internet of Things (IoT)
- Secure guest WLANs

Segmentation:

- Role-based access control for different groups of users
- VLANs/IP Subnets
- Firewall policies
- Leverage RADIUS attributes
- Consolidate SSIDS



Wireless Network

SSID: AH-Employee-UK

AH-Employee-UK

Authentication

WPA / WPA2 802.1X (Enterprise)

RADIUS servers for authentication:

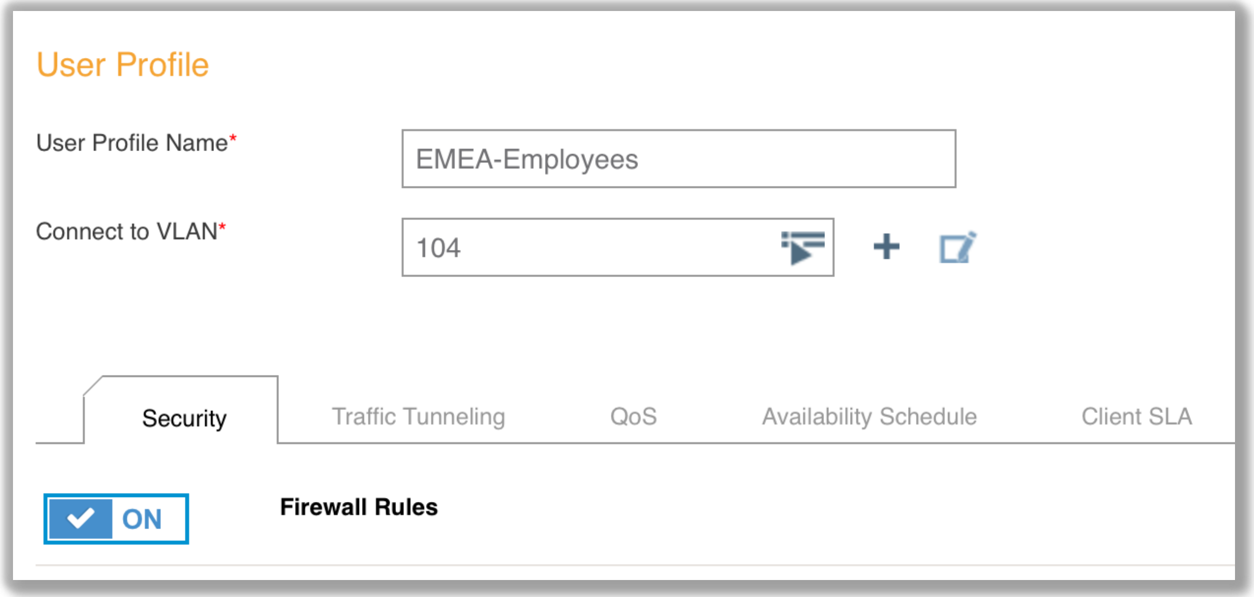
10.128.0.220

User Profiles(VLAN)

EMEA-Default (UK-Office) - default

EMEA-Employees (UK-Office)

EMEA-Contractors



User Profile

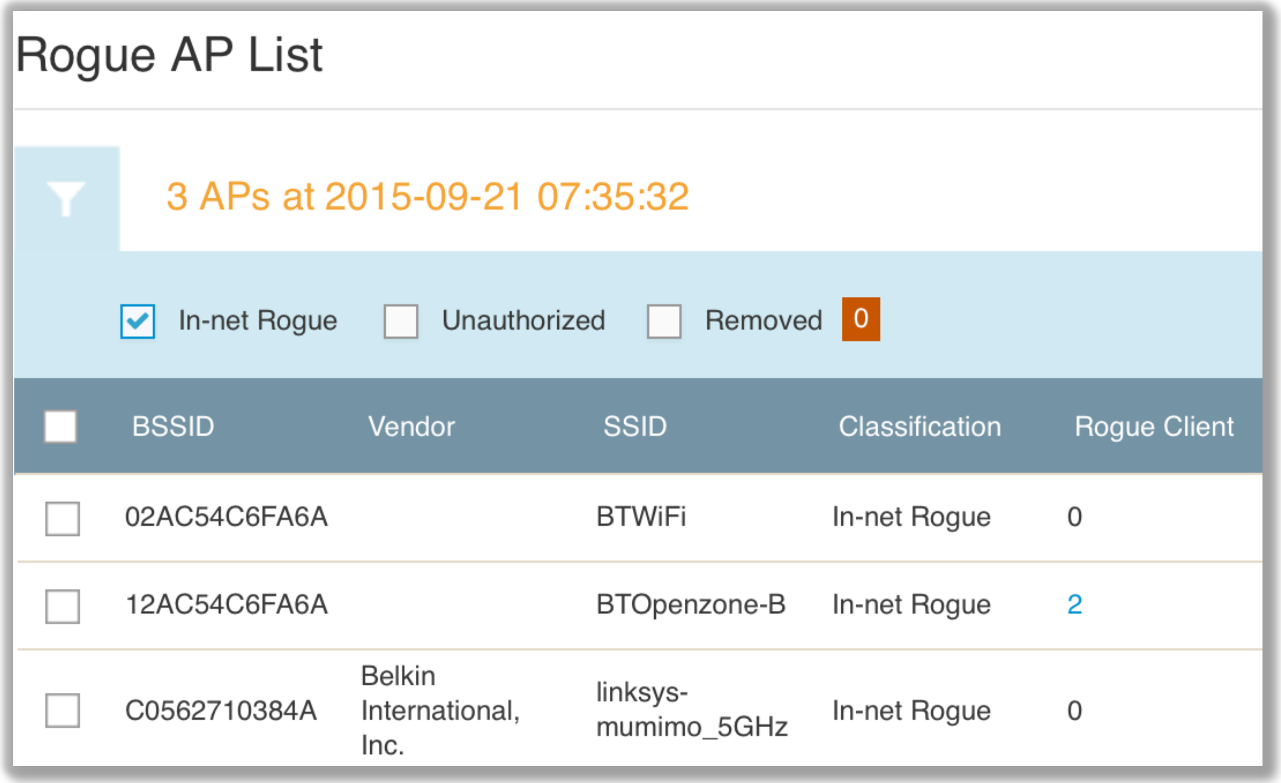
User Profile Name*: EMEA-Employees

Connect to VLAN*: 104

ON Firewall Rules

Monitoring:

- WIPS monitoring
- Rogue AP detection and mitigation
- Layer 2 DoS and other attacks
- 802.11w – Management Frame Protection (MFP)
  - Protection against more common L2 DoS attacks
  - Not a lot of client support



Rogue AP List

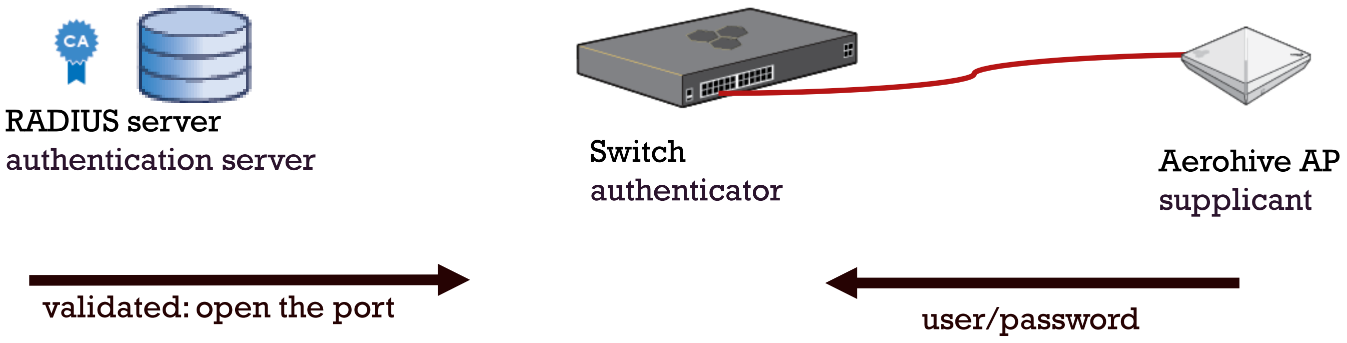
3 APs at 2015-09-21 07:35:32

☑ In-net Rogue □ Unauthorized □ Removed 0

□	BSSID	Vendor	SSID	Classification	Rogue Client
□	02AC54C6FA6A		BTWiFi	In-net Rogue	0
□	12AC54C6FA6A		BTOpenzone-B	In-net Rogue	2
□	C0562710384A	Belkin International, Inc.	linksys-mumimo_5GHz	In-net Rogue	0

Monitoring:

- Integrated versus Overlay
- Wired 802.1X/EAP port control for rogue protection is more prevalent
- Some vendor APs can also be validated as supplicants



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

New Tenets of WLAN Security

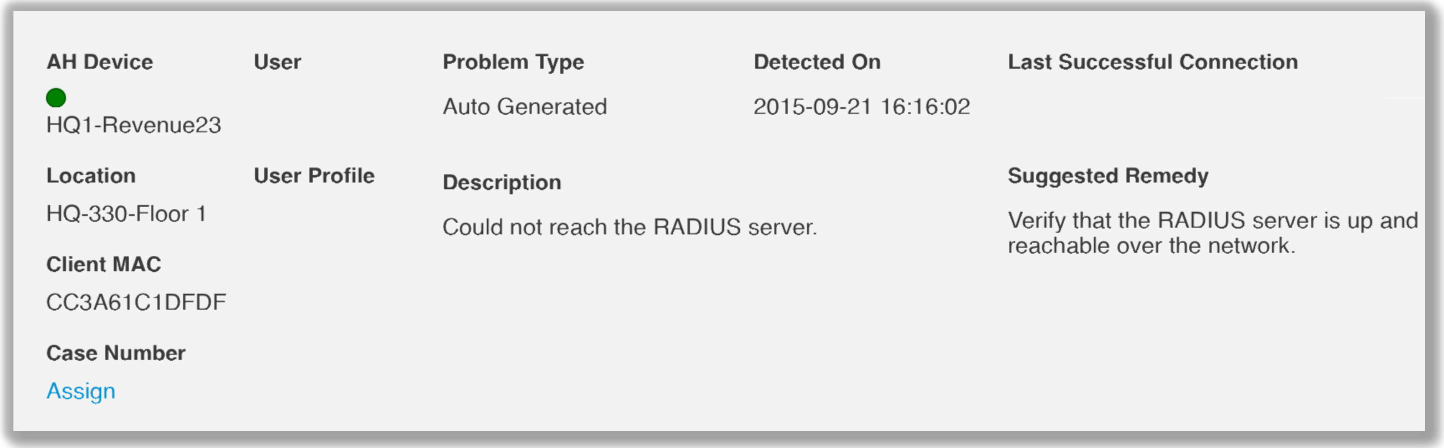
- WLAN Security Troubleshooting
- Client Device Management
- Guest Management
- Future of WLAN Security

WLAN Security Troubleshooting

- WLAN Security Troubleshooting

Troubleshooting 802.1X/EAP blog

- Multiple points of failure with 802.1X
  - RADIUS server does not respond
    - Mismatched shared secret
    - Misconfigured network settings
    - Incorrect RADIUS ports
    - Incorrect LDAP credentials
  - Supplicant problems
    - Certificate issues
    - Credential issues



AH Device
● HQ1-Revenue23

User

Problem Type
Auto Generated

Detected On
2015-09-21 16:16:02

Last Successful Connection

Location
HQ-330-Floor 1

User Profile

Description
Could not reach the RADIUS server.

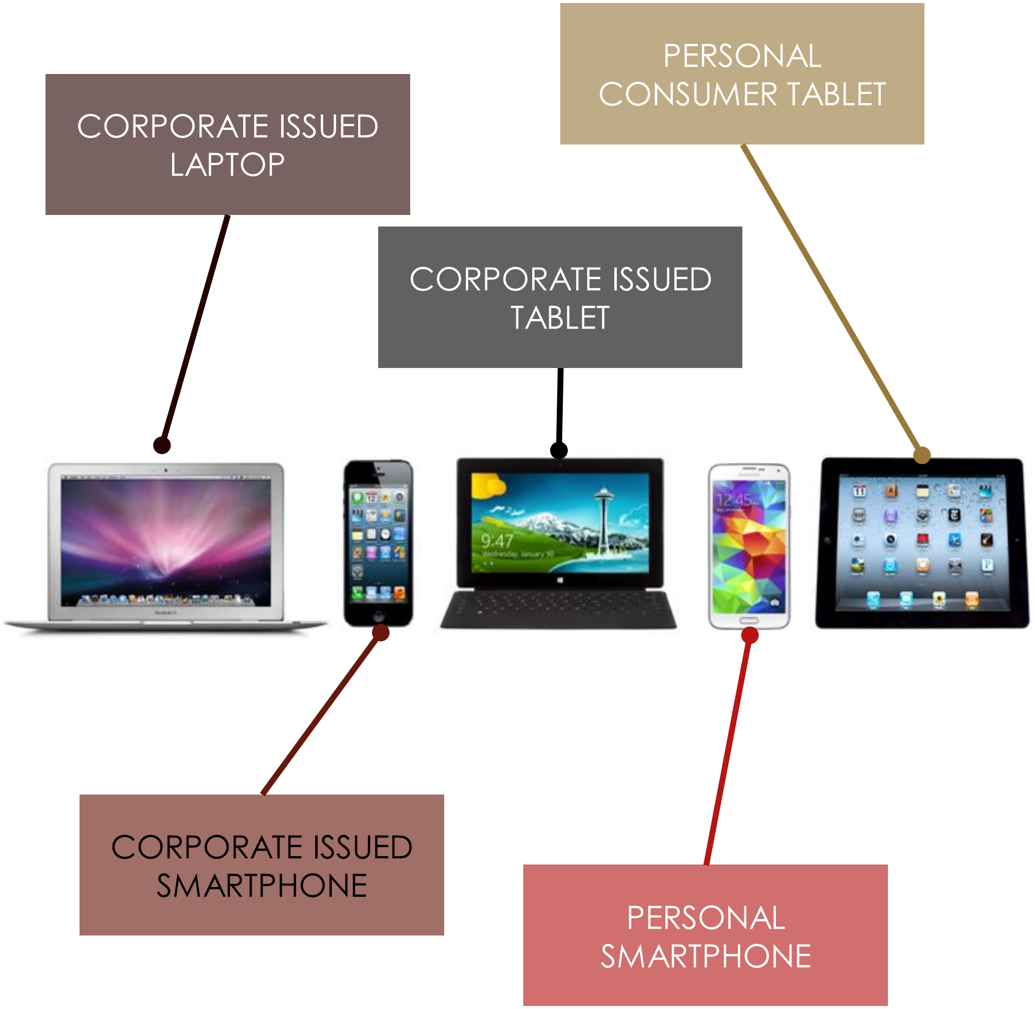
Suggested Remedy
Verify that the RADIUS server is up and reachable over the network.

Client MAC
CC3A61C1DFDF

Case Number
Assign

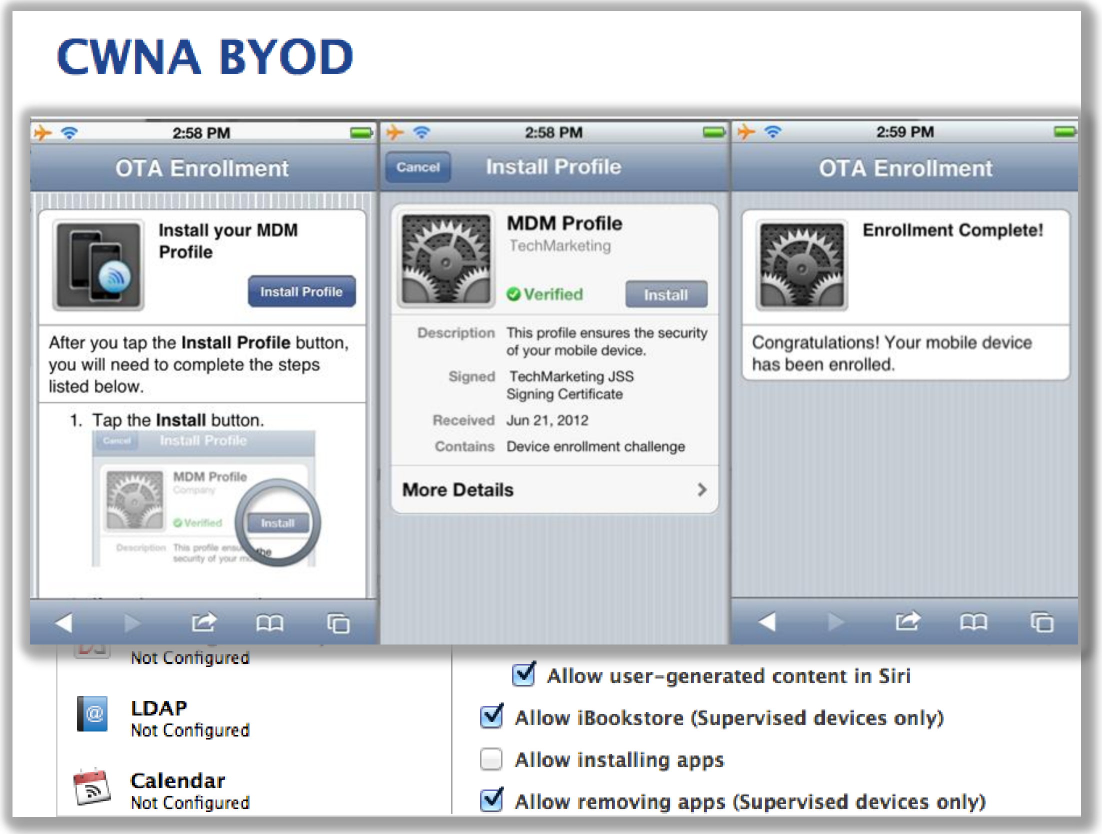
Client Device Management

- Bring Your Own Device (BYOD)
  - Although mobile devices initially were intended for personal use, employees now want to use their personal mobile devices in the workplace.
  - Employees have expectations of being able to connect to a corporate WLAN with multiple personal mobile devices.
  - We live in a BYOD world



Client Device Management

- Mobile Device Management (MDM)
- MDM solution might be needed for onboarding personal mobile devices as well as corporate issued devices
- Corporate IT departments can deploy MDM to manage, secure, and monitor the mobile devices



CWNA BYOD

Install your MDM Profile

After you tap the **Install Profile** button, you will need to complete the steps listed below.

1. Tap the **Install** button.

MDM Profile
TechMarketing

Description: This profile ensures the security of your mobile device.

Signed: TechMarketing JSS Signing Certificate

Received: Jun 21, 2012

Contains: Device enrollment challenge

Enrollment Complete!

Congratulations! Your mobile device has been enrolled.

Not Configured

LDAP
Not Configured

Calendar
Not Configured

☑ Allow user-generated content in Siri

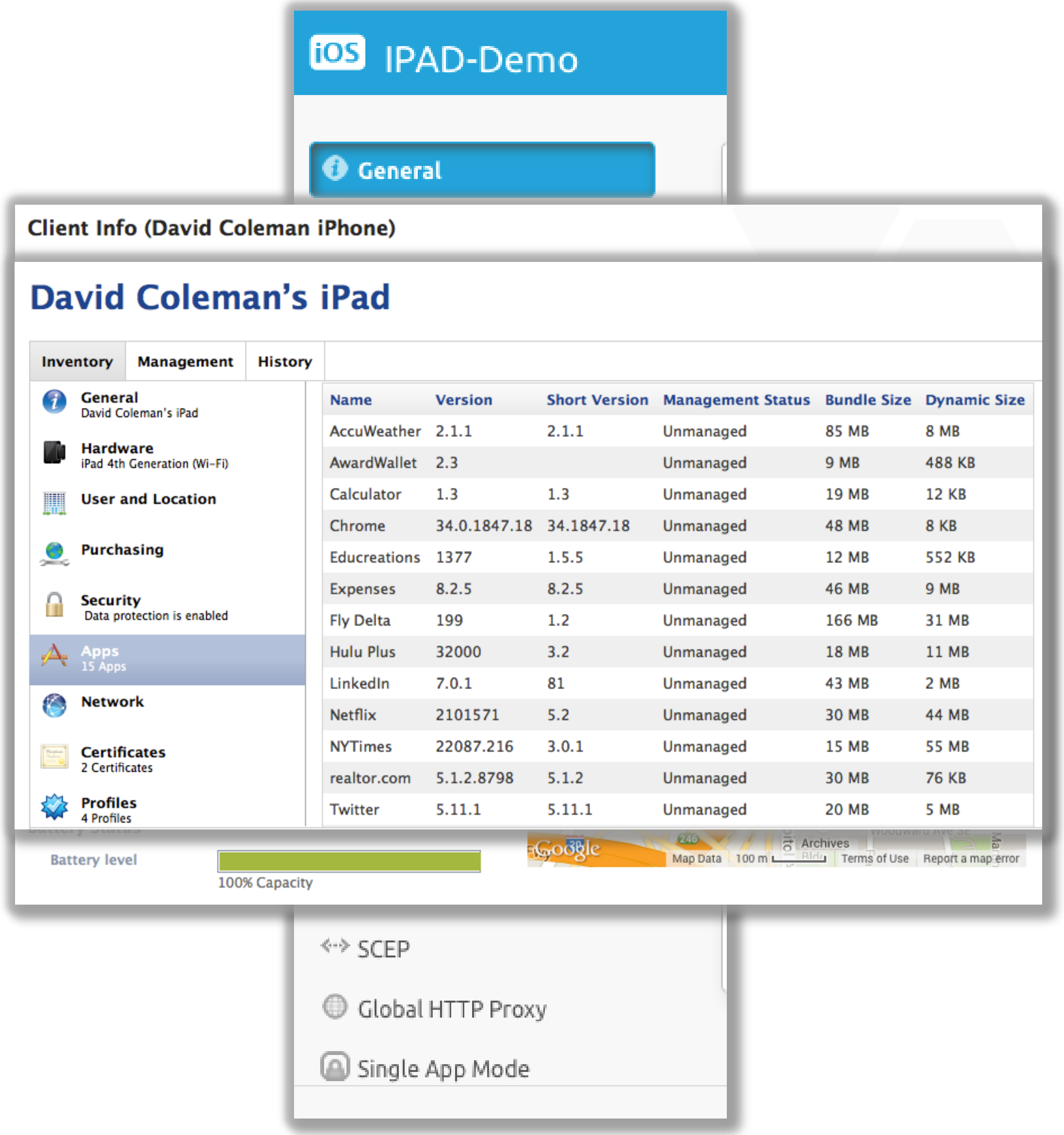
☑ Allow iBookstore (Supervised devices only)

□ Allow installing apps

☑ Allow removing apps (Supervised devices only)

Client Device Management

- Mobile Device Management (MDM)
- Secure over-the-air provisioning of MDM profiles - Device restrictions
- Easy way to distribute root CA certificates for 802.1X security with mobile devices
- Over-The-Air Management
- Application Management



Client Info (David Coleman iPhone)

David Coleman's iPad

Name	Version	Short Version	Management Status	Bundle Size	Dynamic Size
AccuWeather	2.1.1	2.1.1	Unmanaged	85 MB	8 MB
AwardWallet	2.3		Unmanaged	9 MB	488 KB
Calculator	1.3	1.3	Unmanaged	19 MB	12 KB
Chrome	34.0.1847.18	34.1847.18	Unmanaged	48 MB	8 KB
Educreations	1377	1.5.5	Unmanaged	12 MB	552 KB
Expenses	8.2.5	8.2.5	Unmanaged	46 MB	9 MB
Fly Delta	199	1.2	Unmanaged	166 MB	31 MB
Hulu Plus	32000	3.2	Unmanaged	18 MB	11 MB
LinkedIn	7.0.1	81	Unmanaged	43 MB	2 MB
Netflix	2101571	5.2	Unmanaged	30 MB	44 MB
NYTimes	22087.216	3.0.1	Unmanaged	15 MB	55 MB
realtor.com	5.1.2.8798	5.1.2	Unmanaged	30 MB	76 KB
Twitter	5.11.1	5.11.1	Unmanaged	20 MB	5 MB

Battery level: 100% Capacity

Client Device Management

- Internet of Things (IoT)
- 802.1X not always an option
- PPSK provides unique secure credentials

Why Provide Guest Access?

Many studies have shown that providing WLAN guest access is beneficial to your business:

- **Improved Productivity:** Customers and contractors often need access to the Internet to accomplish job-related duties. If customers and contractors are more productive, your company employees will also be more productive.
- **Customer Loyalty:** In today’s world, business customers have come to expect Guest WLAN access. Free guest access is often considered a value-added service. There is a good chance that your customers will move towards your competitors if you do not provide WLAN guest access.

Guest Management

Four guest WLAN common best practices include:

- **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:** A guest firewall policy is the most important component of WLAN guest management.

Guest Management

Different ways to skin a cat:

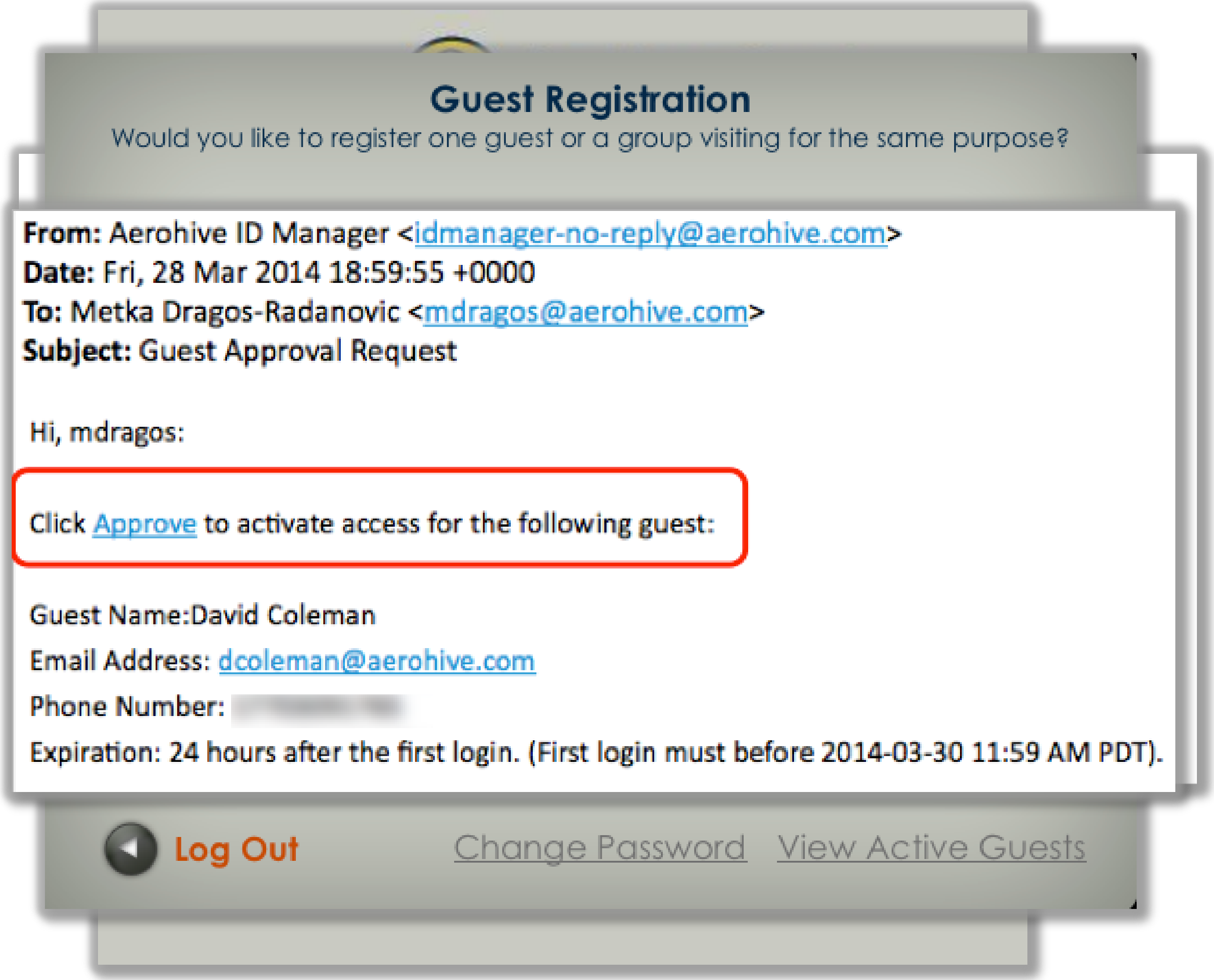
- **Corporate SSID:** Wireless guest users can be placed on the employee SSID if there is a way to use RBAC mechanisms to isolate them with strong firewall policies.
  - Still segment in a separate VLAN
  - May not be acceptable for certain verticals such as finance or government
- **Captive Web Portal:** Captive web portals are often more trouble than they are worth and are sometimes simply not used.

Other suggestions:

- **Rate Limiting:** The bandwidth of guest traffic can be throttled with a rate control policy.
- **Peer Blocking:** Guest users should be prevented from peer-to-peer connectivity on the guest VLAN/subnet. This prevents peer-to-peer attacks.

Guest Management

- Robust guest management solutions
  - Time based guest credentials
  - Guest credential delivery printed receipt, email, SMS
  - Self-service kiosks
  - Employee sponsorship



Guest Registration

Would you like to register one guest or a group visiting for the same purpose?

From: Aerohive ID Manager <idmanager-no-reply@aerohive.com>
Date: Fri, 28 Mar 2014 18:59:55 +0000
To: Metka Dragos-Radanovic <mdragos@aerohive.com>
Subject: Guest Approval Request

Hi, mdragos:

Click Approve to activate access for the following guest:

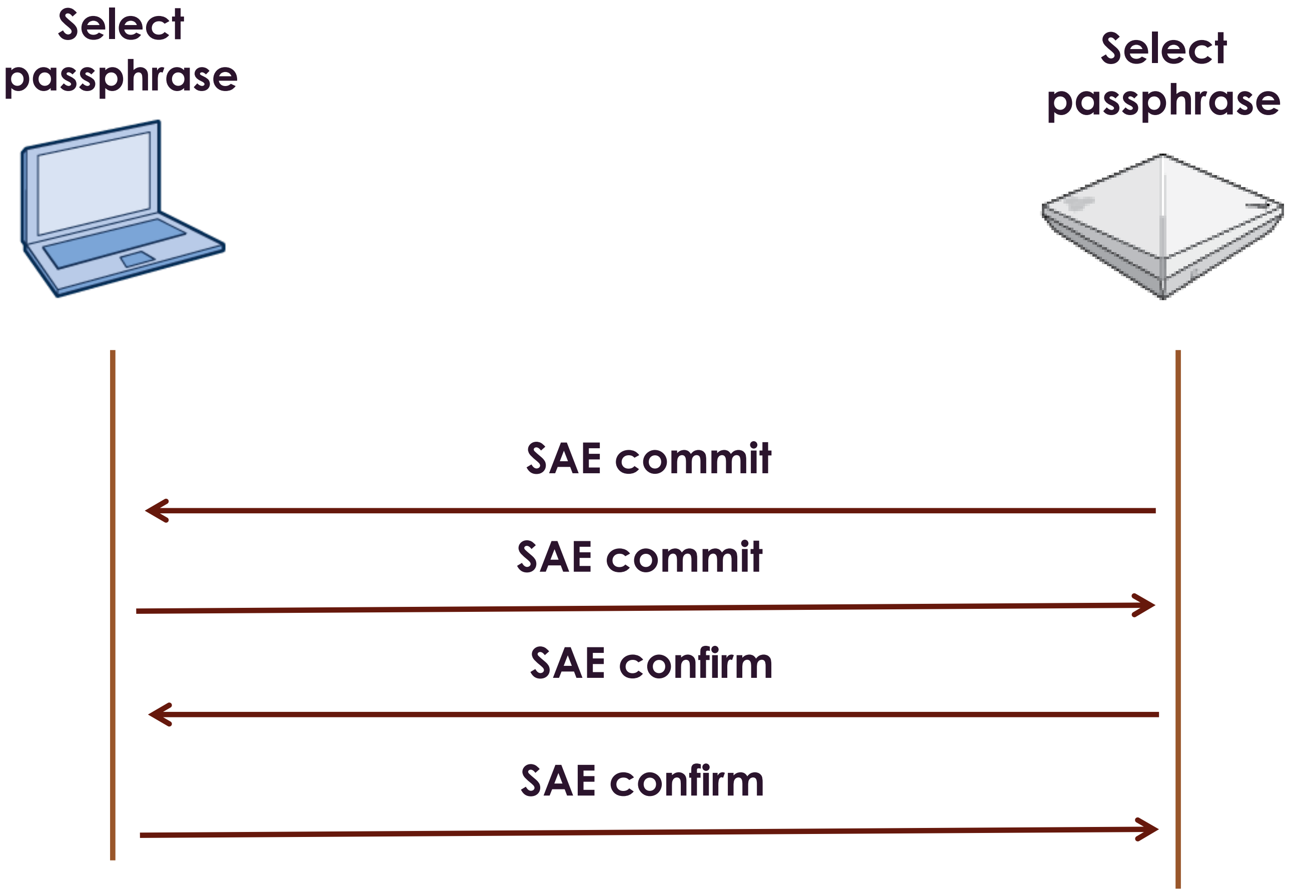
Guest Name:David Coleman
Email Address: dcoleman@aerohive.com
Phone Number: [redacted]
Expiration: 24 hours after the first login. (First login must before 2014-03-30 11:59 AM PDT).

Guest Management

- Encrypted guest access
  - PPSK
  - Hotspot 2.0
- Social Login

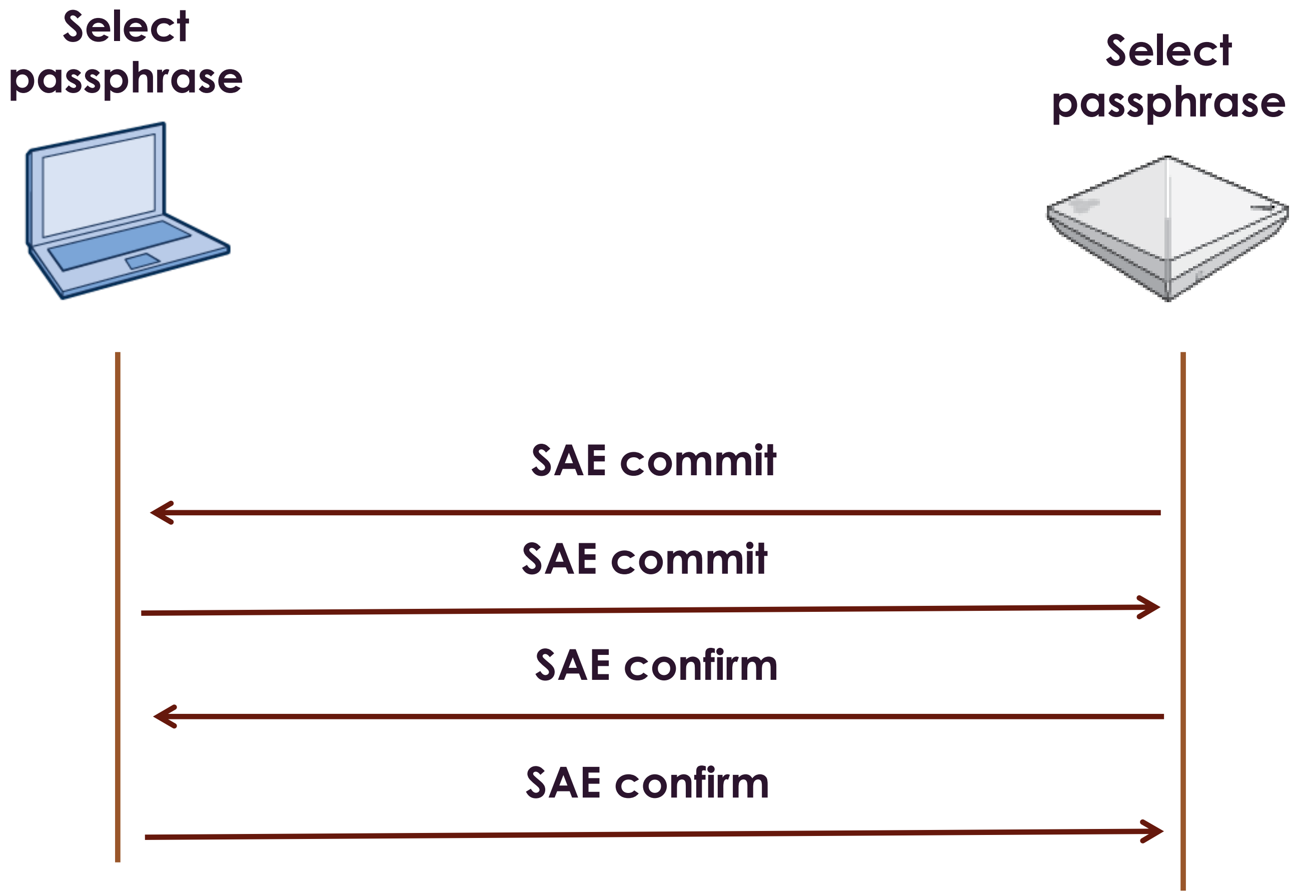
Future of WLAN Security

- Future 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



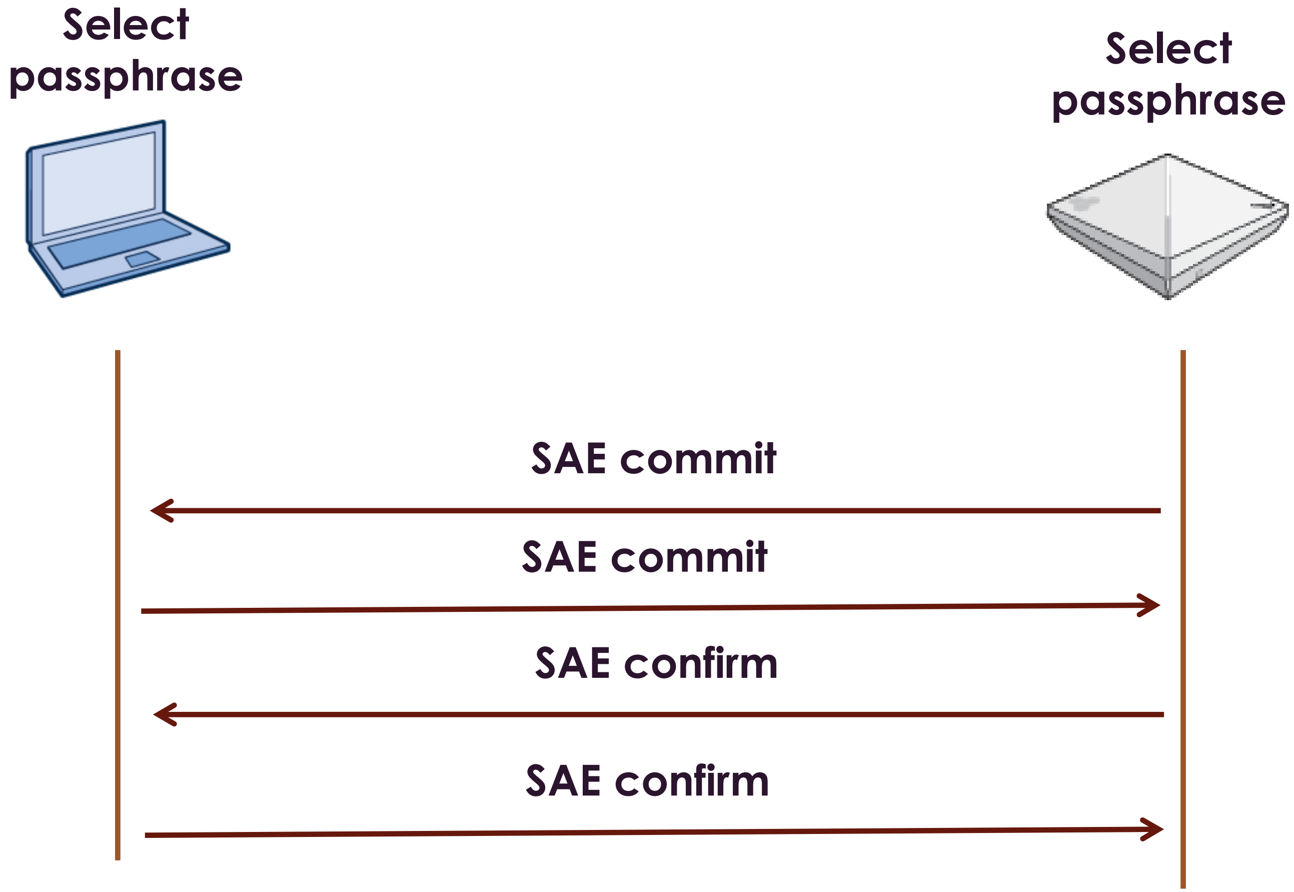
Future of WLAN Security

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



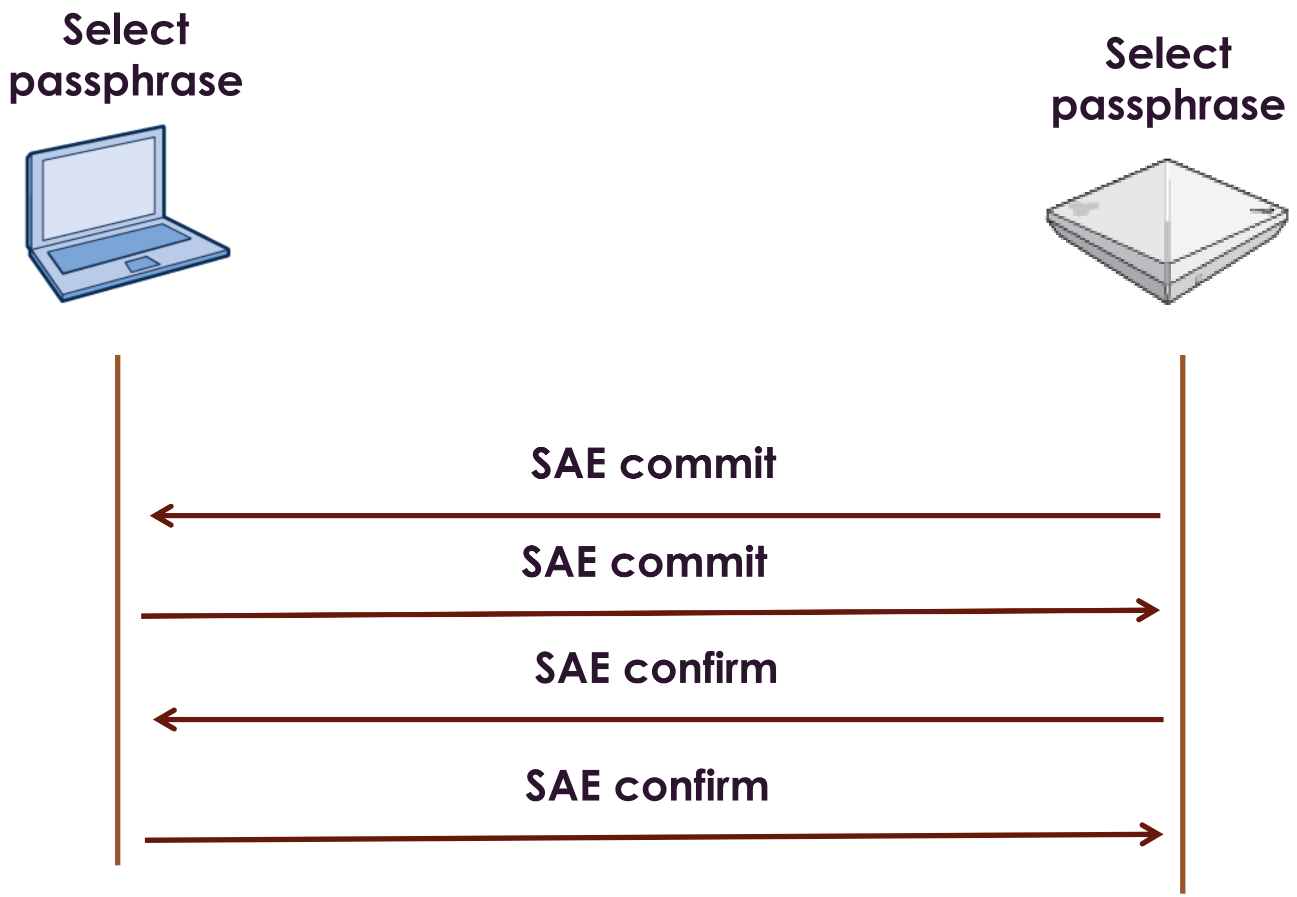
Future of WLAN Security

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



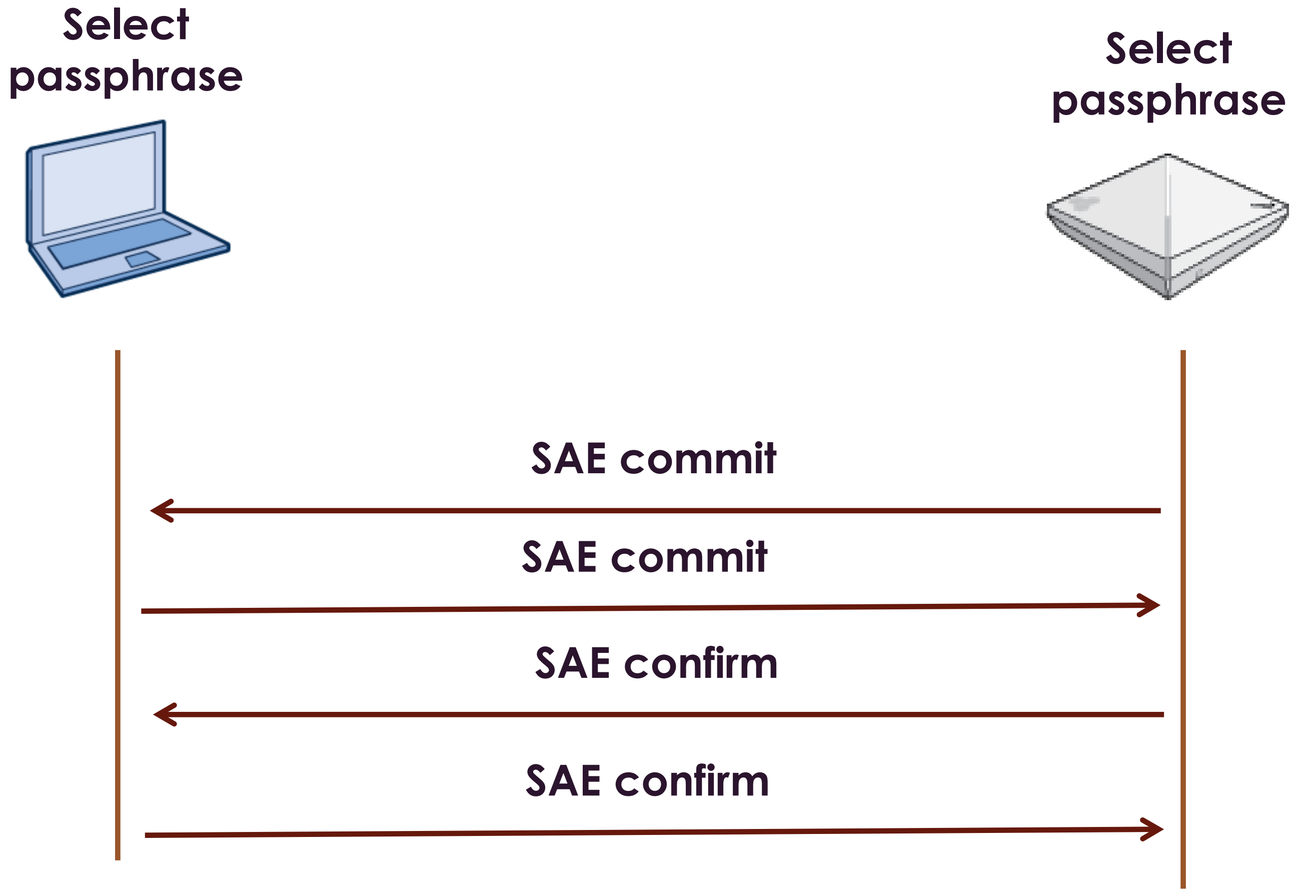
Future of WLAN Security

- Two authentication message exchanges:
  - commitment exchange used to guess password
  - confirmation exchange to prove password was guessed correctly
- PMK is then derived
- 4-Way Handshake



Future of WLAN Security

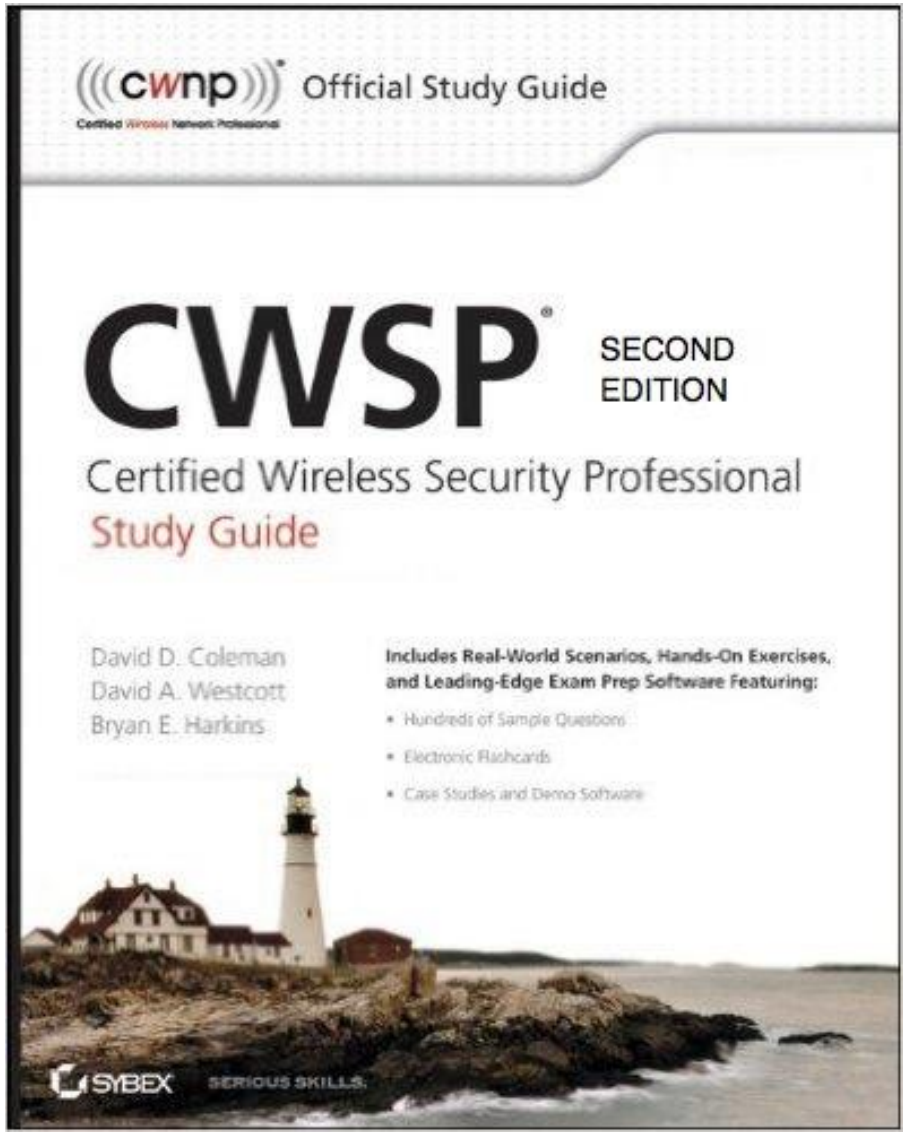
- Prove you know the passphrase without compromising the passphrase
- No forging, modification or replay attacks
- No offline dictionary attacks



Coming Soon:

- Sybex CWSP Study Guide
  Second Edition
- Amazon preorder:

http://amzn.com/1119211085



cwnp Official Study Guide

Certified Wireless Network Professional

CWSP SECOND EDITION

Certified Wireless Security Professional
Study Guide

David D. Coleman
David A. Westcott
Bryan E. Harkins

Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Hundreds of Sample Questions
- Electronic Flashcards
- Case Studies and Demo Software

SYBEX SERIOUS SKILLS.

Questions?

Thank you!

Aerohive NETWORKS