Hole196 Vulnerability in WPA2

AirTight® NETWORKS

Hole196 Vulnerability in WPA2

Presenters:

Anthony Paladino, Managing Director, Systems Engineering

Dr. Kaustubh Phanse, Principal Wireless Architect

Md. Sohail Ahmad, Senior Security Researcher

Moderator:

Della Lowe, Sr. Director, Corporate Marketing

AirTight NETWORKS

What happened last week in Las Vegas?

NETWORKWORLD®	Upshot of the WPA2 brouhaha
TechRepublic	WPA/WPA2 not as secure as we would like to believe
GCN GOVERNMENT COMPUTER NEWS	How malicious insiders could hack your Wi-Fi -- easily!
darknet.org.uk	WPA2 vulnerability uncovered – “Hole196”

This webinar

Is there a fix

?

Should I worry about it

What’s wrong with WPA2

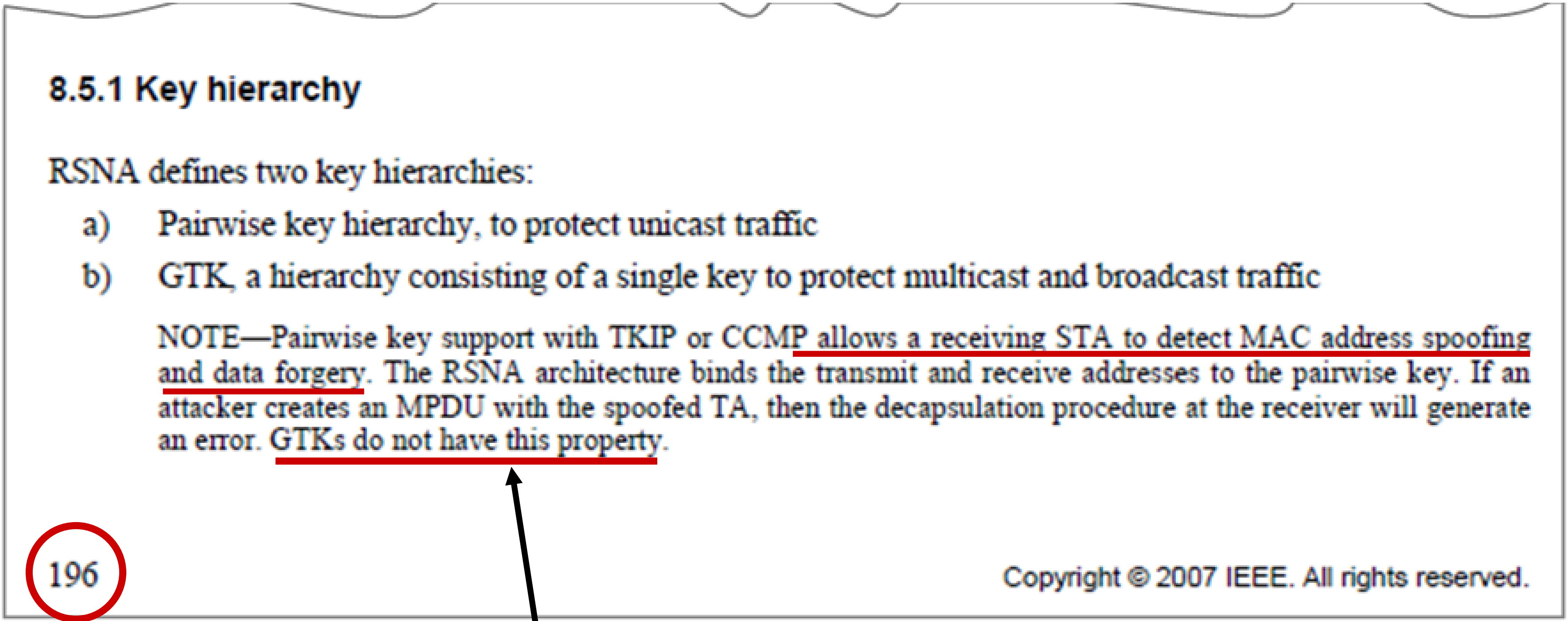
But, I have heard that…

What’s Hole196

?

?

What’s Hole196?



8.5.1 Key hierarchy

RSNA defines two key hierarchies:

a) Pairwise key hierarchy, to protect unicast traffic

b) GTK, a hierarchy consisting of a single key to protect multicast and broadcast traffic

NOTE—Pairwise key support with TKIP or CCMP allows a receiving STA to detect MAC address spoofing and data forgery. The RSNA architecture binds the transmit and receive addresses to the pairwise key. If an attacker creates an MPDU with the spoofed TA, then the decapsulation procedure at the receiver will generate an error. GTKs do not have this property.

196

Hole 196!!!

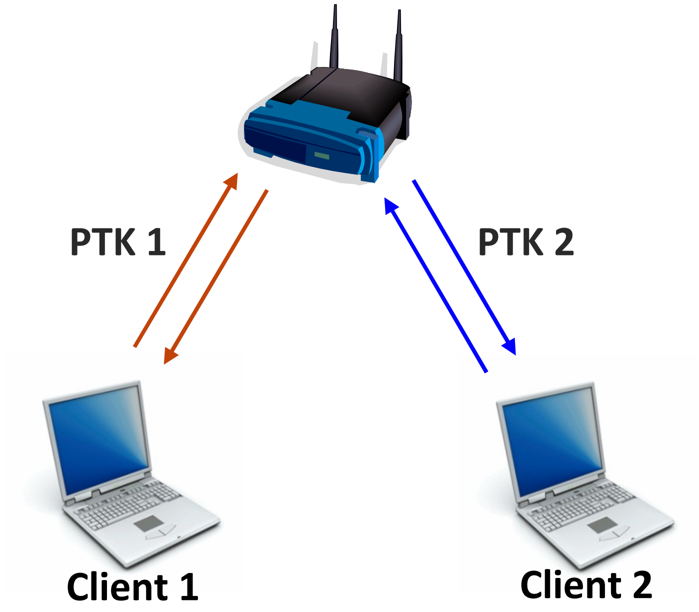
It’s right here!

Buried inside the 1232-page
IEEE 802.11 Standard (Revision, 2007)

WPA/WPA2 defines two types of keys to protect data frames

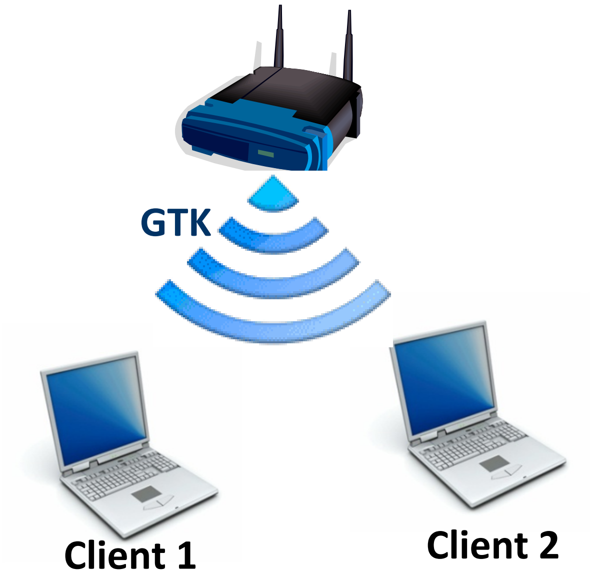
Pairwise Transient Key (PTK)

- Unique for each client
- Protect unicast data frames

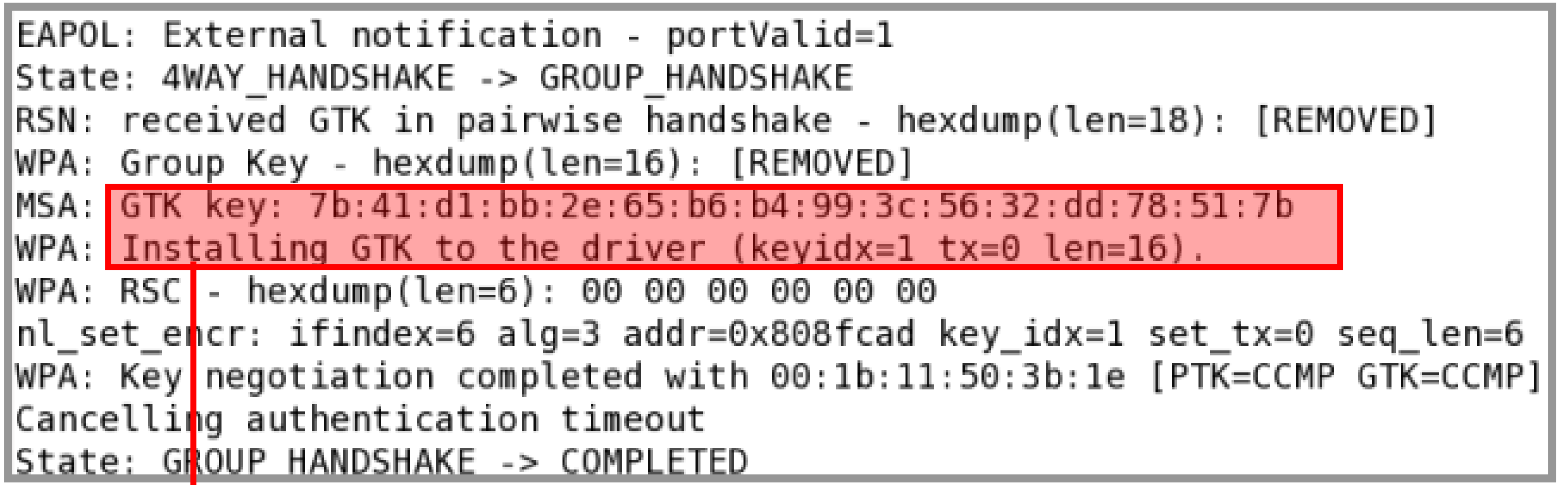


Group Temporal Key (GTK)

- Shared by all clients in a BSS
- Protect group addressed data frames (e.g., broadcast, multicast)



GTK: Key to the kingdom!



```
EAPOL: External notification - portValid=1
State: 4WAY_HANDSHAKE -> GROUP_HANDSHAKE
RSN: received GTK in pairwise handshake - hexdump(len=18): [REMOVED]
WPA: Group Key - hexdump(len=16): [REMOVED]
MSA: GTK key: 7b:41:d1:bb:2e:65:b6:b4:99:3c:56:32:dd:78:51:7b
WPA: Installing GTK to the driver (keyidx=1 tx=0 len=16).
WPA: RSC - hexdump(len=6): 00 00 00 00 00 00
nl_set_encr: ifindex=6 alg=3 addr=0x808fcad key_idx=1 set_tx=0 seq_len=6
WPA: Key negotiation completed with 00:1b:11:50:3b:1e [PTK=CCMP GTK=CCMP]
Cancelling authentication timeout
State: GROUP_HANDSHAKE -> COMPLETED
```

Parameters (GTK, KeyID and PN) required to send group addressed data frame is known to all connected clients

If you dream it, you can hide it!

- “Overhear” VoIP over Wi-Fi conversations
- Steal intellectual property/trade secrets
- Steal identity and password
- Sniff credit card transactions over Wi-Fi PoS
- Denial of Service (DoS)
- Port scanning, malware injection, key logger, etc.

What’s your domestic policy?

“…51% of respondents were still victims of an insider attack.”

“ The most costly or damaging attacks are more often caused by insiders (employees or contractors with authorized access) .”

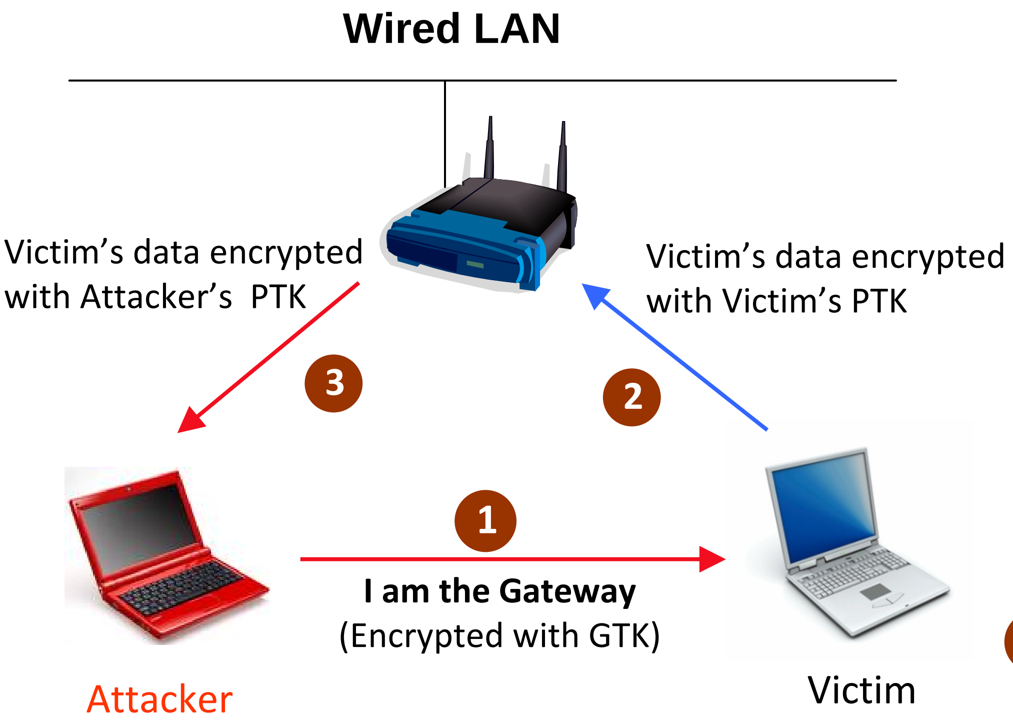
**- 2010 CyberSecurity Watch Survey
by CERT, CSO and Deloitte**

“ Breaches Down, Insider Attacks Up!”

**- 2010 Data Breaches Investigation
by Verizon and U.S. Secret Service**

Hole 196

Exploit #1: Stealth-mode man in the middle

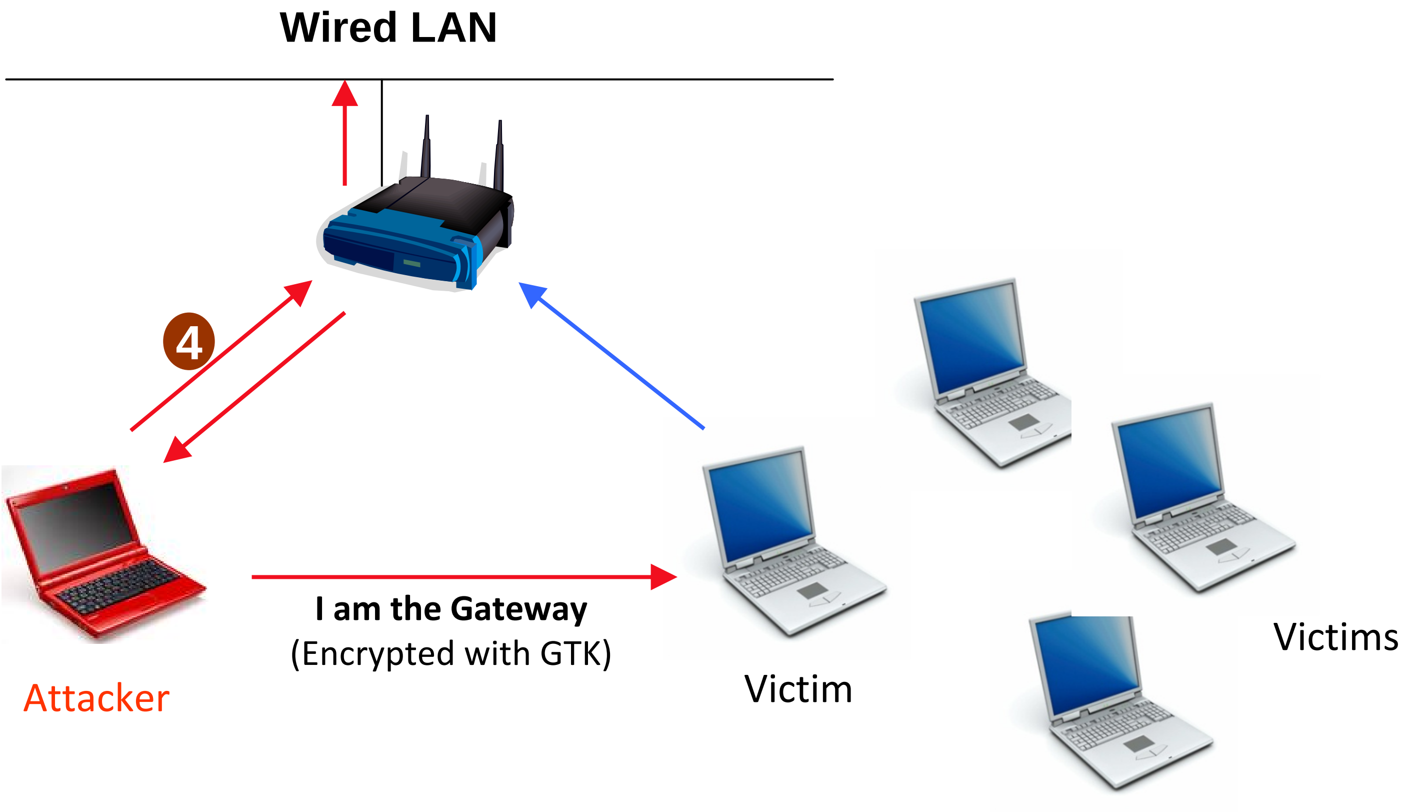

Wired LAN
Victim's data encrypted with Attacker's PTK
Victim's data encrypted with Victim's PTK
3
2
1
I am the Gateway
(Encrypted with GTK)
Attacker
Victim

1. Attacker injects fake ARP Request packet to poison client's cache for gateway.

2. Victim sends all traffic encrypted with its PTK to the AP, with Attacker as the destination (gateway)

3. AP forwards Victim's data to the Attacker encrypting it in the Attacker's PTK. So Attacker can decrypt Victim's private data.

Exploit #1: Stealth mode man in the middle



4 Attacker forwards victim data to actual Gateway to provide a transparent service to the victim

Open source software: Madwifi & WPA supplicant

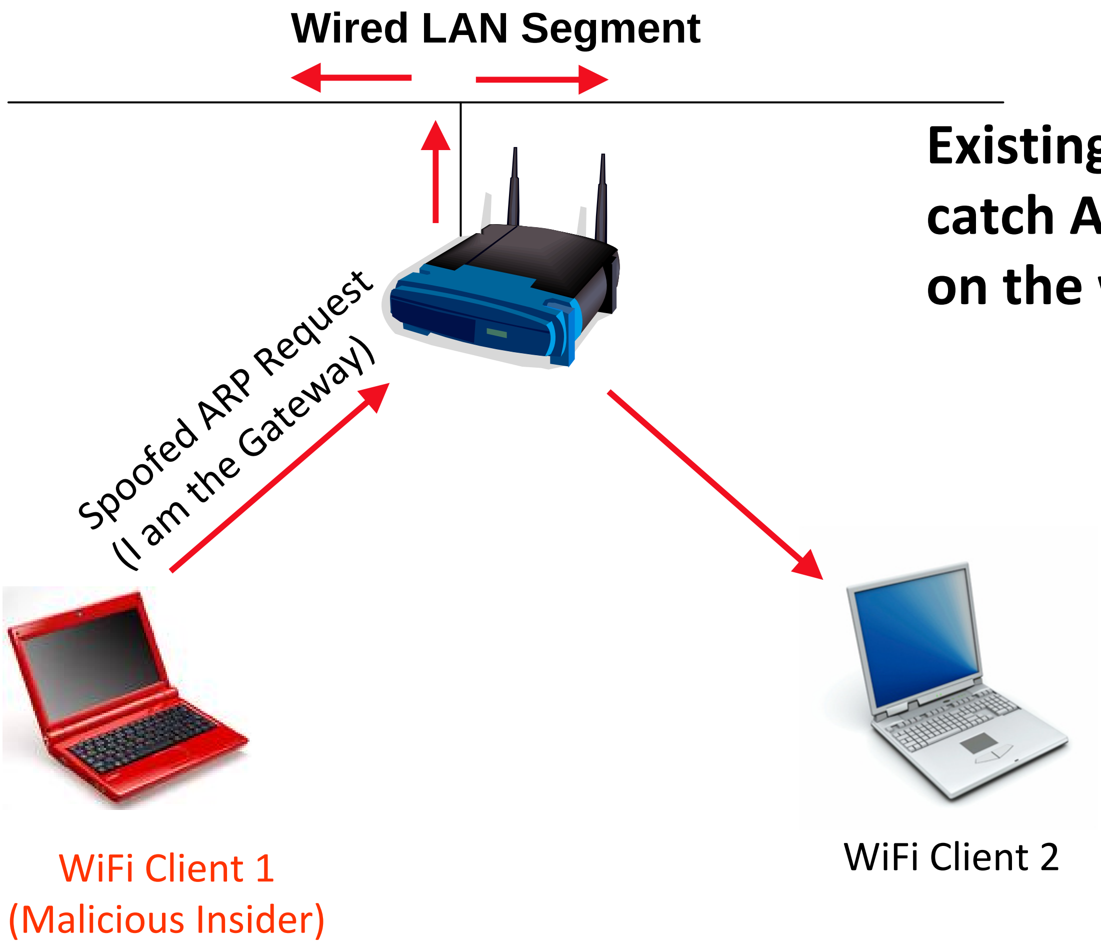
wpa_supplicant (0.7.0)

Used to pass updated GTK and packet number (PN) to the madwifi driver

Madwifi (0.9.4)

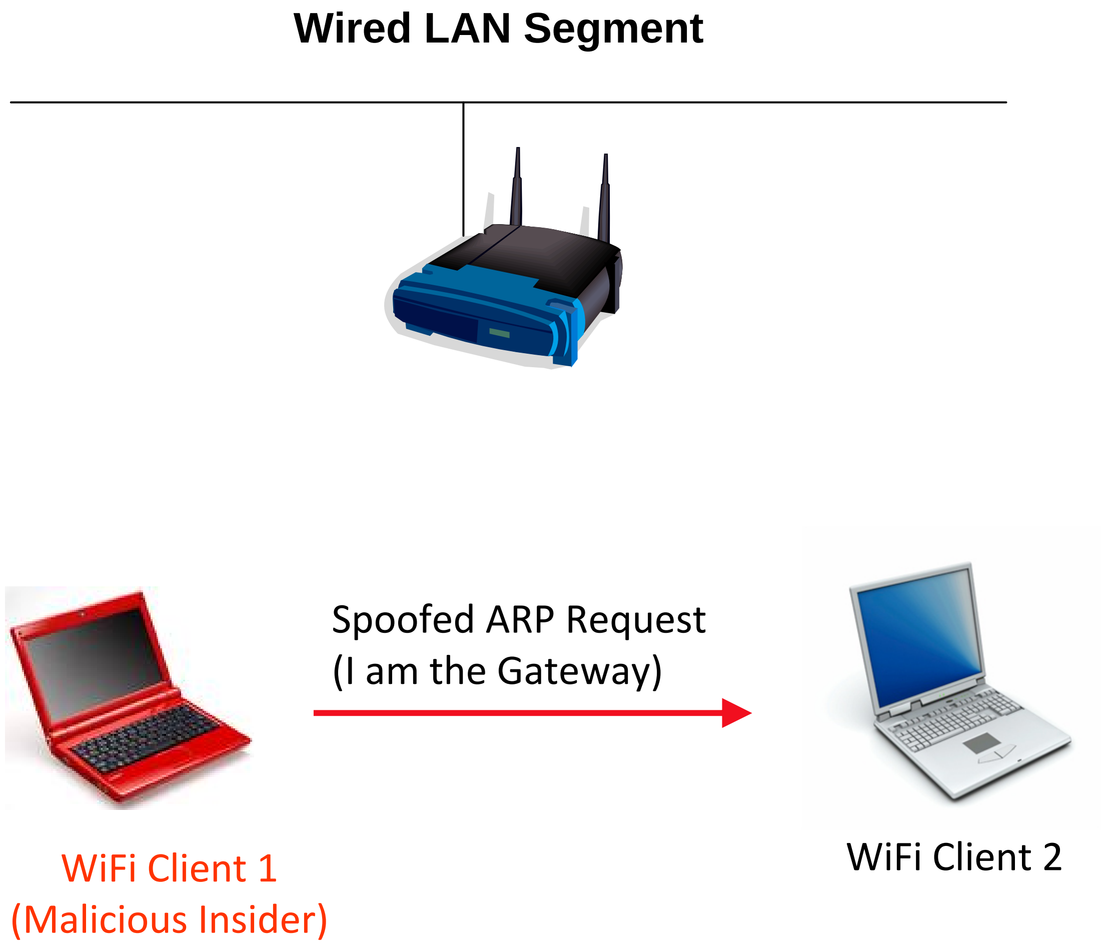
Modified and used to create spoofed group addressed data frames
with AP MAC address as the sender

But you can do ARP spoofing today over WPA2!
So what’s new?

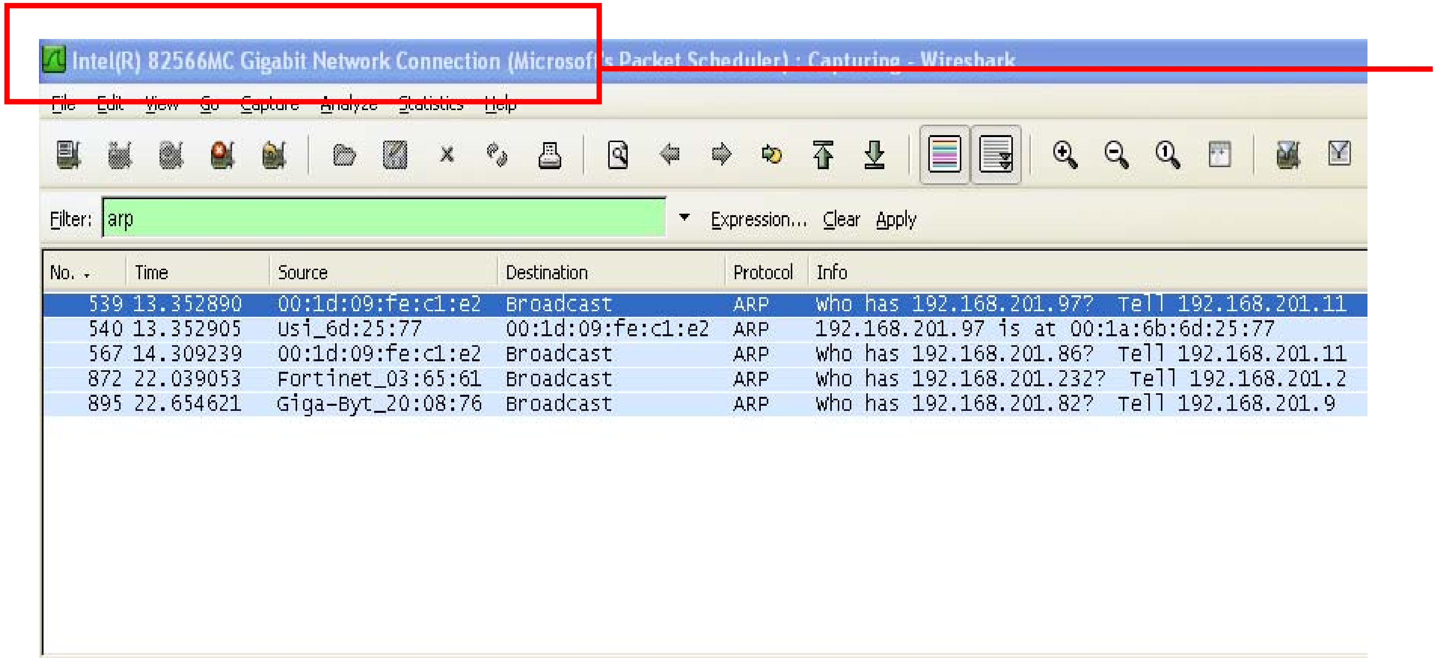


Existing wired IDS/IPS can catch ARP spoofing attack on the wire!

The footprint of ARP spoofing using GTK is limited to the air!



Packet trace of the stealth-mode ARP spoofing

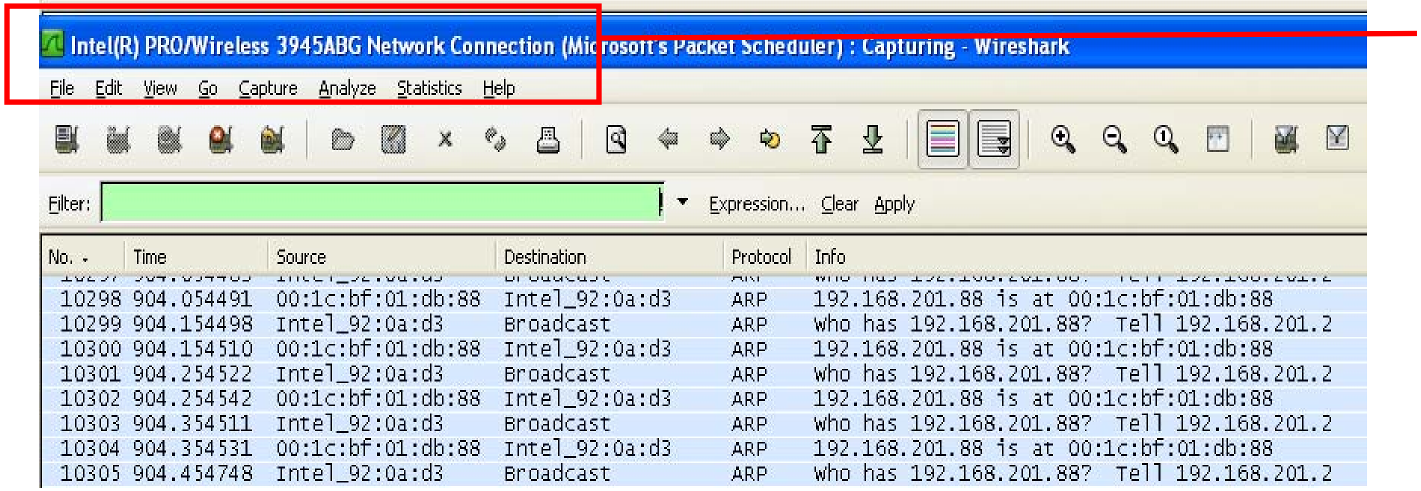

Intel(R) 82566MC Gigabit Network Connection (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: arp

No.	Time	Source	Destination	Protocol	Info
539	13.352890	00:1d:09:fe:c1:e2	Broadcast	ARP	Who has 192.168.201.97? Tell 192.168.201.11
540	13.352905	Usi_6d:25:77	00:1d:09:fe:c1:e2	ARP	192.168.201.97 is at 00:1a:6b:6d:25:77
567	14.309239	00:1d:09:fe:c1:e2	Broadcast	ARP	Who has 192.168.201.86? Tell 192.168.201.11
872	22.039053	Fortinet_03:65:61	Broadcast	ARP	Who has 192.168.201.232? Tell 192.168.201.2
895	22.654621	Giga-Byt_20:08:76	Broadcast	ARP	Who has 192.168.201.82? Tell 192.168.201.9

Packet capture on **wired** interface

Broadcast attack frames not visible on the wire


Intel(R) PRO/Wireless 3945ABG Network Connection (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

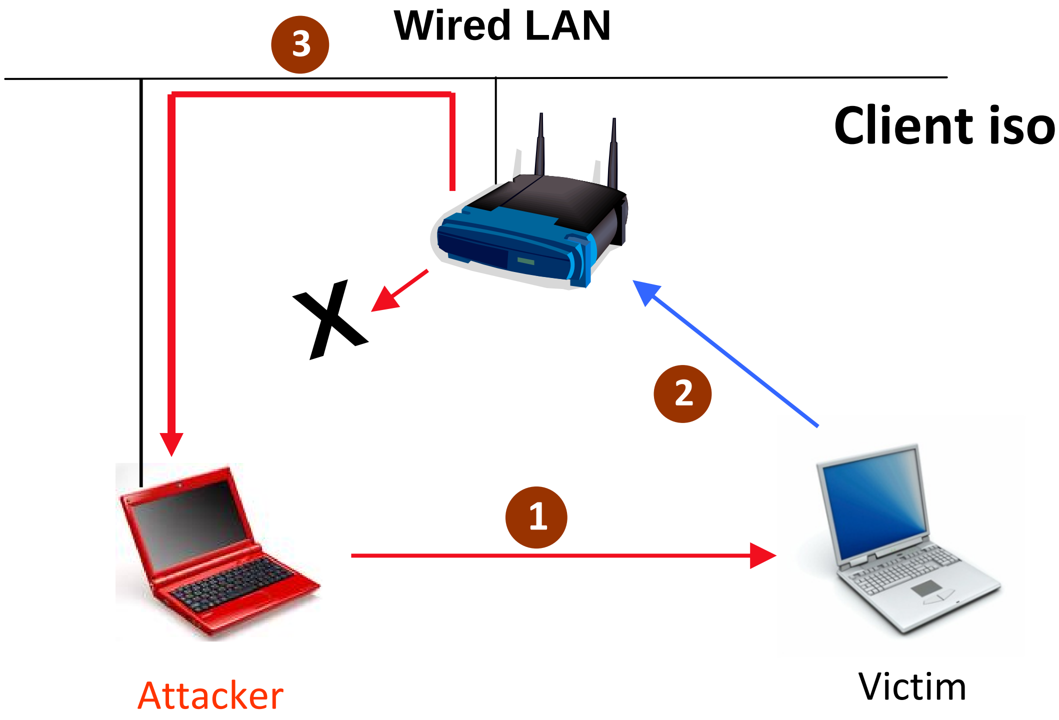
Filter:

No.	Time	Source	Destination	Protocol	Info
10298	904.054491	00:1c:bf:01:db:88	Intel_92:0a:d3	ARP	192.168.201.88 is at 00:1c:bf:01:db:88
10299	904.154498	Intel_92:0a:d3	Broadcast	ARP	Who has 192.168.201.88? Tell 192.168.201.2
10300	904.154510	00:1c:bf:01:db:88	Intel_92:0a:d3	ARP	192.168.201.88 is at 00:1c:bf:01:db:88
10301	904.254522	Intel_92:0a:d3	Broadcast	ARP	Who has 192.168.201.88? Tell 192.168.201.2
10302	904.254542	00:1c:bf:01:db:88	Intel_92:0a:d3	ARP	192.168.201.88 is at 00:1c:bf:01:db:88
10303	904.354511	Intel_92:0a:d3	Broadcast	ARP	Who has 192.168.201.88? Tell 192.168.201.2
10304	904.354531	00:1c:bf:01:db:88	Intel_92:0a:d3	ARP	192.168.201.88 is at 00:1c:bf:01:db:88
10305	904.454748	Intel_92:0a:d3	Broadcast	ARP	Who has 192.168.201.88? Tell 192.168.201.2

Packet capture on **wireless** interface

Broadcast attack frames visible only in the air

If this is not a problem, what are you fixing?

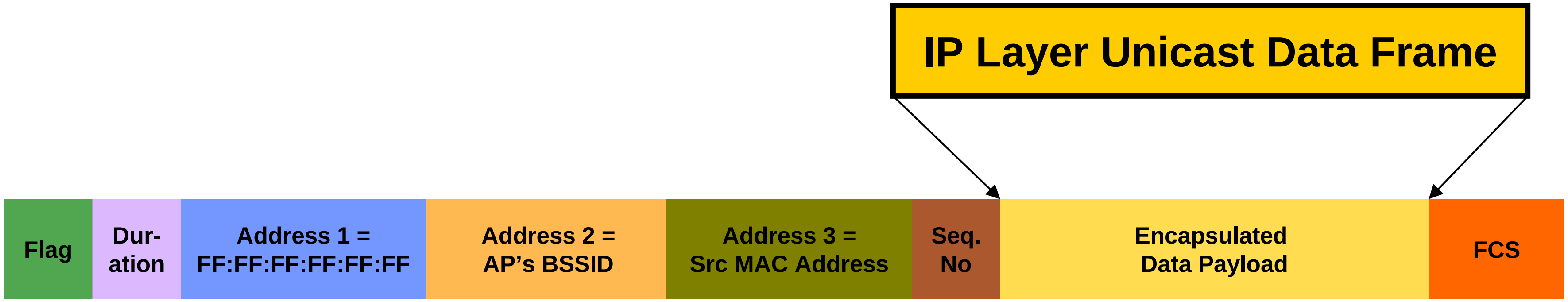


Client isolation (or PSPF)

- **Not always practical**
- **Not the ultimate solution; can be bypassed**
  - ARP poisoning over the air & MITM on wire
  - Other attacks possible that do not involve AP

Exploit #2: IP layer targeted attack

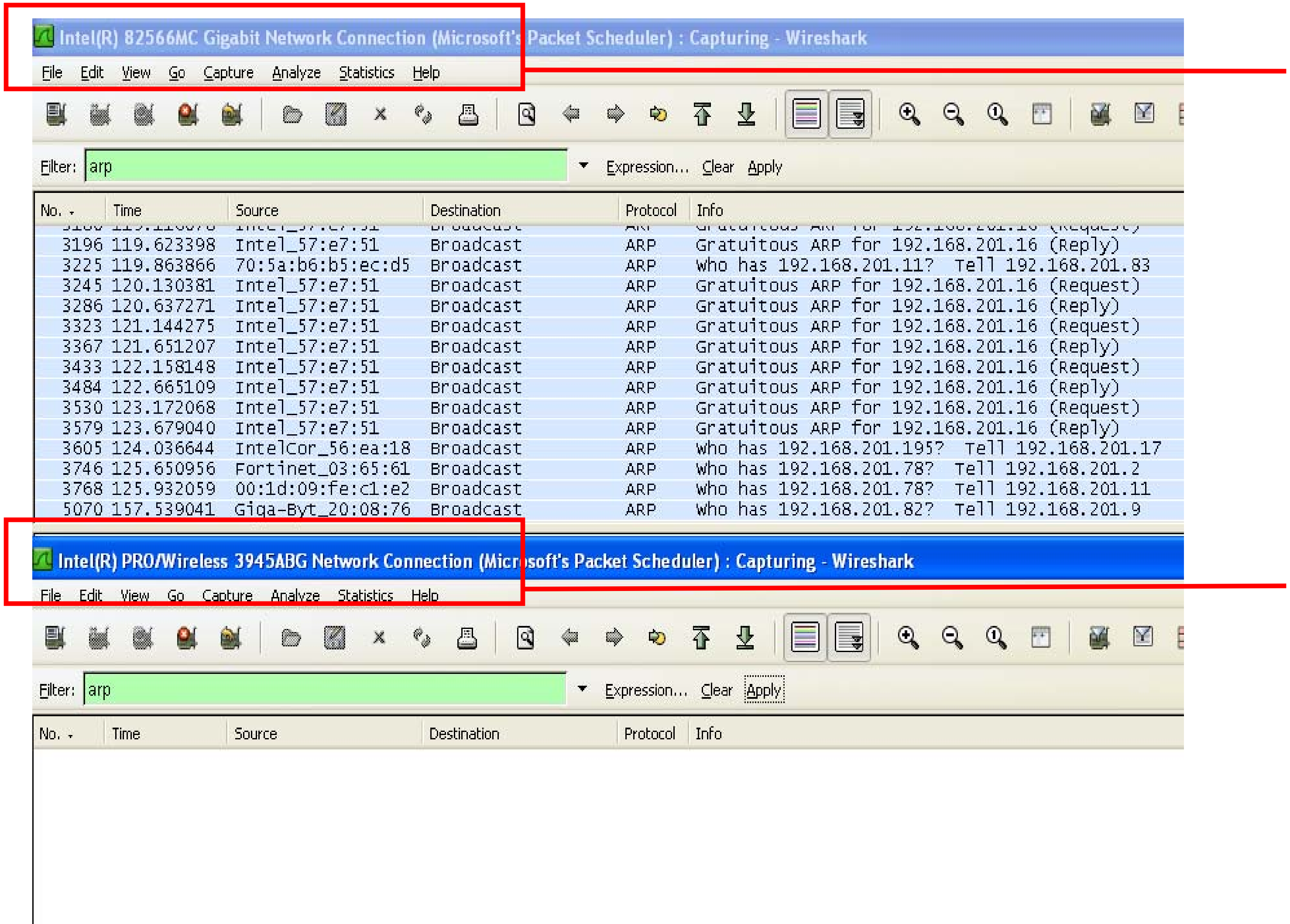
Any data payload can be encapsulated in the GTK-encrypted group addressed 802.11 frames


IP Layer Unicast Data Frame
Flag
Dur-ation
Address 1 = FF:FF:FF:FF:FF:FF
Address 2 = AP's BSSID
Address 3 = Src MAC Address
Seq. No
Encapsulated Data Payload
FCS

IEEE 802.11 Data Frame

Exploit #3: Denial of Service (DoS)

A malicious insider can advance the locally cached PN (replay counter) in victim clients by forging a group addressed data frame with a very large PN


Intel(R) 82566MC Gigabit Network Connection (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: arp

```
No.  Time        Source             Destination  Protocol  Info
3196 119.623398  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Reply)
3225 119.863866  70:5a:b6:b5:ec:d5  Broadcast    ARP       Who has 192.168.201.11?  Tell 192.168.201.83
3245 120.130381  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Request)
3286 120.637271  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Reply)
3323 121.144275  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Request)
3367 121.651207  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Reply)
3433 122.158148  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Request)
3484 122.665109  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Reply)
3530 123.172068  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Request)
3579 123.679040  Intel_57:e7:51     Broadcast    ARP       Gratuitous ARP for 192.168.201.16 (Reply)
3605 124.036644  IntelCor_56:ea:18  Broadcast    ARP       Who has 192.168.201.195?  Tell 192.168.201.17
3746 125.650956  Fortinet_03:65:61  Broadcast    ARP       Who has 192.168.201.78?  Tell 192.168.201.2
3768 125.932059  00:1d:09:fe:c1:e2  Broadcast    ARP       Who has 192.168.201.78?  Tell 192.168.201.11
5070 157.539041  Giga-Byt_20:08:76  Broadcast    ARP       Who has 192.168.201.82?  Tell 192.168.201.9
```

Intel(R) PRO/Wireless 3945ABG Network Connection (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: arp

```
No.  Time        Source             Destination  Protocol  Info
```

Packet capture on **wired** interface

Broadcast traffic visible

Packet capture on **wireless** interface

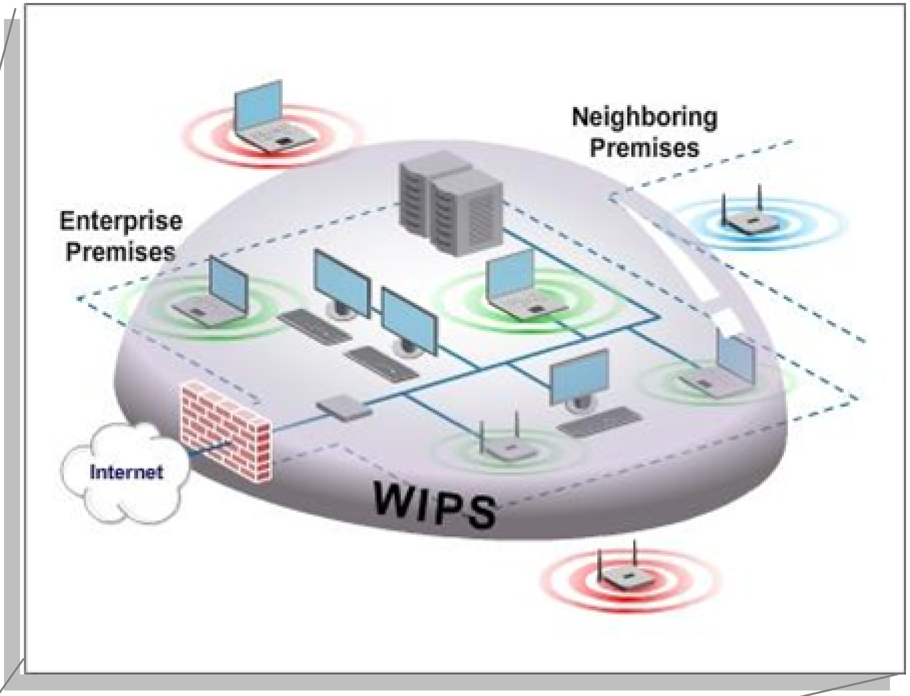
No Broadcast traffic is visible

Fixing the WPA2 protocol

- **Deprecate use of GTK and group-addressed data traffic**
  - APs in controller based WLAN architectures often do not broadcast data frames over the air
  - For backward compatibility, unique GTKs can be assigned to individual authorized Wi-Fi clients in the network
  - If data frames have to be broadcast, then transmit as unicast

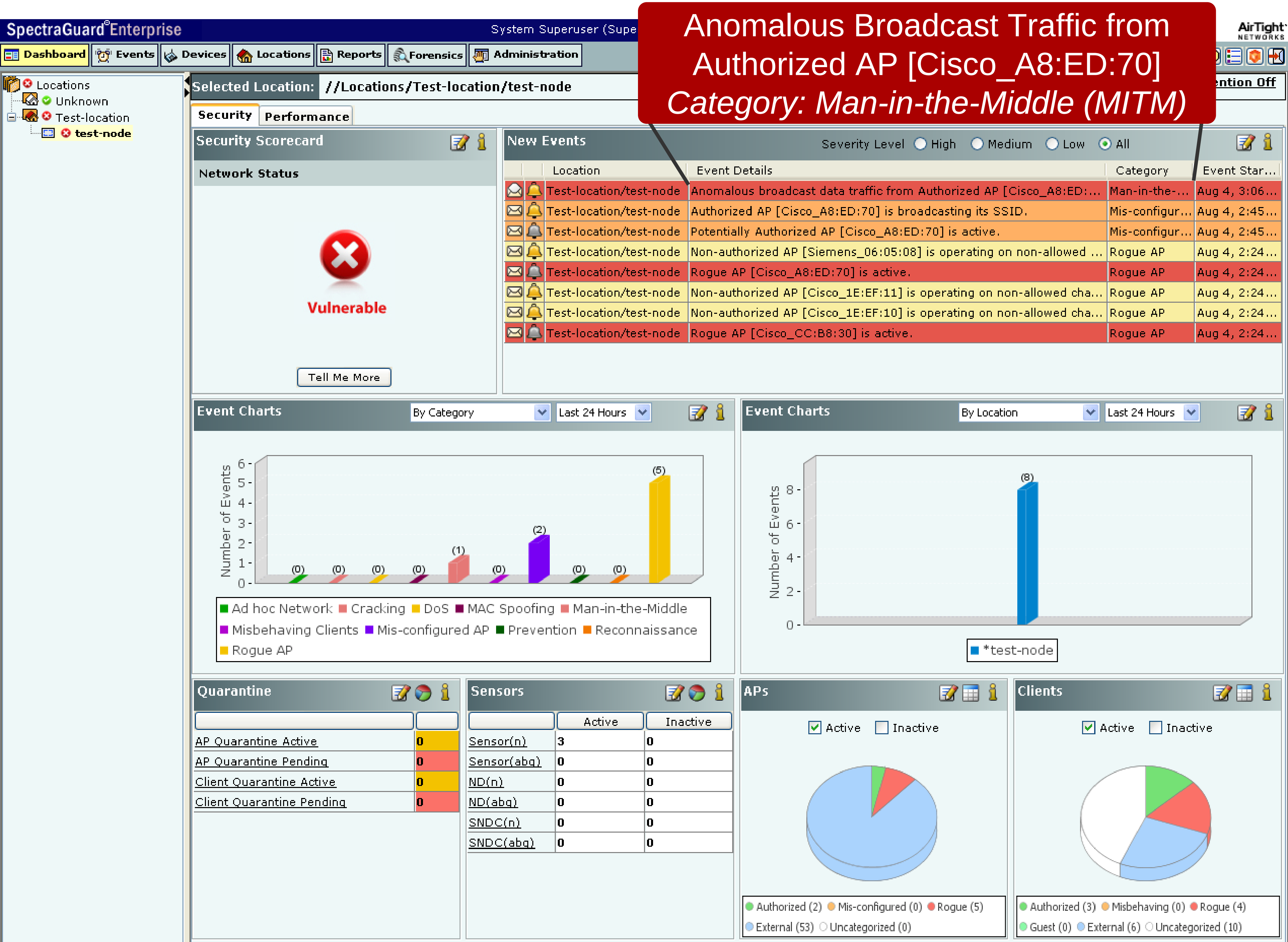
- **Disadvantage**
  - May degrade WLAN throughput if broadcast traffic is sent as unicast
  - Not going to happen overnight!

Wireless intrusion prevention system (WIPS) as an additional layer of defense



AirTight's SpectraGuard Enterprise WIPS

Anomalous Broadcast Traffic from Authorized AP [Cisco_A8:ED:70] *Category: Man-in-the-Middle (MITM)*



Selected Location: //Locations/Test-location/test-node

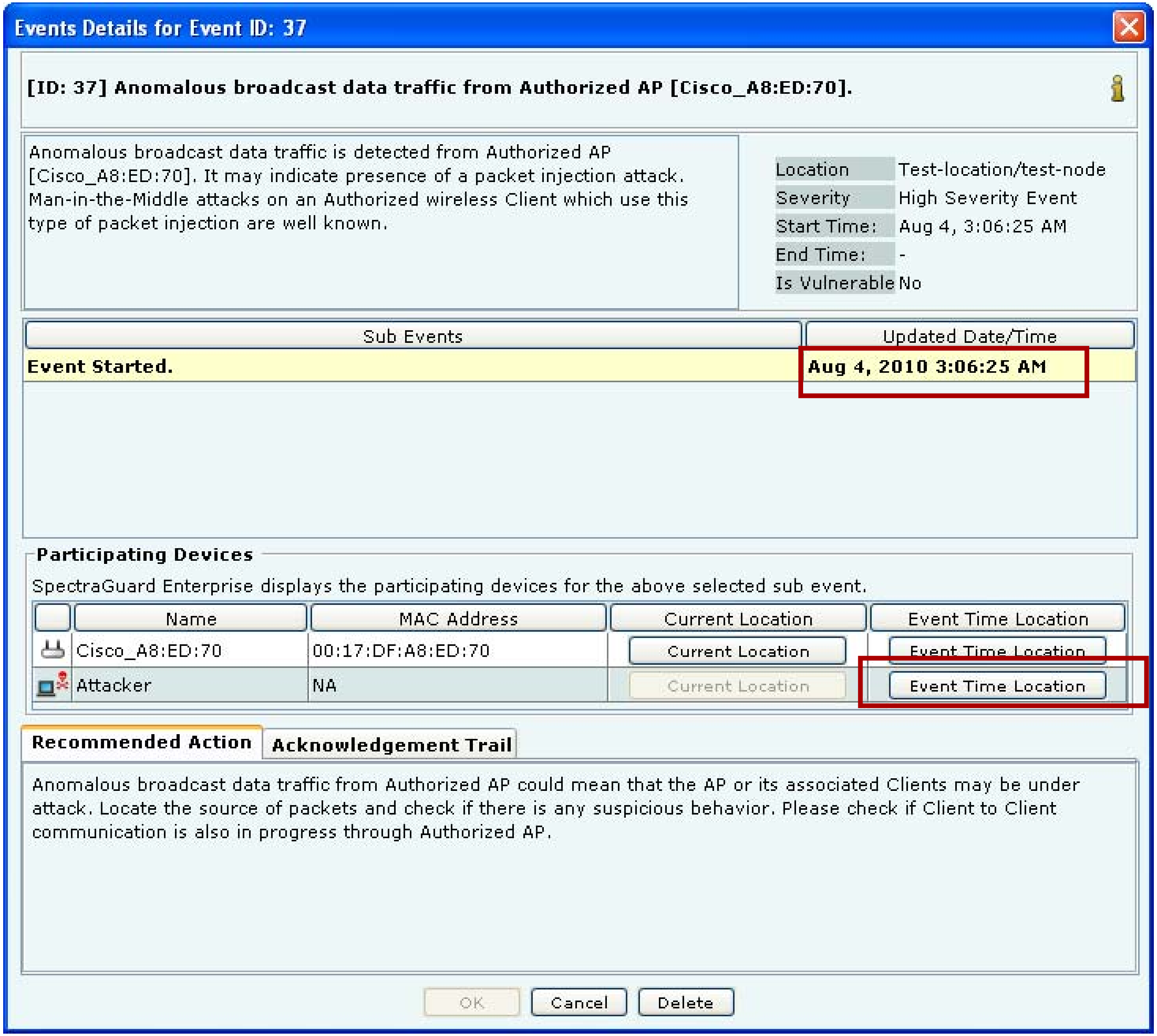
Location	Event Details	Category	Event Star...
Test-location/test-node	Anomalous broadcast data traffic from Authorized AP [Cisco_A8:ED:...	Man-in-the-...	Aug 4, 3:06...
Test-location/test-node	Authorized AP [Cisco_A8:ED:70] is broadcasting its SSID.	Mis-configur...	Aug 4, 2:45...
Test-location/test-node	Potentially Authorized AP [Cisco_A8:ED:70] is active.	Mis-configur...	Aug 4, 2:45...
Test-location/test-node	Non-authorized AP [Siemens_06:05:08] is operating on non-allowed ...	Rogue AP	Aug 4, 2:24...
Test-location/test-node	Rogue AP [Cisco_A8:ED:70] is active.	Rogue AP	Aug 4, 2:24...
Test-location/test-node	Non-authorized AP [Cisco_1E:EF:11] is operating on non-allowed cha...	Rogue AP	Aug 4, 2:24...
Test-location/test-node	Non-authorized AP [Cisco_1E:EF:10] is operating on non-allowed cha...	Rogue AP	Aug 4, 2:24...
Test-location/test-node	Rogue AP [Cisco_CC:B8:30] is active.	Rogue AP	Aug 4, 2:24...

Quarantine

AP Quarantine Active	0
AP Quarantine Pending	0
Client Quarantine Active	0
Client Quarantine Pending	0

Sensors

	Active	Inactive
Sensor(n)	3	0
Sensor(abg)	0	0
ND(n)	0	0
ND(abg)	0	0
SNDC(n)	0	0
SNDC(abg)	0	0



Events Details for Event ID: 37

[ID: 37] Anomalous broadcast data traffic from Authorized AP [Cisco_A8:ED:70].

Anomalous broadcast data traffic is detected from Authorized AP [Cisco_A8:ED:70]. It may indicate presence of a packet injection attack. Man-in-the-Middle attacks on an Authorized wireless Client which use this type of packet injection are well known.

Location	Test-location/test-node
Severity	High Severity Event
Start Time:	Aug 4, 3:06:25 AM
End Time:	-
Is Vulnerable	No

Sub Events	Updated Date/Time
Event Started.	**Aug 4, 2010 3:06:25 AM**

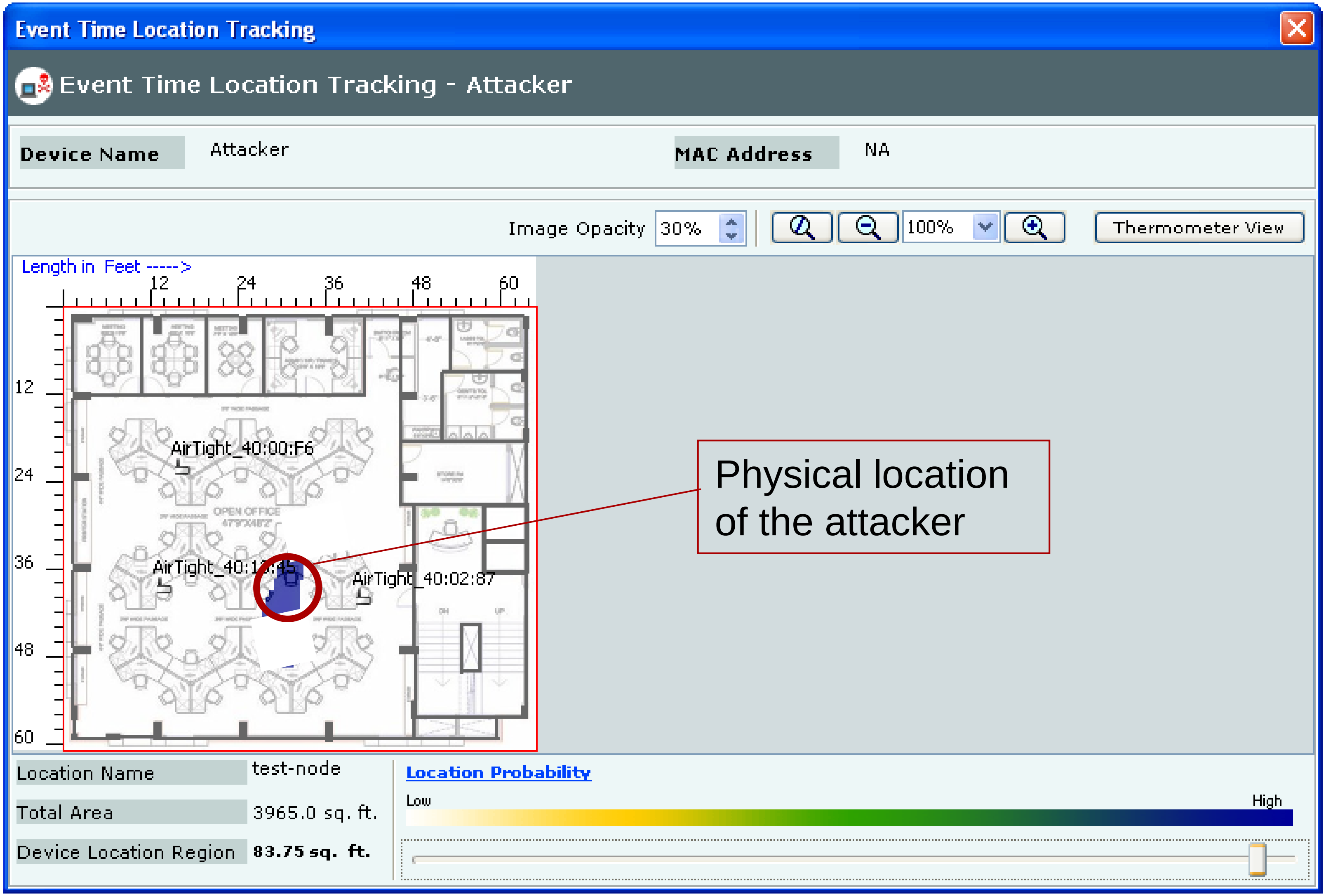
Participating Devices

SpectraGuard Enterprise displays the participating devices for the above selected sub event.

	Name	MAC Address	Current Location	Event Time Location
	Cisco_A8:ED:70	00:17:DF:A8:ED:70	Current Location	Event Time Location
	Attacker	NA	Current Location	Event Time Location

Recommended Action | **Acknowledgement Trail**

Anomalous broadcast data traffic from Authorized AP could mean that the AP or its associated Clients may be under attack. Locate the source of packets and check if there is any suspicious behavior. Please check if Client to Client communication is also in progress through Authorized AP.



Event Time Location Tracking

Event Time Location Tracking - Attacker

Device Name	Attacker	MAC Address	NA

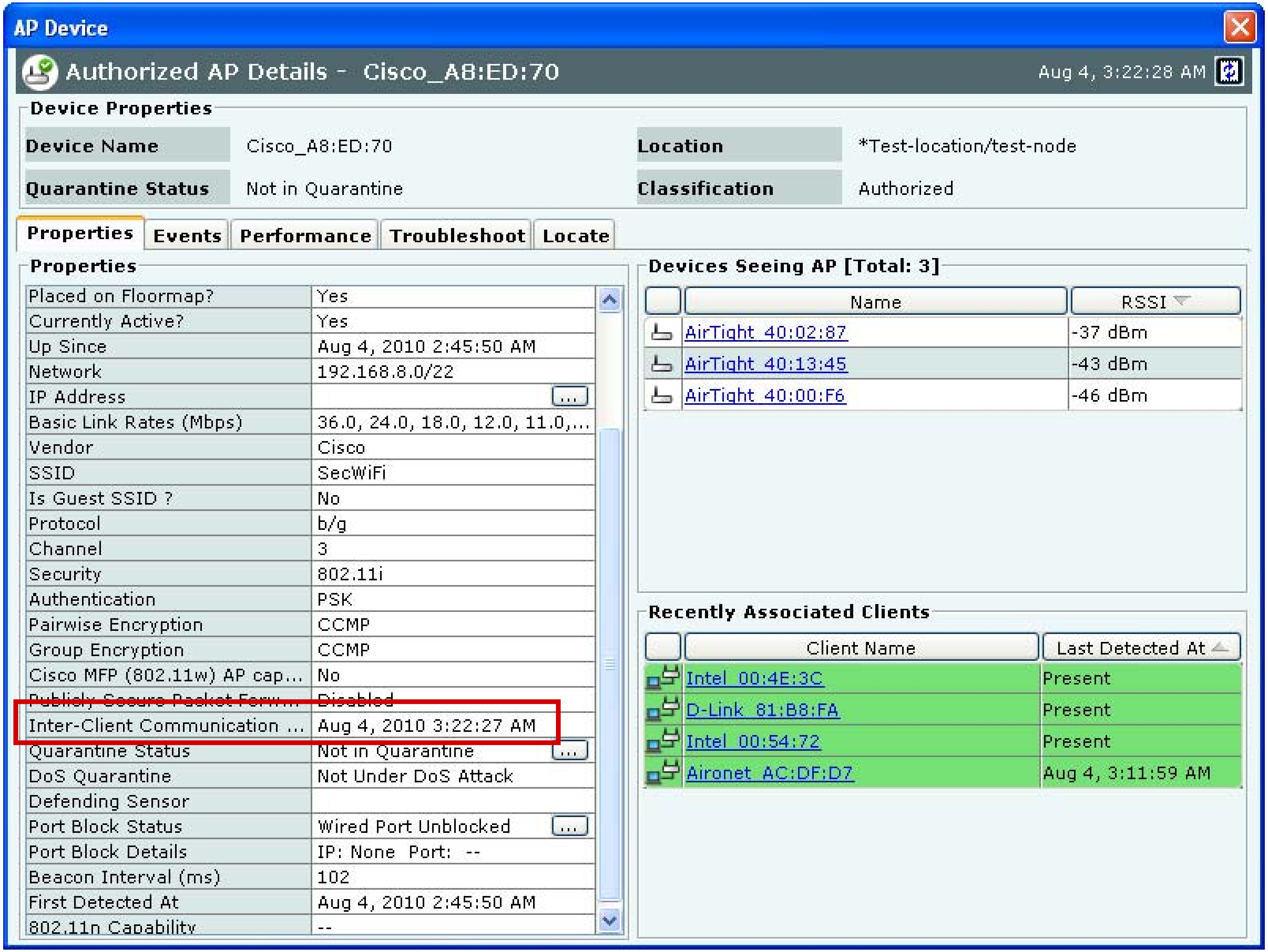
Image Opacity 30%

100%

Location Name	test-node
Total Area	3965.0 sq. ft.
Device Location Region	83.75 sq. ft.

Location Probability

Physical location of the attacker



AP Device

Authorized AP Details - Cisco_A8:ED:70 Aug 4, 3:22:28 AM

Device Properties

Device Name	Cisco_A8:ED:70	**Location**	*Test-location/test-node
Quarantine Status	Not in Quarantine	**Classification**	Authorized

Properties

Placed on Floormap?	Yes
Currently Active?	Yes
Up Since	Aug 4, 2010 2:45:50 AM
Network	192.168.8.0/22
IP Address	...
Basic Link Rates (Mbps)	36.0, 24.0, 18.0, 12.0, 11.0,...
Vendor	Cisco
SSID	SecWiFi
Is Guest SSID ?	No
Protocol	b/g
Channel	3
Security	802.11i
Authentication	PSK
Pairwise Encryption	CCMP
Group Encryption	CCMP
Cisco MFP (802.11w) AP cap...	No
Publicly Secure Packet Forw...	Disabled
Inter-Client Communication ...	Aug 4, 2010 3:22:27 AM
Quarantine Status	Not in Quarantine ...
DoS Quarantine	Not Under DoS Attack
Defending Sensor	
Port Block Status	Wired Port Unblocked ...
Port Block Details	IP: None Port: --
Beacon Interval (ms)	102
First Detected At	Aug 4, 2010 2:45:50 AM
802.11n Capability	--

Devices Seeing AP [Total: 3]

	Name	RSSI
	AirTight_40:02:87	-37 dBm
	AirTight_40:13:45	-43 dBm
	AirTight_40:00:F6	-46 dBm

Recently Associated Clients

	Client Name	Last Detected At
	Intel_00:4E:3C	Present
	D-Link_81:B8:FA	Present
	Intel_00:54:72	Present
	Aironet_AC:DF:D7	Aug 4, 3:11:59 AM

Concluding remarks

- **Hole196: Allows an insider to bypass WPA2 inter-user data privacy**
  - All WPA and WPA2 networks are vulnerable
  - No key cracking! No brute force!

- **Client isolation or PSPF**
  - Use it as a first aid, but it’s not the ultimate solution

- **Proprietary fix to the WPA2 protocol (without breaking the interoperability) is possible**

- **WIPS as an additional layer of security**
  - A dedicated WIPS such as SpectraGuard Enterprise, monitoring the airspace 24/7, can protect enterprise networks from wireless threats

Thank You!

AirTight NETWORKS

The Global Leader in Wireless Security and Compliance Solutions

For more information on wireless security risks, best practices, and solutions, visit:

www.airtightnetworks.com

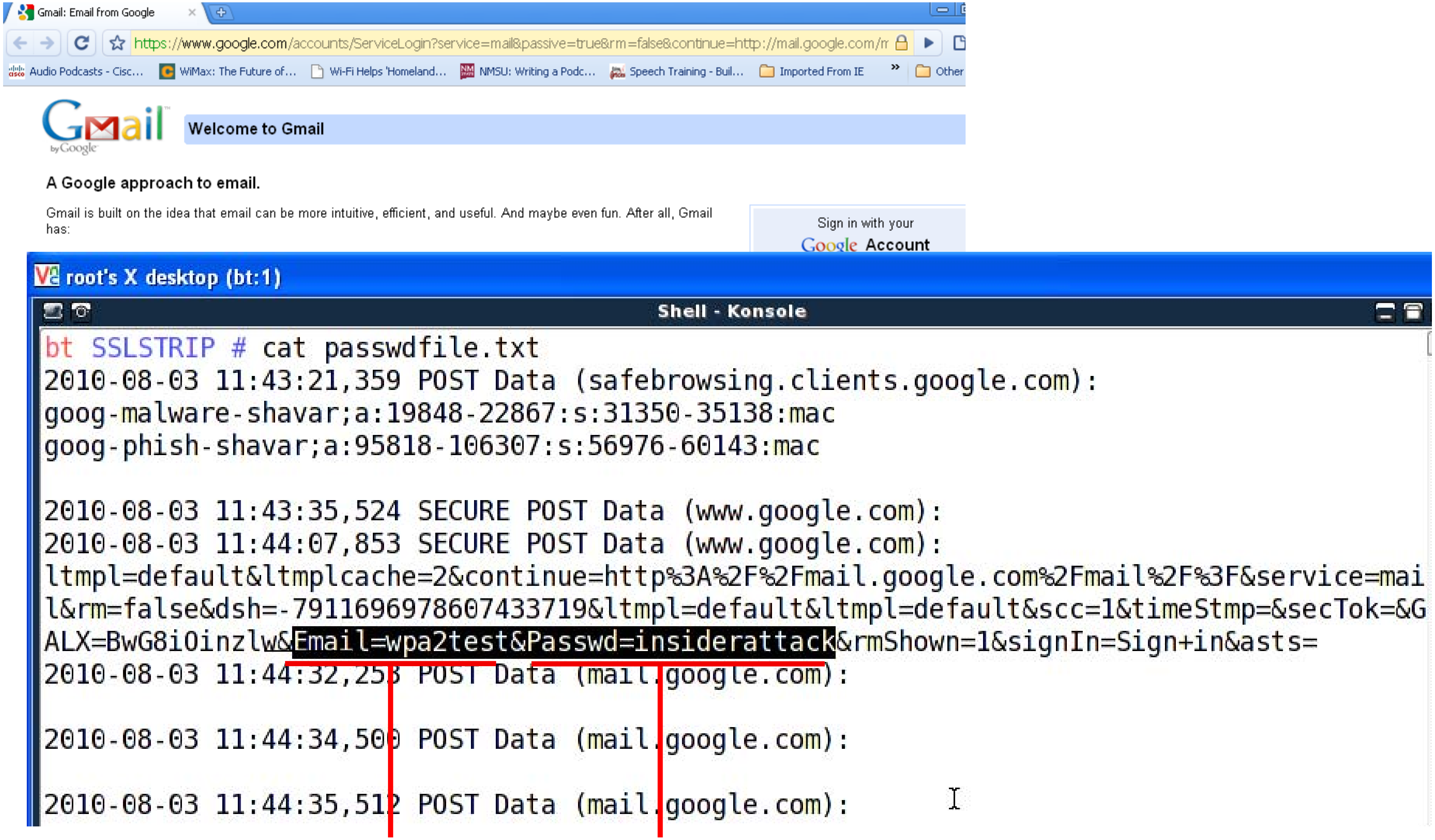
blog.airtightnetworks.com

For more information about our products and services, contact:

+1 877 424 7844

sales@airtightnetworks.com

MITM attack using SSLStrip on top of the Hole196 exploit



Welcome to Gmail

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Sign in with your Google Account

```
bt SSLSTRIP # cat passwdfile.txt
2010-08-03 11:43:21,359 POST Data (safebrowsing.clients.google.com):
goog-malware-shavar;a:19848-22867:s:31350-35138:mac
goog-phish-shavar;a:95818-106307:s:56976-60143:mac

2010-08-03 11:43:35,524 SECURE POST Data (www.google.com):
2010-08-03 11:44:07,853 SECURE POST Data (www.google.com):
ltmpl=default&ltmplcache=2&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3F&service=mai
l&rm=false&dsh=-7911696978607433719&ltmpl=default&ltmpl=default&scc=1&timeStmp=&secTok=&G
ALX=BwG8iOinzlw&Email=wpa2test&Passwd=insiderattack&rmShown=1&signIn=Sign+in&asts=
2010-08-03 11:44:32,253 POST Data (mail.google.com):

2010-08-03 11:44:34,500 POST Data (mail.google.com):

2010-08-03 11:44:35,512 POST Data (mail.google.com):
```

Username

Password