WPA TOO !

Md Sohail Ahmad

AirTight Networks

www.airtightnetworks.com

About the Speaker

2007, Toorcon9

Caffe Latte Attack

2008, Defcon 16

Autoimmunity Disorder in Wireless LANs

2009, Defcon 17

WiFish Finder: Who will bite the bait?

2010, Defcon 18

WPA TOO !

About the Talk

WPA2 is vulnerable under certain conditions. This limitation, though known to the designers of WPA2, is not well understood or appreciated by WiFi users.

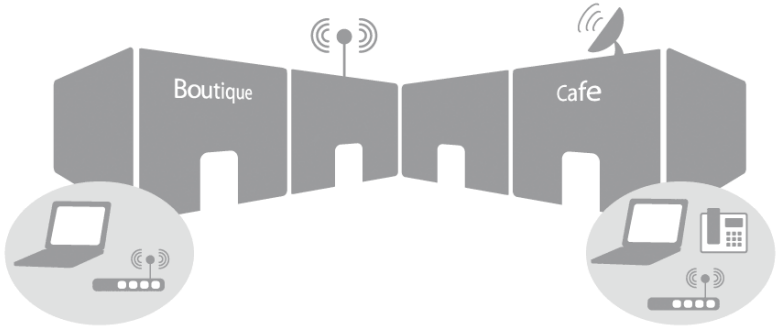
In this talk, I am going to show that exploits are possible using off the shelf tools with minor modifications.

Background

WEP, the one and only security configuration present in the original 802.11 standard, was cracked in 2001. Since then several attacks on WEP have been published and demonstrated

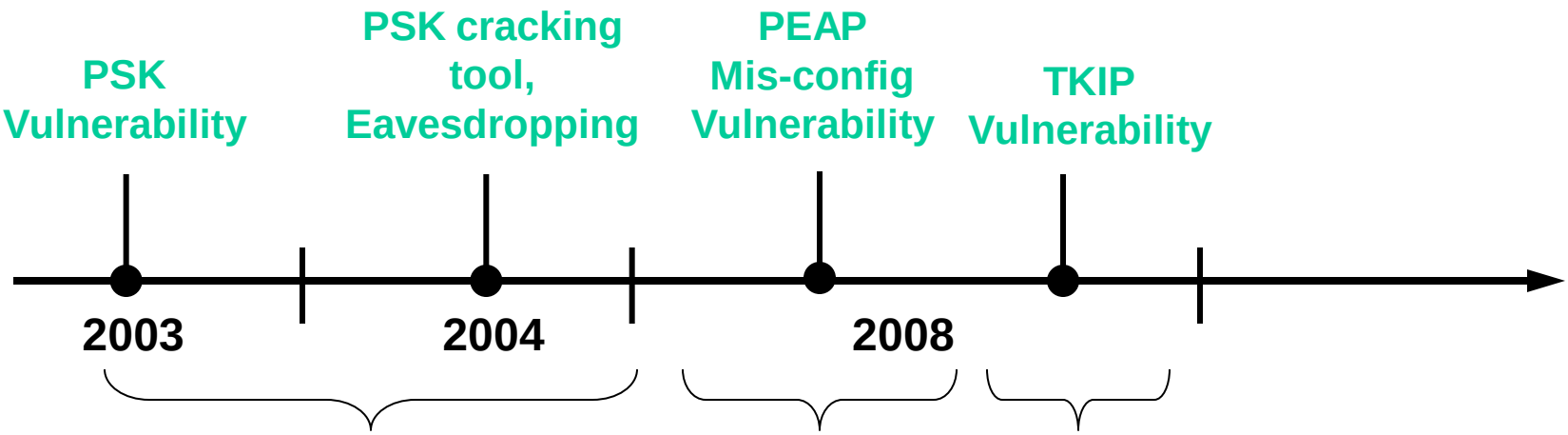
Nowadays most WLANs are secured with a much better and robust security protocol called WPA2.

Interestingly, WPA2 is also being used to secure Guest WiFi, Municipal WiFi (e.g. GoogleWiFi Secure) and Public WiFi (e.g. T-Mobile or AT&T WiFi Hotspot) networks.



Is WPA2 safe to be used in WiFi networks?

Known attacks on WPA/WPA2



Attack on Pre-Shared Key (PSK) Authentication

Implications:

Eavesdropping

Unauthorized Access to the network

Attack on 802.1x Authentication

Implications:

Client compromise

Attack on Encryption

Implications:

Injection of small size frames to create disruption

Solution

1. Do not use PSK authentication in other than private/home network
   (Solves PSK Vulnerability)
2. Do not ignore certificate validation check in client's configuration
   (Solves Client Vulnerability)
3. Use AES encryption
   (Solves TKIP Vulnerability)

Is WPA2 safe to be used in WiFi networks?

Encryption in WPA2

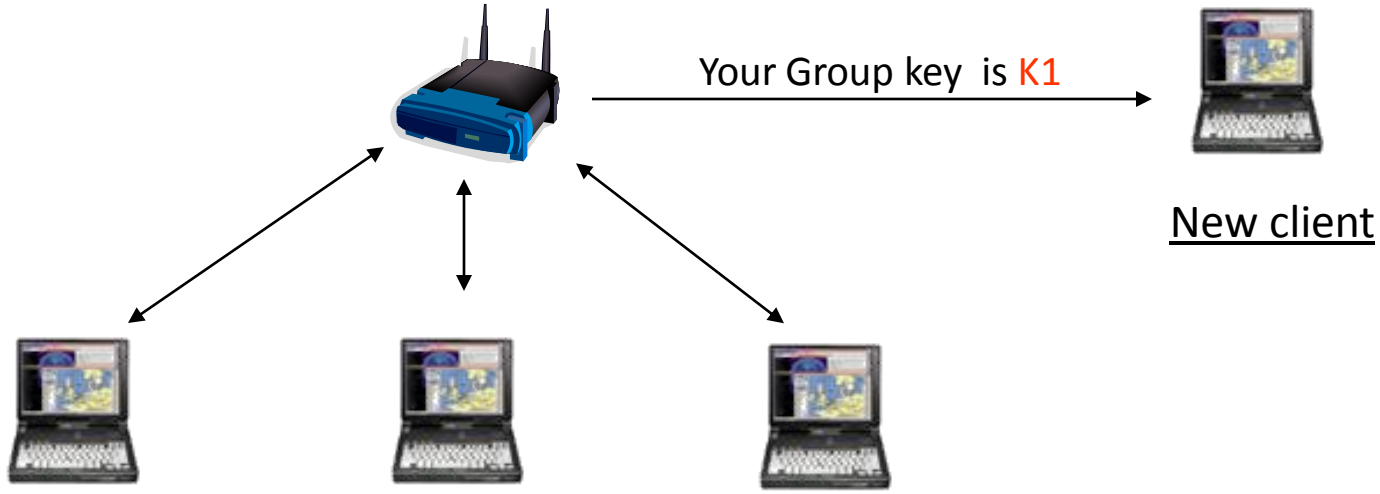
Encryption Keys

Two types of key for data encryption

1. Pairwise Key (PTK)
2. Group 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.

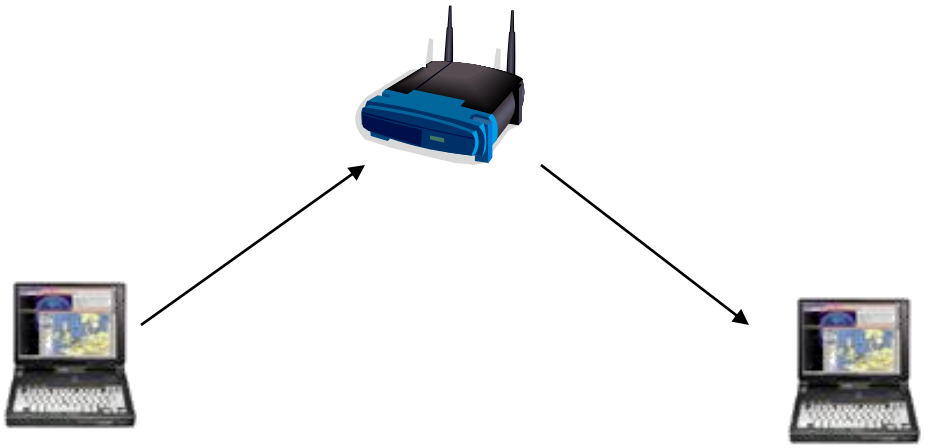
GTK is shared among all associated clients



Three connected clients

Group addressed traffic in a WLAN

Group addressed 802.11 data frames are always sent by an access point and never sent by a WiFi client



ToDS “Broadcast ARP Req” frame

Address 1 (or Destination MAC) = AP/BSSID MAC

From DS “Broadcast ARP Req” frame

Address 1 (or Destination MAC) = FF:FF:FF:FF:FF:FF

GTK is designed to be used as an encryption key in the AP and as a decryption key in the client

What if a client starts using GTK for group addressed frame encryption?

Is it possible for a client to send forged group addressed data frames?

From DS “Broadcast ARP Req.” frame

Actually injected by a client

Address 1 (or Destination MAC) = FF:FF:FF:FF:FF:FF

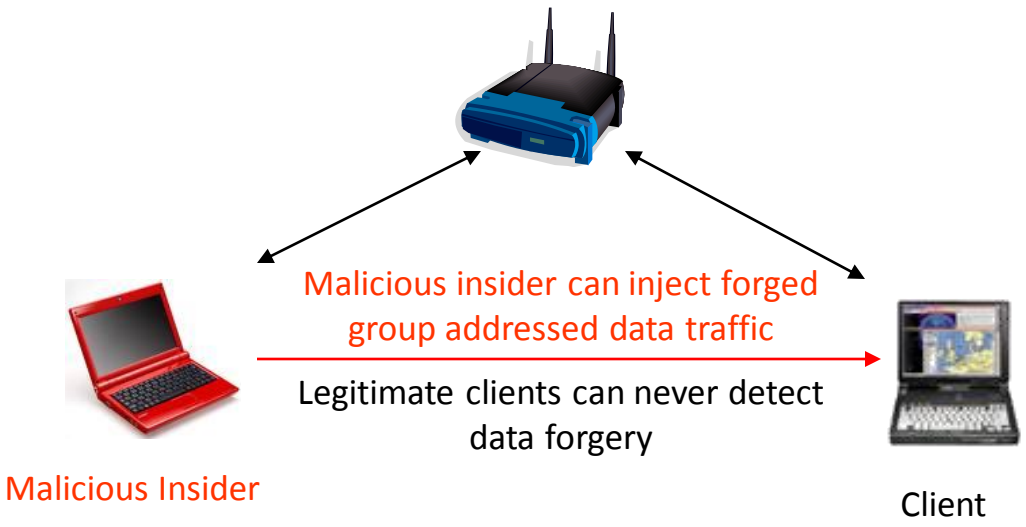
Console log of a WiFi user's machine

```
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.

A malicious user can always create fake packets

WPA2 secured WiFi networks are vulnerable…



…to Insider Attack

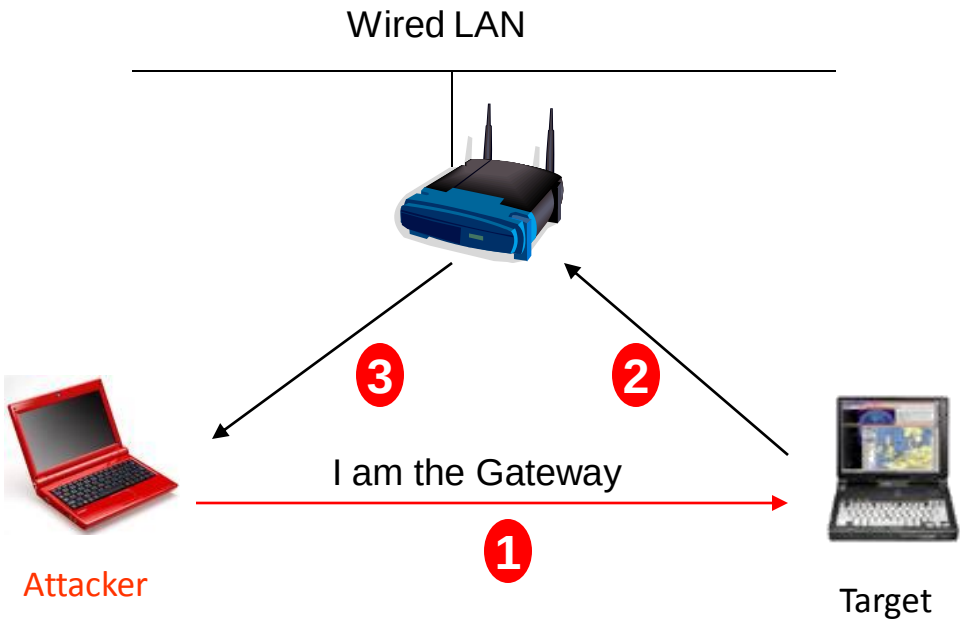
Implications

- **Stealth mode ARP Poisoning/Spoofing attack**
  - Traffic snooping
  - Man in the Middle (MiM): How about “Aurora” ?
  - IP layer DoS attack

- **IP level targeted attack**
  - TCP reset, TCP indirection, Port scanning, malware injection, privilege escalation etc. etc.

- **Wireless DoS attack**
  - Blocks downlink broadcast data frame reception

Stealth mode ARP Poisoning



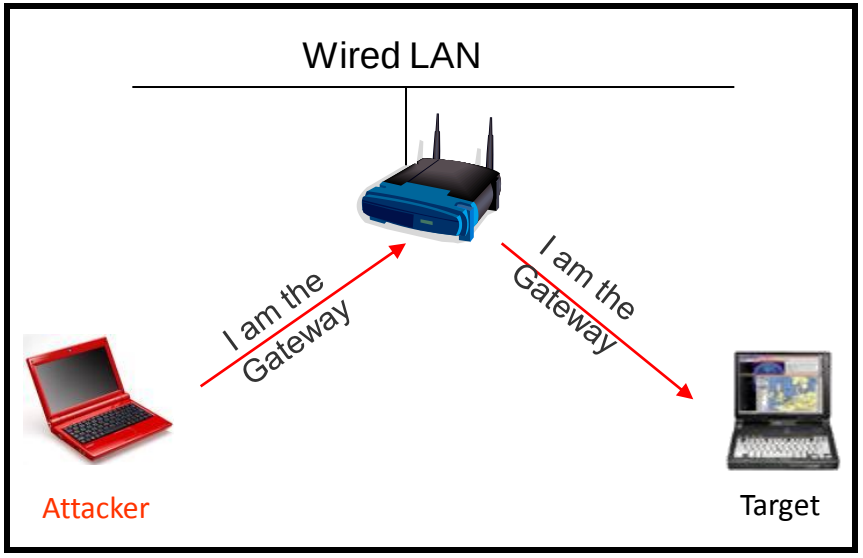
1. Attacker injects fake ARP packet to poison client's cache for gateway.

   The ARP cache of victim gets poisoned. For victim client Gateway is attacker's machine.

2. Victim sends all traffic to attacker
3. Now attacker can either drop traffic or forward it to actual gateway

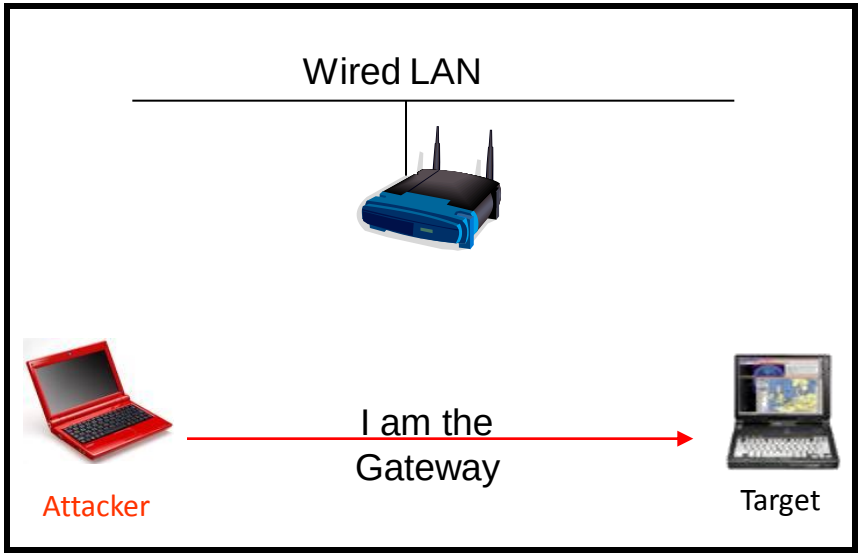
ARP Poisoning Attack: Normal vs Stealth Mode

Normal



ARP poisoning frames appear on wire through AP. Chances of being caught is high.

Stealth Mode

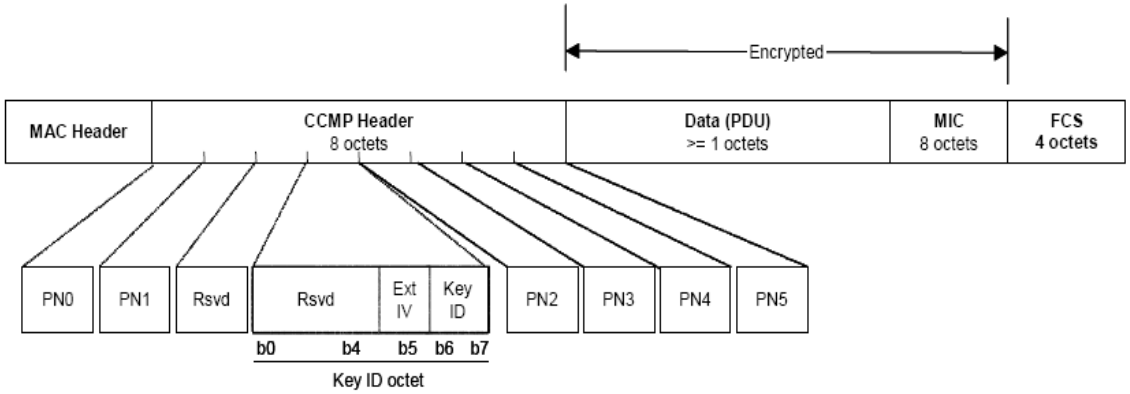


ARP poisoning frames invisible to AP, never go on wire. Can't be detected by any ARP cache poison detection tool.

IP Level Targeted Attack

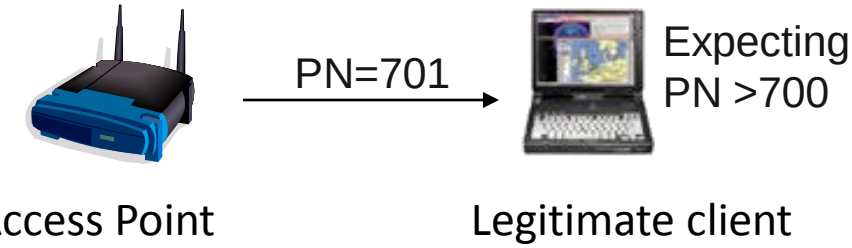
PN or Packet Number in CCMP Header

48 bit Packet Number (PN) is present in all CCMP 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** than packet is decrypted and after successful decryption, old PN is updated with new PN



Wireless DoS Attack (WDoS)

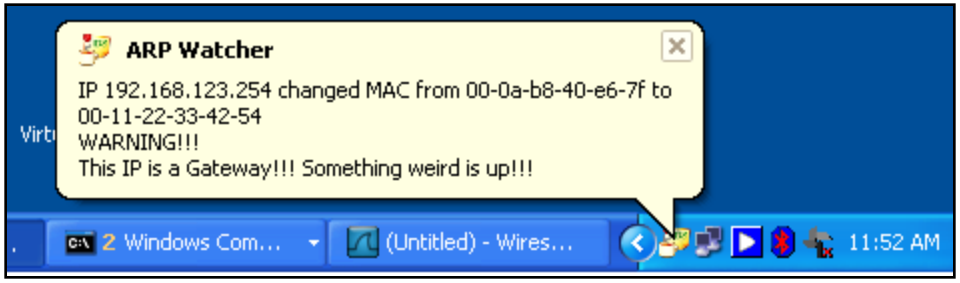
Demo: Stealth mode attack

A live demo of the exploit will be done during presentation

Prevention & Countermeasures

Endpoint Security

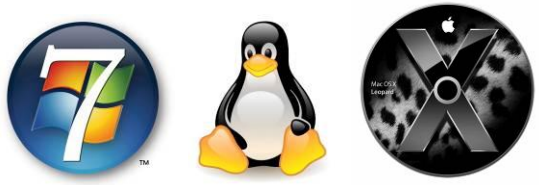
Client software such as DecaffeintID or Snort can be used to detect ARP cache poisoning.



Detects ARP Cache Poisoning attack

Limitations

Varieties of client device which connect to WPA2 secured WiFi networks while software is available only for either Windows or Linux running devices



Operating Systems

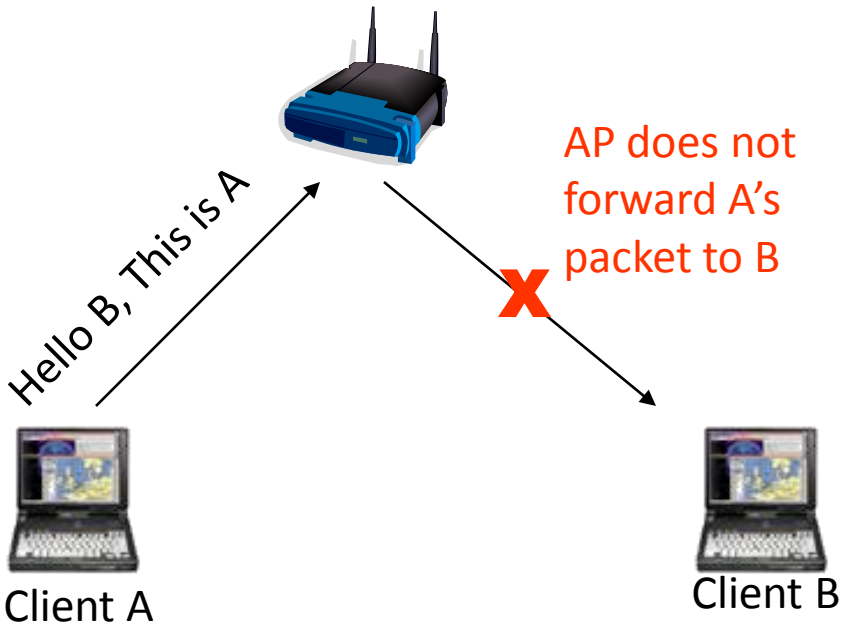
Hardware

Smartphones

Infrastructure Side

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

The feature can be used to stop communication between two WiFi enabled client devices



Limitations

Not all standalone mode APs or WLAN controllers have built-in PSPF or client isolation capabilities

PSPF or Client Isolation does not always work

- It does not work across APs in standalone mode
- In controller based architecture, PSPF (peer2peer) does not work across controllers even the controllers are present in the same mobility group

Attacker can always use WiFi client to launch attack and setup a non-WiFi host to serve the victim and easily bypass PSPF/Client isolation

Long Term Solution: Protocol Enhancement

Deprecate use of GTK and group addressed data traffic from AP

1. Convert all group addressed data traffic into unicast traffic
2. For *backward compatibility* AP should send randomly generated different GTKs to different clients so that all associated clients have different copies of group key

Disadvantages:

a. Brings down total network throughput

b. Requires AP software upgrade

Key Take Away

- WPA2 – secure, but vulnerable to insider attack!
- This limitation known to WPA2 designers, but not well understood by WiFi users
- Countermeasures can be deployed wherever threat of insider attacks is high
  - Using endpoint security; or
  - Using wireless traffic monitoring using WIPS sensors

Thank You!

Md Sohail Ahmad

Email: md.ahmad@airtightnetworks.com

www.airtightnetworks.com

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

blog.airtightnetworks.com

AirTight® NETWORKS

References

[1] Task Group I, IEEE P802.11i Draft 10.0. Project IEEE 802.11i, 2004.

[2] Aircrack-ng

www.aircrack-ng.org

[3] PEAP: Pwned Extensible Authentication Protocol

http://www.willhackforsushi.com/presentations/PEAP_Shmoocon2008_Wright_Antoniewicz.pdf

[4]. WPA/WPA2 TKIP Exploit: Tip of the Iceberg?

www.cwnp.com/pdf/TKIPExploit08.pdf

[5]. Cisco's PSPF or P2P
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00806a4da3.shtml

[6] Client isolation

http://www.cisecurity.org/tools2/wireless/CIS_Wireless_Addendum_Linksys.pdf

[7]. The Madwifi Project

http://madwifi-project.org/

References

[8]. Host AP Driver

http://hostap.epitest.fi/

[9]. ARP Cache Poisoning

http://www.grc.com/nat/arp.htm

[10] Detecting Wireless LAN MAC Address Spoofing

http://forskningsnett.uninett.no/wlan/download/wlan-mac-spoof.pdf

[11]. DecaffeinatID

http://www.irongeek.com/i.php?page=security/decaffeinatid-simple-ids-arpwatch-for-windows&mode=print

[12] SNORT

http://www.snort.org/

[13]. Wireless Hotspot Security

http://www.timeatlas.com/Reviews/Reviews/Wireless_Hotspot_Security