Mobility Day 2019

Tim Cappalli | Identity Architect @ Aruba

6/20/19
New Technologies
WPA3 and Enhanced Open
## WPA3-Personal (SAE)

<table>
<thead>
<tr>
<th>THE TECH</th>
<th>WHAT IT MEANS</th>
<th>UX IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based off a Dragonfly key exchange</td>
<td>&quot;Weak&quot; passwords are less prone to to attack</td>
<td>None!</td>
</tr>
<tr>
<td>Zero knowledge proof</td>
<td>One passphrase guess per attack</td>
<td></td>
</tr>
</tbody>
</table>
# WPA3-Enterprise 192-bit Mode (CNSA)

<table>
<thead>
<tr>
<th><strong>THE TECH</strong></th>
<th><strong>WHAT IT MEANS</strong></th>
<th><strong>UX IMPACT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>192-bit encryption (Suite B)</td>
<td>EAP-TLS Only</td>
<td>Not something an average end-user would need to configure</td>
</tr>
<tr>
<td>TLS 1.2+</td>
<td>Higher security</td>
<td></td>
</tr>
<tr>
<td>Restricted cipher suites</td>
<td>Not backwards compatible</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EAP server certificate changes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3072-bit+</td>
<td>P-384)</td>
</tr>
</tbody>
</table>

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
Enhanced Open

THE TECH
Uses OWE
(Opportunistic Wireless Encryption)
Diffie-Hellman
Key Exchange

WHAT IT MEANS
Datapath encryption
by default!
Backwards compatible
with legacy open

UX IMPACT
Very little
Potential
new indicators
<table>
<thead>
<tr>
<th>OS / Supplicant</th>
<th>WPA3</th>
<th></th>
<th></th>
<th>Enhanced Open (OWE)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Personal</td>
<td>Personal with Password ID</td>
<td>Enterprise 192-bit Mode (CNSA)</td>
<td></td>
</tr>
<tr>
<td>Windows 10</td>
<td>1903*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>Q (10)*</td>
<td>Q (10)</td>
<td>Q (10)</td>
<td>Q (10)*</td>
</tr>
<tr>
<td>macOS</td>
<td>10.15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wpa_supplicant</td>
<td>2.7</td>
<td>2.7</td>
<td>2.7</td>
<td>2.7</td>
</tr>
</tbody>
</table>
iOS and macOS
Profile Installation
Changes in iOS
Certificate Requirements
(macos 10.15)

GENERAL

2048-bit or greater private key

SHA-256+ hash

Max 825 Days (leaf)

EAP SERVER CERTIFICATE

SAN must be present

Non-EV
(DV or OV)
Windows 10
MAC Randomization in Windows 10

GLOBAL

Probe MAC randomized

MAC generated per saved ESSID
Hash(MAC, secret, ESSID, connection ID)

PER-ESSID

A. Use hardware MAC address
B. Use fixed random MAC address
C. Rotate MAC address daily

*** BOTH REQUIRE HARDWARE (AND DRIVER) SUPPORT ***

SOURCE: MICROSOFT
EAP Server Certificate Validation

EAP server identity validation must now be configured

CA certificate
Use system certificates

Domain

Must specify a domain.
MAC Randomization in Android

Enabled by default

Generated when the SSID is

Saved to the network list

Persistent for OS instance

lifetime

Manual control available
Passpoint
Hotspot 2.0
**How does it work?**

**PLMN:**
- 310410
- 310260

**FQDN:**
- harvard.edu
- eduroam.org

**BEACON**
- Hotspot 2.0
- RCOI: 00-1B-C5-04-60

**ESSID:**
- WXYZ

**ANQP Query**
- PLMN: 310410
- PLMN: 310260
- FQDN: harvard.edu
- NAI: eduroam.org
<table>
<thead>
<tr>
<th>OS</th>
<th>R1</th>
<th>R2</th>
<th>R3</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSU</td>
<td></td>
<td>EAP-TLS</td>
<td>EAP-TTLS</td>
</tr>
<tr>
<td>Windows 10</td>
<td></td>
<td>Q (10)</td>
<td>Q (10)</td>
</tr>
<tr>
<td>Android</td>
<td>*</td>
<td>Q (10)</td>
<td>Q (10)</td>
</tr>
<tr>
<td>macOS</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wpa_supplicant</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Current Challenges

– Android EAP server trust
– iOS network selection behavior
– Apple's proprietary configuration format
– Windows 10 provisioning
– Privacy
RADIUS/TLS
RadSec
RadSec Flavors

– RADIUS over TLS
  – Also referred to as RADIUS/TLS
  – TCP 2083

– RADIUS over DTLS
  – Also referred to as RADIUS/DTLS
  – UDP 2083
"EAP Stack" for RADIUS/TLS

- EAP
- RADIUS
- TLS
- TCP
- IP
RADIUS/TLS

RadSec Client Certificate

mTLS

RadSec Server Identity

TLS TUNNEL

RADIUS
RADIUS ACCOUNTING
RADIUS DYNAMIC AUTHORIZATION

TLS TUNNEL

RadSec Client

TCP 2083

RadSec Server
Why is RADIUS/TLS so important?

**PERFORMANCE**
- Congestion control
- No duplicate requests
- Persistent session
- No UDP fragmentation issues

**SECURITY**
- (next few slides)
Why is RADIUS/TLS so important?

Remote Authentication Dial In User Service (RADIUS)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.

Table of Contents
Why is RADIUS/TLS so important?

- **User Datagram Protocol, Src Port: 1812, Dst Port: 36918**
- **RADIUS Protocol**
  - Code: Access-Accept (2)
  - Packet identifier: 0x93 (147)
  - Length: 250
  - Authenticator: 72d6262108a87b241a242183b19eccd4
    
    [This is a response to a request in frame 20744]
    [Time from request: 0.033581000 seconds]
- **Attribute Value Pairs**
  - AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft (311)
    - Type: 26
    - Length: 58
    - Vendor ID: Microsoft (311)
  - VSA: t=MS-MPPE-Recv-Key(17) l=52 val=c8e90f13fdf59ae1ab1b16f1dc1cc5a9057e922ce473ffa...
  - AVP: t=Vendor-Specific(26) l=58 VND=Microsoft(311)
    - Type: 26
    - Length: 58
    - Vendor ID: Microsoft (311)
  - VSA: t=MS-MPPE-Send-Key(16) l=52 val=d1b65014ea21cddb4155c84ec425b12471e6ac33318da373...
  - AVP: t=EAP-Message(79) l=6 Last Segment[1]
  - AVP: t=Message-Authenticator(80) l=18 val=e4915b66043edc0495e0c13f9e73efd2
  - AVP: t=User-Name(1) l=10 val=mlavelle
  - AVP: t=Vendor-Specific(26) l=22 vnd=Aruba Networks Inc(14823)
  - AVP: t=Class(25) l=58 val=e885ee10bf3a420b9cd2e4706a53ea88100c00000000000...
    - Type: 25
Why is RADIUS/TLS so important?

<table>
<thead>
<tr>
<th>Attribute Value Pairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVP: t=User-Name(1) l=35 val=asa-sensor.device.arubaboston.com</td>
</tr>
<tr>
<td>Type: 1</td>
</tr>
<tr>
<td>Length: 35</td>
</tr>
<tr>
<td>User-Name: asa-sensor.device.arubaboston.com</td>
</tr>
<tr>
<td>AVP: t=NAS-IP-Address(4) l=6 val=100.66.1.101</td>
</tr>
<tr>
<td>AVP: t=NAS-Port(5) l=6 val=0</td>
</tr>
<tr>
<td>AVP: t=NAS-Identifier(32) l=12 val=805-7010-A</td>
</tr>
<tr>
<td>AVP: t=NAS-Port-Type(61) l=6 val=Wireless-082.11(19)</td>
</tr>
<tr>
<td>AVP: t=Calling-Station-Id(31) l=19 val=20-4C-03-31-20-8D</td>
</tr>
<tr>
<td>Type: 31</td>
</tr>
<tr>
<td>Length: 19</td>
</tr>
<tr>
<td>Calling-Station-Id: 20-4C-03-31-20-8D</td>
</tr>
<tr>
<td>AVP: t=Called-Station-Id(30) l=29 val=80-08-80-9A-E3-07:cappy roam</td>
</tr>
<tr>
<td>AVP: t=Service-Type(6) l=6 val=Frame d(2)</td>
</tr>
<tr>
<td>AVP: t=Framed-MTU(12) l=6 val=1100</td>
</tr>
<tr>
<td>AVP: t=EAP-Message(79) l=40 Last Segment[1]</td>
</tr>
<tr>
<td>AVP: t=Vendor-Specific(26) l=17 vnd=Aruba Networks Inc(14823)</td>
</tr>
<tr>
<td>Type: 26</td>
</tr>
<tr>
<td>Length: 17</td>
</tr>
<tr>
<td>Vendor ID: Aruba Networks Inc (14823)</td>
</tr>
<tr>
<td>AVP: t=Aruba-Essid-Name(5) l=11 val=cappy roam</td>
</tr>
<tr>
<td>AVP: t=Vendor-Specific(26) l=18 vnd=Aruba Networks Inc(14823)</td>
</tr>
<tr>
<td>Type: 26</td>
</tr>
<tr>
<td>Length: 18</td>
</tr>
<tr>
<td>Vendor ID: Aruba Networks Inc (14823)</td>
</tr>
<tr>
<td>AVP: t=Aruba-Location-Id(6) l=12 val=805-335-LR</td>
</tr>
<tr>
<td>AVP: t=Vendor-Specific(26) l=16 vnd=Aruba Networks Inc(14823)</td>
</tr>
<tr>
<td>Type: 26</td>
</tr>
<tr>
<td>Length: 16</td>
</tr>
<tr>
<td>Vendor ID: Aruba Networks Inc (14823)</td>
</tr>
<tr>
<td>AVP: t=Aruba-AP-Group(10) l=10 val=805-Main</td>
</tr>
<tr>
<td>AVP: t=Acct-Session-Id(44) l=29 val=204C031280D-5C62D97D-1DC0E</td>
</tr>
<tr>
<td>AVP: t=Message-Authenticator(88) l=18 val=4d8e0480be85c23e68aee35a46eb96d</td>
</tr>
</tbody>
</table>
RADIUS/TLS Support

Mobility Controllers
Instant APs
Switches
ClearPass (6.8)

FreeRADIUS (v3) | Packetfence
Thanks!

Questions?