TOO!

WPA 2

"Hole196"

Md Sohail Ahmad

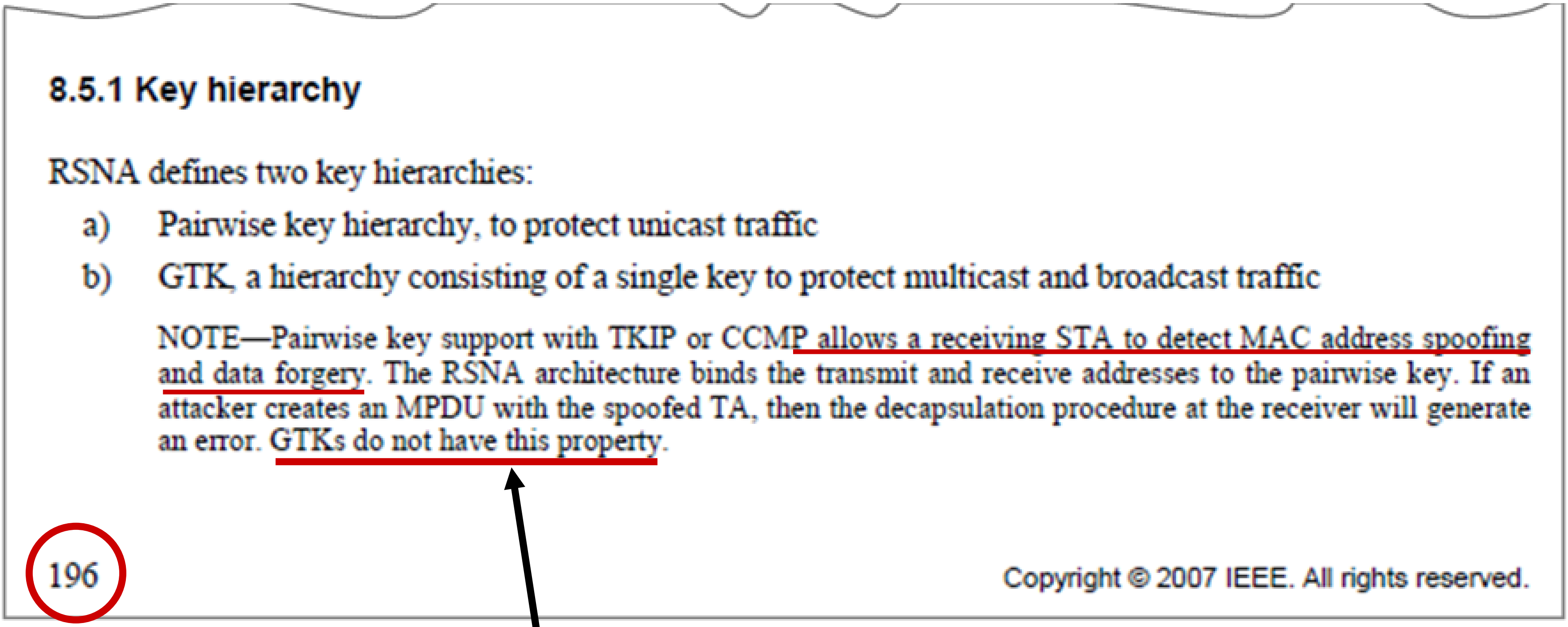
AirTight Networks

www.airtightnetworks.com

A lot of speculations about “Hole196” !

Where did we find this “Hole196” ?

Buried inside the IEEE 802.11 standard for the last six years



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

It's right here!

Hole 196!!!

The Talk is

NOT about:

Unauthorized user gaining access to WPA2 secured network, or

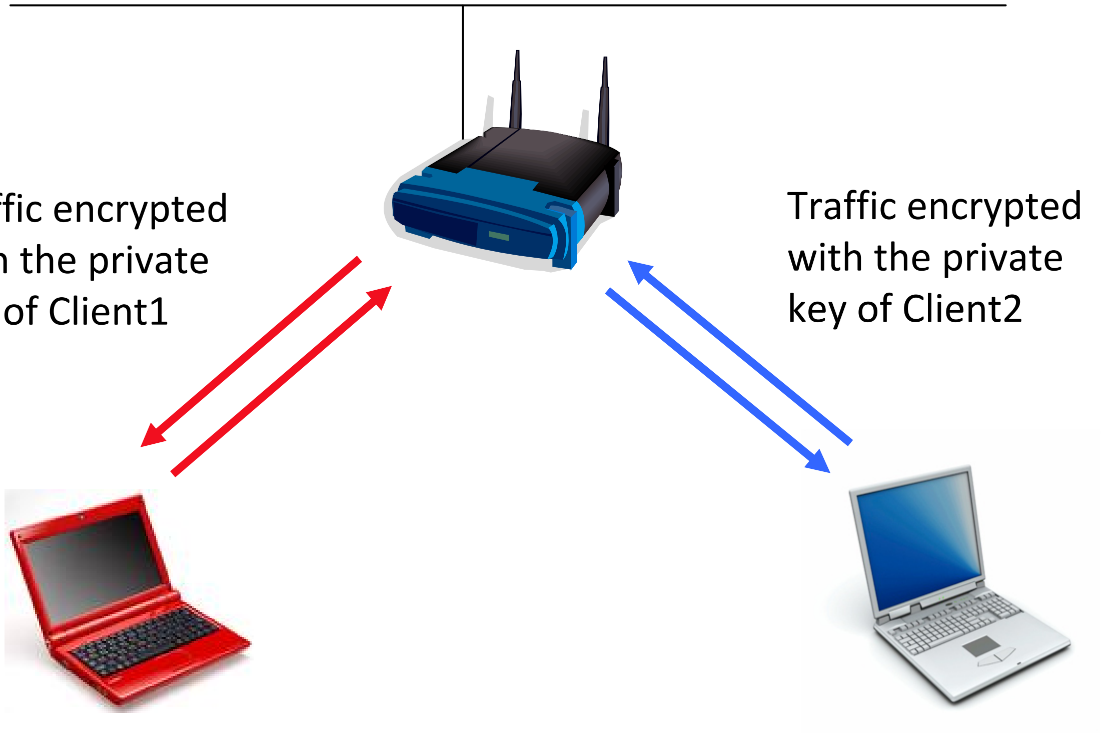
Cracking private key of a WPA2 user

About:

An insider attack, which can be carried out by a malicious user present inside the network

Can you sniff private in-flight data of other WiFi users?

Wired LAN Segment



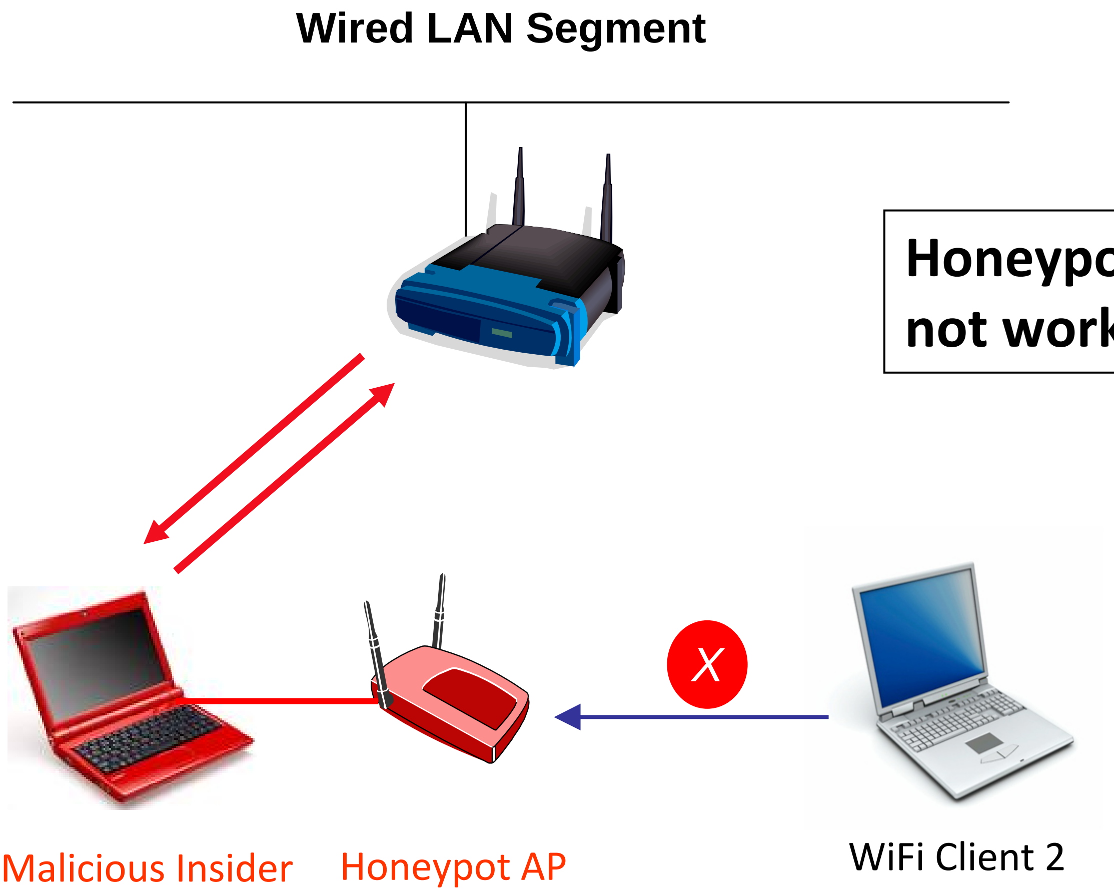
Traffic encrypted with the private key of Client1

Traffic encrypted with the private key of Client2

WiFi Client 1
(Malicious Insider)

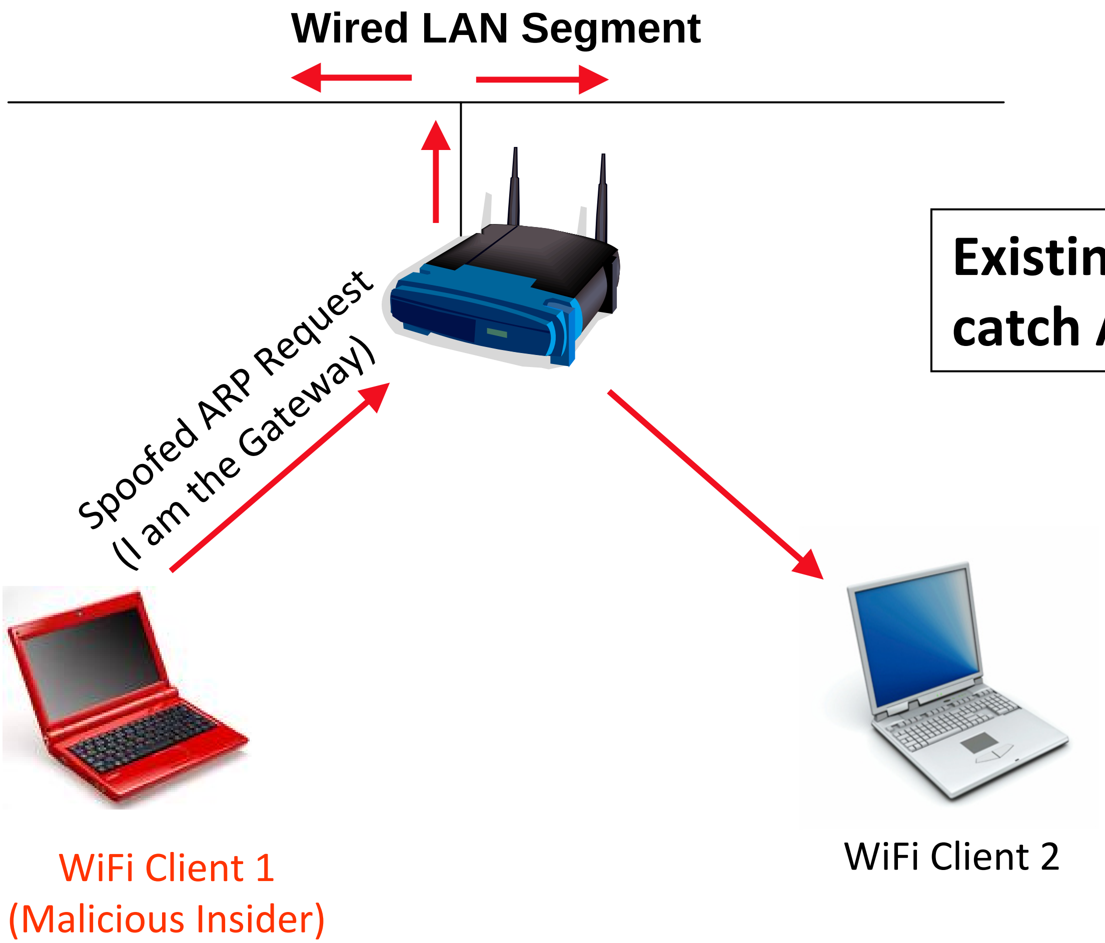
WiFi Client 2

Can you sniff private in-flight data of other WiFi users?



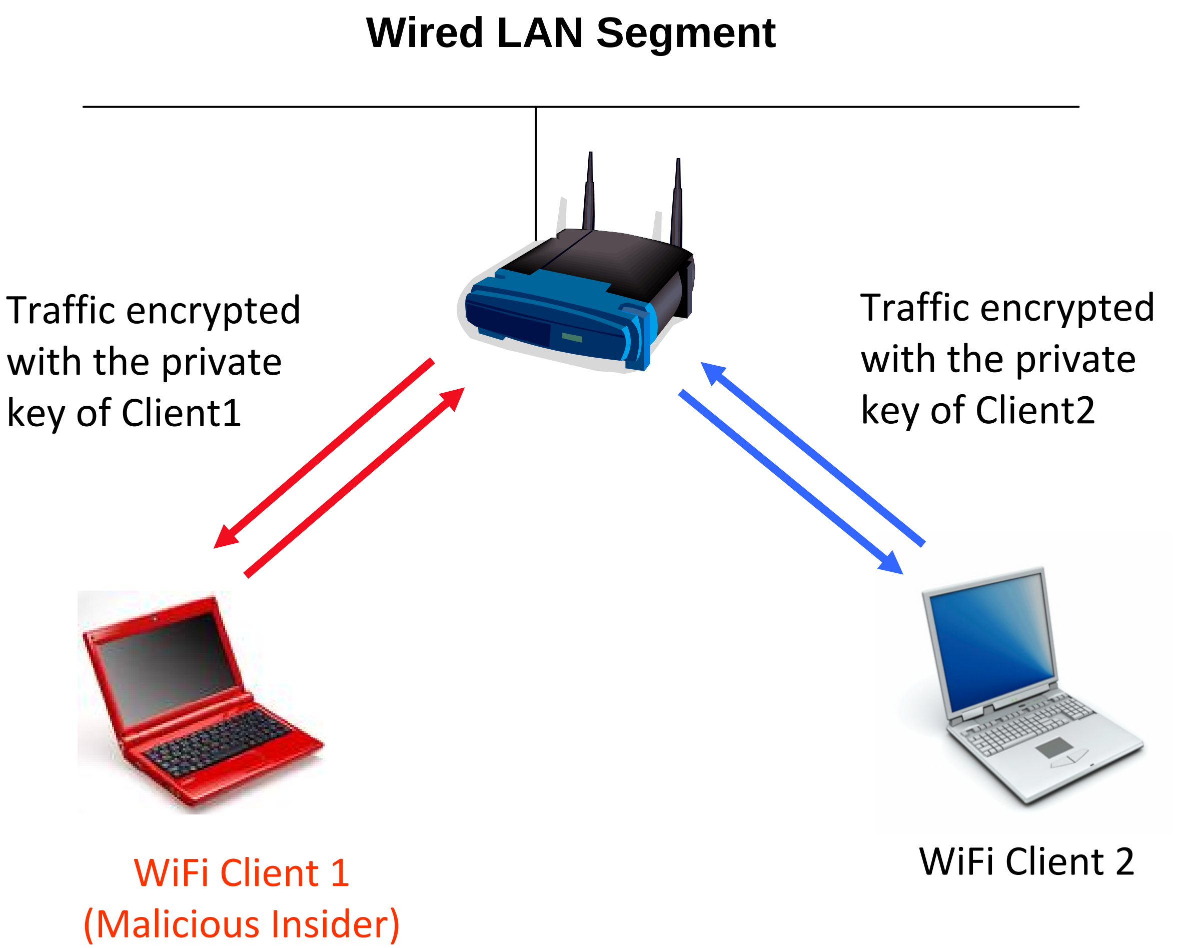
Honeypot style of attack will not work!

Can you sniff private in-flight data of other WiFi users?



Existing wired IDS/IPS can catch ARP spoofing attack!

No key cracking! No brute force!



Wired LAN Segment

Traffic encrypted with the private key of Client1

Traffic encrypted with the private key of Client2

WiFi Client 1 (Malicious Insider)

WiFi Client 2

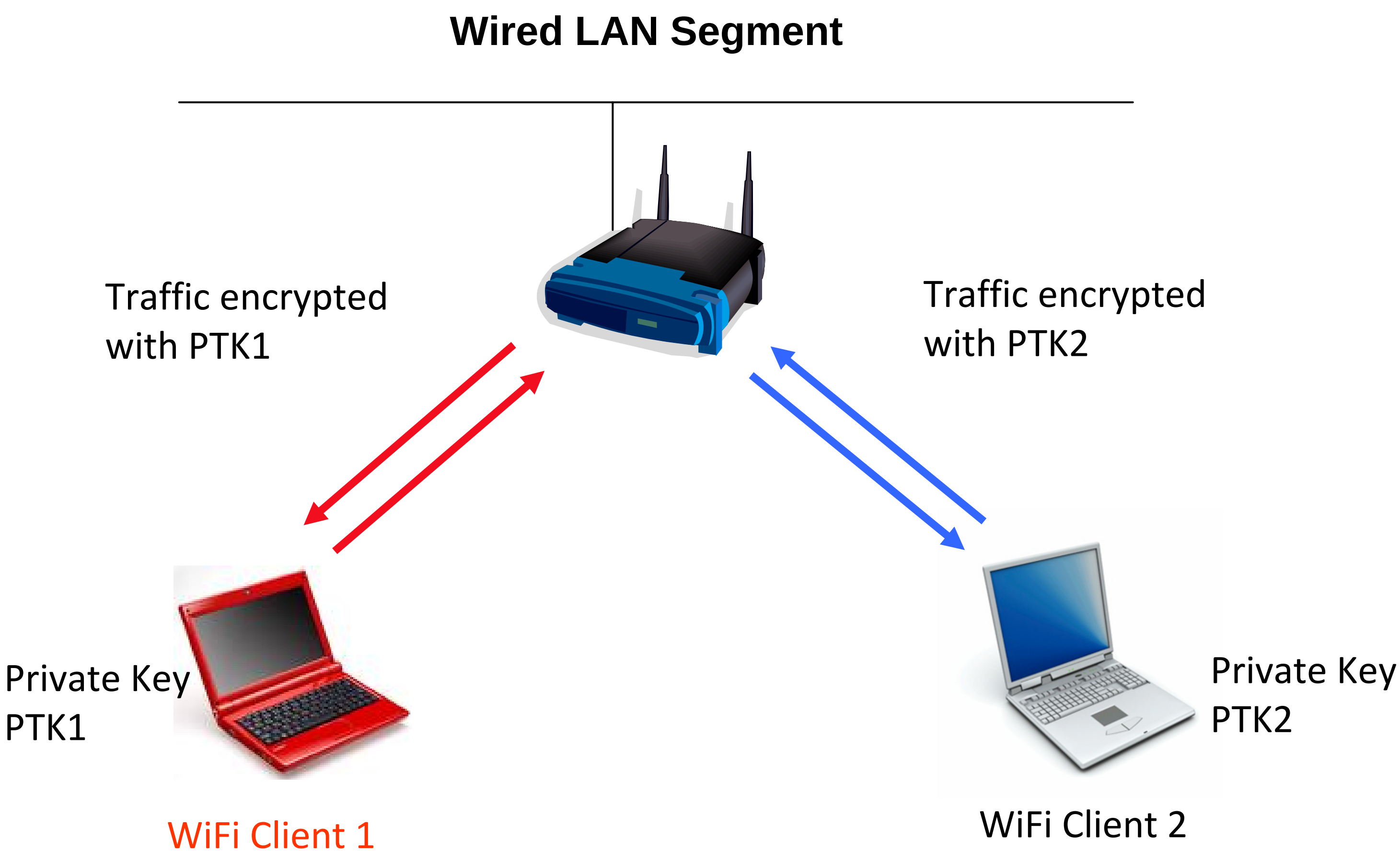
Encryption Keys

Two types of keys for data encryption

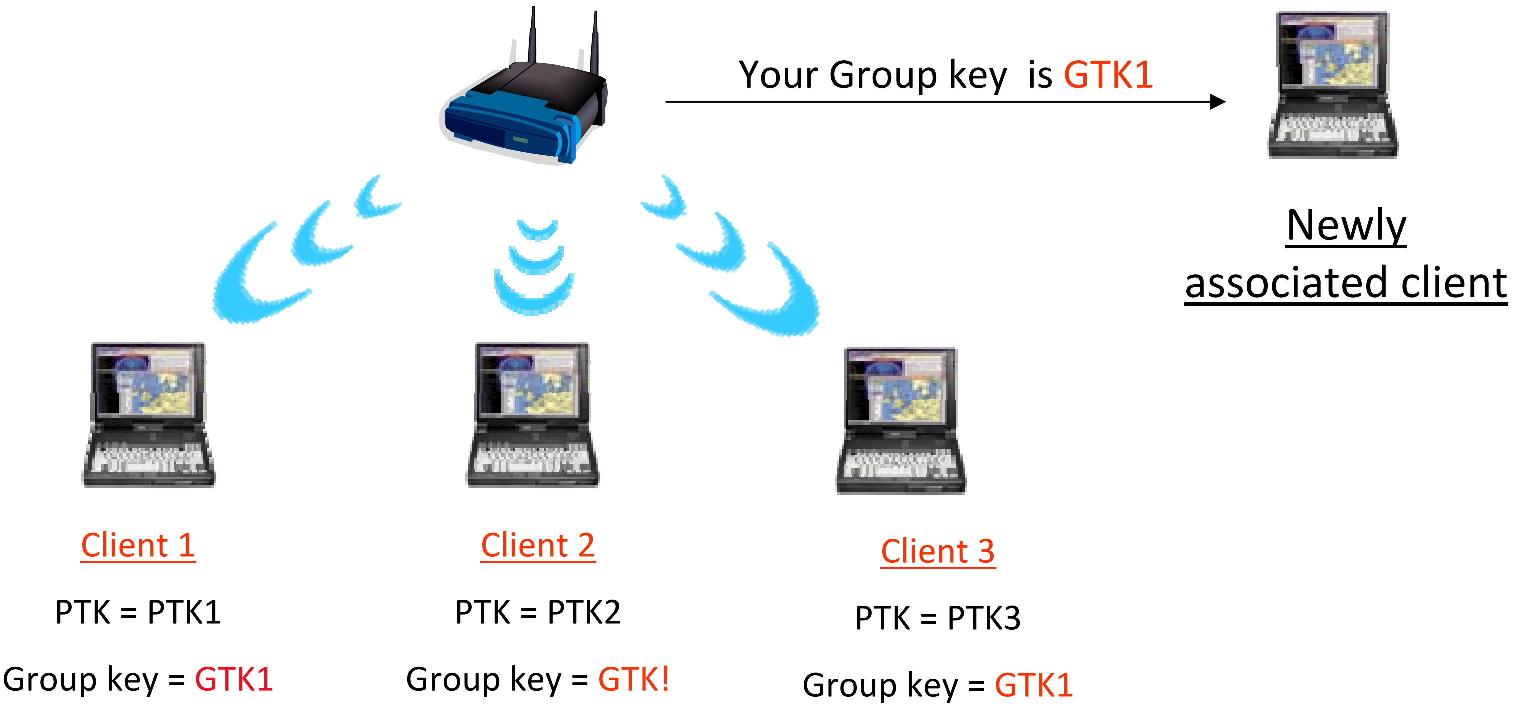
1. Pairwise Transient Key (PTK)
2. Group Temporal Key (GTK)

While PTK is used to protect unicast data frames , GTK is used to protect group addressed data frames e.g. broadcast ARP request frames.

PTK is unique, derived per session



GTK is shared among all associated clients



Your Group key is GTK1

Newly associated client

Client 1

PTK = PTK1

Group key = GTK1

Client 2

PTK = PTK2

Group key = GTK!

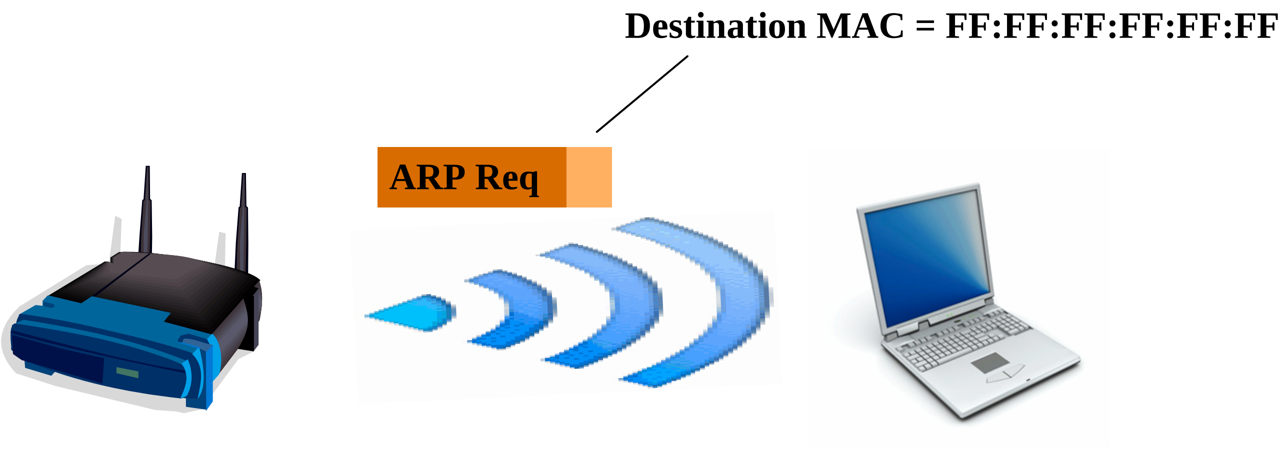
Client 3

PTK = PTK3

Group key = GTK1

Three connected clients

WPA2 standard defines GTK as a one-way key

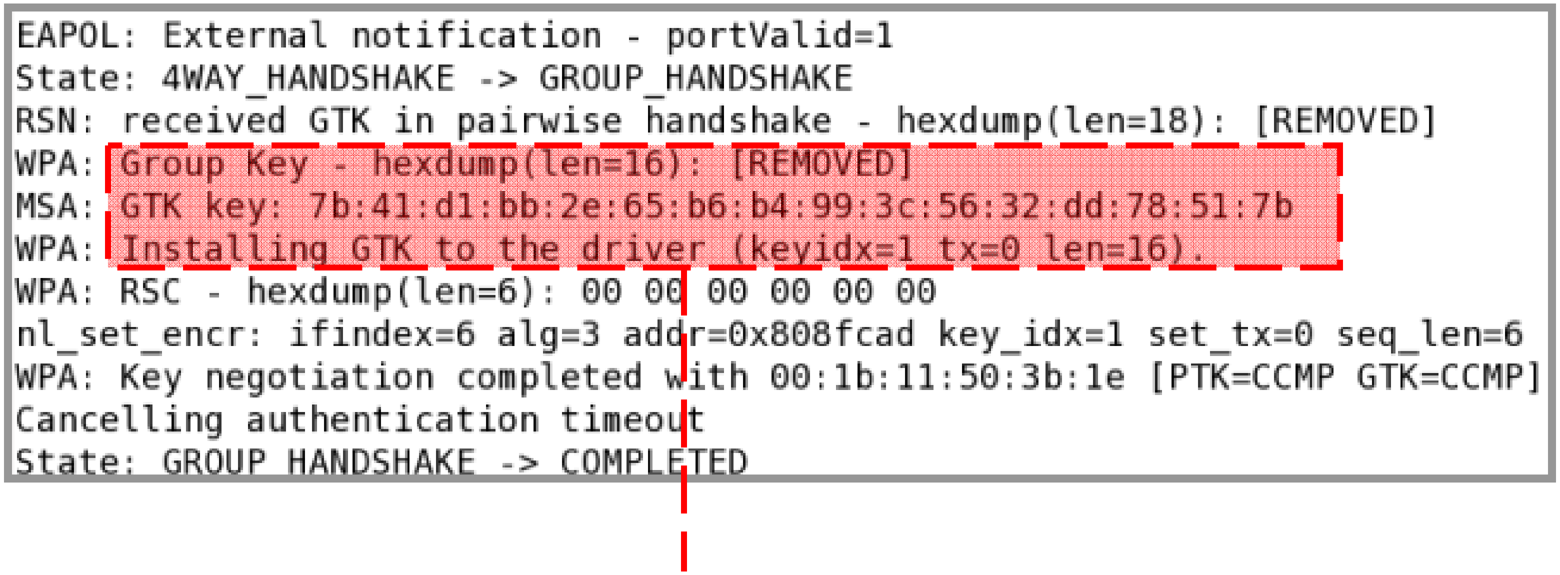


Destination MAC = FF:FF:FF:FF:FF:FF

ARP Req

GTK should be used as an encryption key by an AP and as a decryption key by a wireless client

A WiFi client always keeps a copy of GTK

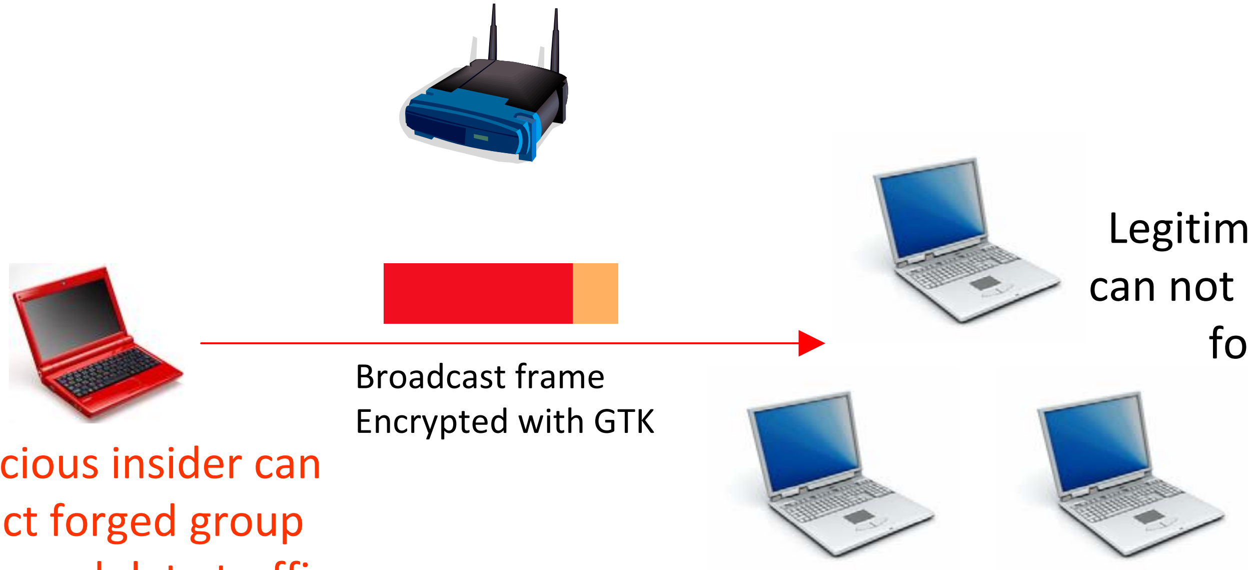


```
EAPOL: External notification - portValid=1
State: 4WAY_HANDSHAKE -> GROUP_HANDSHAKE
RSN: received GTK in pairwise handshake - hexdump(len=18): [REMOVED]
WPA: Group Key - hexdump(len=16): [REMOVED]
MSA: GTK key: 7b:41:d1:bb:2e:65:b6:b4:99:3c:56:32:dd:78:51:7b
WPA: Installing GTK to the driver (keyidx=1 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
```

wpa_supplicant *software is used on WiFi client devices.*

The log of wpa_supplicant software shows that GTK is always known to a WiFi client device

A malicious client can inject encrypted group addressed data frames to other clients

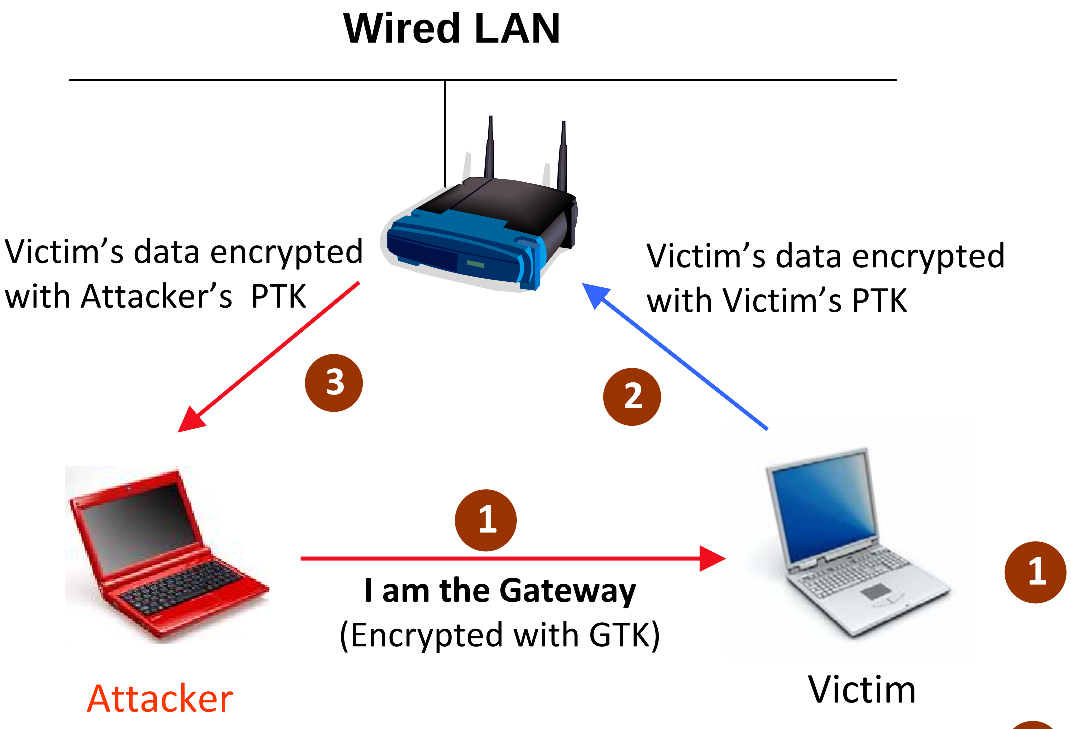


Legitimate clients can not detect data forgery

Broadcast frame
Encrypted with GTK

Malicious insider can inject forged group addressed data traffic

Exploit #1: Stealth ARP Poisoning

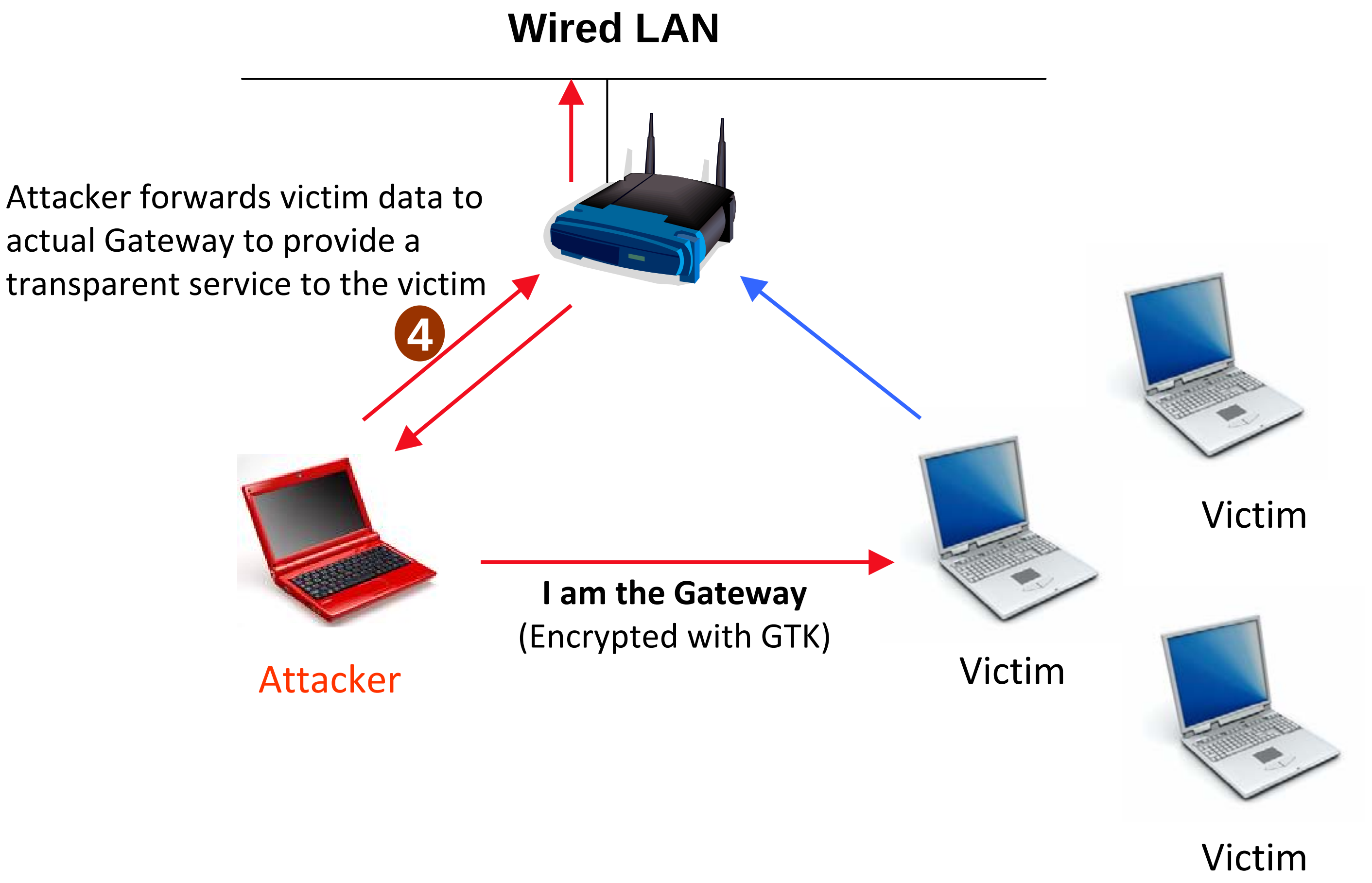

Wired LAN
Victim's data encrypted with Attacker's PTK
Victim's data encrypted with Victim's PTK
3
2
1
I am the Gateway
(Encrypted with GTK)
Attacker
Victim

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)

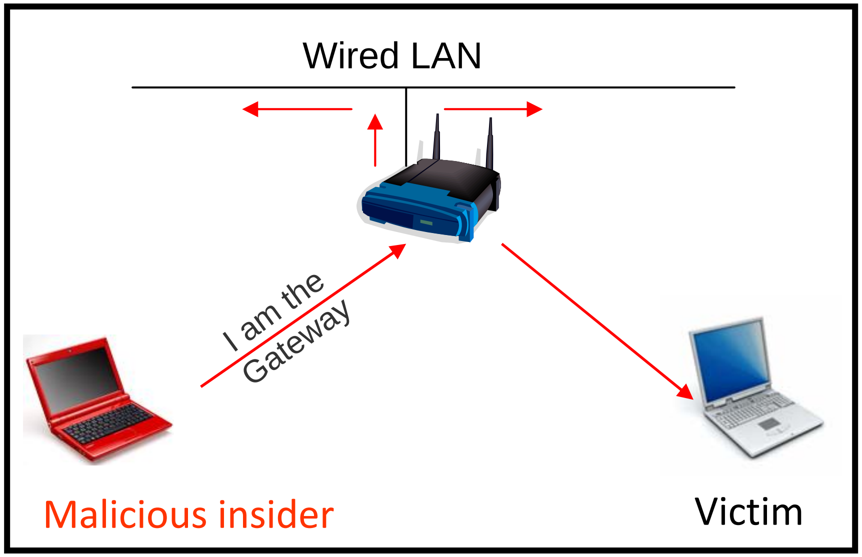
3 AP forwards Victim's data to the Attacker encrypting it in the Attacker's PTK. So Attacker can decrypt Victim's private data.

Man-in-the-middle (MITM) Attack


Wired LAN
Attacker forwards victim data to actual Gateway to provide a transparent service to the victim
4
I am the Gateway
(Encrypted with GTK)
Attacker
Victim
Victim
Victim

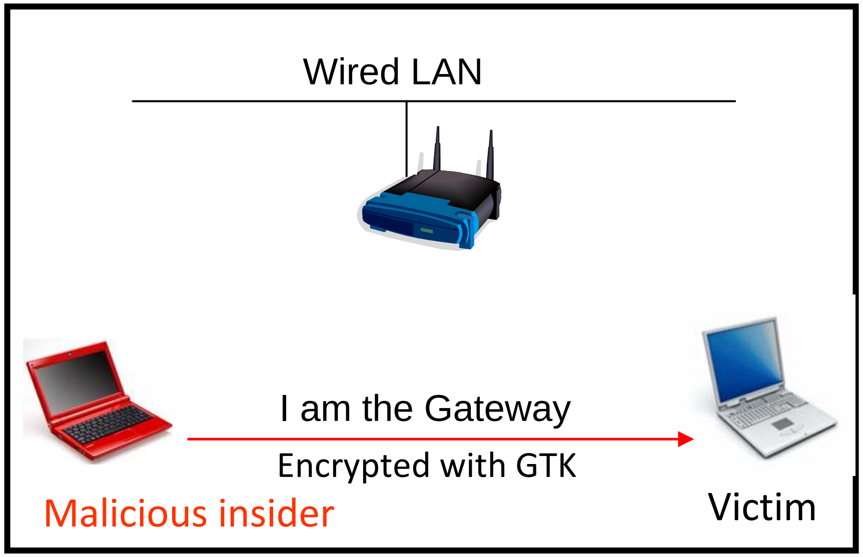
ARP Poisoning: Detectable vs Stealth

Detectable (Old style)



Spoofed ARP Request frames are sent on the wire and wireless medium by an AP. The attack **can be detected by wired IDS/IPS.**

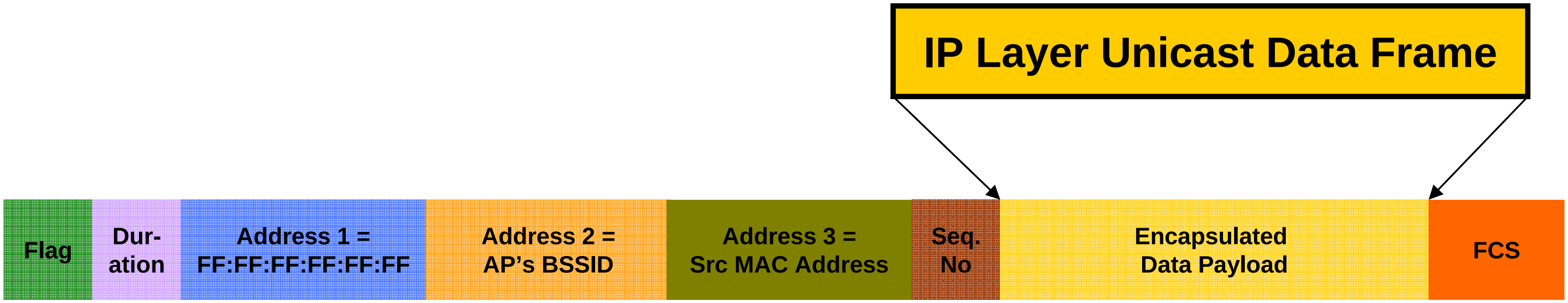
Stealth (Hole196)



Spoofed ARP Request frames are not sent to AP and never go on wire; hence **cannot be detected by wired IDS/IPS**

Exploit #2: IP Level Targeted Attack

Any data payload can be encapsulated in the group addressed IEEE 802.11 data frames

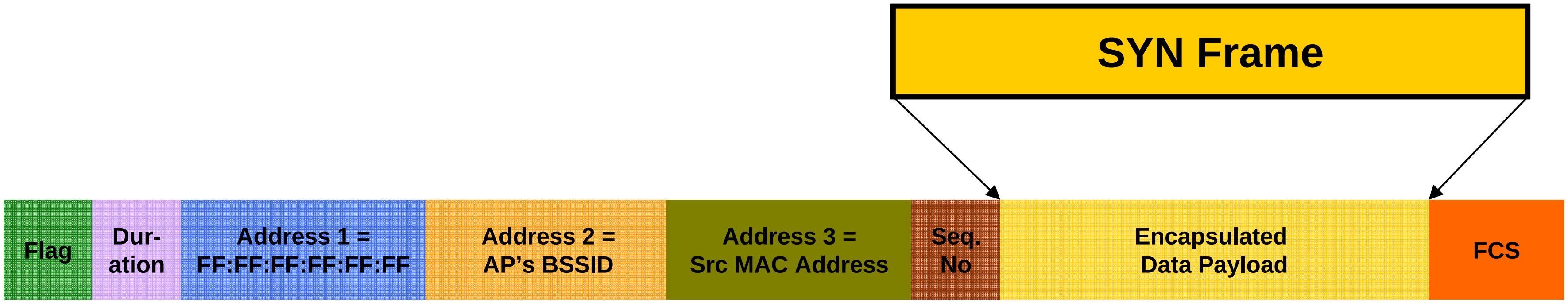


IP Layer Unicast Data Frame

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 Packet

Example: Port Scanning



SYN Frame

Flag	Duration	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 Packet

What else is possible ?

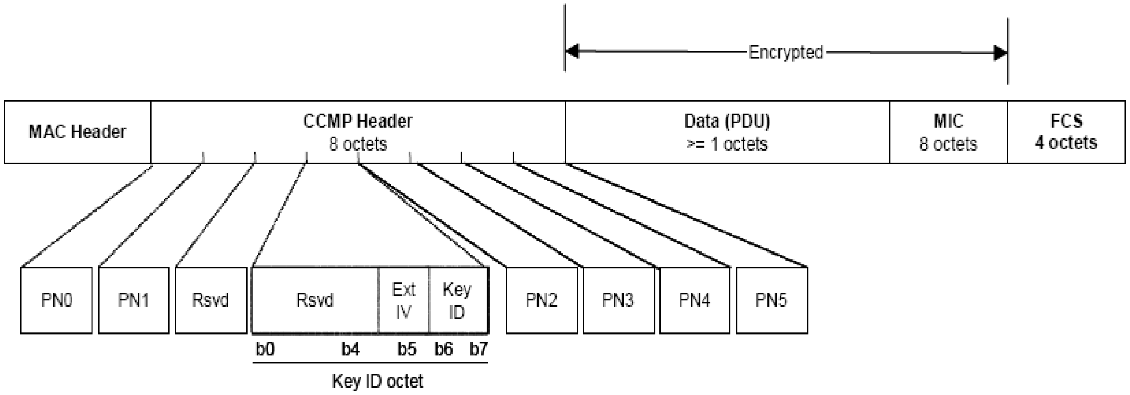
- Buffer overflow exploit

- Malware Injection

- ???

Replay Detection in WPA2

48 bit Packet Number (PN) is present in all encrypted DATA frames

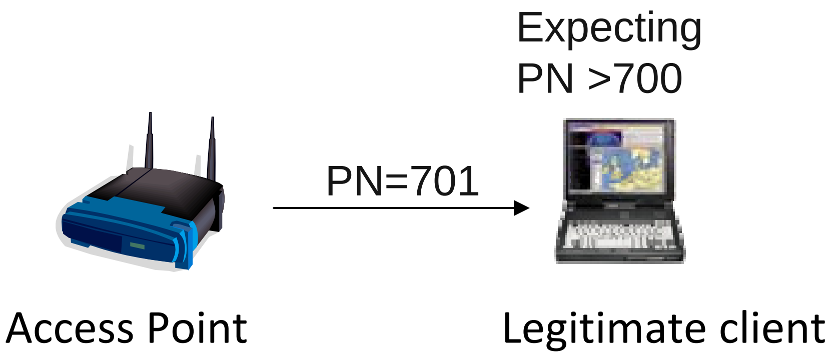


Replay Attack Detection in WPA2

1. All clients learn the PN associated with a GTK at the time of association

2. AP sends a group addressed data frame to all clients with a new PN

3. If **new PN > locally cached PN,** then packet is decrypted and after successful decryption, cached PN is updated with new PN


Expecting PN >700

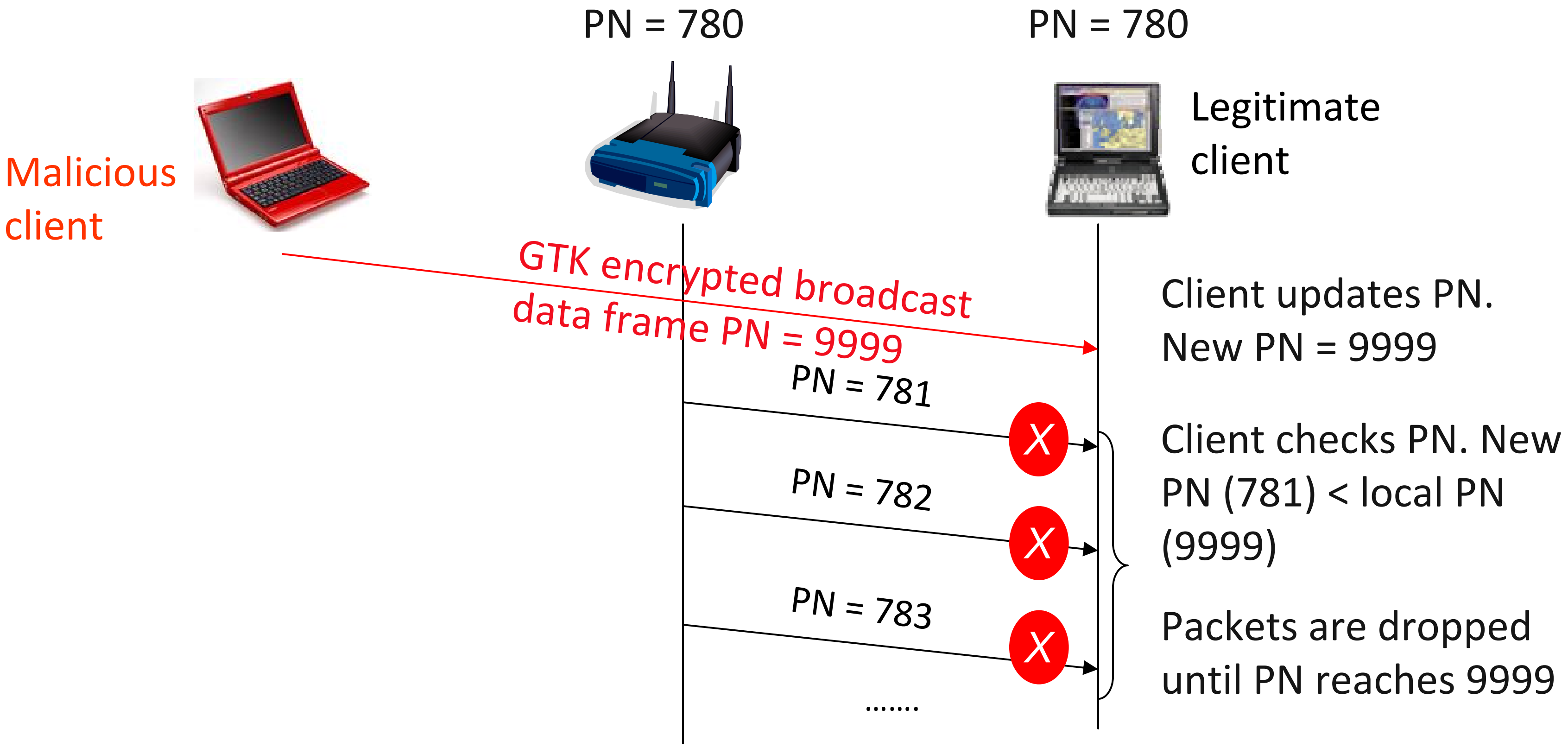
PN=701

Access Point

Legitimate client

Exploit #3: WDoS on Broadcast Downlink Traffic

A malicious user can advance the locally cached PN (replay counter) in all peer clients by forging a group addressed data frames with a very large PN



PN = 780

PN = 780

Malicious client

Legitimate client

GTK encrypted broadcast data frame PN = 9999

Client updates PN. New PN = 9999

PN = 781

PN = 782

PN = 783

....

Client checks PN. New PN (781) < local PN (9999)

Packets are dropped until PN reaches 9999

POC: GTK Exploit

Few lines of code + Off-the-shelf hardware

Open Source Software: Madwifi & WPA Supplicant Software

wpa_supplicant (0.7.0)

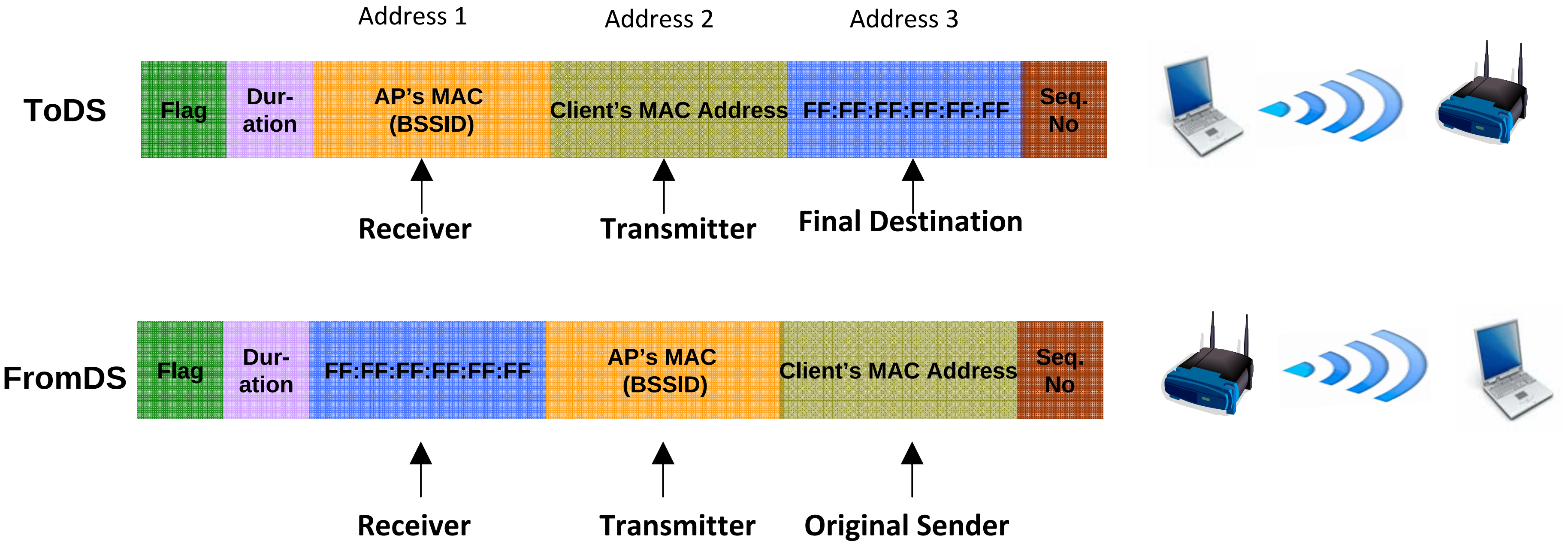
Supplicant software is used to pass updated GTK and PN to be by madwifi driver

Madwifi (0.9.4)

Software is modified to create spoofed group addressed data frames with sender as AP address

Modification in the madwifi driver

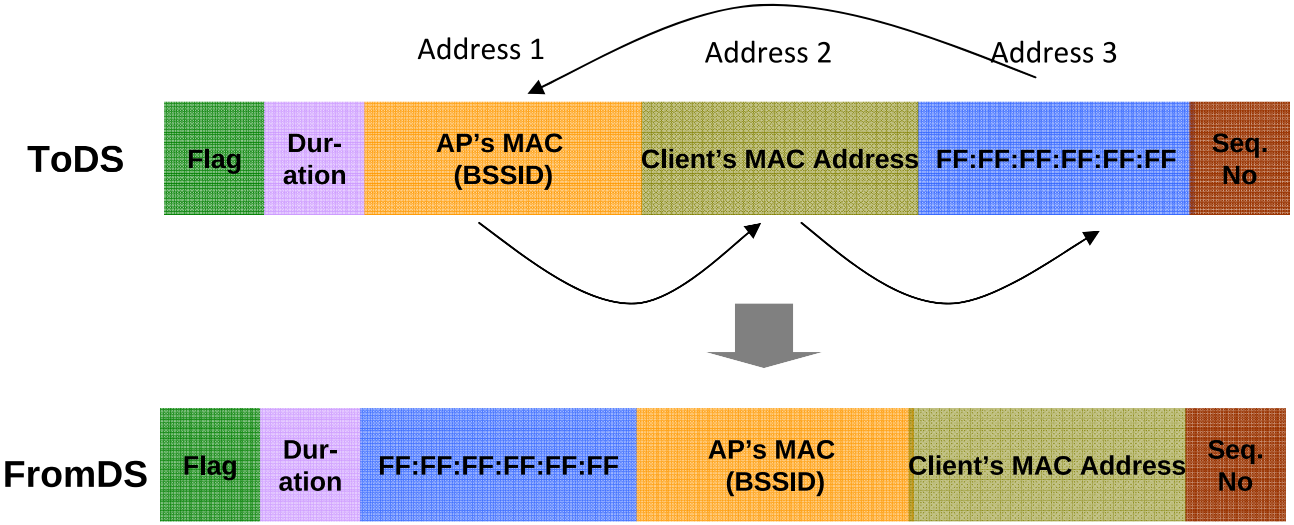
Broadcast IEEE 802.11 Frame



			Address 1	Address 2	Address 3	
ToDS	Flag	Dur-ation	AP's MAC (BSSID)	Client's MAC Address	FF:FF:FF:FF:FF:FF	Seq. No
			Receiver	Transmitter	Final Destination	
FromDS	Flag	Dur-ation	FF:FF:FF:FF:FF:FF	AP's MAC (BSSID)	Client's MAC Address	Seq. No
			Receiver	Transmitter	Original Sender	

Modification in the madwifi driver

1. Cyclic shift of addresses, convert ToDS flag into FromDS: 4 Lines



Address 1 Address 2 Address 3

ToDS: Flag | Dur-ation | AP's MAC (BSSID) | Client's MAC Address | FF:FF:FF:FF:FF:FF | Seq. No

FromDS: Flag | Dur-ation | FF:FF:FF:FF:FF:FF | AP's MAC (BSSID) | Client's MAC Address | Seq. No

2. Selection of right key for frame encryption: 6 Lines

10 lines of driver code to exploit GTK vulnerability!

Demo: Stealth mode MITM attack

The Arsenal of MITM Attack

Cain & Abel

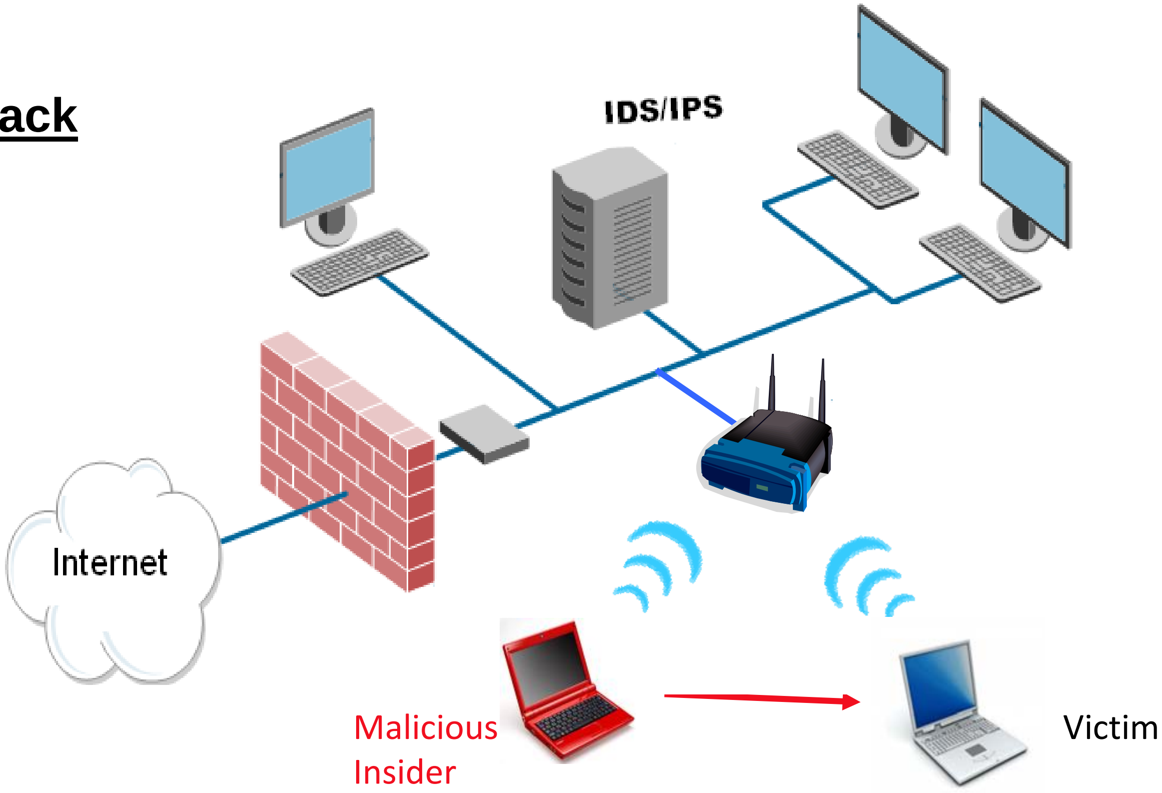
Ettercap

Delegated/DNSSpoof

SSLSniff

SSLSTRIP

…



Who is vulnerable to “Hole196” ?

All implementation of WPA and WPA2, regardless of

- Type of encryption used in the network (AES or TKIP)
- Type of authentication used in the network (PSK or 802.1x/EAP)
- Type of WLAN architectures (Standalone, Locally controlled or Centrally Controlled)

Countermeasures

The Real Fix: Protocol Enhancement

- **Deprecate use of GTK and group addressed data traffic**
  1. For *backward compatibility* AP should send randomly generated different GTKs to different clients so that all associated clients have different copy of group key
  2. AP should deliver group addressed data traffic by converting them into unicast traffic

Disadvantages:

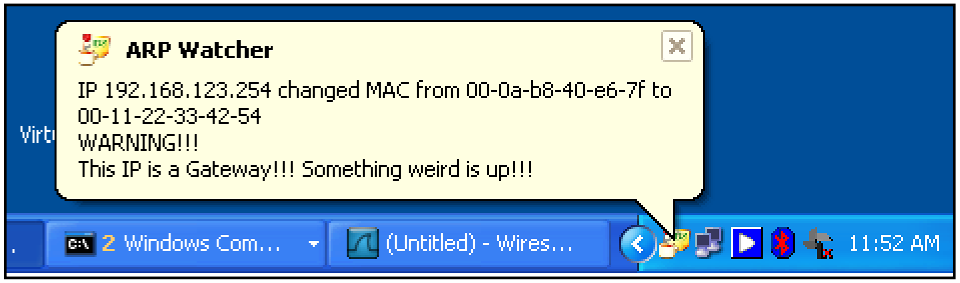
a. Impact on network throughput

b. Requires AP software upgrade (Not going to happen overnight !)

What should we do now?

Can we rely on end point security software?

Client software such as DecaffeintID or Snort detects change in the ARP cache.



ARP Watcher

IP 192.168.123.254 changed MAC from 00-0a-b8-40-e6-7f to 00-11-22-33-42-54
WARNING!!!
This IP is a Gateway!!! Something weird is up!!!

Detects ARP Cache Poisoning attack

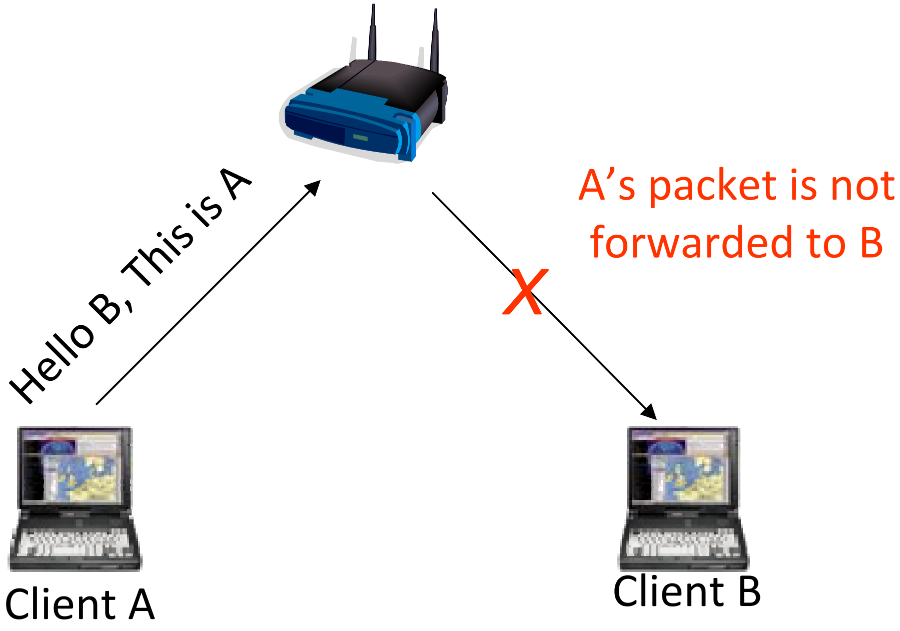
Limitations:

1. Client software is available only for limited operating systems and hardware platforms

2. Not enterprise grade; Impractical to manually install on large number of endpoints

Can we rely on WLAN infrastructure ?

Public Secure Packet Forwarding (PSPF)/peer-to-peer (P2P) or Client Isolation



Legitimate users might want to download songs/pics from say laptop to smartphone!

What’s about Voice-over-WiFi deployment ?

Can we rely on Wireless Monitoring Systems (WIPS/WIDS) ?

Similar to WEP Cracking, Skyjacking and WPA-TKIP, Hole 196 exploit is carried out entirely over the air

WIPS can serve as an additional layer of defense in detecting and protecting from such attacks

Concluding Remarks

- All WPA2 networks are exposed with the “Hole 196” vulnerability; **Inter user privacy is broken in WPA2**

- The real fix requires enhancement in the WPA2 protocol. In long term, standard can fix the problem but in short term AP vendors should provide a patch (proprietary solution)

- In the mean time, enterprises should consider turning ON Client isolation (PSPF) features on their WLANs and use endpoint security (ARP poisoning detector like Snort or other higher layer security like IPSec)

- A multi-layered security approach should be adopted; A dedicated WIPS monitoring the airspace 24/7 can detect and mitigate zero-day vulnerabilities such as “Hole 196”

Be Aware, Be Secure !

Thank You

Md Sohail Ahmad

md.ahmad@airtightnetworks.com

www.airtightnetworks.com

For up-to-date information on developments in wireless security, visit

blog.airtightnetworks.com

AirTight® NETWORKS