ERNW GmbH

Hardening Cisco Access Points

Version 0.9

von Enno Rey (erey@ernw.de**)**

Table of Contents

1 INTRODUCTION 3

2 SOFTWARE IMAGE 3

3 DISABLE ALL UNUSED RADIO INTERFACES/SERVICES/INTERFACE FUNCTIONALITY 4

3.1 Unused radio interface 4

3.2 Unused services 4

3.3 Disable unused interface functionality 5

4 MANAGEMENT 5

4.1 SSH 5

4.2 Web-Interface 6

4.3 SNMP 6

4.4 Configuration of time 7

4.4.1 Standard stuff that should be in the config 7

5 AUTHENTICATION 8

5.1 Local user database 8

5.2 Authentication with local AAA server 8

5.3 External AAA server 9

5.4 Login Enhancements 9

6 SEGMENTATION/SEGREGATION 10

6.1 Associated configuration of trunk port on switch (here Cisco 3550) 11

6.2 Mapping of VLANs to SSIDs 11

7 WLAN AUTHENTICATION AND ENCRYPTION 12

7.1 MAC-based authentication 12

7.2 WEP 12

7.3 WPA 13

7.4 LEAP with local AAA server 13

8 MISCELLANEOUS 14

8.1 ACLs 14

8.2 PSPF 14

8.3 Monitoring/Intrusion Detection 14

8.3.1 Logmessages to look for 14

9 CHECKLIST 14

10 APPENDIX A: SAMPLE CONFIG WITH SOME PARTS DESCRIBED IN THIS DOC 15

1 INTRODUCTION

In this document a basic hardening methodology for Cisco Access Points (of the 1200 series, most steps should apply to others as well) is described. It's assumed the AP(s) work(s) autonomously (i.e. not managed by a WLAN Controller) and there's no central management entity (like WLSE). Thus the main audience of this doc will be SOHO environments disposing of not more than a handful of APs. This doc is just a rough outline, without the intent of being complete, overly well structured or stylishly expressed.

Everything is done via CLI, for the following reasons:

- it's easier to understand (at least for me ;-)
- it can be scripted more easily, be for configuration, be for audit scripts.
- to show everything can (still) be done via CLI.
- most web based GUIs contain application based errors… so turn them off if not needed.

Please note: if the personnel operating the APs is not seasoned/trained properly in doing so, it might be a good idea to leave the GUI turned on (to avoid configuration errors with security impact). Recent examples of vulnerable web interfaces in the Cisco world include:
http://www.cisco.com/en/US/products/products_security_advisory09186a00806cd92f.shtml
http://www.cisco.com/en/US/products/products_security_response09186a00807b8f76.html
http://www.cisco.com/en/US/products/products_security_advisory09186a00806e0bc3.shtml

2 SOFTWARE IMAGE

The following image is running on the lab device; at least newer images should be capable of performing everything described herein.

```
Cisco IOS Software, C1200 Software (C1200-K9W7-M), Version 12.3(8)JA2,
…
System image file is "flash:/c1200-k9w7-mx.123-8.JA2/c1200-k9w7-mx.123-8.JA2
```

3 DISABLE ALL UNUSED RADIO INTERFACES/SERVICES/INTERFACE FUNCTIONALITY

3.1 Unused radio interface

The AP in question here has an 802.11 b/g radio interface as well as an 802.11a interface.

```
ap>sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
BVI1                       10.1.1.51       YES other  down                  down

Dot11Radio0                unassigned      YES unset  administratively down down
Dot11Radio1                unassigned      YES unset  administratively down down
FastEthernet0              unassigned      YES other  up                    down
```

We don't need the latter one so it can be disabled:

```
ap(config)#int Dot11Radio1
ap(config-if)#shut
ap(config-if)#exi
ap(config)#
```

Please note that the default state is "shut" anyway. This step is included here for the sake of completeness and to provide a kind of checklist or recipe for APs already running.

3.2 Unused services

All probably unused services should be disabled at this point. Note we still leave the HTTP(S) server enabled… just in case you still want to configure things in a GUI based way. It will be turned off later on.

```
ap(config)#no service tcp-small-servers
ap(config)#no service udp-small-servers
ap(config)#no ip finger
ap(config)#no service finger
ap(config)#no service config
ap(config)#no service pad
ap(config)#no service dhcp
ap(config)#no ip source-route
ap(config)#no boot system
ap(config)#no ip gratuitous-arps
ap(config)#no cdp run
```

Some of these may be debatable (maybe you want to use the built-in DHCP server); your mileage will vary then…

Please note, that CDP might be needed for discovery purposes when using *CiscoWorks* or *WLSE*.

3.3 Disable unused interface functionality

```
ap(config)#int bvi1
ap(config-if)#no ip proxy-arp
ap(config-if)#no ip mask-reply
ap(config-if)#no ip directed-broadcast
ap(config-if)#no keepalive
ap(config-if)#no cdp enable
ap(config-if)#exi
ap(config)#
```

Again: you may (for whatever reason) need some of these. If in doubt check the command reference and understand what the respective commands perform.

It should be sufficient to use (most of) these ones on the BVI interface(s). If paranoid feel free to perform them on the physical interfaces too.

4 MANAGEMENT

4.1 SSH

Enable SSH and disable telnet (and anything else) on the VTYs. To enable SSH the device needs a FQDN. If needed restrict mgmt access to some source IPs only.

```
ap(config)#hostname hdz-ap-001
hdz-ap-001(config)#ip domain-name ernw.de
hdz-ap-001(config)#crypto key gen rsa
The name for the keys will be: hdz-ap-001.ernw.de
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys ...[OK]

hdz-ap-001(config)#
*Mar  1 00:23:43.710: %SSH-5-ENABLED: SSH 1.99 has been enabled
hdz-ap-001(config)#line vty 0 15
hdz-ap-001(config-line)#transport input ssh
hdz-ap-001(config-line)#exi
hdz-ap-001(config)#
```

In this example line access will only be permitted for the hosts 192.168.96.12 and 192.168.96.83.

```
hdz-ap-001(config)#ip access-list standard 1
hdz-ap-001(config-std-nacl)#permit 192.168.96.12
hdz-ap-001(config-std-nacl)#permit 192.168.96.83
hdz-ap-001(config-std-nacl)#exi
hdz-ap-001(config)#line vty 0 15
hdz-ap-001(config-line)#access-class 1 in
hdz-ap-001(config-line)#exi
```

Test if SSH access is working!

4.2 Web-Interface

If you want to use the Web-Interface at all, only use the HTTPS-variant and restrict the allowed source addresses also.

Keep in mind that most web interfaces are vulnerable in some way (see above). To disable 'plain http' and enable https, perform:

```
hdz-ap-001(config)#no ip http server
hdz-ap-001(config)#ip http secure-server
% Generating 1024 bit RSA keys ...[OK]

hdz-ap-001(config)#
*Mar  1 00:32:16.872: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue
"write memory" to save new certificate
hdz-ap-001(config)#do wr mem
Building configuration...
[OK]
```

You should now have a certificate and be able to connect when needed. I myself will disable the whole web-based stuff anyway[1].

Though not mentioned in the command reference, "crypto pki trustpoint" commands can be performed to enroll certificates of other CAs than the built-in. At a first glance (not tested) the "usual Cisco enrollment methods" (SCEP ['url'], manual enrollment ['terminal']) seem available.

4.3 SNMP

What can I say here? See my presentation at *IT-Underground 2007*[2] (and at other occasions) to understand why SNMP is dangerous (you knew that already, didn't you?). Suffice to say you should be extremely cautious if using SNMP on APs. When using

[1] The associated ('internal') trustpoint can be deleted then (and with it the certificate).
[2] *http://www.itunderground.org/en/conferences/it_underground/praga2007/agenda.html*

community based SNMP (SNMPv3 seems supported on this AP/IOS, however I did not test) in addition to the 'usual stuff' (use of good RW community strings [if RW at all], restriction of authorized managers etc.), restricting the views can be helpful:

```
snmp-server view basic iso included
snmp-server view basic ieee802dot11 included
snmp-server community n0_wlan_xyz_ro view basic RO
snmp-server community n0_wlan_xyz_rw view basic RW
```

Please note that the handy command "logging snmp-authfail" seems supported (though undocumented). You should definitely use this when SNMP is needed/enabled:

```
hdz-ap-001(config)#logging snmp-authfail
Logging of %SNMP-3-AUTHFAIL is enabled
hdz-ap-001(config)#
```

4.4 Configuration of time

Why this is important? See RFC 3871, section 2.11.5 or ISO 17799:2005, section 10.10.6.
The IOS used here does not support NTP, but SNTP:

```
hdz-ap-001(config)#sntp ?
  broadcast  Configure SNTP broadcast services
  logging    Enable SNTP message logging
  server     Configure SNTP server
```

A sample configuration could look like this, depending on your [security] needs:

```
sntp server 192.168.126.31
sntp broadcast client
```

4.4.1 Standard stuff that should be in the config

```
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
clock timezone GMT 1
clock summer-time mesz recurring last Sun Mar 2:00 last Sun Oct 3:00
```

5 AUTHENTICATION

The authentication (of mgmt access or for WLAN clients via 802.1x) can be performed either locally (with a local user database or a local AAA server) or by means of one/some AAA server(s).

5.1 Local user database

This is the easiest variant (the 'classical'):

```
hdz-ap-001#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
hdz-ap-001(config)#service password-encryption
hdz-ap-001(config)#enable secret xyz
hdz-ap-001(config)#no user Cisco
hdz-ap-001(config)#username erey secret abc
```

Please note that you should use the username command together with the "secret" keyword for the password. This leads to an MD5 encrypted pw instead of the legacy type-7 password encryption (that could easily be cracked with tools like *getpass*). Be aware, that MD5 hashed passwords *may* still be cracked (e.g. with tools like tomas[3])

Do not forget to delete the default account "Cisco"!

5.2 Authentication with local AAA server

The 1200 series (with certain IOSs?) dispose of a local AAA server (with max. 50 Users) that can be used e.g. for LEAP authentication. This avoids the necessity of running an external AAA server and may thus be well suited for small environments or remote sites. You should be aware that LEAP is considered broken (see papers/tool of *Joshua Wright*). Cracking LEAP is done by bruteforcing so choosing a long complex password may help, depending on your risk-analysis. In scenarios without external AAA server this *may* be a better solution than using a shared WPA key (e.g. with temporary users).

Depending on the (WPA2-) capabilities of the AP the configuration could look like this (with LEAP authentication):

```
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.78.3 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
aaa session-id common
!
dot11 ssid xyz
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   guest-mode
```

[3] *www.ernw.de/tools/tomas.zip*

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip         ! better aes, depends on AP capabil.
 !
 ssid xyz

radius-server local
  no authentication eapfast
  no authentication mac
  nas 192.168.78.3  key 7 some_key_here_same_as_below
  user erey nthash 7 41331234411B1230D2FFF323C205E5A
  user miller ...

!
radius-server  host  192.168.78.3  auth-port  1812  acct-port  1813  key  7
     same_key_here_as_above    ! address of BVI
```

Take care that something like

`ip radius source-interface BVI1`

can be found in your config (I assume I do not need to explain the function of this command, do I?). This is added by default anyway.

5.3 External AAA server

The config here is the same as in routers' IOS... copy+paste from respective devices or check cco.

5.4 Login Enhancements

Current IOS versions support so-called (and btw: long awaited) "Login enhancements"[4] to defeat password bruteforcing. Stuff like this might be needed (e.g. for 'compliance reasons') and can be helpful in stopping (slowing down) attackers, so use it (modify parameters for your needs):

```
hdz-ap-001(config)#login block-for 300 attempts 5 within 30
hdz-ap-001(config)#login delay 2
hdz-ap-001(config)#login on-failure log
hdz-ap-001(config)#login on-failure trap
hdz-ap-001(config)#login on-access
```

[4] *http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455b93.html*

6 SEGMENTATION/SEGREGATION

The basic network security principles of segmentation and segregation apply equally to wireless networks. Most modern APs support VLANs. This is here the case as well.

The basis for segmentation may be

- different management structures
- different security needs
- different level of exposure/vulnerabilities
- different client capabilities (printers/mobile data agents/etc. vs. WinXP)

We will use three VLANs here: one for mgmt that will serve no wireless segment. One with lower security requirements (for legacy clients) and another one for higher security requirements (for modern clients). These are just examples to show the configuration of VLANs, use any other technology at your will.

For these ones we will use according subinterface ids on the respective radio and fasteth interfaces. The VLANs are associated to SSIDs then.

Mgmt Vlan (Vlan ID 96)

```
hdz-ap-001(config)#int fa0.96
hdz-ap-001(config-subif)#no shut
hdz-ap-001(config-subif)#no ip dir
hdz-ap-001(config-subif)#no ip proxy
hdz-ap-001(config-subif)#no ip mask
hdz-ap-001(config-subif)#encapsulation dot1Q 96
hdz-ap-001(config-subif)#bridge-group 1
hdz-ap-001(config-subif)#exi
hdz-ap-001(config)#int bvi1
hdz-ap-001(config-if)#no shut
hdz-ap-001(config-if)#ip add 192.168.96.10 255.255.255.0
hdz-ap-001(config-if)#exi
hdz-ap-001(config)#exi
```

Client VLAN 97

```
hdz-ap-001(config)#int dot11r0.97
hdz-ap-001(config-subif)#no shut
hdz-ap-001(config-subif)#encapsulation dot1Q 97
hdz-ap-001(config-subif)#bridge-group 97
hdz-ap-001(config-subif)#exi
hdz-ap-001(config)#int fa0.97
hdz-ap-001(config-subif)#encapsulation dot1Q 97
hdz-ap-001(config-subif)#bridge-group 97
hdz-ap-001(config-subif)#exi
hdz-ap-001(config)#
```

Client VLAN 90

The resulting (sub-) interface config should look like this:

```
interface Dot11Radio0.90
 encapsulation dot1Q 90
 no ip route-cache
 no cdp enable
 bridge-group 90
 bridge-group 90 subscriber-loop-control
 bridge-group 90 block-unknown-source
 no bridge-group 90 source-learning
 no bridge-group 90 unicast-flooding
 bridge-group 90 spanning-disabled
```

Please note, that the last five parameters are default ones; so modify if needed. From a security point of view these are reasonable.

If needed the *native vlan* can be configured with something like:
`encapsulation dot1Q 96 native`
in (sub-) interface configuration mode.

6.1 Associated configuration of trunk port on switch (here Cisco 3550)

Enable trunk on switch and limit vlans to be transported:

hdz-core-002(config-if)#switchport trunk encapsulation dot1q
hdz-core-002(config-if)#switchport mode trunk
hdz-core-002(config-if)#switchport trunk allowed vlan 90,96,97

6.2 Mapping of VLANs to SSIDs

The two VLANs are mapped to SSIDs with different security parameters (example with WPA-PSK and MAC-based auth):

```
dot11 ssid first!
   vlan 90
   authentication open
   authentication key-management wpa
   wpa-psk ascii 7 some_wpa_key
!
dot11 ssid second
   vlan 97
   authentication open mac-address mac_methods
```

7 WLAN AUTHENTICATION AND ENCRYPTION

There's pretty much stuff out there on this, discussing the pros and cons of different WLAN security technologies. Basically the discussions can be broken down to:

WEP, MAC-based authentication, LEAP (depends) and WPA-PSK (depends) are generally considered broken or 'weak', some 802.1x flavors (in particular the ones using certificates) are regarded as 'strong' and thus recommended. Being a risk-analysis advocate and trying to keep an eye on the reality out there I just recommend to perform some individual risk-analysis and to understand the benefits, threats, risks and mitigating controls of each technology. Here I'll just describe to configure them, I leave it up to the reader to use these or others. The main requirement/restriction here is independence of an external AAA server.

7.1 MAC-based authentication

Pros: you don't need to touch the client.

Cons: may easily be subverted by skilled & motivated attacker. Difficult to manage.

Necessary configuration steps (example):

```
aaa new-model
!
aaa authentication login mac_methods local
aaa session-id common
!
dot11 ssid wlan567
   authentication open mac-address mac_methods

username 0012f34e81b0 password 0012f34e81b0        ! password = MAC address
username 0012f34e81b0 autocommand exit             ! mandatory
```

Please note: the mac-address must be entered in the format aabbccddeeff (without the points).

7.2 WEP

Pros: traffic is scrambled ("better than nothing").

Cons: may easily be subverted by skilled & motivated attacker.

Necessary configuration steps (example):

```
interface Dot11Radio0
 ip address 192.168.96.123 255.255.255.0
 no ip route-cache
 !
 encryption key 1 size 128bit 7 770212830D516D5A59822DD72BC2 transmit-key
 encryption mode wep mandatory
```

7.3 WPA

Pros: traffic is encrypted [security highly depends on key quality (length, characters)!]
Cons: may not be supported by every SOHO client (printers). Shared key for all clients.
Necessary configuration steps (example):

```
dot11 ssid wpa2
   authentication open
   authentication key-management wpa
   wpa-psk ascii 7 08294D420516544541
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm            ! wpa2, 'tkip' if wpa1
 !
```

7.4 LEAP with local AAA server

Pros: user-based auth [security highly depends on key quality (length, characters)!]
Cons: broken with weak passwords
Necessary configuration steps (example): see above in section on authentication.

8 MISCELLANEOUS

8.1 ACLs

tbd (VLAN ACLs etc.)

8.2 PSPF

Several APs support "wireless client isolation".The idea is basically to isolate the associated stations against each other, so that one associated client can't "see" and subsequently attack another (which is desirable e.g. in public hotspots). The Cisco flavor is called "Public Secure Packet Forwarding" (PSPF). Please note: this relies on the AP, so it can be circumvented by directed attacks against clients (e.g. with *wifitap*[5]).

This feature should be used with caution in corporate environments as the clients evidently won't "see" each other anymore. So network based printing may be blocked or ad-hoc CIFS based filesharing between colleagues won't work either.

It's configured on bridge-group level:

```
AP1(config-if)#bridge-group 1 port-protected
```

8.3 Monitoring/Intrusion Detection

tbd

8.3.1 Logmessages to look for

This is how a failed mac-based auth looks like:

```
*Mar      1   00:38:30.308:   %DOT11-7-AUTH_FAILED:   Station   0012.234e.81b0
Authentication failed
*Mar      1   00:38:35.329:   %DOT11-7-AUTH_FAILED:   Station   0012.234e.81b0
Authentication failed
*Mar      1   00:38:40.363:   %DOT11-7-AUTH_FAILED:   Station   0012.234e.81b0
Authentication failed
```

9 CHECKLIST

tbd

[5] *By Cedric Blancher, e.g. see http://securecon.unimelb.edu.au/data/2006/wireless_injection.pdf.*

10 APPENDIX A: SAMPLE CONFIG WITH SOME PARTS DESCRIBED IN THIS DOC

```
Current configuration : 5090 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
service password-encryption
no service dhcp
!
hostname hdz-ap-001
!
logging snmp-authfail
enable secret 5 xxx
!
clock timezone GMT 1
clock summer-time mesz recurring last Sun Mar 2:00 last Sun Oct 3:00
ip subnet-zero
no ip source-route
no ip gratuitous-arps
no ip domain lookup
ip domain name ernw.de
!
!
login block-for 300 attempts 5 within 30
login delay 2
login on-failure trap
login on-success
aaa new-model
!
!
dot11 ssid first
   vlan 90
   authentication open
   authentication key-management wpa
   wpa-psk ascii 7 xxx
!
dot11 ssid second
   vlan 97
   authentication open mac-address mac_methods
!
!
!
username erey secret 5 xxx
username 0030ab147b67 password 0030ab147b67
username 0030ab147b67 autocommand exit

bridge irb
```

```
!
!
interface Dot11Radio0
 no ip address
 no ip proxy-arp
 no ip route-cache
 !
 encryption vlan 90 mode ciphers tkip
 !
 ssid first
 !
 ssid second
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 station-role root
 no keepalive
 no cdp enable
 bridge-group 1
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.90
 encapsulation dot1Q 90
 no ip route-cache
 no cdp enable
 bridge-group 90
 bridge-group 90 subscriber-loop-control
 bridge-group 90 block-unknown-source
 no bridge-group 90 source-learning
 no bridge-group 90 unicast-flooding
 bridge-group 90 spanning-disabled
!
interface Dot11Radio0.97
 encapsulation dot1Q 97
 no ip route-cache
 no cdp enable
 bridge-group 97
 bridge-group 97 subscriber-loop-control
 bridge-group 97 block-unknown-source
 no bridge-group 97 source-learning
 no bridge-group 97 unicast-flooding
 bridge-group 97 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
```

```
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip proxy-arp
 no ip route-cache
 duplex auto
 speed auto
 no keepalive
 no cdp enable
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 hold-queue 160 in
!
interface FastEthernet0.90
 encapsulation dot1Q 90
 no ip route-cache
 no cdp enable
 bridge-group 90
 no bridge-group 90 source-learning
 bridge-group 90 spanning-disabled
!
interface FastEthernet0.96
 encapsulation dot1Q 96
 no ip proxy-arp
 no ip route-cache
 no cdp enable
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.97
 encapsulation dot1Q 97
 no ip route-cache
 no cdp enable
 bridge-group 97
 no bridge-group 97 source-learning
 bridge-group 97 spanning-disabled
!
interface BVI1
 ip address 192.168.96.10 255.255.255.0
 no ip proxy-arp
 no ip route-cache
 no keepalive
!
ip default-gateway 192.168.96.254
no ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
```

```
ip radius source-interface BVI1
!
access-list 1 permit 192.168.96.19
access-list 1 permit 192.168.96.112
no cdp run

control-plane
!
bridge 1 route ip
!
line con 0
line vty 0 4
 session-timeout 60
 access-class 1 in
 exec-timeout 60 0
 transport input ssh
line vty 5 15
 session-timeout 60
 access-class 1 in
 exec-timeout 60 0
 transport input ssh
!
End
```

Kontakt:

Roland Fiege
Kaufm. Geschäftsführer
ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 151 16 22 7557
rfiege@ernw.de
www.ernw.de