WPA Migration Mode: WEP is back to haunt you…

Leandro Meiners (lmeiners@coresecurity.com / @gmail.com)
Diego Sor (dsor@coresecurity.com / 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

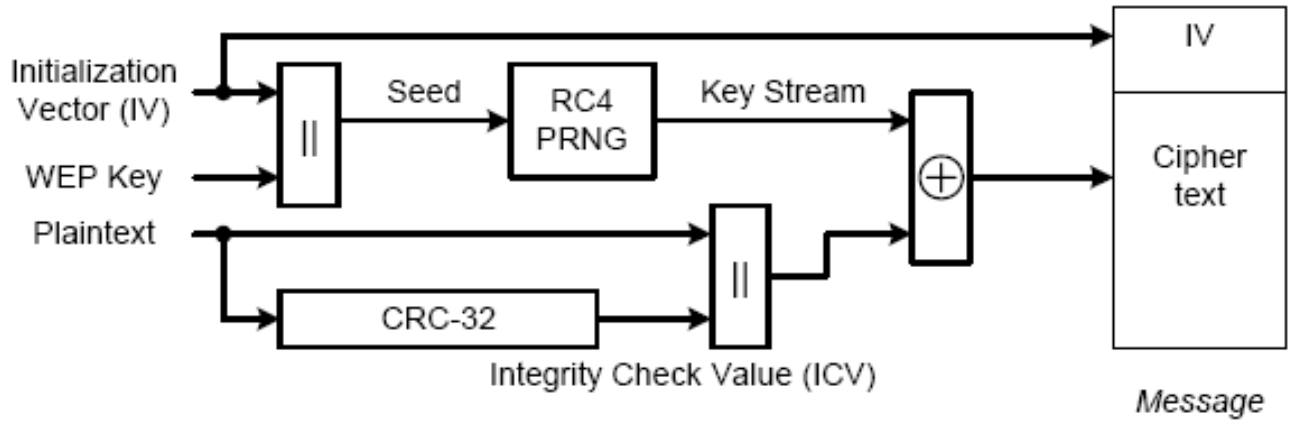
- **WEP's confidentiality:**
  - Based on RC4, which is a symmetric stream cipher:
    - » Symmetric: the encryption and decryption keys are the same.
    - » Stream cipher: encryption occurs one digit at a time.

- **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.

Introduction to WEP

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:**
  - CRC-32(A XOR B) = CRC-32(A) XOR CRC-32(B)

- **Let M = Plaintext message and K = Keystream, then:**
  - C = [M || ICV(M)] XOR K

- **It is possible to construct C_2, where C_2's plaintext is M_2 = M XOR Δ, knowing only C and Δ, in the following manner:**
  - C_2 = C XOR [Δ || ICV(Δ)]

Or… in layman's terms:

- XOR the data with the mask (Δ)
- XOR the ICV with the ICV of the mask (ICV(Δ))

Introduction to WPA Migration Mode

Starting to get interesting…

What is WPA Migration Mode?

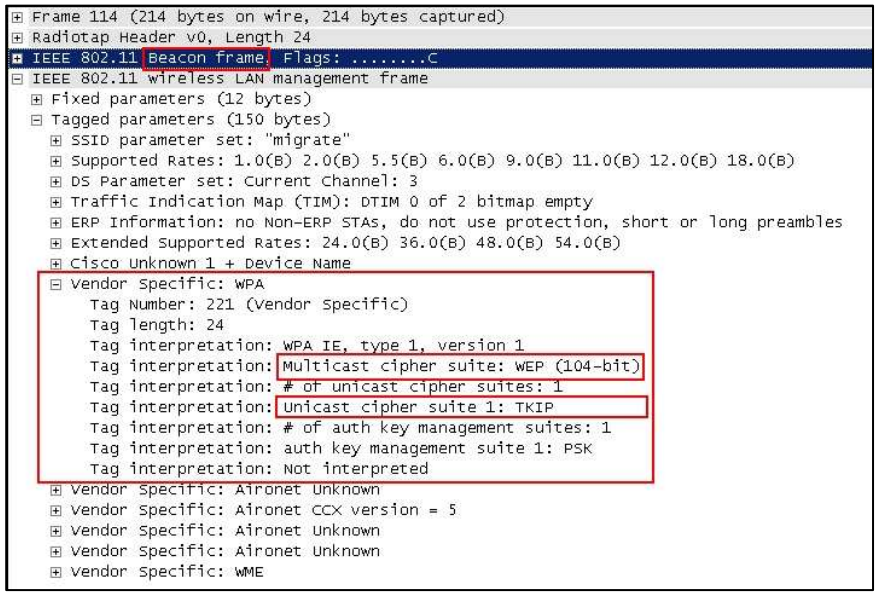
Cisco's WPA Migration Mode allows stations that support the following types of authentication and encryption schemes, to associate to the access point using the same SSID:

- **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.**

WPA Migration Mode

How WPA Migration Mode works

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



- **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
AAAAAAAAAAAAAAAAAAAAAAAAAA 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

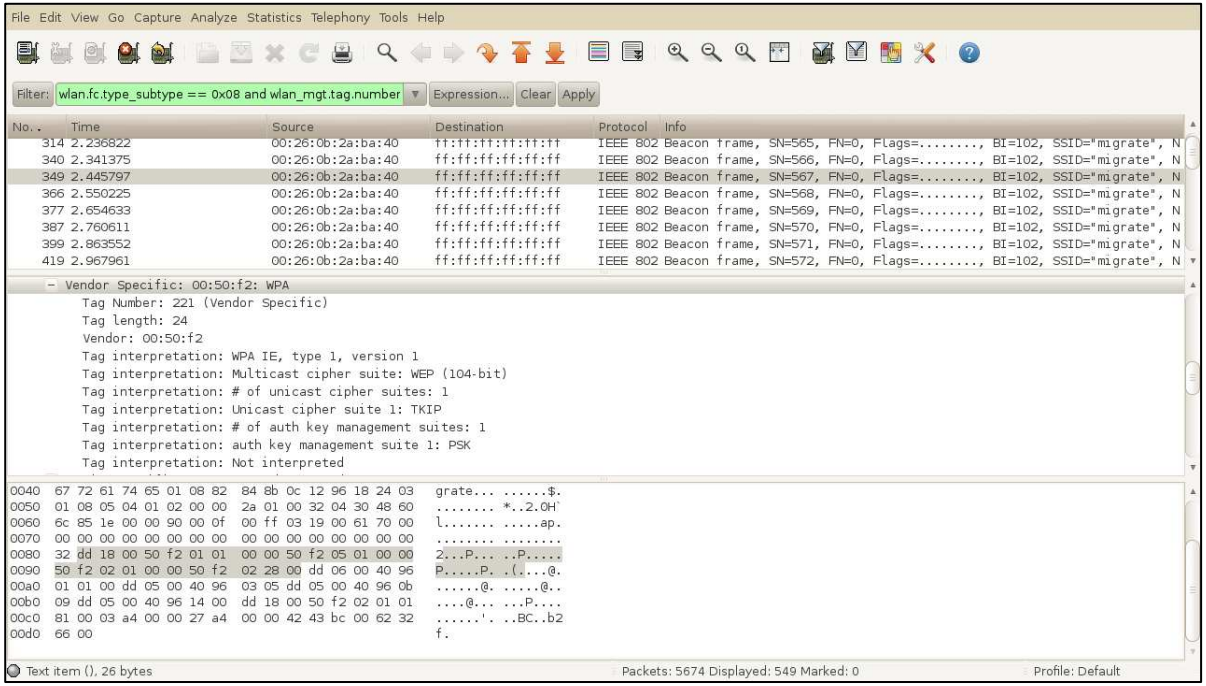
Wireshark Filter:

- **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"

Detecting an AP with WPA Migration Mode (2)

Wireshark Filter:

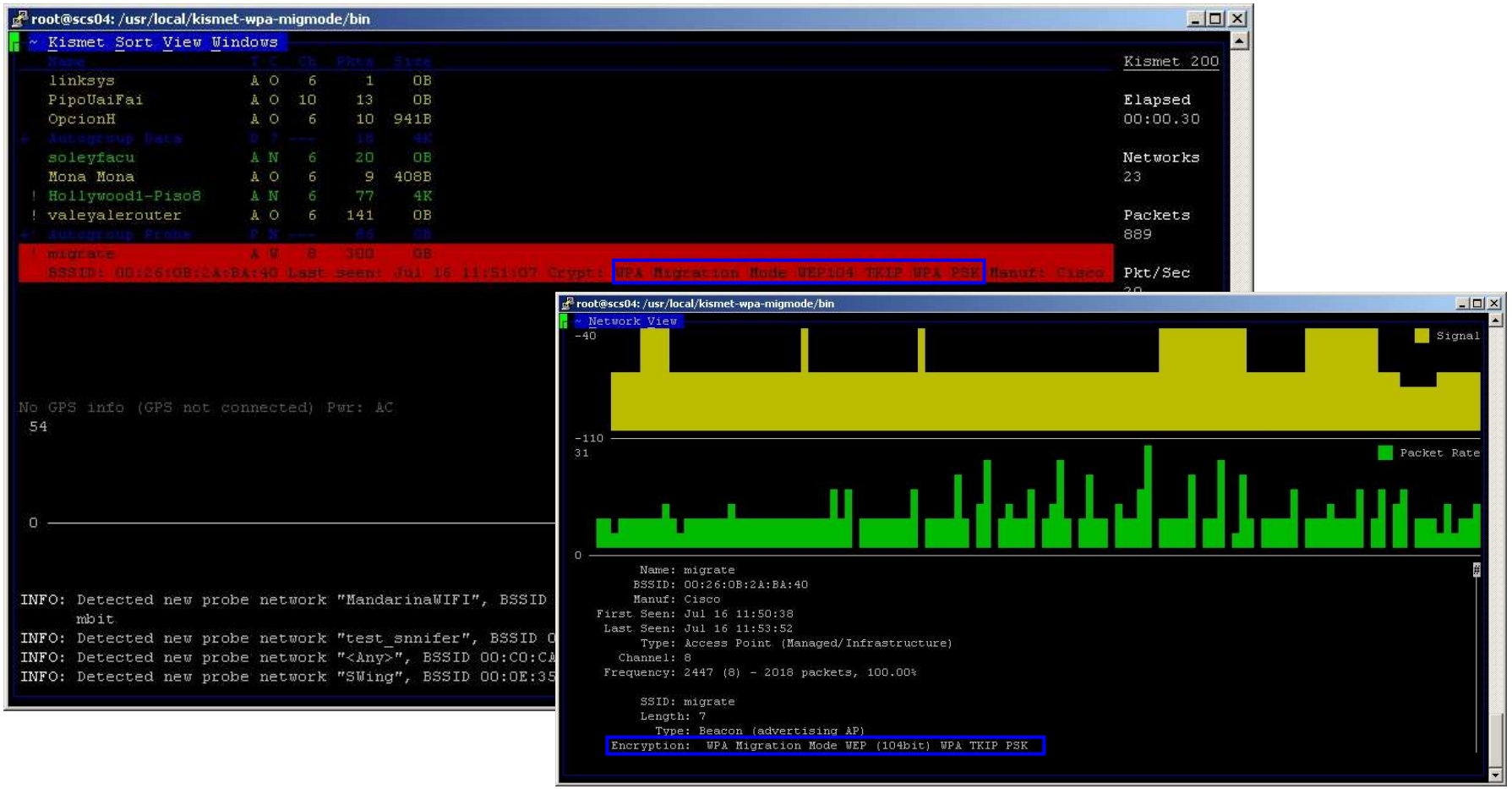
```
wlan.fc.type_subtype == 0x08 and wlan_mgt.tag.number == 221 and
(wlan_mgt.tag.interpretation == "Multicast cipher suite: WEP (40-
bit)" or wlan_mgt.tag.interpretation == "Multicast cipher suite:
WEP (104-bit)") and wlan_mgt.tag.interpretation == "Unicast cipher
suite 1: TKIP"
```



WPA Migration Mode

Detecting an AP with WPA Migration Mode (3)

Kismet (patched):



Attacking WPA Migration Mode

Now we are talking…

Attacking WPA Migration Mode

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…**

Attacking WPA Migration Mode

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

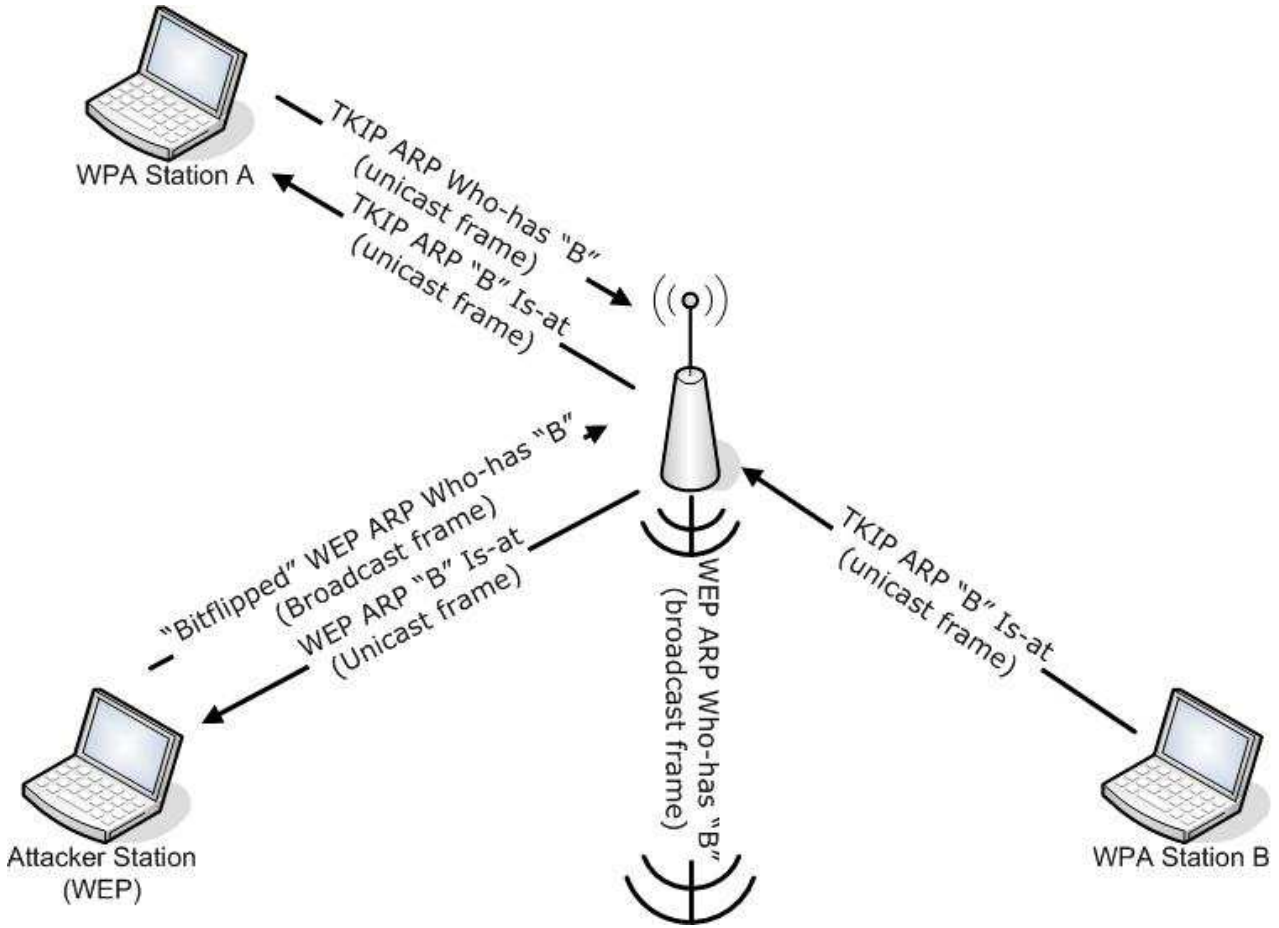
No WEP stations in sight…

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

No WEP stations in sight: in drawing



Attacking WPA Migration Mode

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

Demo: Attacking WPA Migration Mode

After all, it is what we came for…

Attacking WPA Migration Mode

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"

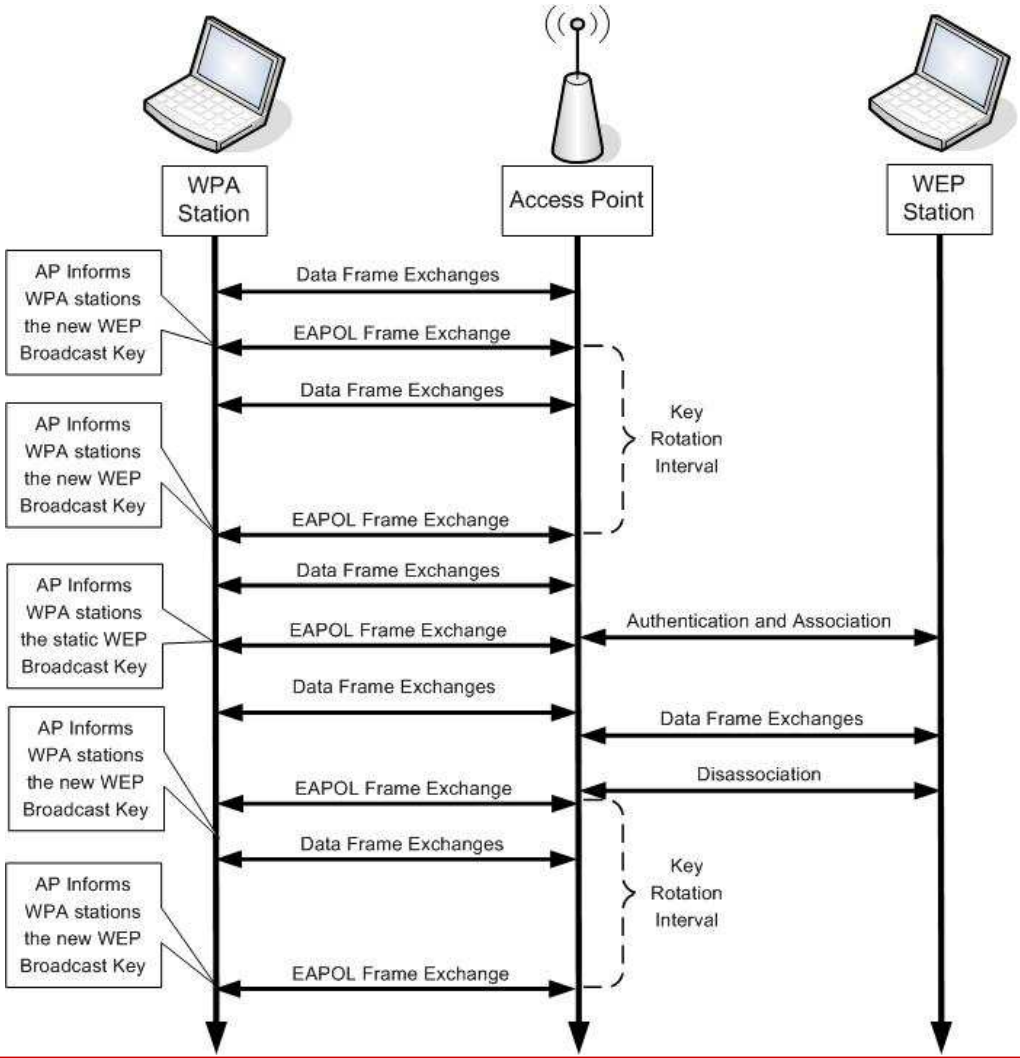
-- Cisco Systems
Cisco IOS Software Configuration Guide for Cisco Aironet Access Points

- **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#
```

Attacking WPA Migration Mode

Broadcast Key Rotation: in drawing



Attacking WPA Migration Mode

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

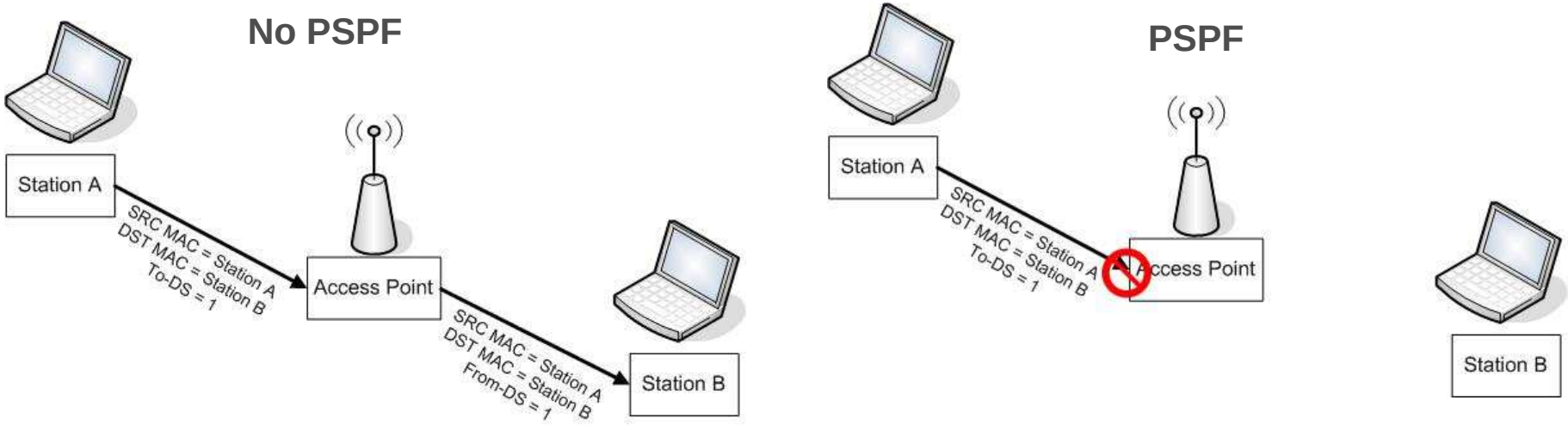
Demo: Bypassing Broadcast Key Rotation

Everybody likes a second demo…

Attacking WPA Migration Mode

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).

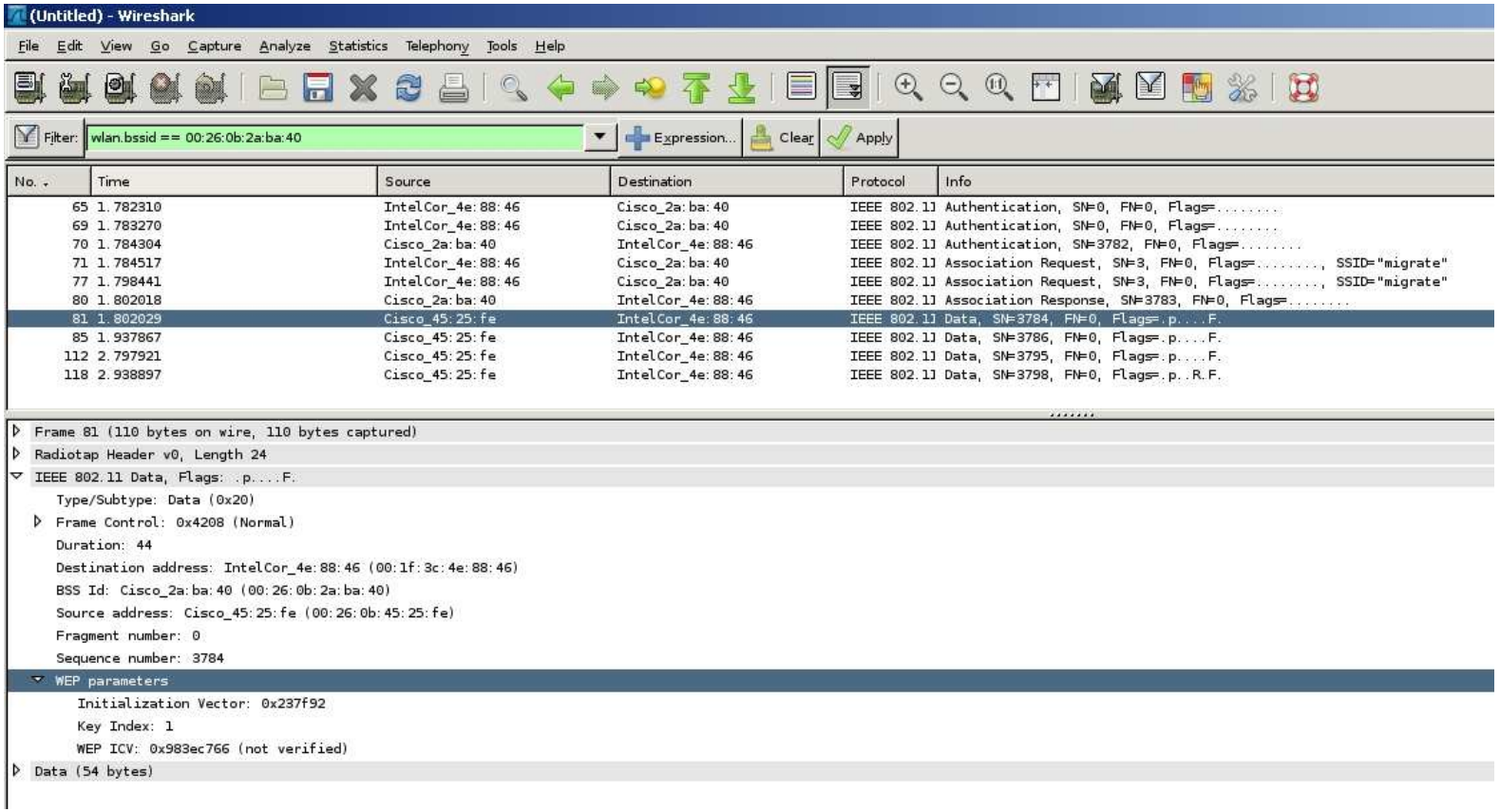



```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config)# bridge-group 1 port-protected
ap(config)# end
```

Attacking WPA Migration Mode

With PSPF Enabled…

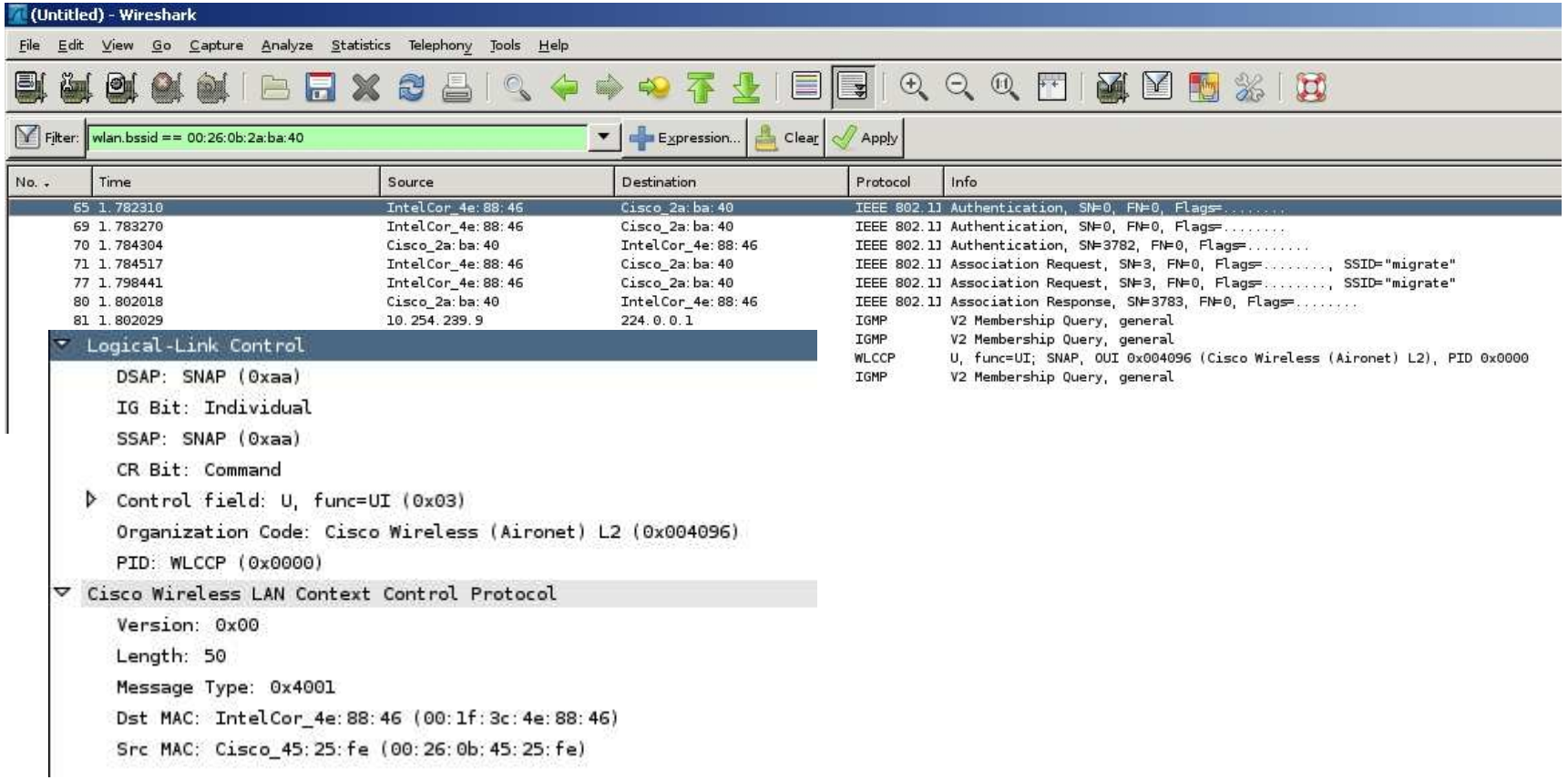
- Each time a WEP station joins…



Attacking WPA Migration Mode

With PSPF Enabled…(2)

- Each time a WEP station joins… (decrypted)



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.

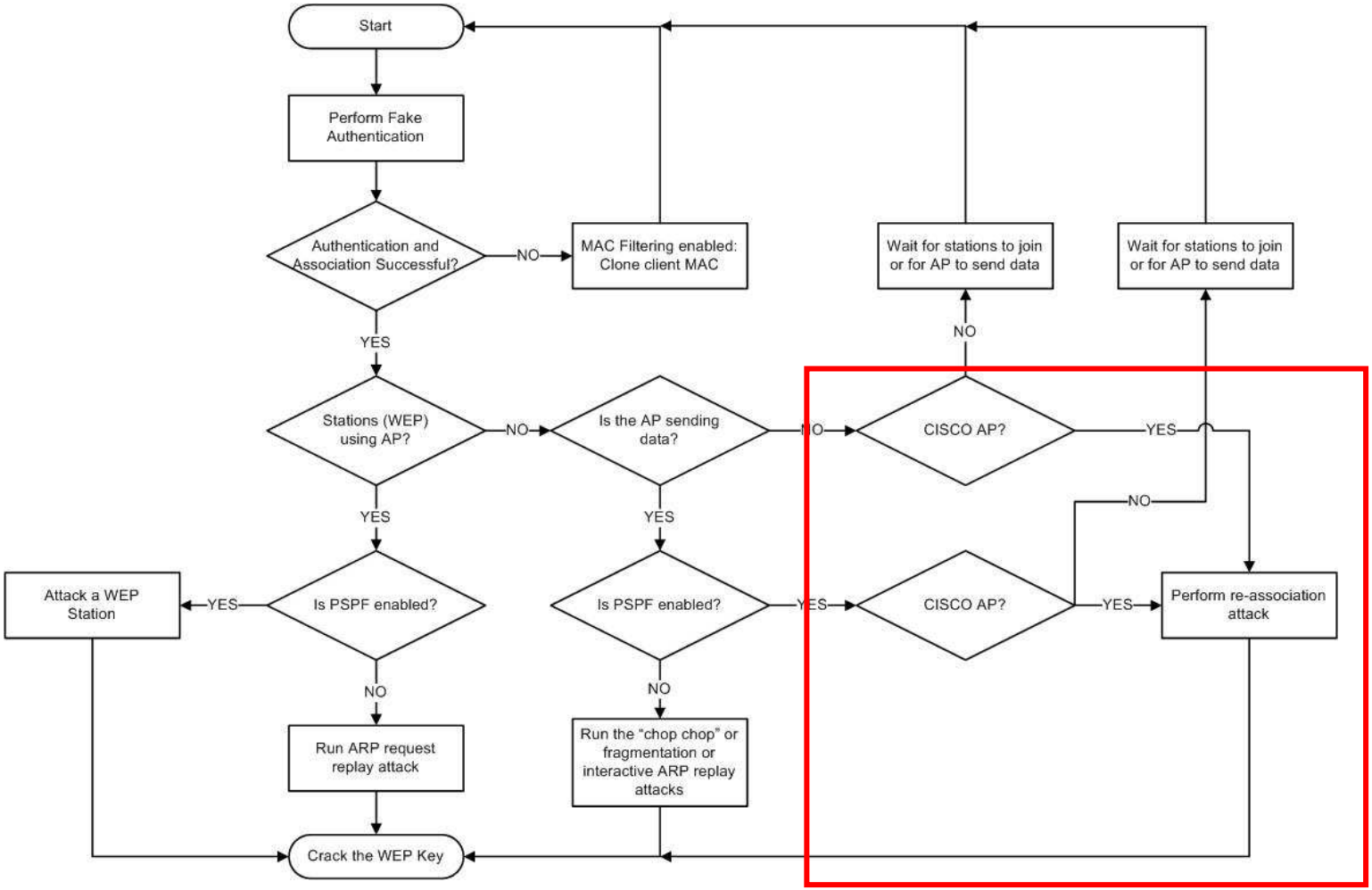
Attacking WPA Migration Mode

Demo: Bypassing PSPF

Who doesn't like a third demo…?

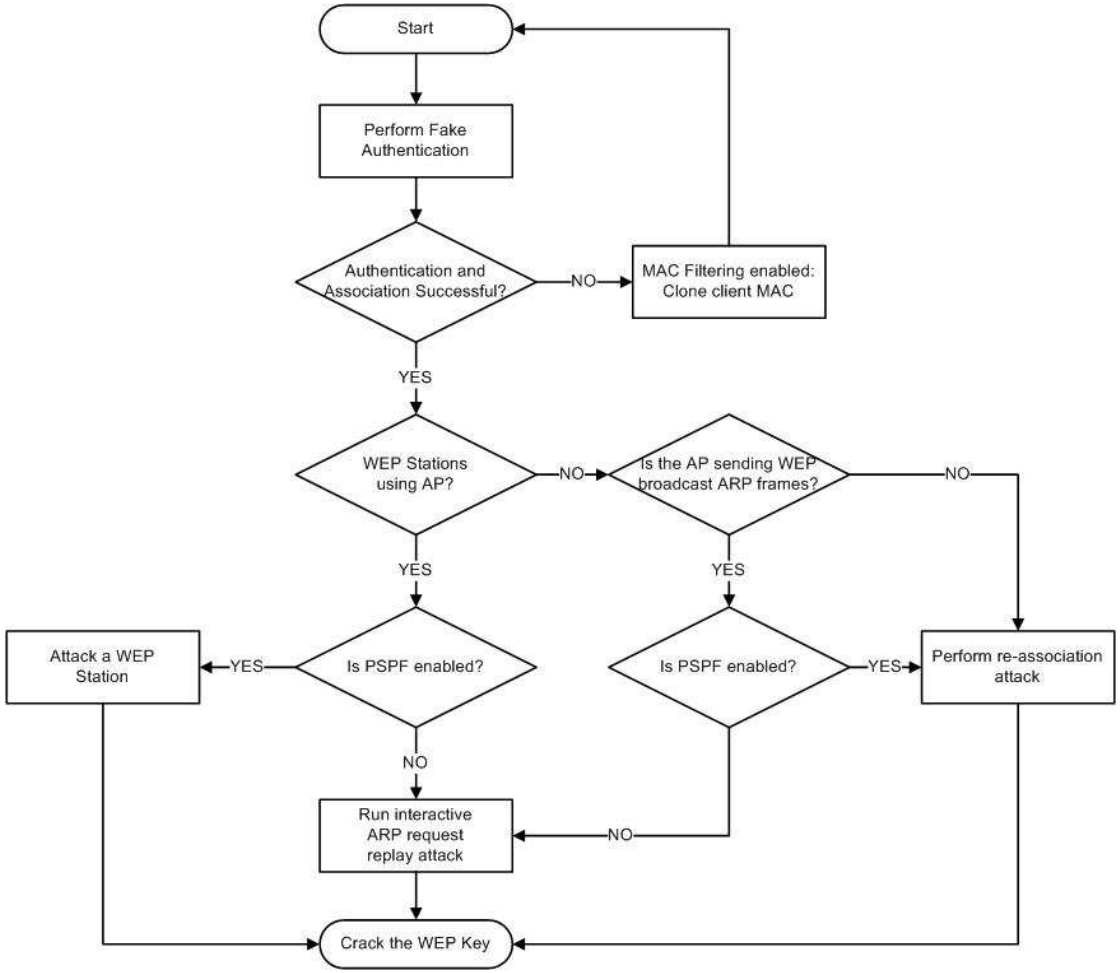
Attacking WPA Migration Mode

WEP Cracking Flowchart



Attacking WPA Migration Mode

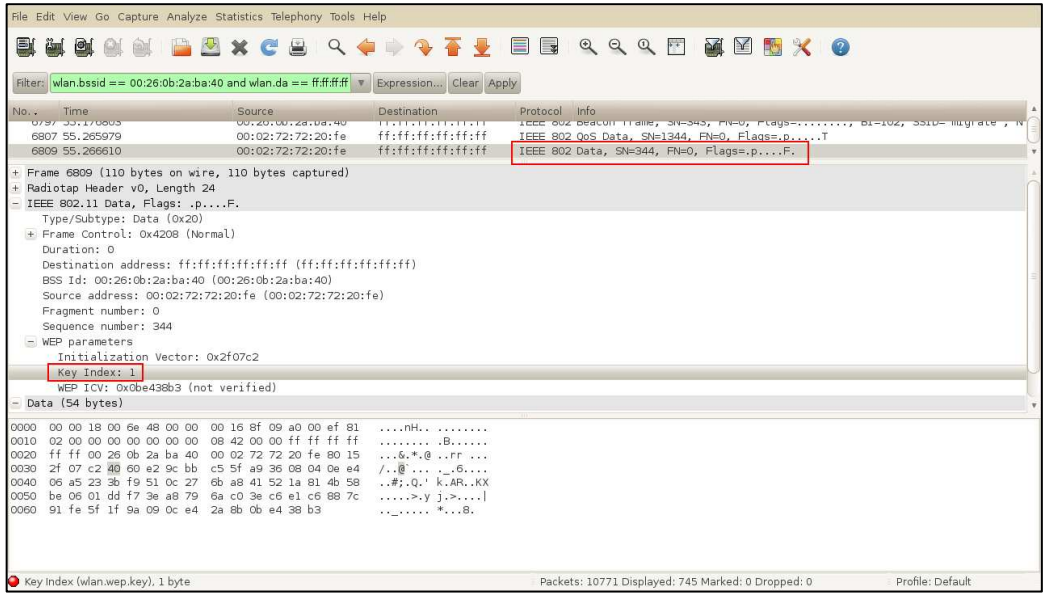
WPA Migration Mode Cracking Flowchart

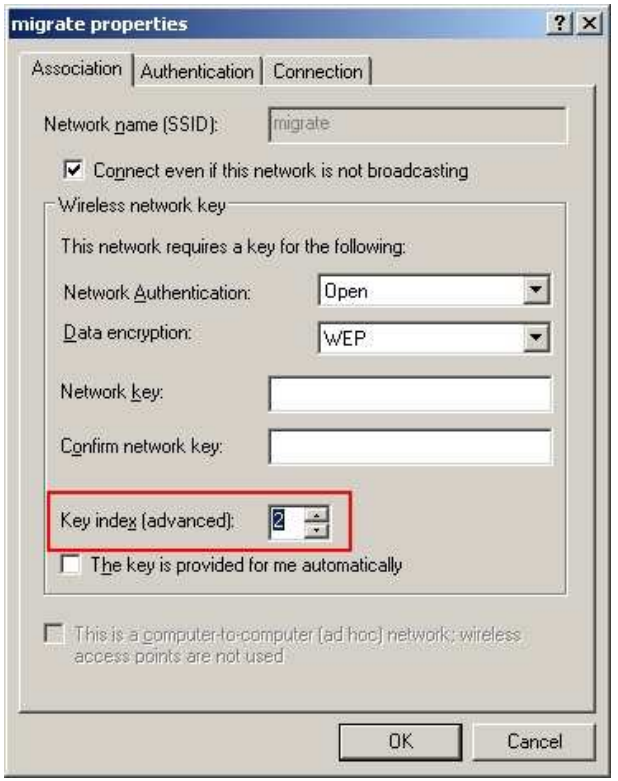


Attacking WPA Migration Mode

We have the WEP key… now what?

- Obtain the SSID
- Obtain the WEP key ID





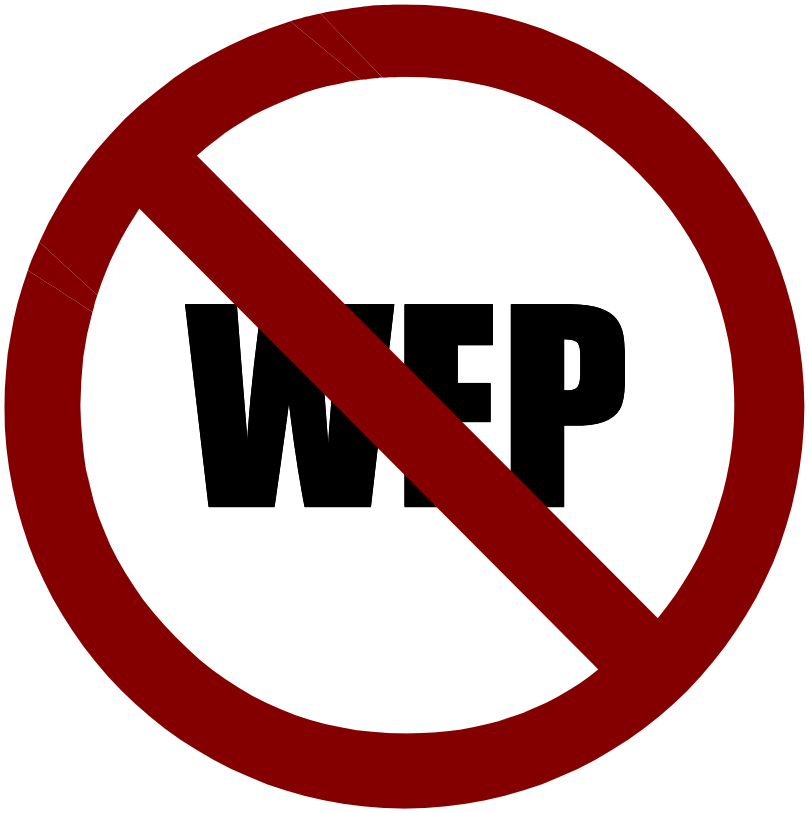

```
# iwconfig <WIFI INTERFACE> essid <SSID> key [<KEY_ID>] <KEY>
```

Mitigations and Recommendations

The “truly” interesting…

Mitigations and Recommendations

Solutions…



Mitigations and Recommendations

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

Questions…?

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