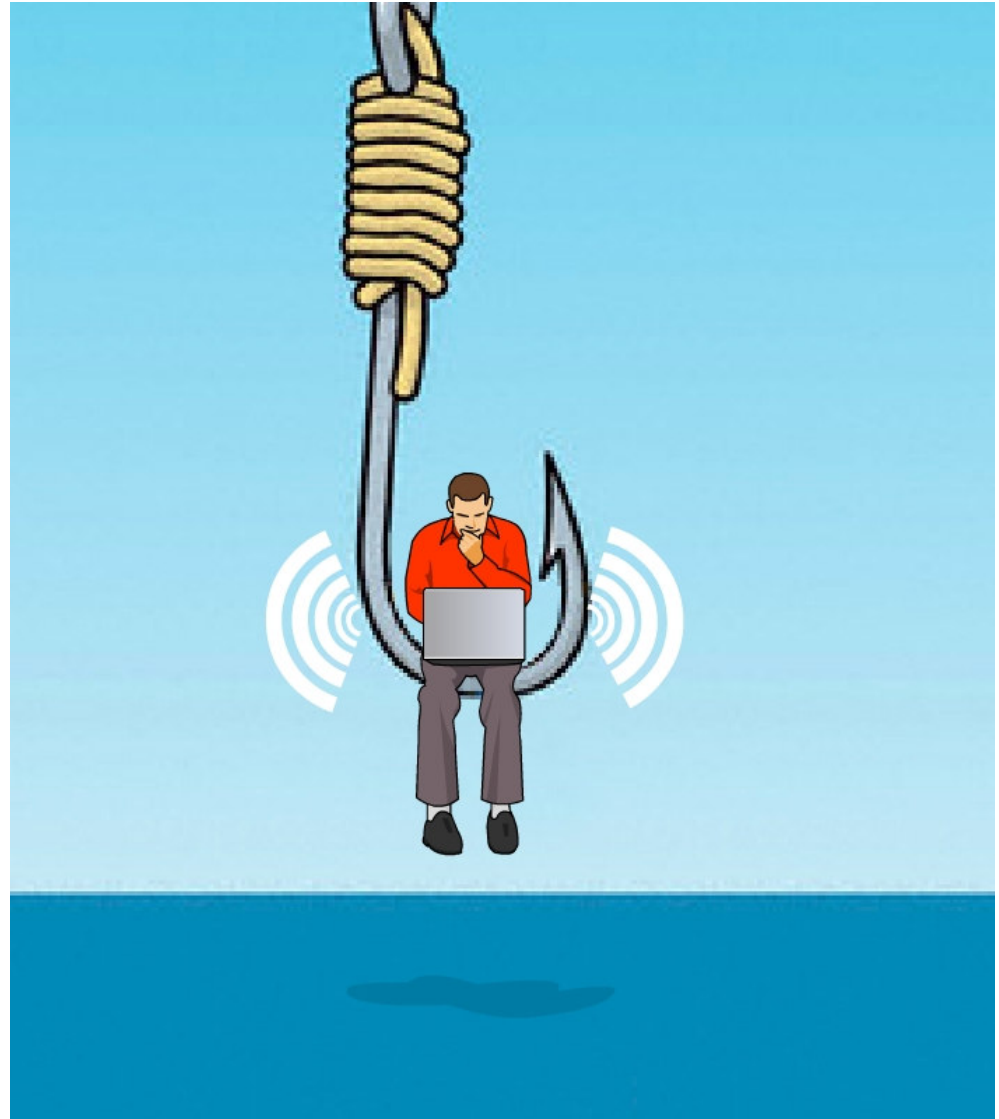


Wi-Fish Finder: Who will bite the bait?

**There is >50 % chance that
your laptop will!**

**Md Sohail Ahmad
Prabhash Dhyani**
AirTight Networks
www.airtightnetworks.com



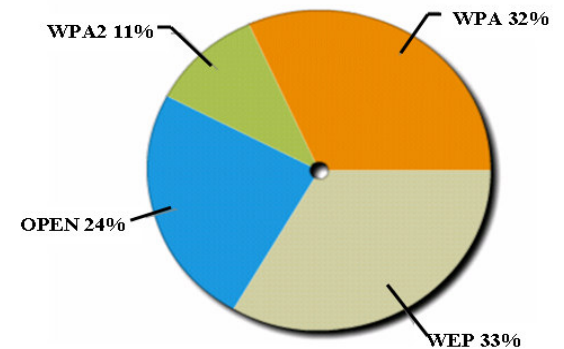
Background

For last 2-3 years we have been conducting WiFi scan in various cities in the world and studying the trend of WiFi security adoption



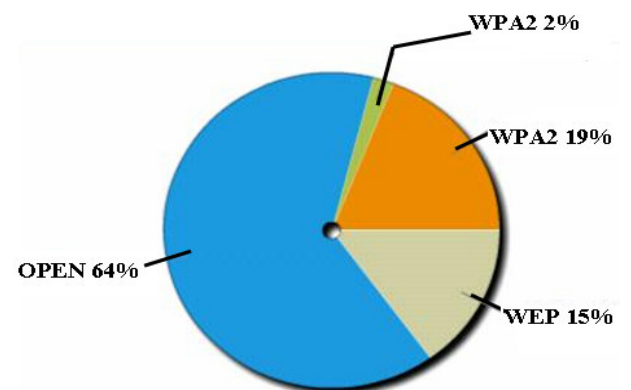
Financial Districts WiFi Scan Study (April, 2009)

<http://www.airtightnetworks.com/finance-wifi-study>



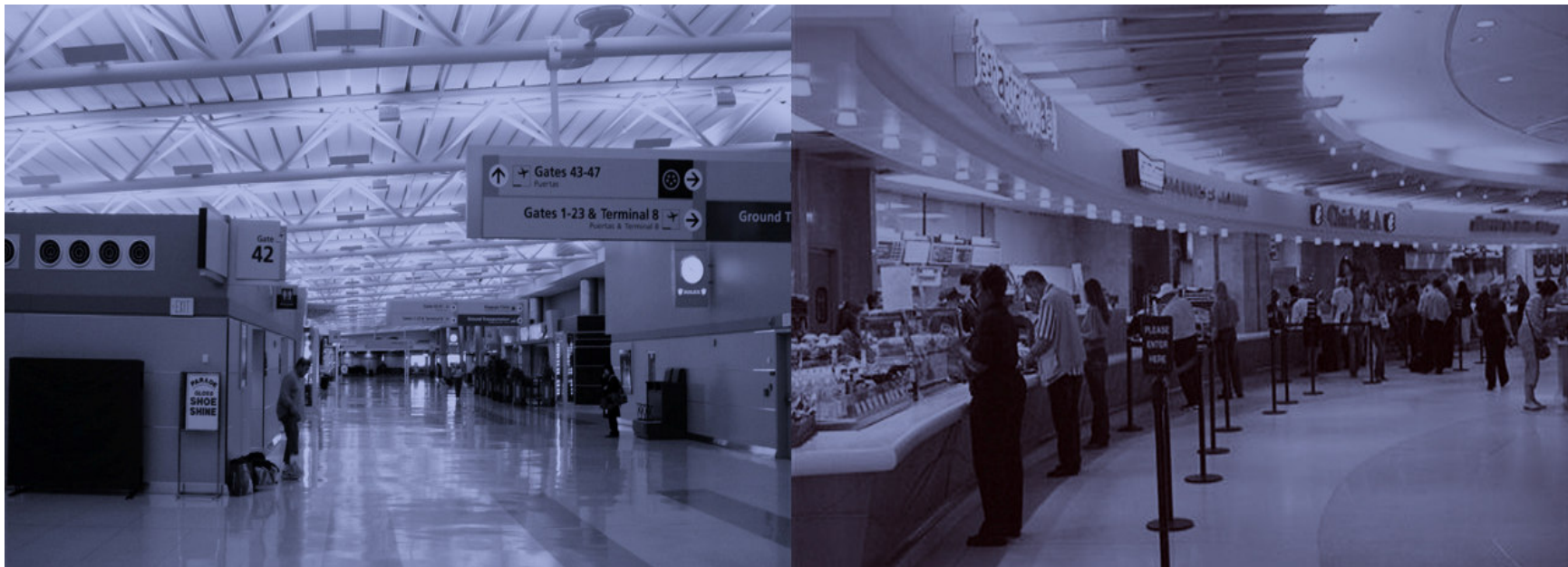
Airport WiFi Scan Study (March, 2008)

<http://www.airtightnetworks.com/airport-wifi-study>



A Thought

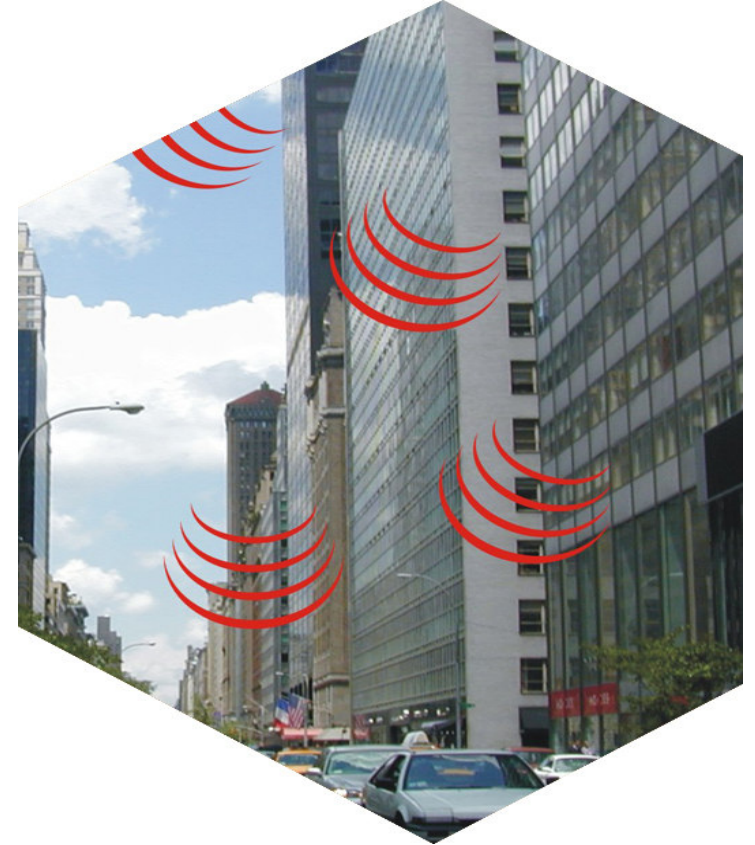
There are places like airports where thousands of people from different parts of the globe transit everyday. Most are business travelers and carry a WiFi enabled laptop, smartphone, PDAs etc.



Smart WiFi Study



Scanning WiFi Clients



Scanning WiFi APs

So, a very interesting client based WiFi scan study was possible right there instead of us going to different locations

A Scan Sample of WiFi Clients

Client

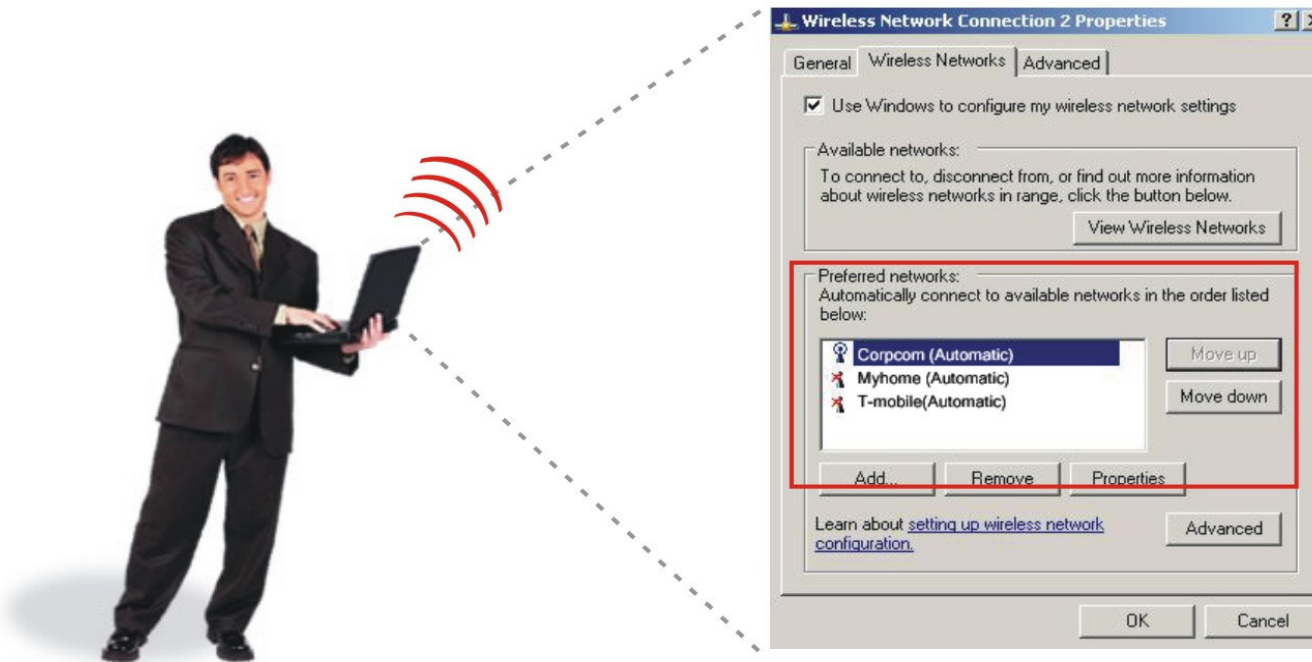
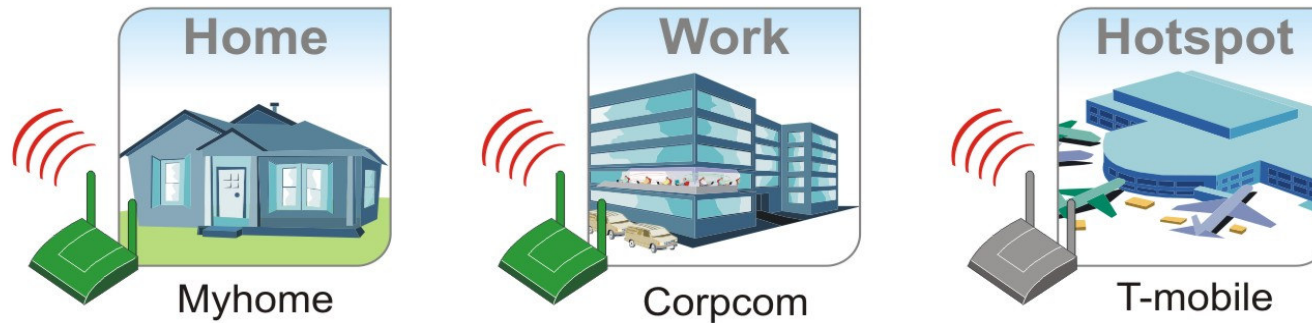


Laptop is probing for SSIDs from preferred list (cached).

```
0:ld:e0:90:1[redacted] | 15827258f644cc7e635a8bc, Booyakasha, MikesGiantPenis, mobile  
point, 5d52f14f3d5c0954f4fe6d39, tmobile stayonline, deloro  
0:ld:e0:c:[redacted] | concourse, Guimond, ramada  
0:le:4c:67:[redacted] | IMCCENTRAL  
0:le:4c:67:[redacted] | RRDUIR1  
0:le:4c:b3:[redacted] | kendog4, MBTA_WiFi_Coach0708_Box-062  
0:le:8c:2b:[redacted] | Skywriter, BUCKINGHAM, IOSConf, Conference, CudziloC-Wirele  
ss, martinipark  
0:le:8c:4c:[redacted] | AMF, loganwifi, Cammocks Network, SRHSWiFi, ihs, M1M1 Wirele  
ss, eircom6526 6330, eircom6542 6404, Hoffmanns
```

Popular Hotspot WiFi Networks

Client Probes For WiFi Networks Present in PNL



The Problem



Can Security Mode of Each Probed Network (OPEN, WEP, WPA or WPA2) be Determined?

Time To Do A Live Demo !!!

Wi-Fish Finder
 Security Assessment Tool for WiFi Clients
 (c)2009 Md Sohail Ahmad, Prabhash Dhyani, AirTight Networks
 =====

CH 6 [Elapsed: 5 mins][2009-07-30 11:47]

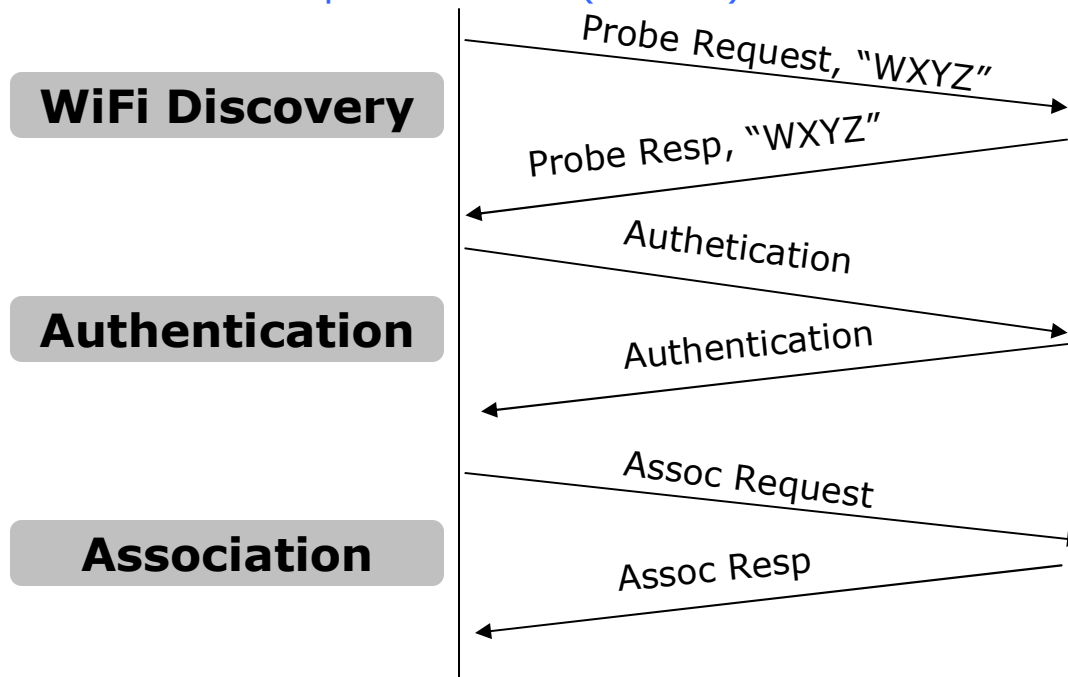
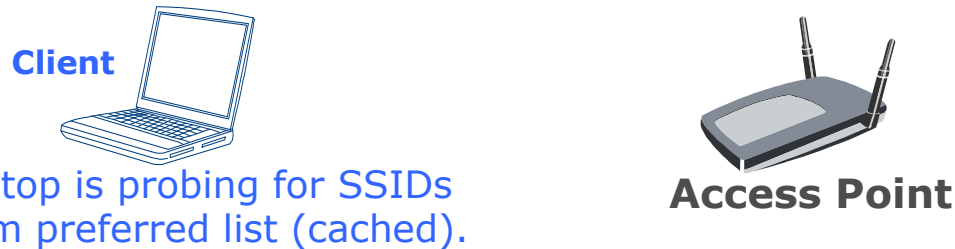
STATION	AUTH	ENC	Security-Posture	MODE	Probed SSID
00:1C:BF:01:E8:99	WPA2-802.1x	CCMP	vuln	Infra	Test-PEAP-Vulnerable
--:--:--:--:--:--	WPA2-802.1x	CCMP	Secure	Infra	Test-WPA2-1X-AES
--:--:--:--:--:--	WPA2-802.1x	TKIP	Secure	Infra	Test-WPA2-1X-TKIP
--:--:--:--:--:--	WPA2-PSK	CCMP	Secure	Infra	Test-WPA2-PSK-AES
--:--:--:--:--:--	WPA2-PSK	TKIP	Secure	Infra	Test-WPA2-PSK-TKIP
--:--:--:--:--:--	WPA1-802.1x	CCMP	Secure	Infra	Test-WPA1-1X-AES
--:--:~:~:~:~:~:~	WPA1-802.1x	TKIP	Secure	Infra	Test-WPA1-1X-TKIP
--:~:~:~:~:~:~	WPA1-PSK	CCMP	Secure	Infra	Test-WPA1-PSK-AES
--:~:~:~:~:~:~	WPA1-PSK	TKIP	Secure	Infra	Test-WPA1-PSK-TKIP
--:~:~:~:~:~:~	WEP -Open	WEP	vuln (WEP Cracking)	Infra	Test-WEP-Open
--:~:~:~:~:~:~	-Open	OPEN	vuln (Unencrypted)	Infra	Test-Open
--:~:~:~:~:~:~	WEP -SKA	WEP	vuln (WEP Cracking)	Infra	WEP_Shared

Security of a Probed SSID

Security posture

Probed SSID

A Naïve Approach



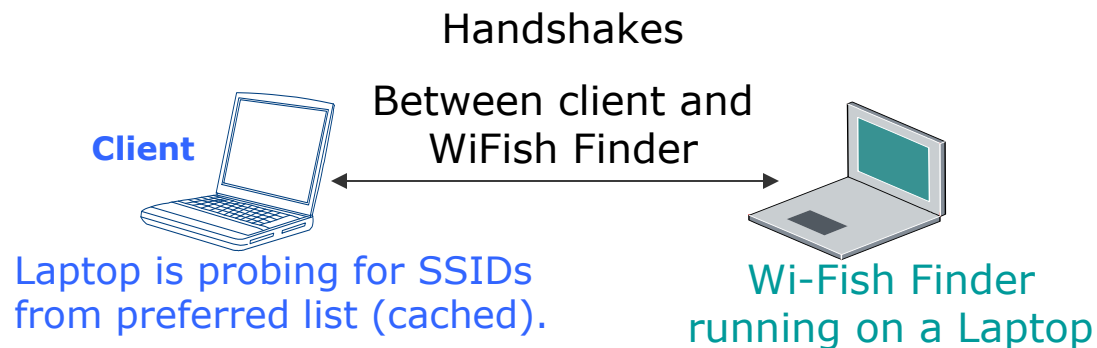
Practical Issues:

1. Probes for multiple SSIDs
2. Probes from multiple clients
3. Total 11 commonly used security configurations (1-Open, 2-WEP, 4-WPA, 4-WPA2)

Wi-Fish Finder Automates That For You

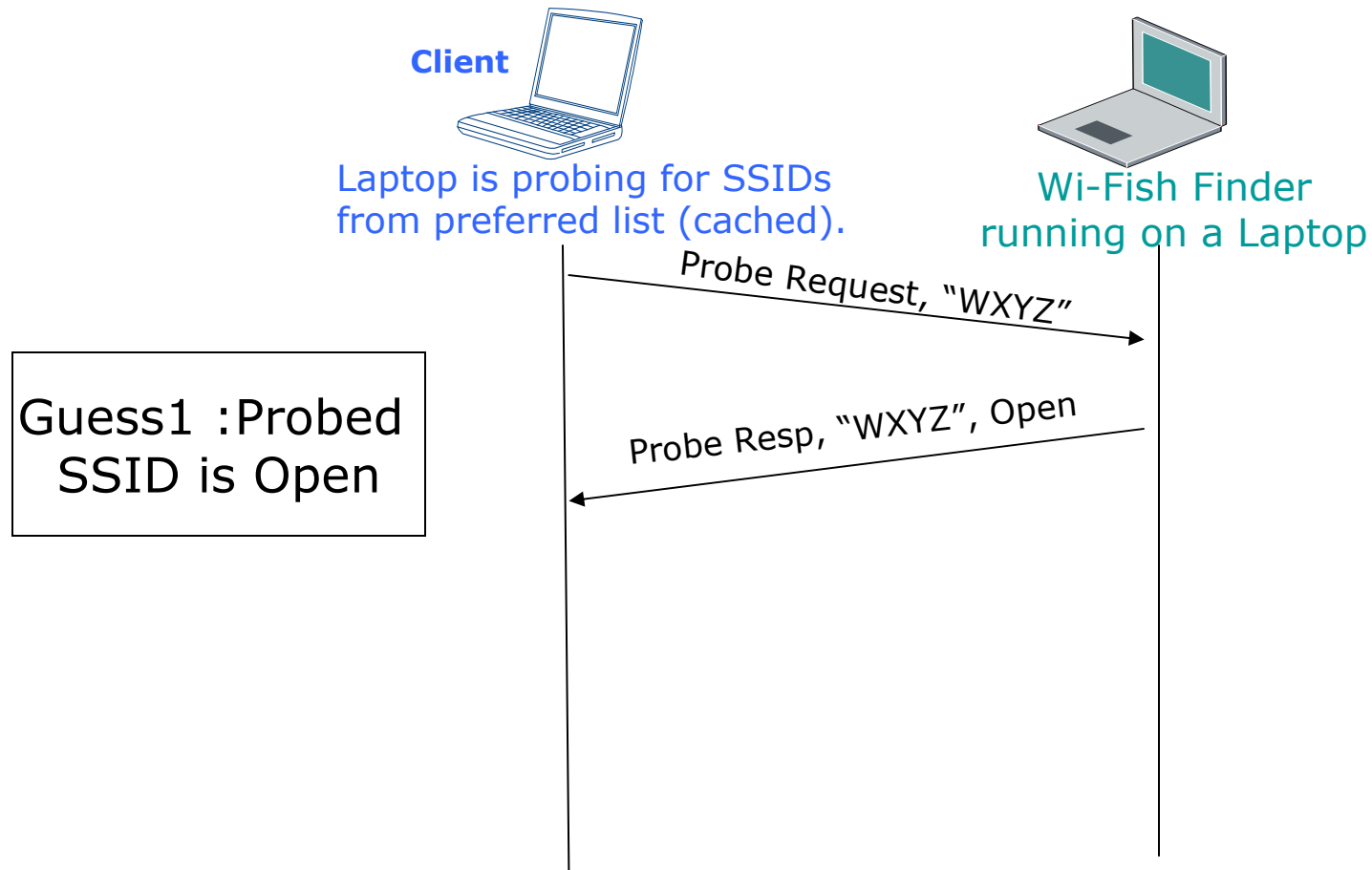
WiFish Finder:

1. Handles probes for Multiple SSIDs
2. Handles probes from Multiple Clients
3. Works for almost all commonly used security configurations (1-Open, 2-WEP, 4-WPA, 4-WPA2)

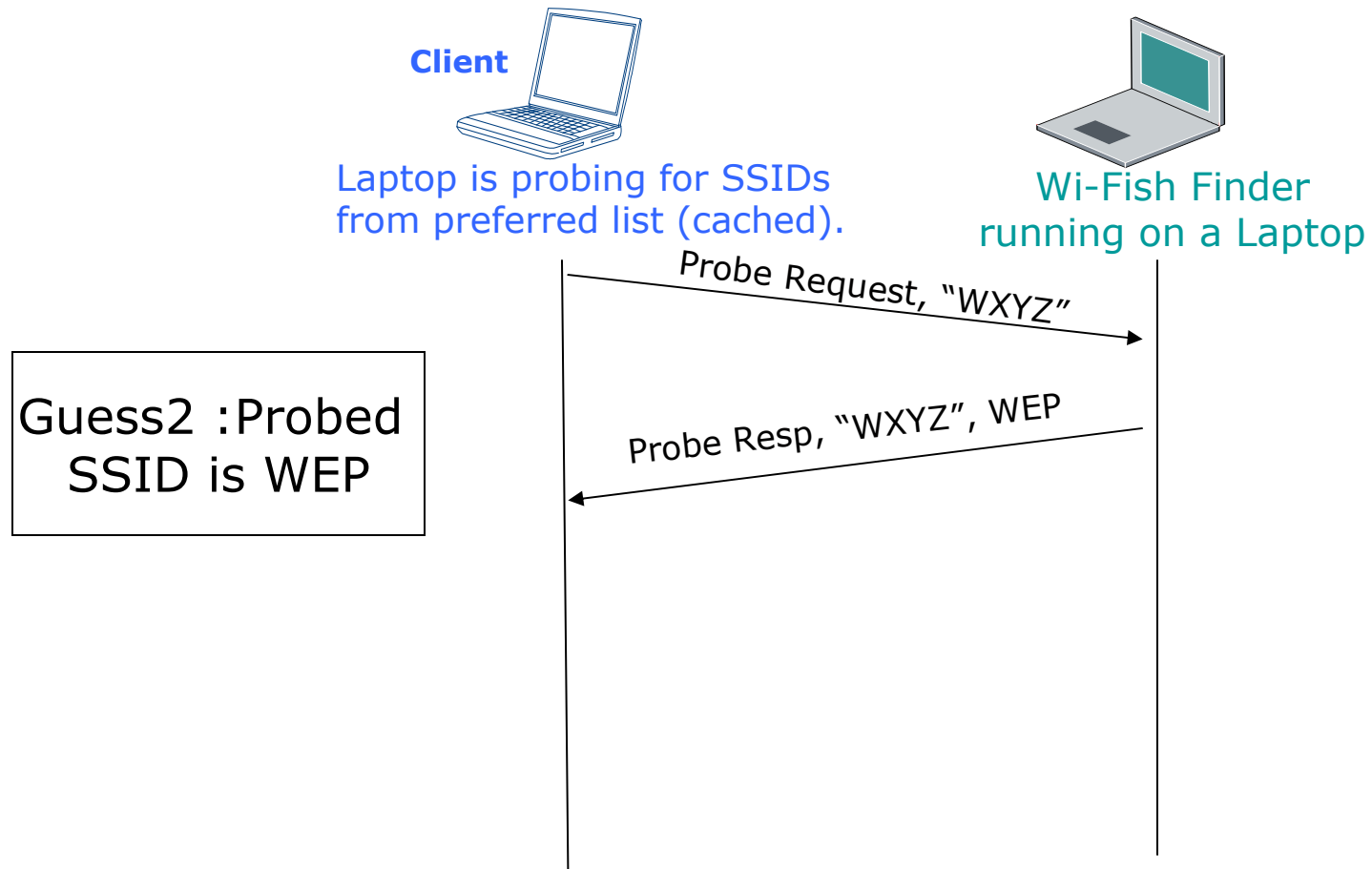


WiFish Finder simulates a virtual WiFi network environment around a probing client

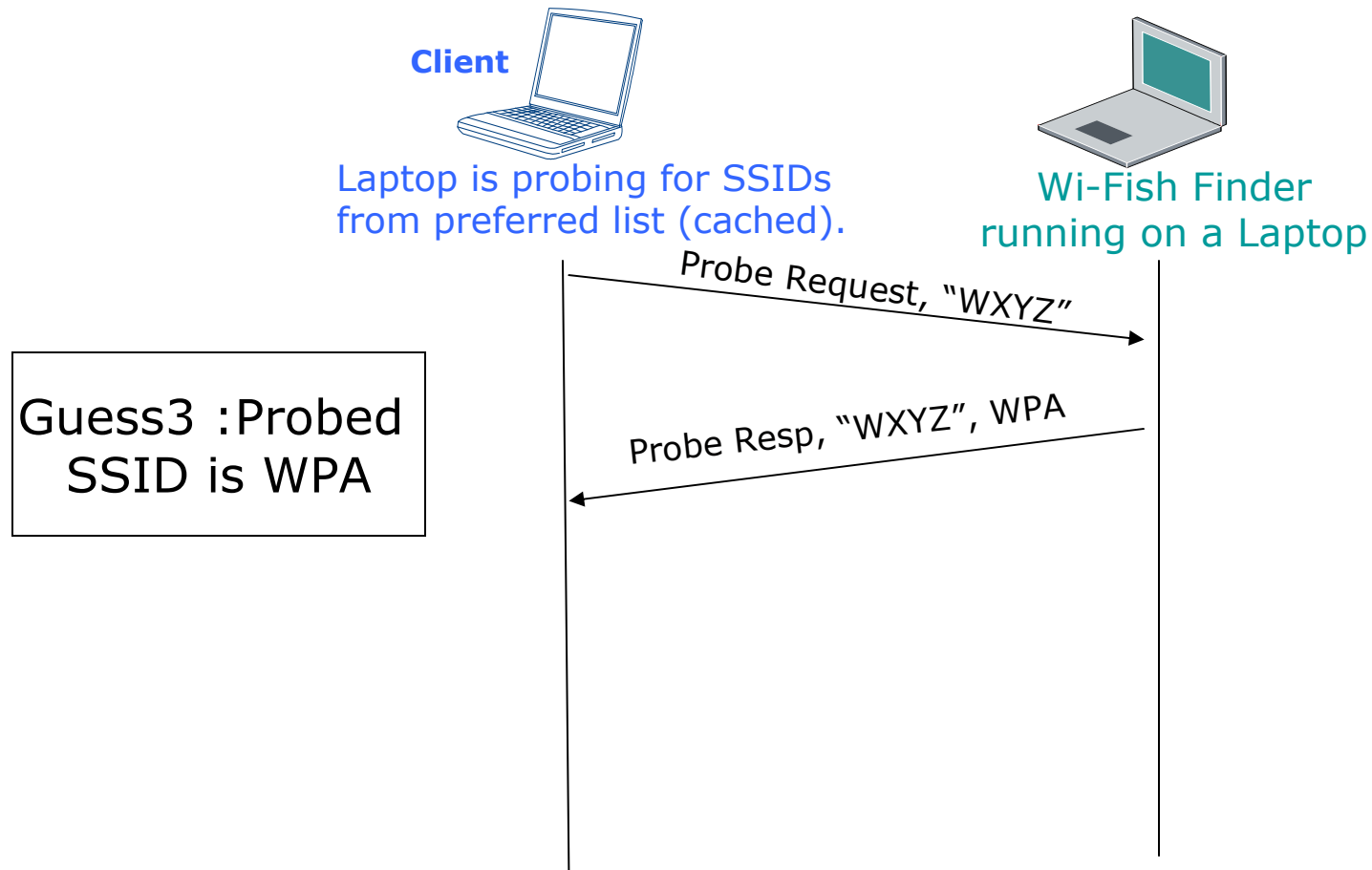
Implementation: Wi-Fish Finder



Implementation: Wi-Fish Finder



Implementation: Wi-Fish Finder

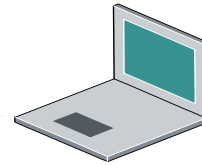


Implementation: Wi-Fish Finder



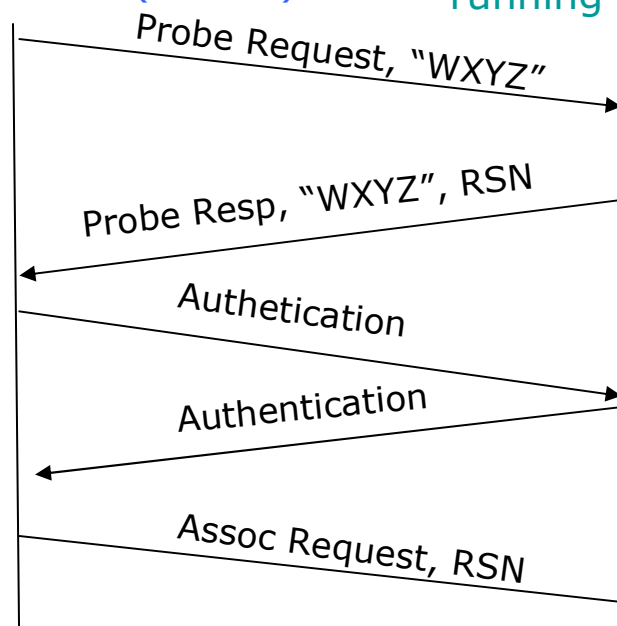
Client

Laptop is probing for SSIDs from preferred list (cached).



Wi-Fish Finder running on a Laptop

Guess4 : Probed SSID is WPA2



Security settings of SSID "WXYZ" found

An Snippet of the Scan Study Done In This Conference

From thousands of miles away, I know

STATION	AUTH	ENC	Security-Posture	Probed SSID	
00:22:FA:93:D2:74	WEP -Open	WEP	Vuln (WEP Cracking)	pgp-d	Home Network
--:--:--:--:--:--	WPA1-PSK	CCMP	Secure	Mama's Boy	
00:21:06:E2:DD:44	WEP -Open	WEP	Vuln (WEP Cracking)	home123	Home Network
00:24:9F:E7:38:74	WEP -Open	WEP	Vuln (WEP Cracking)	HomeNet	
00:26:08:E4:B9:55	WPA2-PSK	CCMP	Secure	CoolHouse	Default Config
00:13:E8:04:3B:66	-Open	OPEN	Vuln (Unencrypt)	default	
00:24:9F:67:97:C5	WPA1-PSK	CCMP	Secure	wowhacker	Insecure Profile In PNL
--:--:--:--:--:--	-Open	OPEN	Vuln (Unencrypt)	hgvc	
--:--:--:--:--:--	WEP -Open	WEP	Vuln (WEP Cracking)	BY3ST	
00:1E:C2:3E:07:8F	-Open	OPEN	Vuln (Unencrypt)	hpsetup	Viral SSID or adhoc mode
00:17:C4:11:85:67	-Open	OPEN	Vuln (Unencrypt)	olpc-mesh	

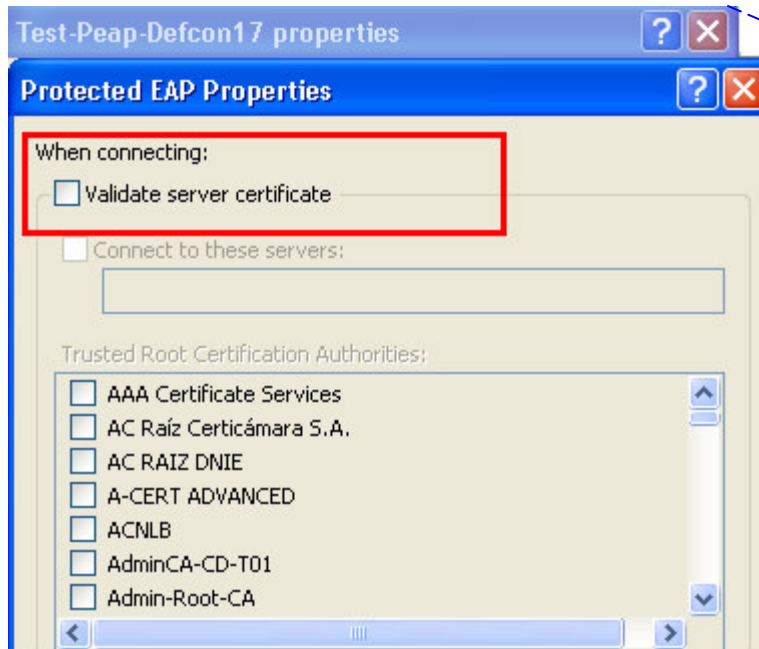
So a WiFi scan study is possible using this tool, what else ?

Client Vulnerability Assessment

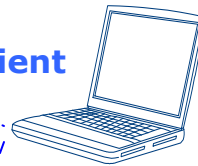
Security of a Probed SSID	It is possible to launch
Probed SSID -> WEP	Caffe Latte Attack
Probed SSID -> WPA/WPA2 (Pre Shared Key)	Dictionary Attack (if Weak Passphrase)
Probed SSID -> WPA/WPA2 (MGT, 802.1x)	PEAP Attack (if Certificate Validation Uncheck)

Wi-Fish Finder can be used in identifying such vulnerable clients well in advance

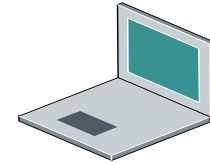
PEAP Vulnerability Detection



Client

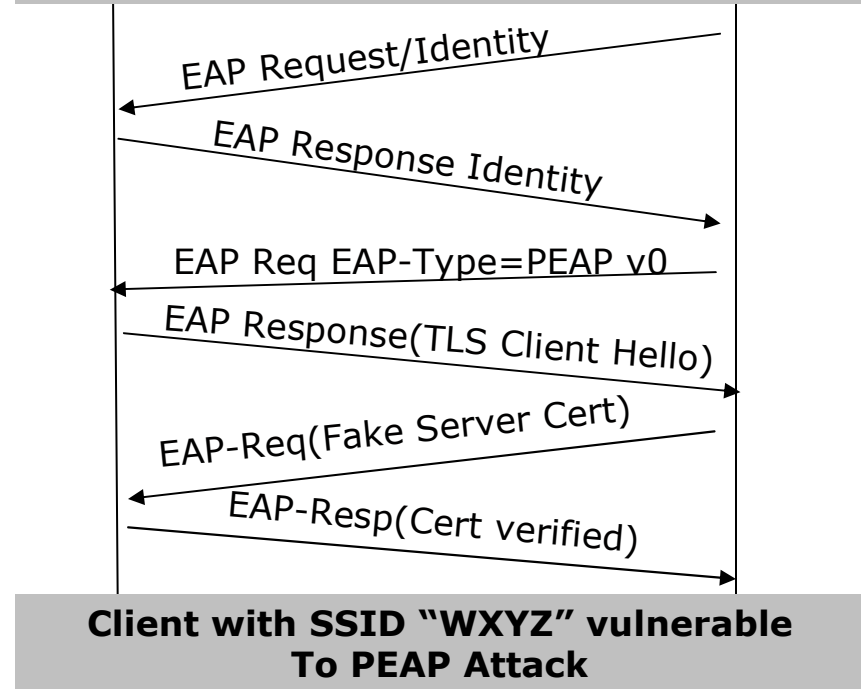


Laptop is probing for SSIDs from preferred list (cached).



Wi-Fish Finder running on a Laptop

Client is associated with Wi-Fish Finder, Probed SSID "WXYZ", Security WPA2+.1x



Conclusion

While lot of measures have been taken to secure WiFi infrastructure (both APs and Client in the vicinity) by following best practices and deploying various forms of WIPS solution,
An isolated WiFi client device still need adequate security cover to prevent it from Honey pots

Wi-Fish Finder can be served as **“WiFi Client Security Assessment Tool”** and can be used by **security auditors** or **network admins** in identifying clients vulnerable to **Wi-Fishing or Honey pots**

Download WiFish Finder:

<http://blog.airtightnetworks.com>

Thanks !

Md Sohail Ahmad

md.ahmad@airtightnetworks.com
sohail_alig@yahoo.com

Prabhash Dhyani

prabhash.dhyani@airtightnetworks.com

AirTight Networks
www.airtightnetworks.com



References

- ◆ Aircrack Suite
<http://www.aircrack-ng.org/doku.php>
- ◆ Attacking Automatic Wireless Network Selection
<http://www.theta44.org/karma/aawns.pdf>
- ◆ Hotspotter-Automatic wireless client penetration http://www.remote-exploit.org/codes_hotspotter.html
- ◆ Karma Main <http://wirelessdefence.org/Contents/KARMAMain.htm>
- ◆ Cafe Latte attack
<http://www.airtightnetworks.com/home/resources/knowledge-center/caffe-latte.html>
- ◆ PEAP: Pwned Extensible Authentication Protocol
<http://www.willhackforsushi.com/papers/shmoocon-rfp-joshua-wright.pdf>