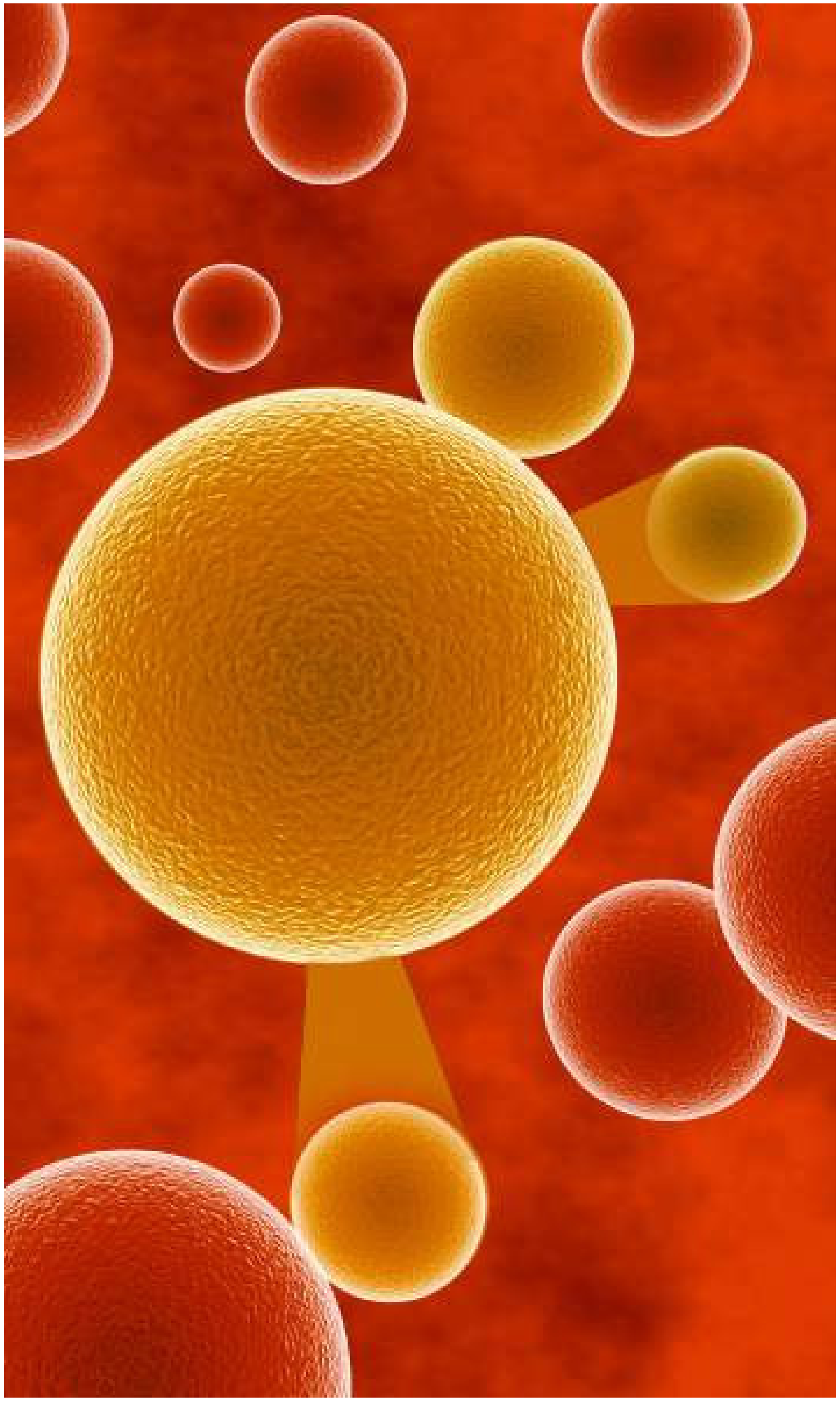


Autoimmunity Disorder in Wireless LANs

By

Md Sohail Ahmad

J V R Murthy, Amit Vartak

AirTight Networks

AirTight NETWORKS

Disclaimer & About Us

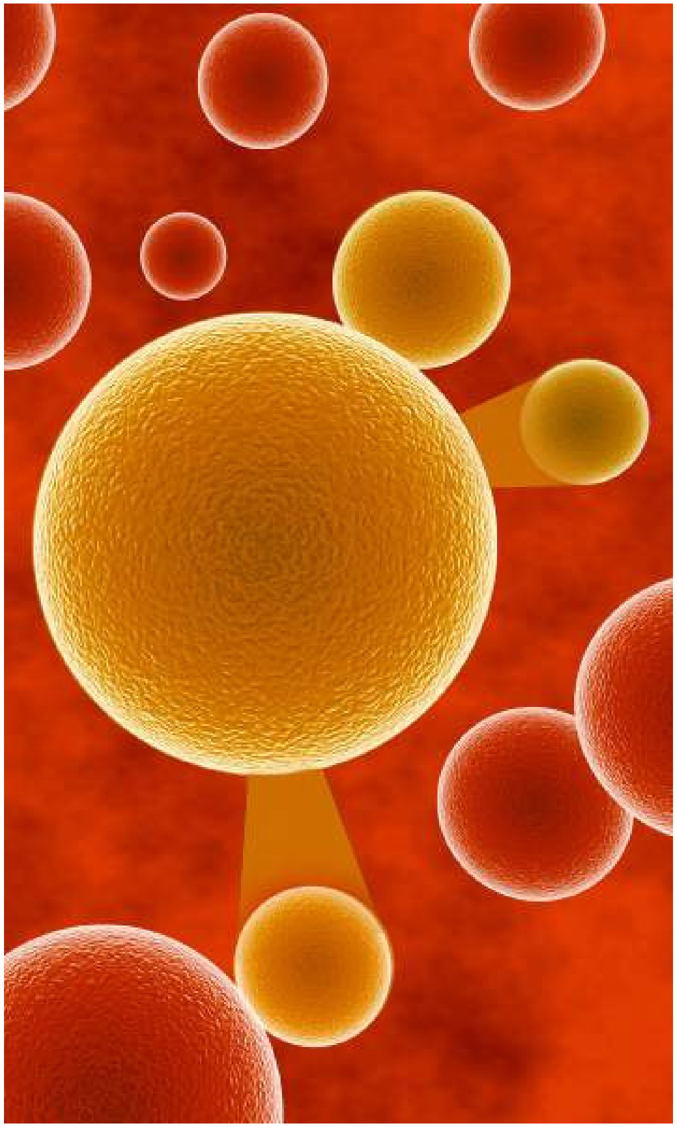
We are no medical doctors – our only competency is coffee drinking. The last year we brought to you ‘Café Latte with free topping of cracked WEP’.

This year we’d like to share with you rather interesting observations about Wireless LAN behavior – some of which have an interesting parallel with a previously known disorder in medical science.

1

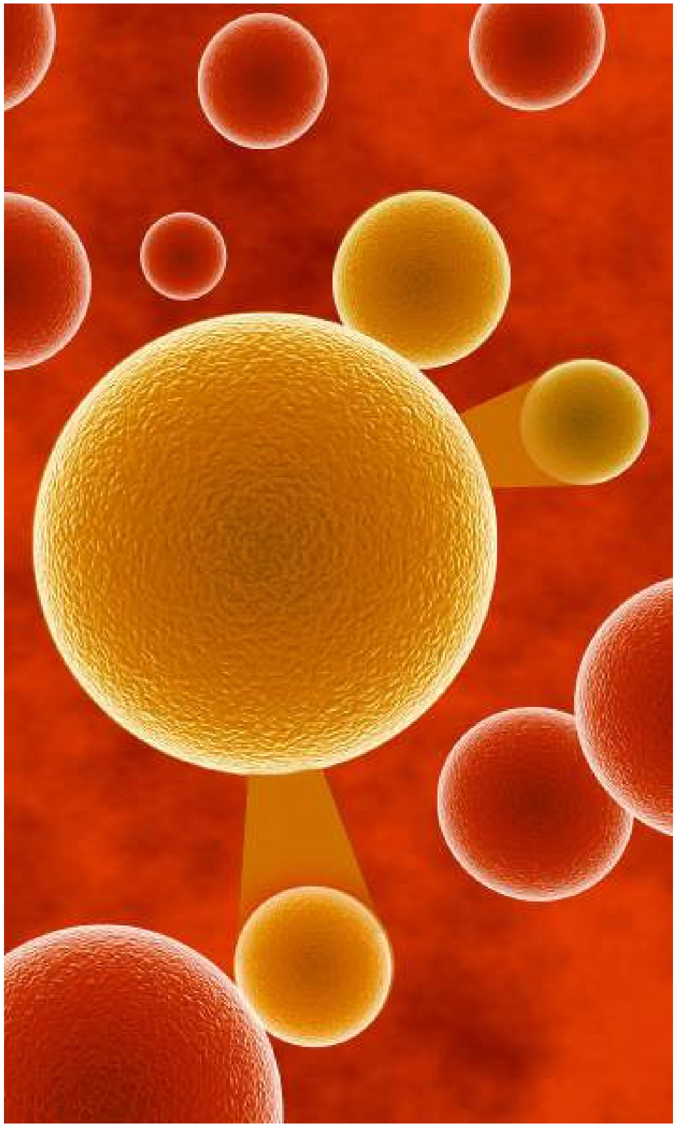
What has Autoimmunity disorder got to do with Wireless LANs?

Autoimmunity Disorder



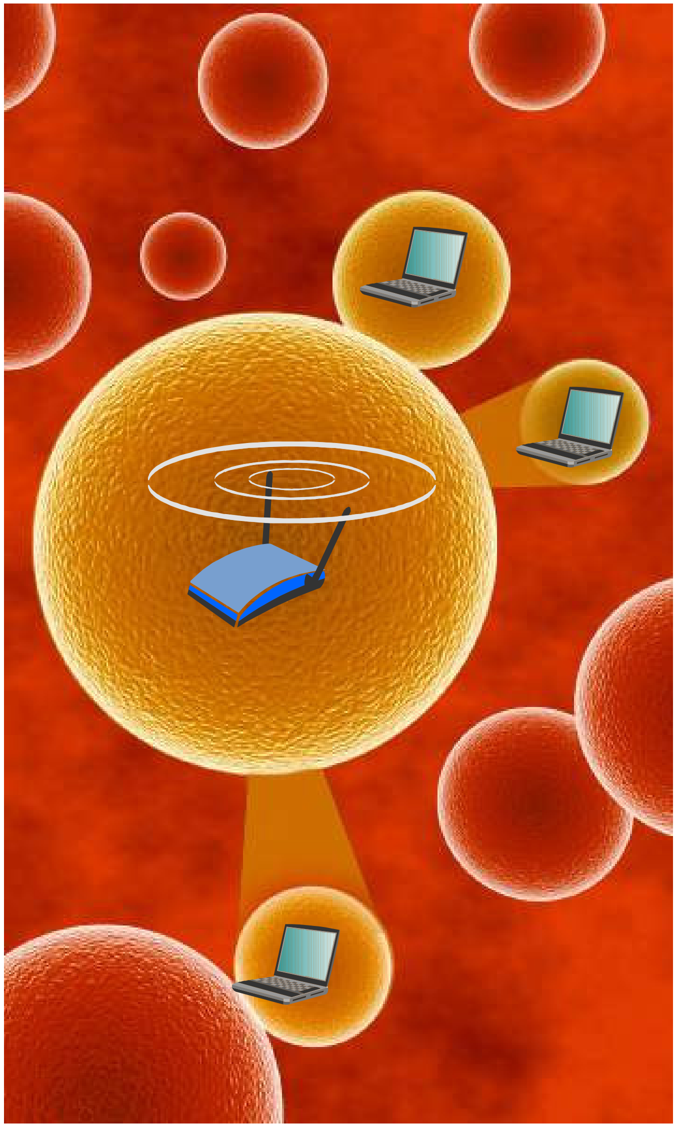
An autoimmune disorder is a condition that occurs when the immune system mistakenly attacks and destroys healthy body cell.

Why it Caught Our Attention?



An autoimmune disorder is **a condition that occurs when the** immune **system mistakenly attacks and destroys healthy** body **cell (or client).**

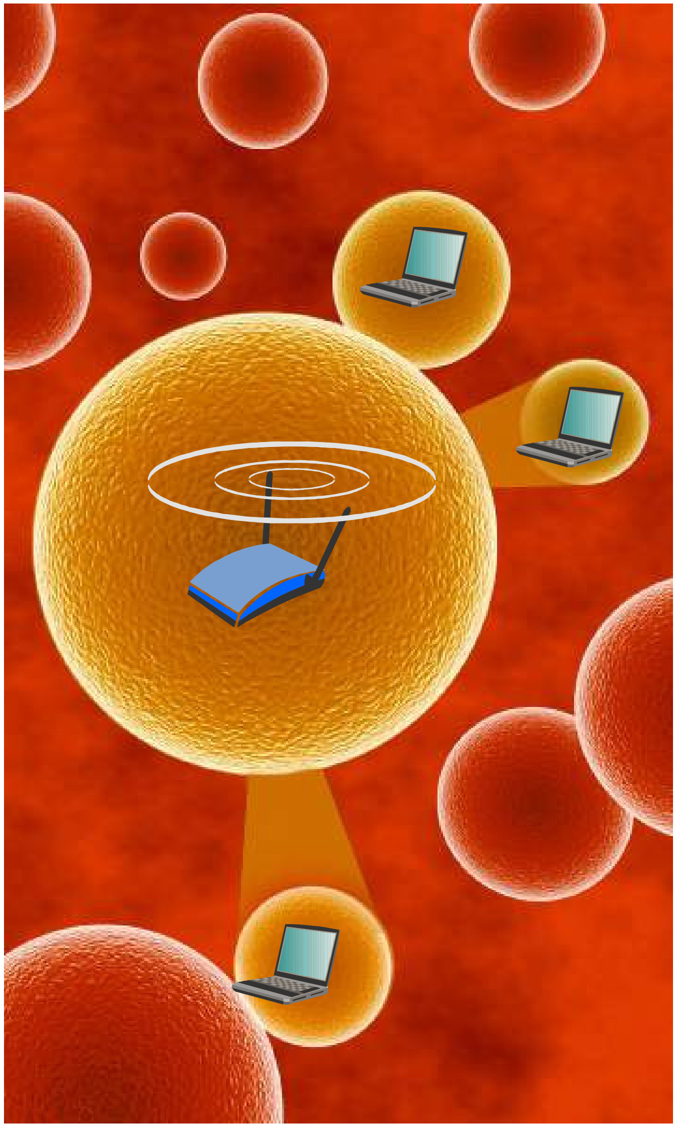
Over many late night coding and debugging sessions, we spotted ..



An autoimmune disorder is a condition that occurs when an Access Point mistakenly attacks and destroys authorized body cell (or client).

Not just one.. we spotted many instances of this interesting, self-destructive behavior!

So What?



Our findings suggest that new avenues for launching DoS attacks are possible. Majority of vulnerabilities reported here are implementation dependent and are found to exist in select open source AP and commercial Access Point S/W.

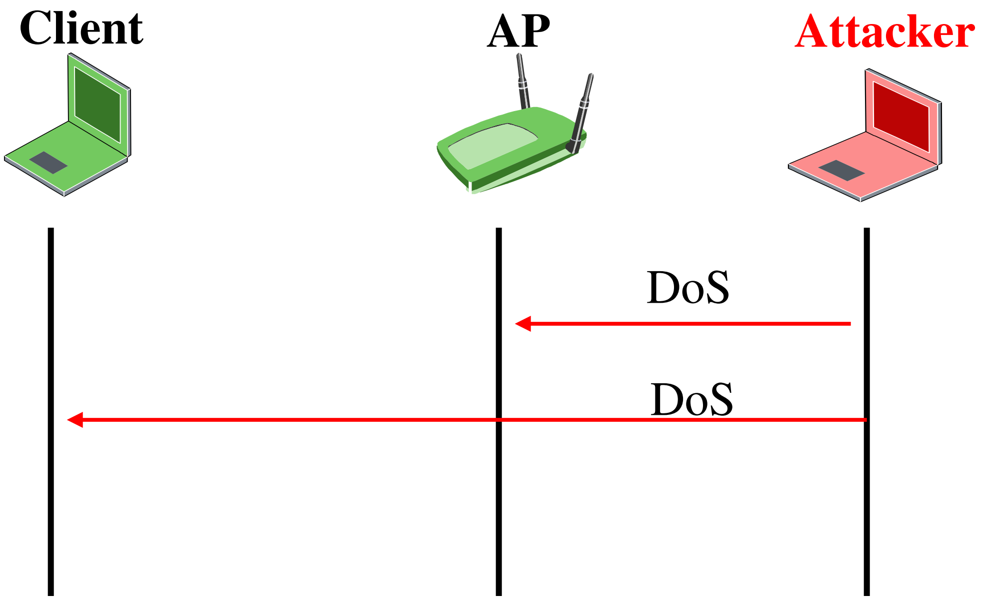
MFP(11w) is also vulnerable to DoS attacks!

2

Background

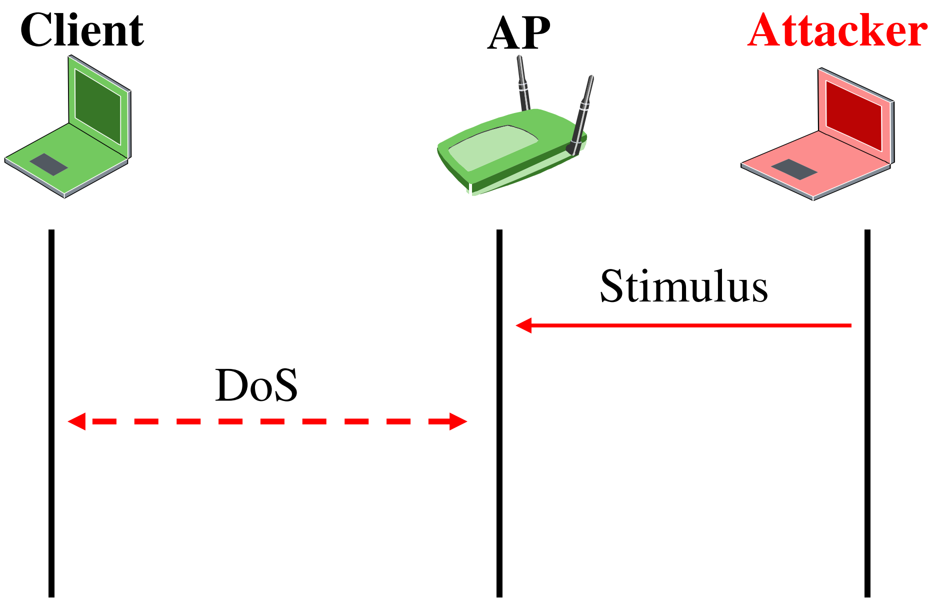
What’s Well Known -- DoS from an External Source

- It is well known that by sending spoofed De-authentication or Dis-association packets it is possible to break AP to client connections.
- A De-authentication packet spoofed with source address = AP MAC address causes disconnection in client’s state machine.
- Likewise, a De-authentication packet spoofed with source address = Client MAC address causes disconnection in AP’s state machine.



What's New – Self DoS Triggered by an External Stimulus

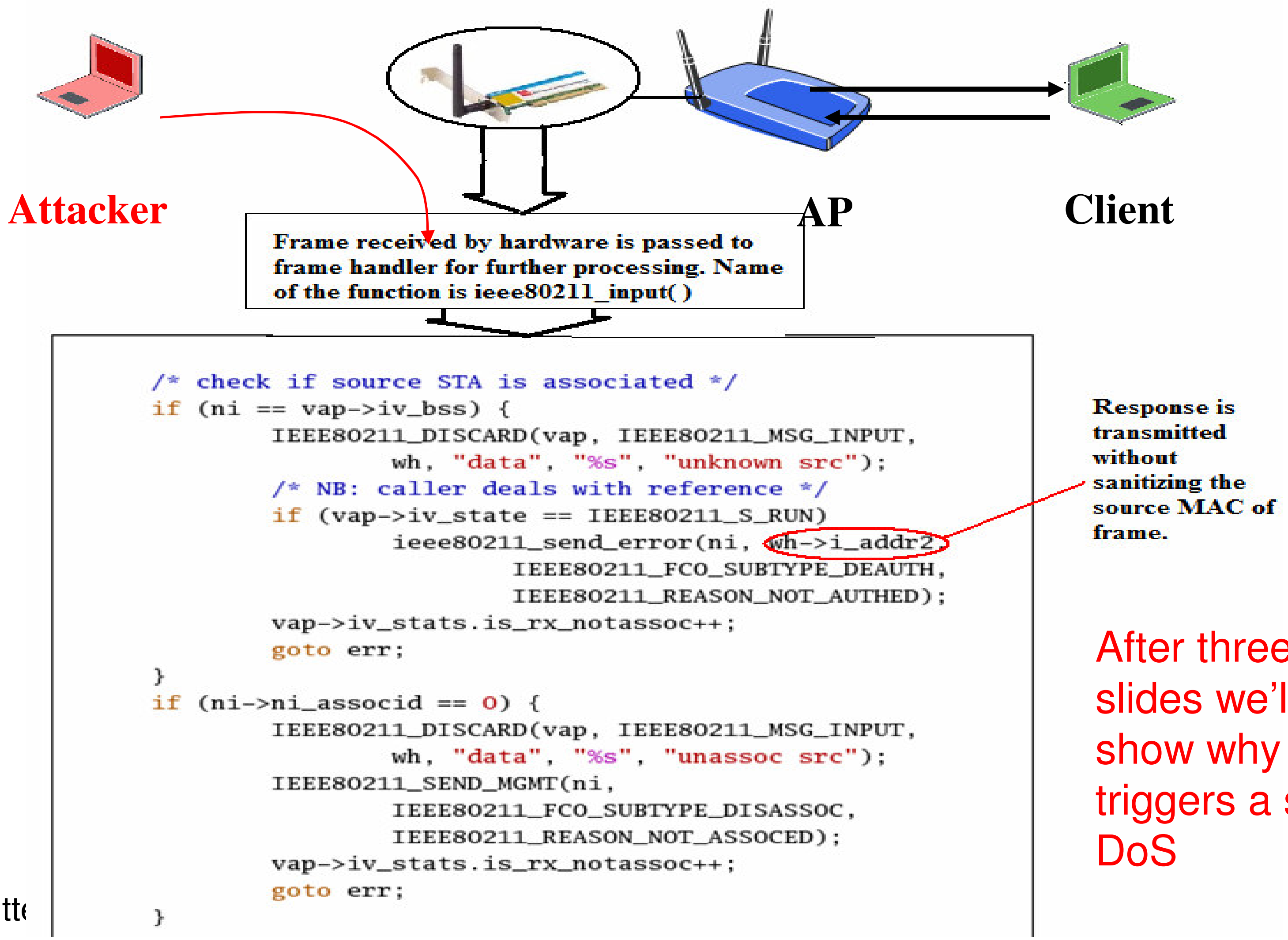
- **There exist mal-formed packets whose injection can turn an AP into a connection killing machine.**
- **We'll demonstrate 8 examples of this behavior**



Why Does Self DoS Happen?

- Standard Protocol specs are often unclear about how an AP should respond to malformed frames. Different AP implementations behave differently. Some survive, some crash and some turn themselves into killing machines.

An Example from madwifi-0.9.4



Frame received by hardware is passed to frame handler for further processing. Name of the function is ieee80211_input( )

```
/* check if source STA is associated */
if (ni == vap->iv_bss) {
        IEEE80211_DISCARD(vap, IEEE80211_MSG_INPUT,
                wh, "data", "%s", "unknown src");
        /* NB: caller deals with reference */
        if (vap->iv_state == IEEE80211_S_RUN)
                ieee80211_send_error(ni, wh->i_addr2,
                        IEEE80211_FC0_SUBTYPE_DEAUTH,
                        IEEE80211_REASON_NOT_AUTHED);
        vap->iv_stats.is_rx_notassoc++;
        goto err;
}
if (ni->ni_associd == 0) {
        IEEE80211_DISCARD(vap, IEEE80211_MSG_INPUT,
                wh, "data", "%s", "unassoc src");
        IEEE80211_SEND_MGMT(ni,
                IEEE80211_FC0_SUBTYPE_DISASSOC,
                IEEE80211_REASON_NOT_ASSOCED);
        vap->iv_stats.is_rx_notassoc++;
        goto err;
}
```

Response is transmitted without sanitizing the source MAC of frame.

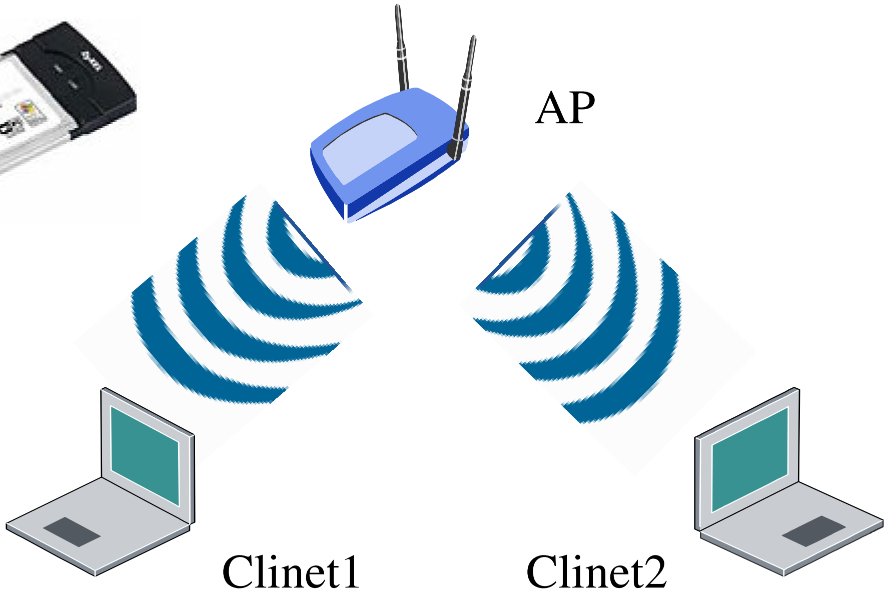
After three slides we’ll show why this triggers a self DoS

3

Let the game begin

WLAN Test Lab

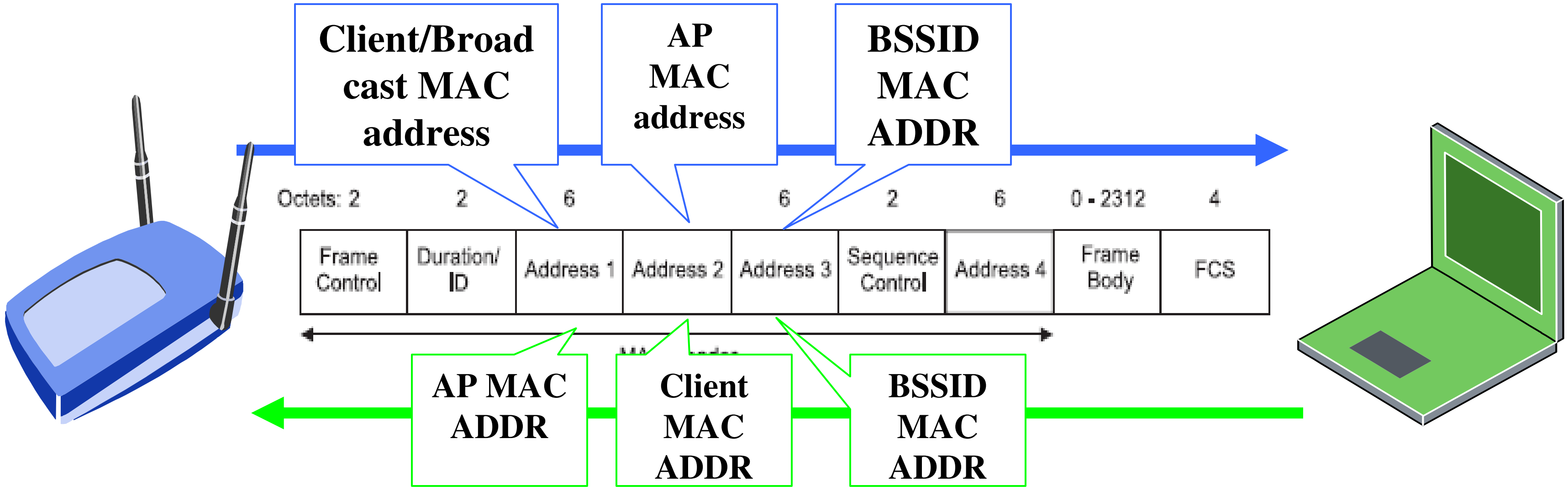
- Autoimmunity Disorder Test Requirements
  - A Raw Frame Injection Tool (e.g. wireshark-inject)
  - Wireless LAN card (preferable .11abg) connected to BackTrack 2 (Linux box which supports raw wireless frame injection) box
  - An operational wireless LAN (with at least one AP and couple of clients)



Submitted to DefCon16

Stimulus for Autoimmunity Disorder Test

- WLAN Frame
  - Association Request/Response
  - Re-association Request/Response
  - Authentication
- WLAN Address Fields
  - Address1, Address2, Address3, Address4
  - Modified Information Elements (IE)



Client/Broadcast MAC address

AP MAC address

BSSID MAC ADDR

Octets: 2	2	6		6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

AP MAC ADDR

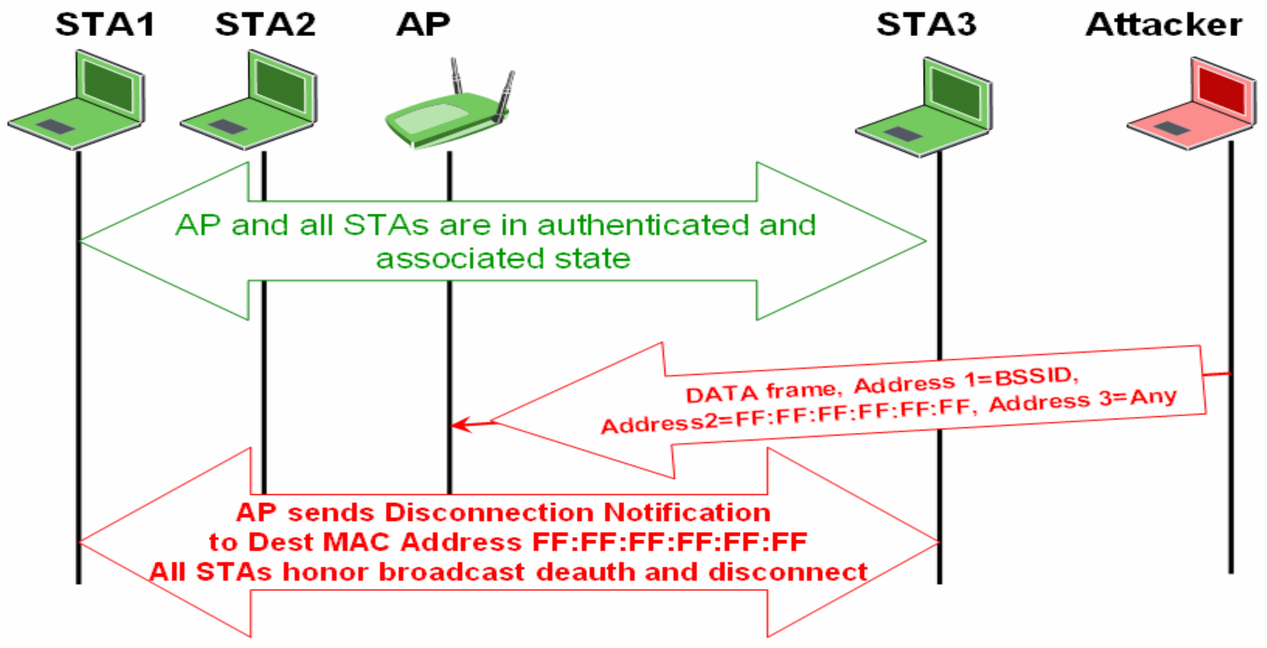
Client MAC ADDR

BSSID MAC ADDR

Submitted to DefCon16

Stimulus #1

- **Use of Broadcast MAC address in Address 2 Field**
  - ⇨ Send Broadcast MAC address (**FF:FF:FF:FF:FF:FF**) as source MAC address (Address 2 in WLAN Frame Header) in any class 2 or 3 (e.g. TO DS DATA) frame.
    - Since FF:FF:FF:FF:FF:FF is a special type address and is not present in Access Point association table, AP is likely to send Deauthentication Notification frame with Reason Code *“Class 3 frame received from nonassociated station”*
    - Associated STAs honor the **Broadcast Disconnection** frame and disconnect from associated AP



AP and all STAs are in authenticated and associated state

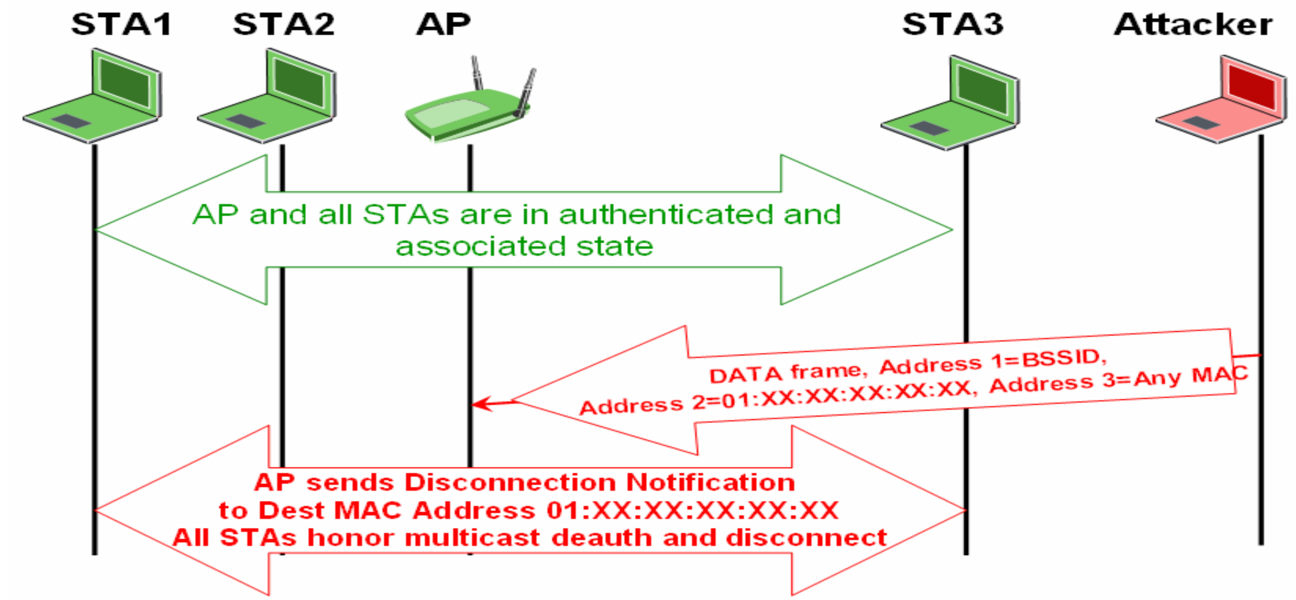
DATA frame, Address 1=BSSID, Address2=FF:FF:FF:FF:FF:FF, Address 3=Any

AP sends Disconnection Notification to Dest MAC Address FF:FF:FF:FF:FF:FF

All STAs honor broadcast deauth and disconnect

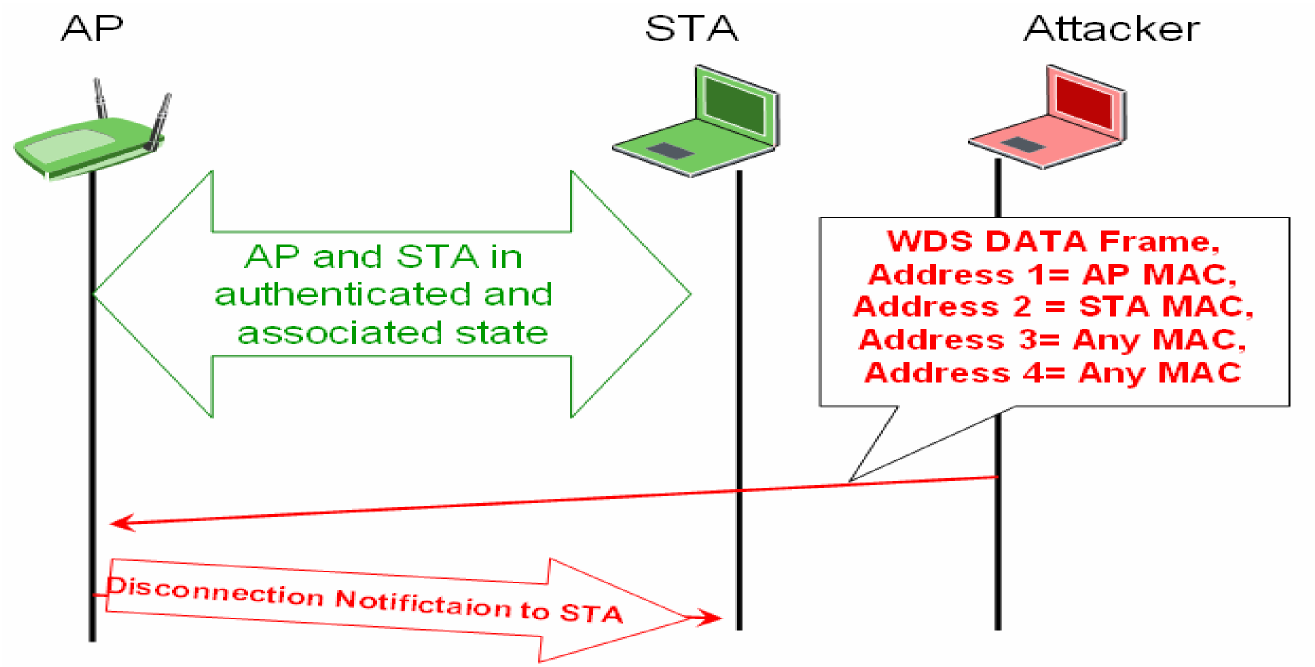
Stimulus #2

- **Use of Multicast MAC address in Address 2 Field**
  - ⇨ Send Multicast MAC address (**01:XX:XX:XX:XX:XX**) as Source MAC address in any class 2 or 3 frame (e.g. TODS DATA frame).
    - Since 01:XX:XX:XX:XX:XX is a multicast address, It does not appear in the AP's association table.
    - On reception of DATA frame with Multicast MAC address as source address, Access Point is likely to send Disconnection Notification frame with Reason Code *"Class 3 frame received from nonassociated station"*
    - All associated node honors the **Multicast Disconnection** Notification frame and disconnects from associated AP


STA1
STA2
AP
STA3
Attacker
AP and all STAs are in authenticated and associated state
DATA frame, Address 1=BSSID,
Address 2=01:XX:XX:XX:XX:XX, Address 3=Any MAC
AP sends Disconnection Notification
to Dest MAC Address 01:XX:XX:XX:XX:XX
All STAs honor multicast deauth and disconnect

Stimulus #3

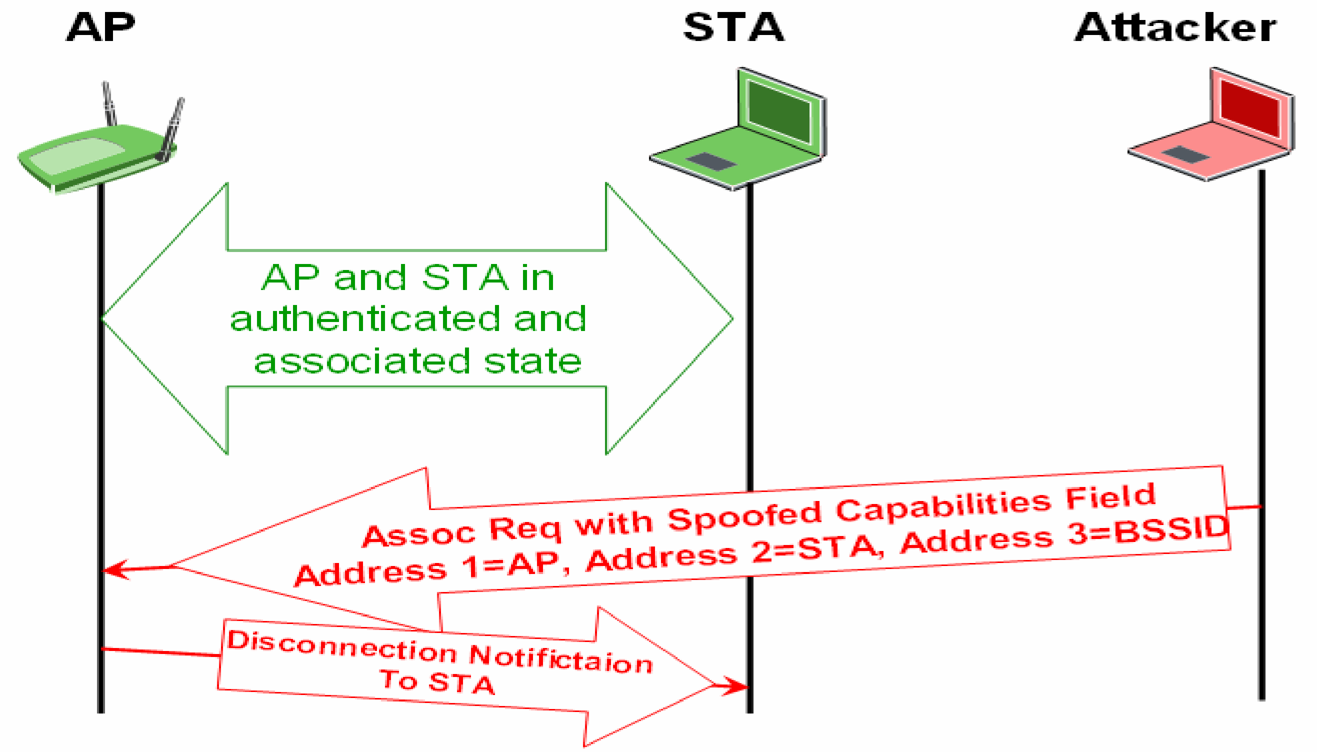
- **Use of 4 MAC address WLAN Frame**
  - ⇨ Send 4-MAC address WDS DATA frame with victim’s STA MAC as source MAC address (Address 2 in WLAN Frame header) in WDS DATA frame.
    - Access Point not capable to handle 4MAC address DATA frame, likely to send disconnection notification to that Client


AP
STA
Attacker
AP and STA in authenticated and associated state
WDS DATA Frame, Address 1= AP MAC, Address 2 = STA MAC, Address 3= Any MAC, Address 4= Any MAC
Disconnection Notifictaion to STA

Submitted to DefCon16

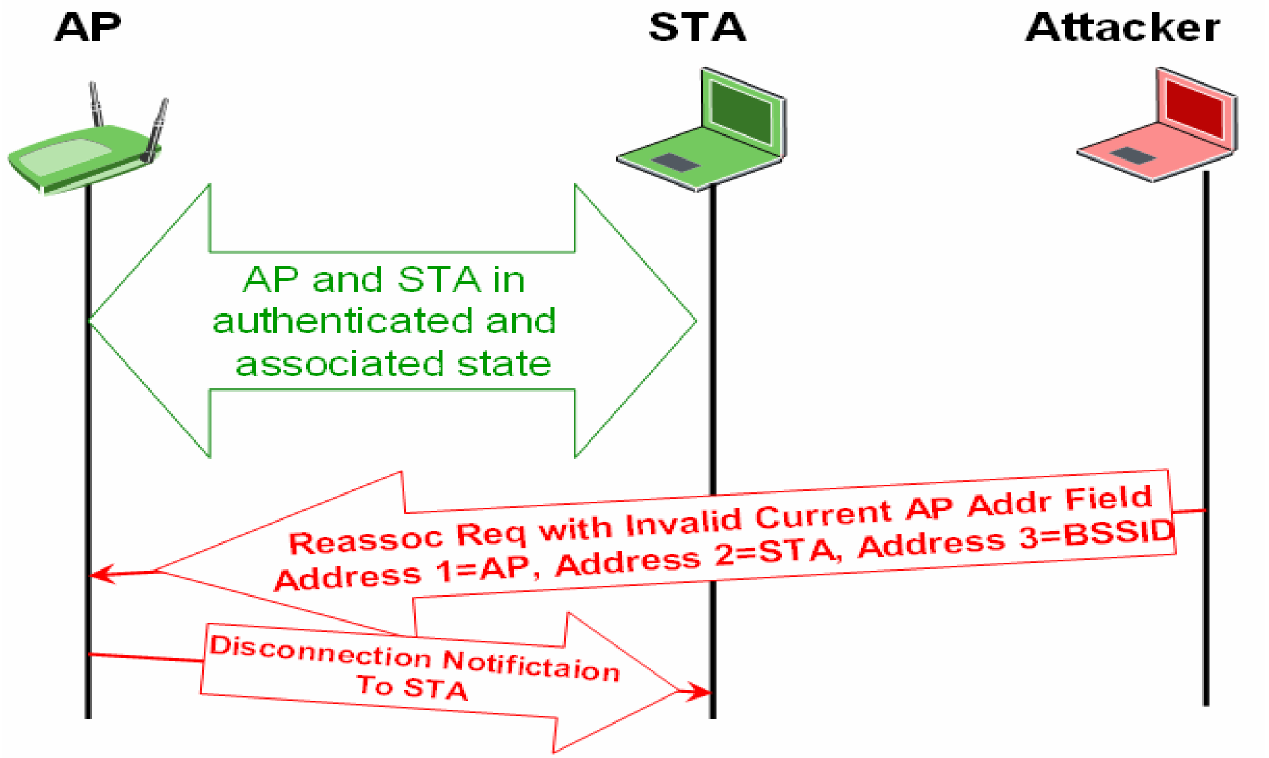
Stimulus #4

- An **Association Request** with spoofed **Capabilities Field** sent to an Access Point can potentially drops client's connection at AP and likely to trigger a response with **Status Code 10** (Cannot support all requested capabilities in the Capability Information field)


AP
STA
Attacker
AP and STA in authenticated and associated state
Assoc Req with Spoofed Capabilities Field
Address 1=AP, Address 2=STA, Address 3=BSSID
Disconnection Notifictaion
To STA

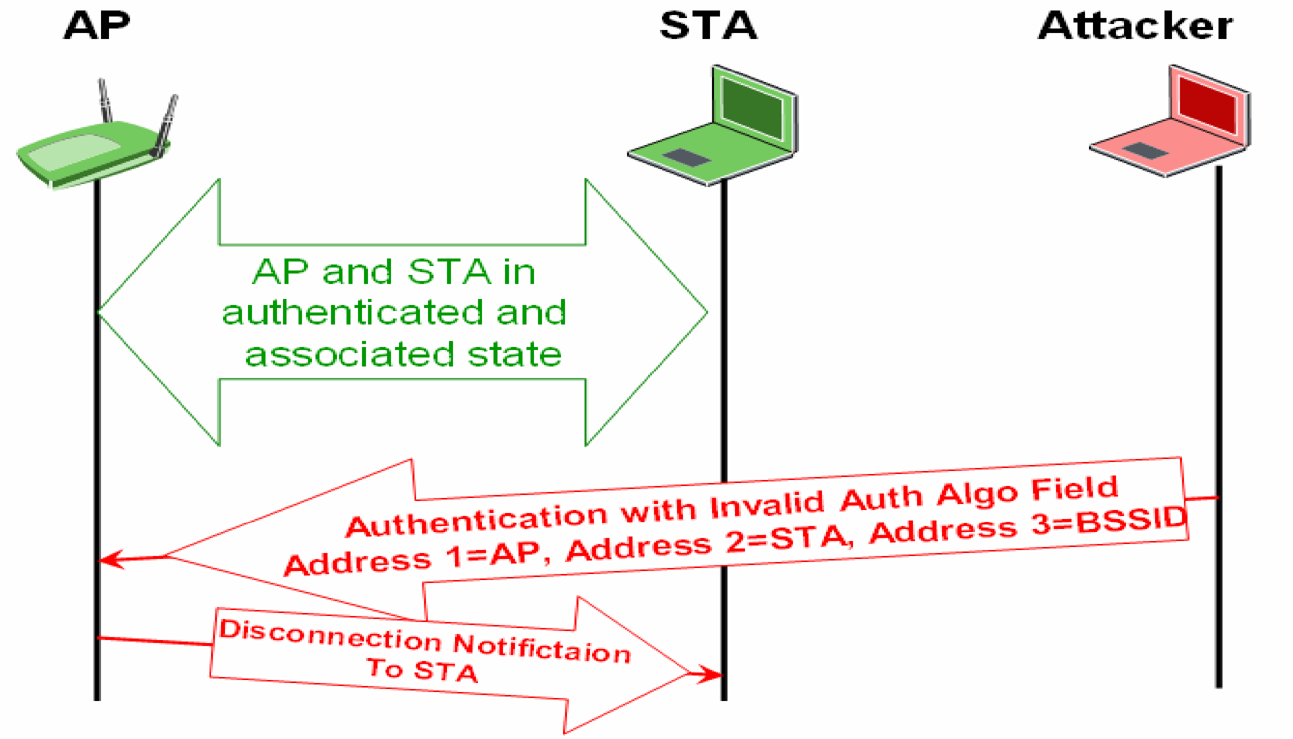
Stimulus #5

- A **Reassociation Request** with spoofed **Current AP Address** field sent to an Access Point can potentially disconnect an associated client and can trigger a response with **Status Code 11** (Reassociation denied due to inability to confirm that association exists)


AP
STA
Attacker
AP and STA in authenticated and associated state
Reassoc Req with Invalid Current AP Addr Field
Address 1=AP, Address 2=STA, Address 3=BSSID
Disconnection Notifictaion
To STA

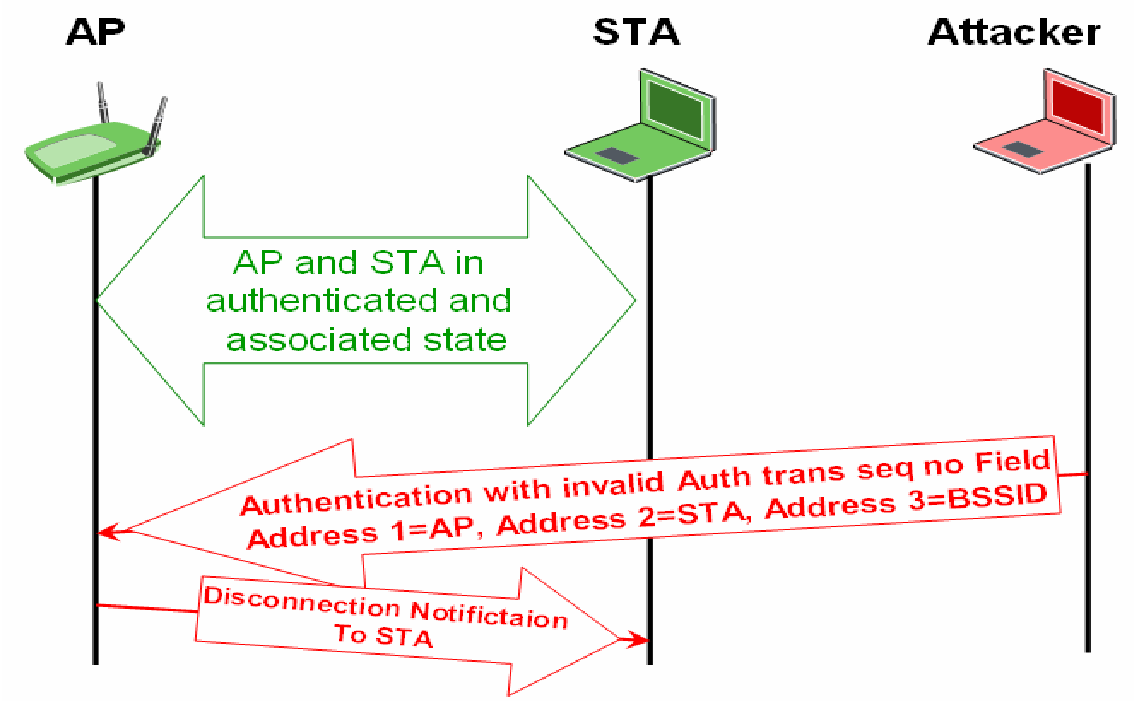
Stimulus #6

- An **Authentication** frame with invalid **Authentication Algorithm** sent to an Access Point can potentially disconnect an associated client and can trigger a response with **Status Code 13** (Responding station does not support the specified authentication algorithm)


AP
STA
Attacker
AP and STA in authenticated and associated state
Authentication with Invalid Auth Algo Field
Address 1=AP, Address 2=STA, Address 3=BSSID
Disconnection Notifictaion
To STA

Stimulus #7

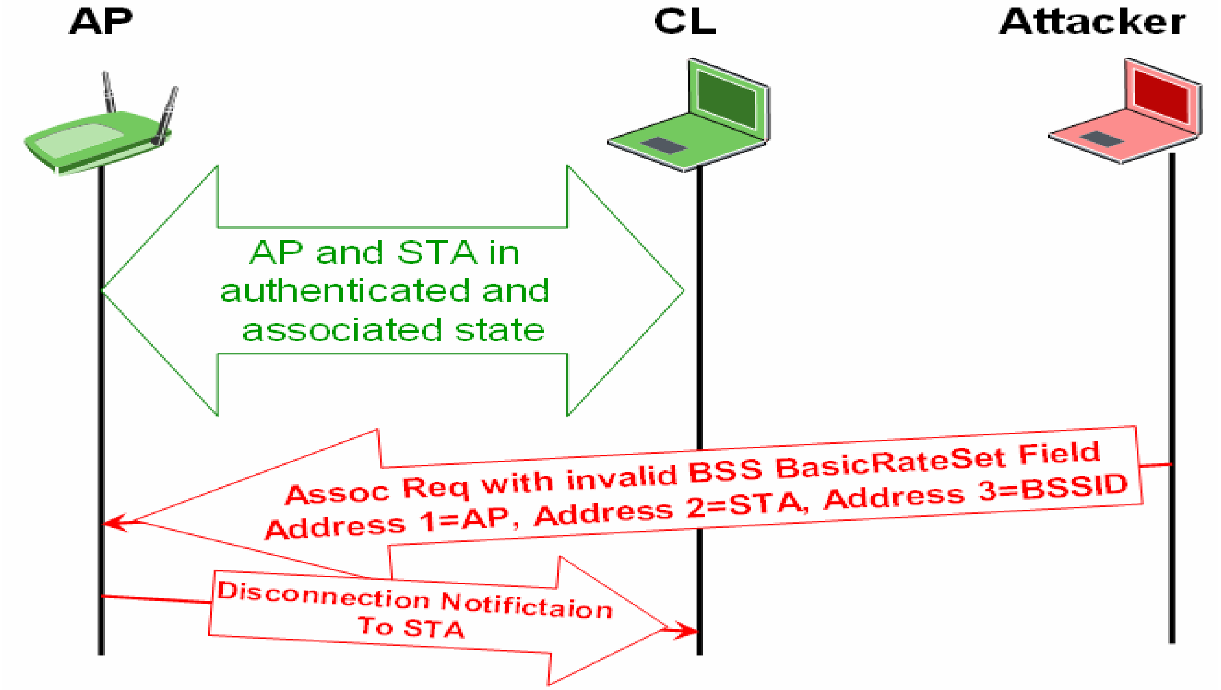
- An **Authentication** frame with invalid **Authentication Transaction Sequence Number** sent to an Access Point can potentially disconnect an associated client and can trigger a response with **Status Code 14** (Received an Authentication frame with authentication transaction sequence number out of expected sequence)


AP
STA
Attacker
AP and STA in authenticated and associated state
Authentication with invalid Auth trans seq no Field
Address 1=AP, Address 2=STA, Address 3=BSSID
Disconnection Notifictaion
To STA

Submitted to DefCon16

Stimulus #8

- An **Association Request** frame with invalid **BSS BasicRateSet** parameter sent to an Access Point can potentially disconnect an associated client and can trigger a response with **Status Code 18** (Association denied due to requesting station not supporting all of the data rates in the BSS BasicRateSet parameter)


AP
CL
Attacker
AP and STA in authenticated and associated state
Assoc Req with invalid BSS BasicRateSet Field
Address 1=AP, Address 2=STA, Address 3=BSSID
Disconnection Notifictaion
To STA

Autoimmunity Disorder Report

Attack Type	DLink, Model No DIR-655, Firmware Ver 1.1	Linksys Model No WRT350N, Firmware Ver 1.0.3.7	Cisco Model No AIR-AP1230A-A-K9 Firmware Ver 12.3(2)JA2	Cisco Model No AIR-AP1232AG-A-K9 Firmware Ver 12.3(8)JEA3	Buffalo Model No-WZR-AG300NH, Firmware ver 1.48	Madwifi-0.9.4 driver with Cisco Aironet a/b/g Card
Spoofed Authentication Frame	Yes	Yes	Yes	Yes	Yes	Yes
Spoofed Association Request Frame	Yes	No	Yes	Yes	No	Yes
Spoofed ReAssociation Request Frame	Yes	Yes	Yes	Yes	Yes	Yes

Autoimmunity Disorder Report

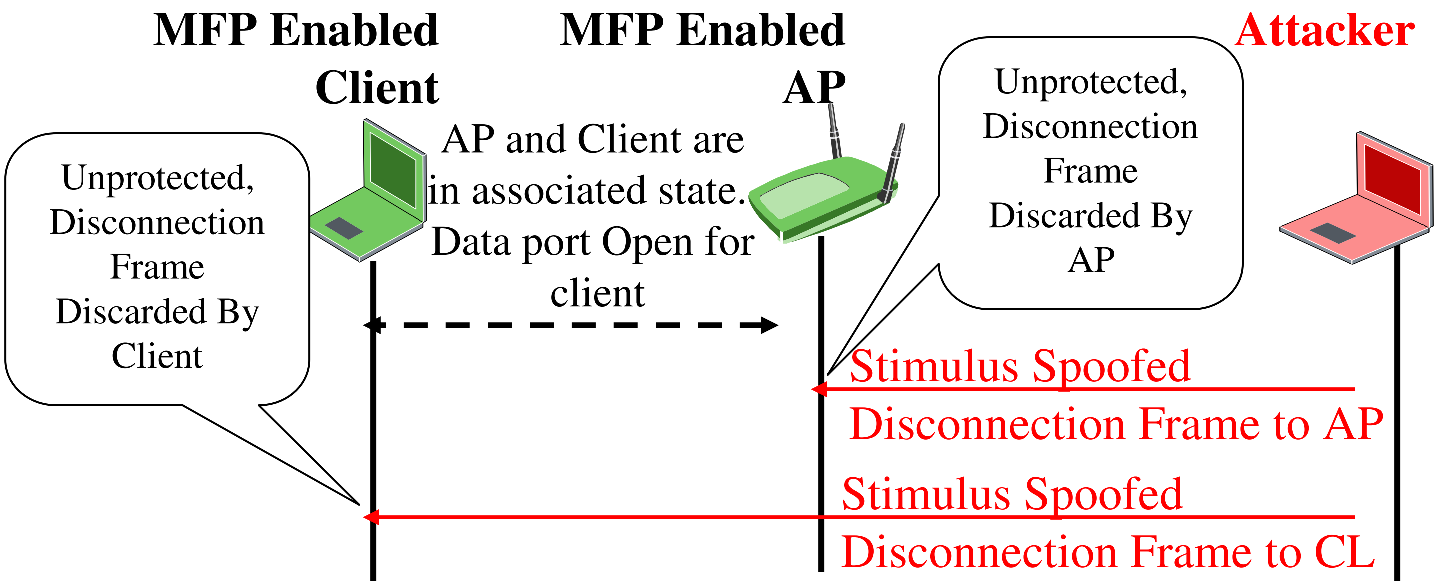
Attack Type	DLink, Model No DIR-655, Firmware Ver 1.1	Linksys Model No WRT350N, Firmware Ver 1.0.3.7	Cisco Model No AIR-AP1230A-A-K9 Firmware Ver 12.3(2)JA2	Cisco Model No AIR-AP1232AG-A-K9 Firmware Ver 12.3(8)JEA3	Buffalo Model No-WZR-AG300NH, Firmware ver 1.48	Madwifi-0.9.4 driver with Cisco Aironet a/b/g Card
Use of Broadcast MAC as Source MAC	Yes	No	No	No	Yes	Yes
Use of Multicast MAC as a Source MAC	Yes	No	No	No	Yes	Yes
Use of WDS DATA Frame	No	No	No	No	Yes	Yes

4

Does Cisco MFP also suffer from **Autoimmunity disorder**?

MFP Background

- The root cause of disconnection based DoS vulnerability in 802.11 is that management frames used for connection establishment and termination are not protected. Hence, a connection can easily be terminated by spoofing these frames.
- **Management Frame Protection MFP** (or 802.11w) aims to solve this problem by protecting connection termination frames.


MFP Enabled Client
MFP Enabled AP
Attacker
Unprotected, Disconnection Frame Discarded By Client
AP and Client are in associated state. Data port Open for client
Unprotected, Disconnection Frame Discarded By AP
Stimulus Spoofed Disconnection Frame to AP
Stimulus Spoofed Disconnection Frame to CL

Autoimmunity Disorder in MFP Infrastructure WLANs

- Autoimmunity Disorder in MFP (L)APs

Details will be provided during presentation !!!

Autoimmunity Disorder in MFP Infrastructure WLANs

- Autoimmunity Disorder in MFP Clients

Details will be provided during presentation !!!

Autoimmunity Disorder Report of MFP Protocol

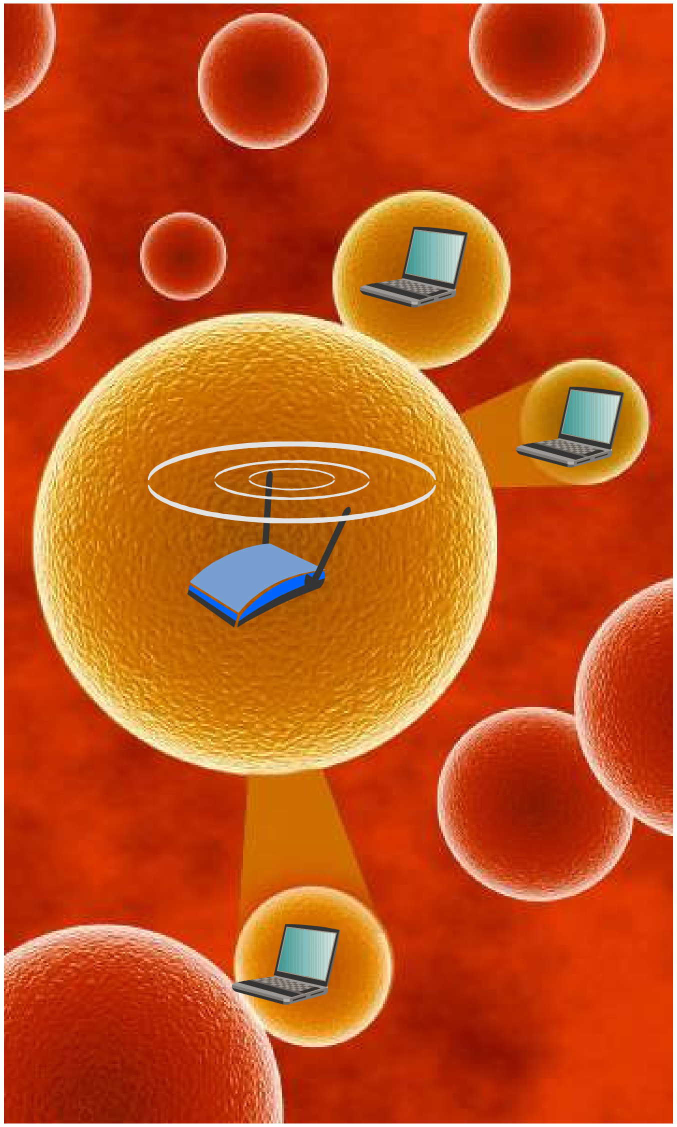
Details will be provided during presentation !!!

Submitted to DefCon16

5

The key take away

The Key Point



Without MFP protection

New avenues for launching DoS attacks are possible. Majority of vulnerabilities reported here are implementation dependent and are found to exist in select open source AP and commercial Access Point S/W.

With MFP protection

DoS vulnerabilities could not be completely eliminated. Even MFP was found vulnerable!

Food for Thought

- A fix for MFP vulnerability has already been attempted in the latest 11w draft. Future revisions of 11w draft will continue to raise the bar & try to make 802.11 DoS attack proof.

Will the dream of attack proof 802.11 be ever realized?

References

- www.cs.ucsd.edu/users/**savage**/**papers**/UsenixSec03.pdf
- http://en.wikipedia.org/wiki/IEEE_802.11w
- http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008080dc8c.shtml

Contact Us

- Md Sohail Ahmad
  md.ahmad@airtightnetworks.com

- Amit Vartak
  amit.vartak@airtightnetworks.com

- J V R Murthy
  murthy.jvr@airtightnetworks.com