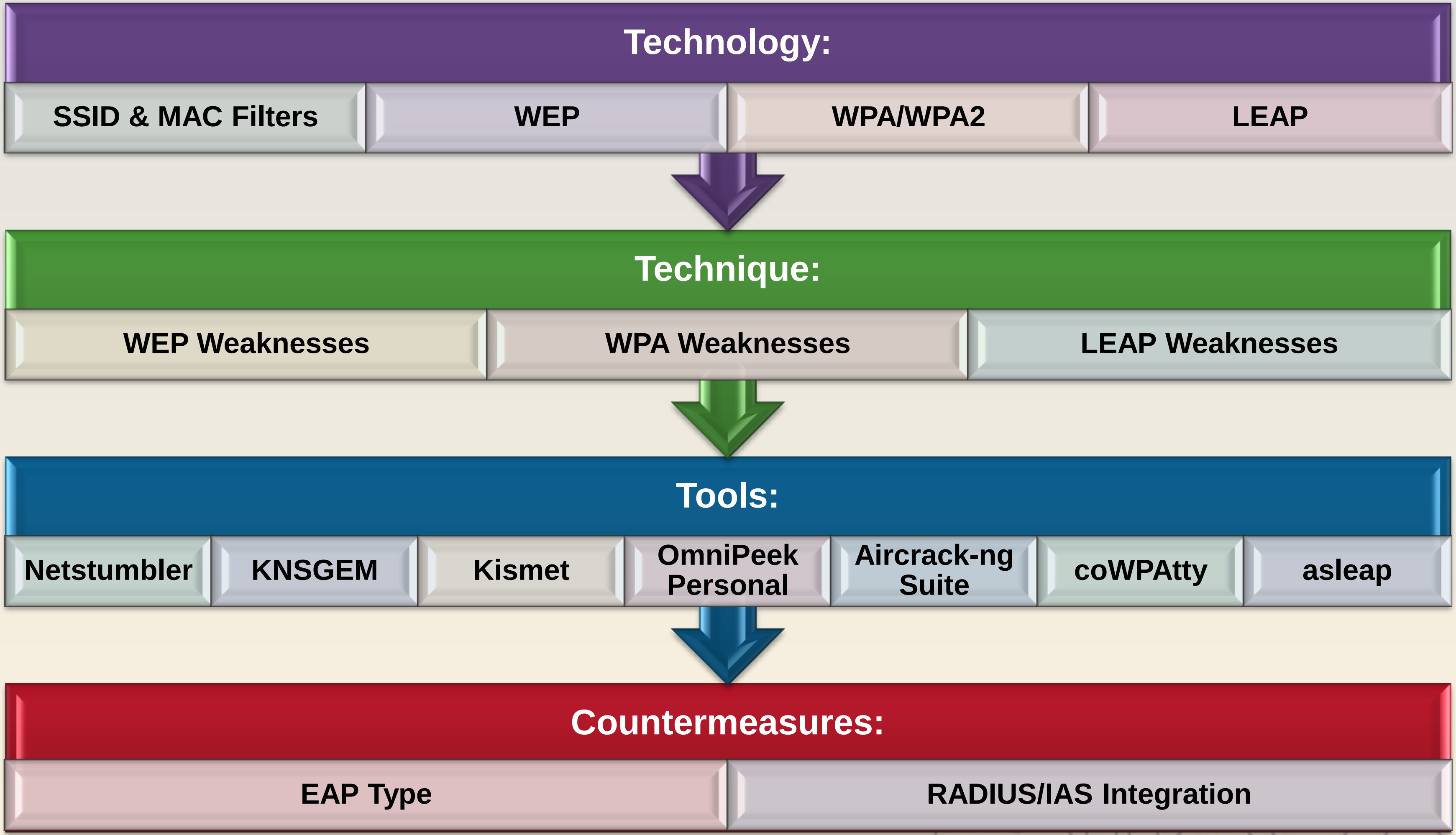
Pen Testing Wireless Networks

Overview



Technology:

- SSID & MAC Filters
- WEP
- WPA/WPA2
- LEAP

Technique:

- WEP Weaknesses
- WPA Weaknesses
- LEAP Weaknesses

Tools:

- Netstumbler
- KNSGEM
- Kismet
- OmniPeek Personal
- Aircrack-ng Suite
- coWPAtty
- asleap

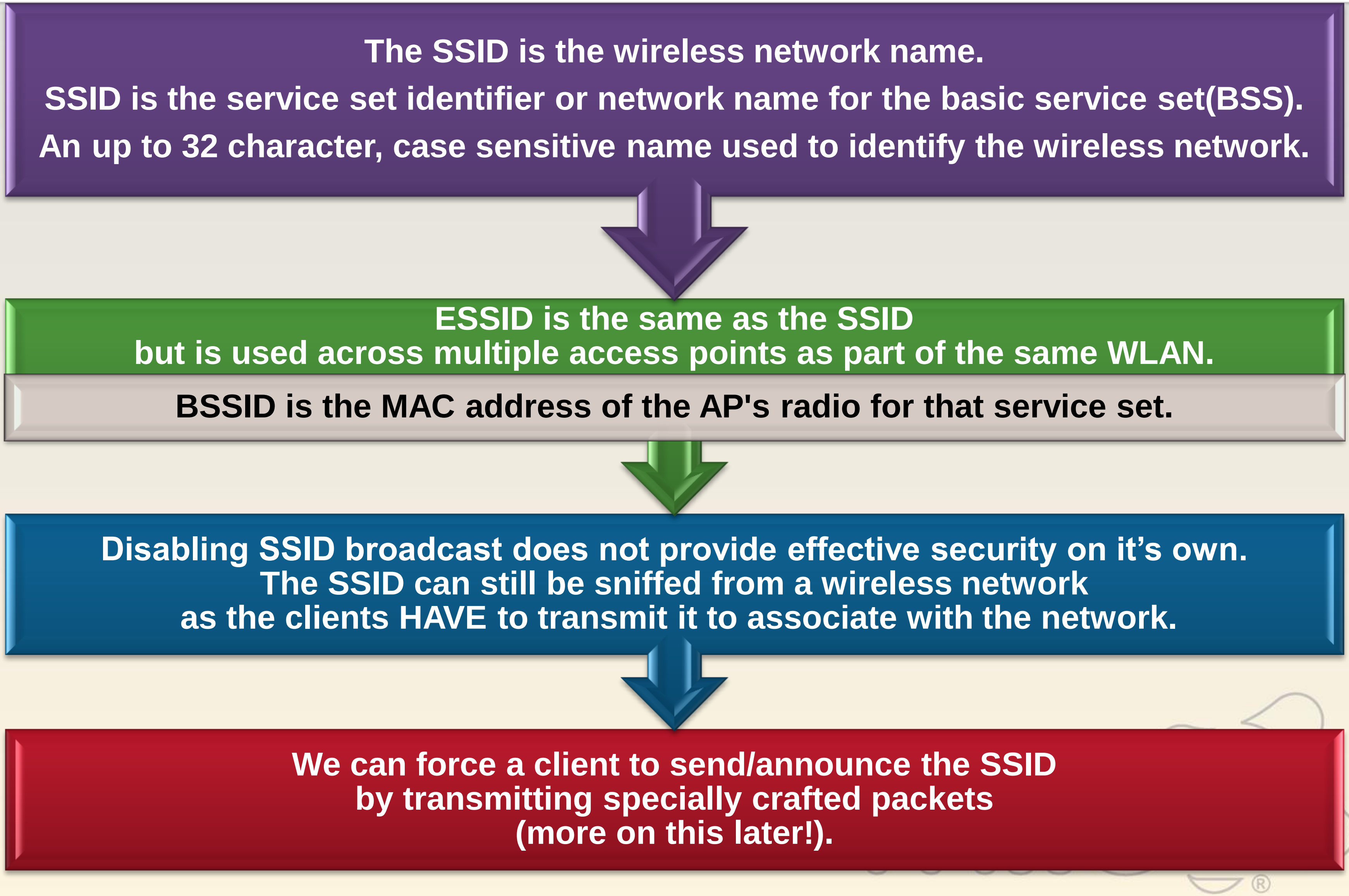
Countermeasures:

- EAP Type
- RADIUS/IAS Integration

Standards Comparison

820.11 Protocol	Release	Freq. (GHz)	Thru. (Mbit/s)	Data (Mbit/s)	Mod.	Radius In – (m)	Radius Out – (m)
-	1997	2.4	0.9	2	FHSS	~20	~100
a	1999	5	23	54	OFDM	~35	~120
b	1999	2.4	4.3	11	DSSS	~38	~140
g	2003	2.4	19	54	OFDM	~38	~140
n	2009	2.4, 5	74	248	OFDM	~70	~250
y	2008	3.7	23	54		~50	~5000

SSID (Service Set Identity)



The SSID is the wireless network name.

SSID is the service set identifier or network name for the basic service set(BSS).

An up to 32 character, case sensitive name used to identify the wireless network.

ESSID is the same as the SSID
but is used across multiple access points as part of the same WLAN.

BSSID is the MAC address of the AP's radio for that service set.

Disabling SSID broadcast does not provide effective security on it’s own.
The SSID can still be sniffed from a wireless network
as the clients HAVE to transmit it to associate with the network.

We can force a client to send/announce the SSID
by transmitting specially crafted packets
(more on this later!).

MAC Filtering

One defensive method is known as MAC filtering. Only the clients with specific MAC addresses can connect to the AP.

MAC addresses are easily sniffed by an attacker since they must be communicated in clear text, even with WEP or WPA, in order for the receiver to obtain the transmission.

An attacker can masquerade as a valid MAC address by MAC spoofing the wireless card.

The attacker would have to wait until the targeted MAC address shuts down or disassociates from the network to prevent network errors from occurring.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a security system that uses a static key on both sides of a wireless transmission to encrypt data for secure transmission.

The WEP encryption method is designed to provide the "equivalent" security available in wired networks. (But it failed to live up to its name)

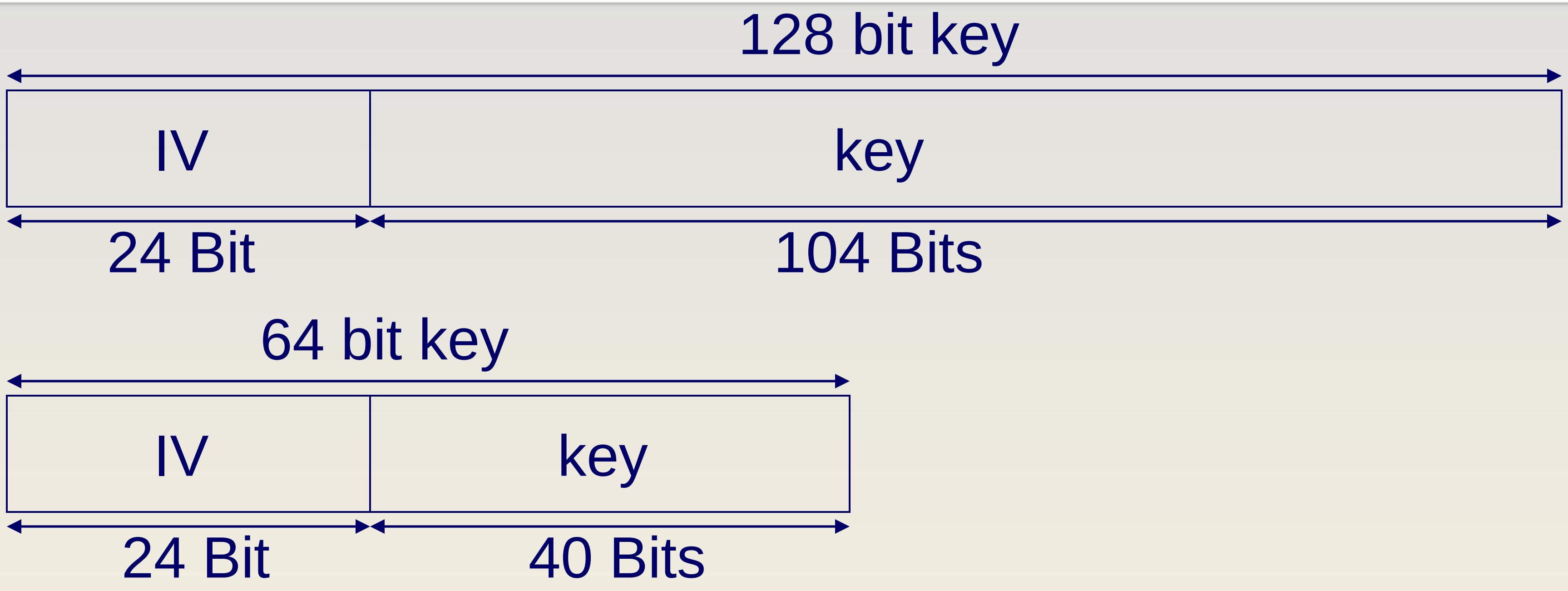
Provides Authentication and Encryption.

Uses RC4 for Confidentiality.

- 64/128-bit RC4 keys.
- Non-standard extensions use 256/512 bit keys.
- Keys are constructed of 24 bits Initialization Vector (IV) and the remaining 40/104 bits are the user defined key.
- The IV is a rolling counter used to change the entire key per packet.

Uses CRC-32 for Integrity.

Weak IV Packets



128 bit key

IV

key

24 Bit

104 Bits

64 bit key

IV

key

24 Bit

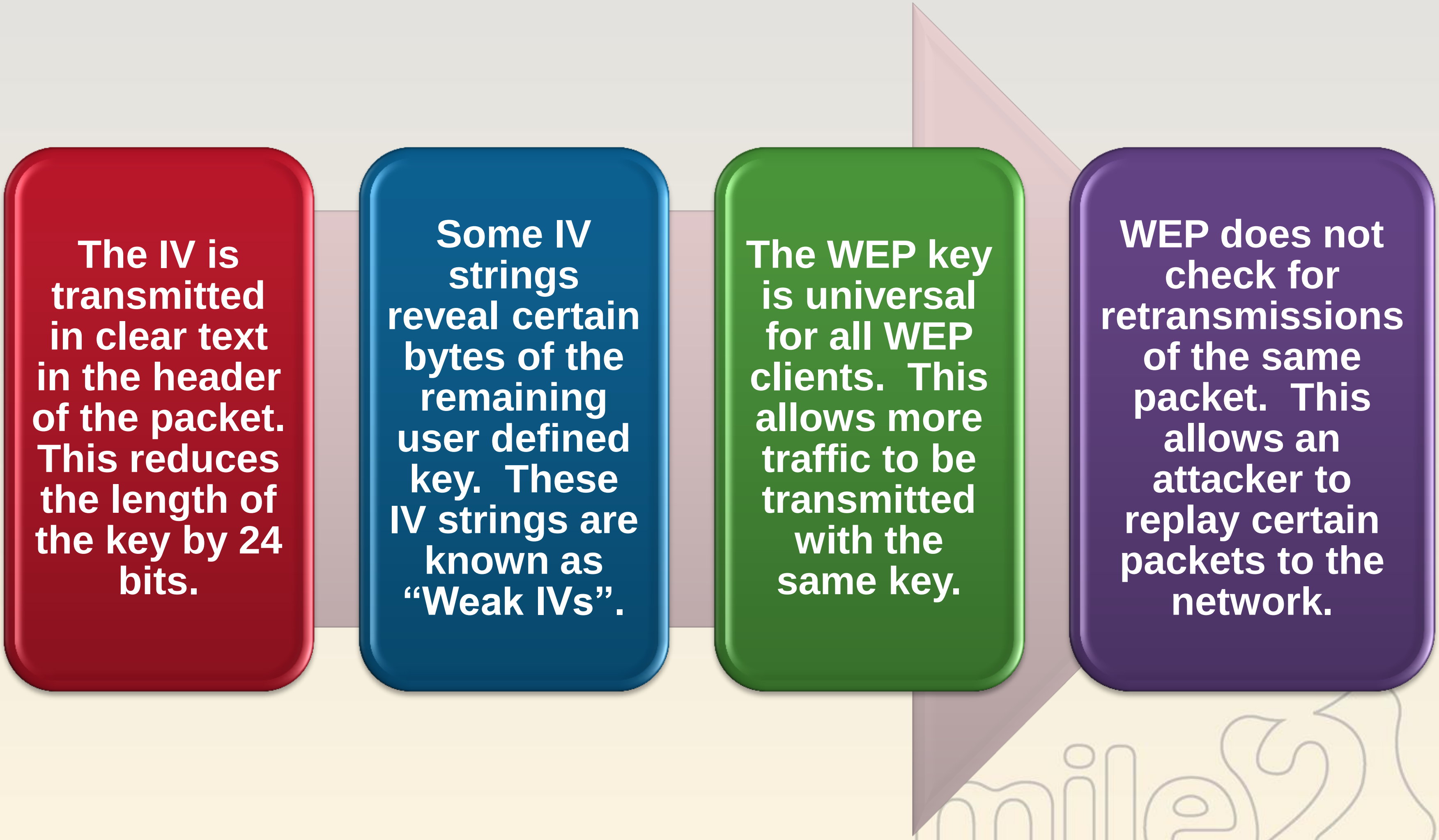
40 Bits

A busy access point, sending 1500 byte packets at 11Mbps, will exhaust all IVs after 1500*8/(11*10^6)*2^24 = ~18000 seconds, or 5 hours.

A 24 bit IV has a 50% probability that it will repeat after 5000 packets.

Modern attacks can crack captured or live wireless WEP encrypted data in less than 3 minutes. (http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy)

WEP Weaknesses



The IV is transmitted in clear text in the header of the packet. This reduces the length of the key by 24 bits.

Some IV strings reveal certain bytes of the remaining user defined key. These IV strings are known as “Weak IVs”.

The WEP key is universal for all WEP clients. This allows more traffic to be transmitted with the same key.

WEP does not check for retransmissions of the same packet. This allows an attacker to replay certain packets to the network.

XOR – Encryption Basics

When discussing WEP encryption, it is important to understand the ‘Exclusive Or’ Gate (XOR) because it is used in the encryption process.

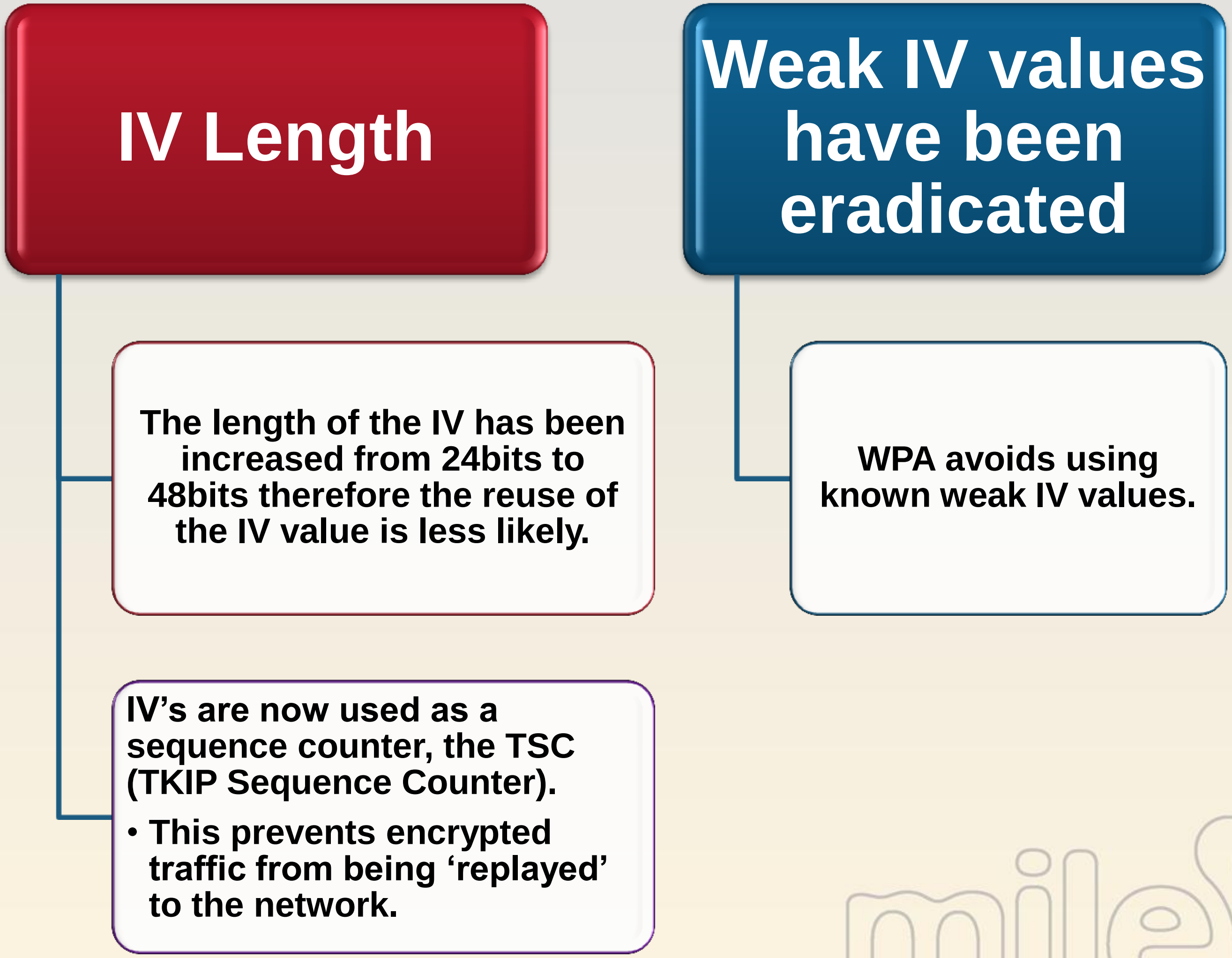
XOR is a simple comparison of binary bits, the output is the result of the difference between the two bits.

If the compared bits match, the output is 0. If they do not match, the output is 1.

Original bit	XOR bit	Resulting bit
1	1	0
0	0	0
1	0	1
0	1	1

Data	1	0	1	1	0
Key	1	0	0	1	1
Cipher	0	0	1	0	1

How WPA improves on WEP



IV Length

The length of the IV has been increased from 24bits to 48bits therefore the reuse of the IV value is less likely.

IV’s are now used as a sequence counter, the TSC (TKIP Sequence Counter).

- This prevents encrypted traffic from being ‘replayed’ to the network.

Weak IV values have been eradicated

WPA avoids using known weak IV values.

How WPA improves on WEP

Master Keys

Static master keys are never used directly in WPA, unlike WEP. In WPA, a hierarchy of keys is used and each client uses a different encryption key.

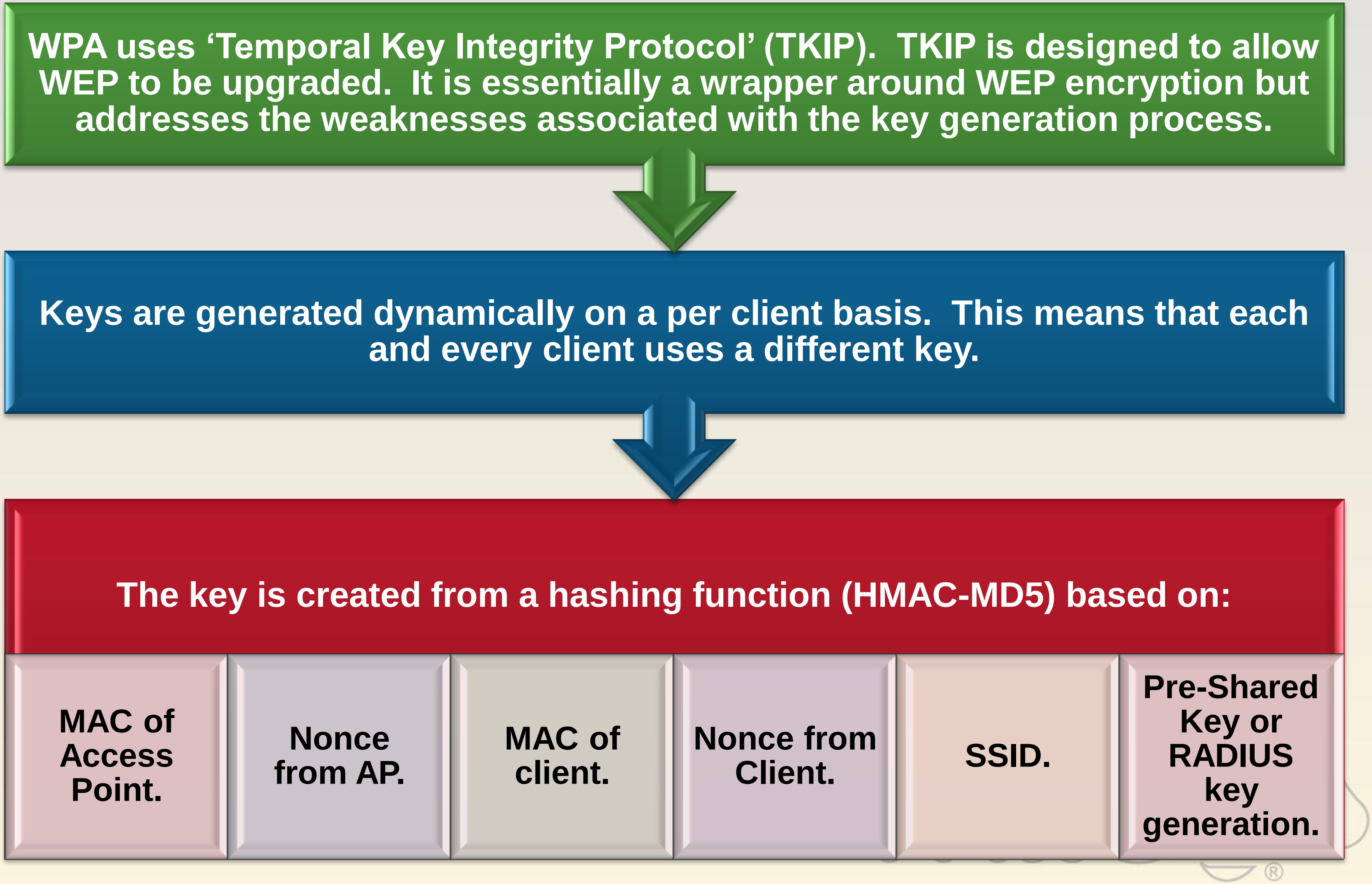
Key Management

Secure key management isn't an issue with WPA due to the key generation system.

Message integrity checking

WPA uses a Message Integrity Check (MIC) called, Michael. Although relatively simple, there is a one in a million chance of guessing a MIC. This prevents attackers from altering packets of data.

TKIP



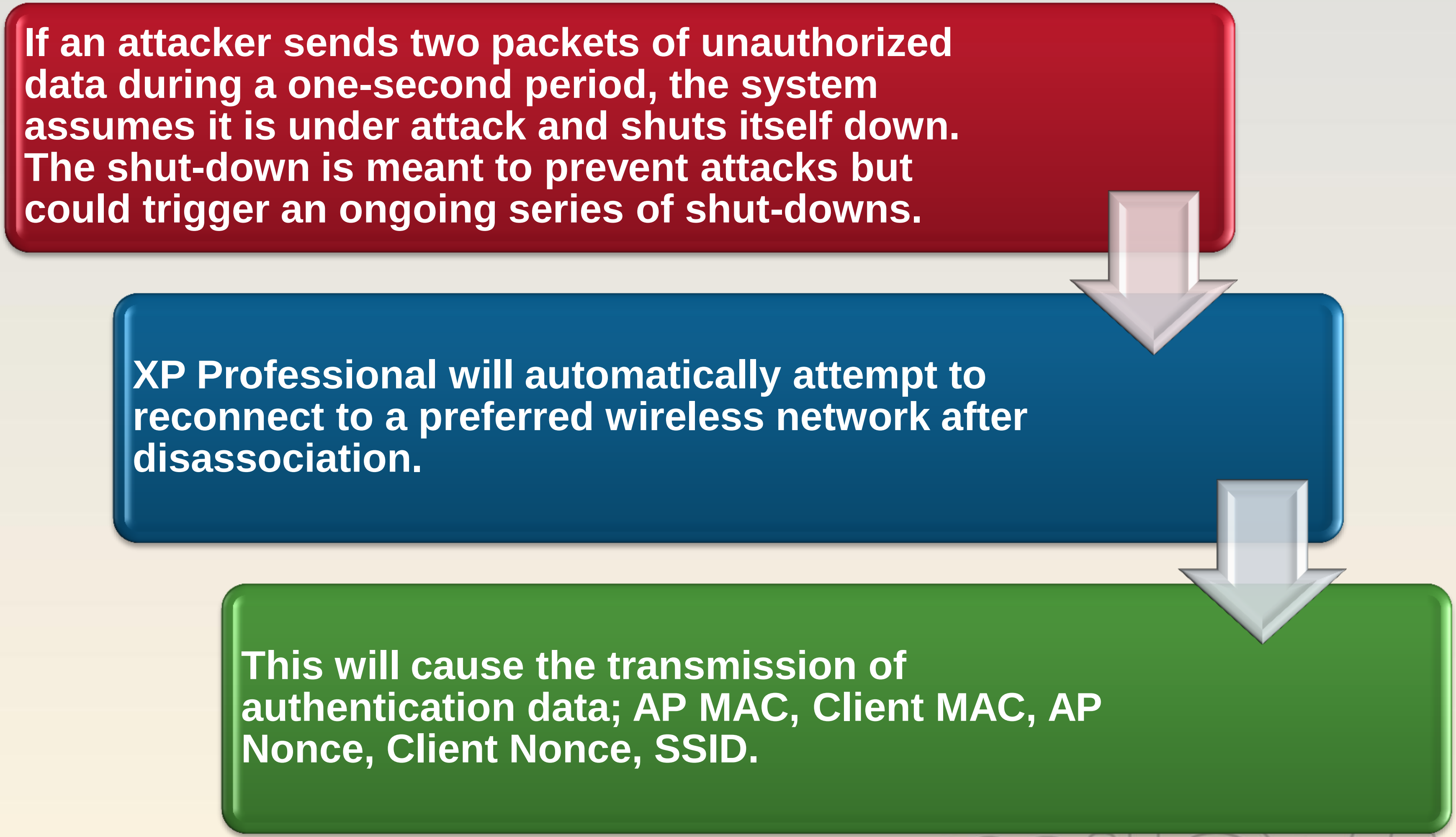
WPA uses ‘Temporal Key Integrity Protocol’ (TKIP). TKIP is designed to allow WEP to be upgraded. It is essentially a wrapper around WEP encryption but addresses the weaknesses associated with the key generation process.

Keys are generated dynamically on a per client basis. This means that each and every client uses a different key.

The key is created from a hashing function (HMAC-MD5) based on:

- MAC of Access Point.
- Nonce from AP.
- MAC of client.
- Nonce from Client.
- SSID.
- Pre-Shared Key or RADIUS key generation.

The WPA MIC Vulnerability



If an attacker sends two packets of unauthorized data during a one-second period, the system assumes it is under attack and shuts itself down. The shut-down is meant to prevent attacks but could trigger an ongoing series of shut-downs.

XP Professional will automatically attempt to reconnect to a preferred wireless network after disassociation.

This will cause the transmission of authentication data; AP MAC, Client MAC, AP Nonce, Client Nonce, SSID.

802.11i - WPA2

WPA and WPA2 are virtually identical. Both are derived from 802.11i with WPA being an early snapshot of 802.11i.

The major difference between WPA and WPA2 is the encryption algorithm used, RC4/TKIP and AES-CCMP respectively.

AES-CCMP is abbreviated from Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol.

WPA and WPA2 Mode Types

	WPA	WPA2
Enterprise Mode	Authentication: 802.1X/EAP Encryption: TKIP/RC4	Authentication: 802.1X/EAP Encryption: AES-CCMP
Personal Mode	Authentication: PSK Encryption: TKIP/RC4	Authentication: PSK Encryption: AES-CCMP

WPA-PSK Encryption

The problem with WPA and WPA2 Pre-Shared Key security is the key generation process.

Remember that the key is generated from the MAC of Access Point, Nonce from AP, MAC of client, Nonce from Client, PSK and SSID.

All of the above information is transmitted in clear text (except the PSK!) when a client associates.

If an attacker is able to intercept the traffic, they can take a PSK from a dictionary file and combine it with the rest of the data. An attacker can then compare MIC values until a match is found.

Most administrators use a weak, dictionary based key as they believe WPA encryption is much more secure than WEP. But that is only true if the PSK is long and complex (20+ characters)

LEAP

Lightweight Extensible Authentication Protocol

- Proprietary wireless LAN authentication method developed by Cisco Systems.

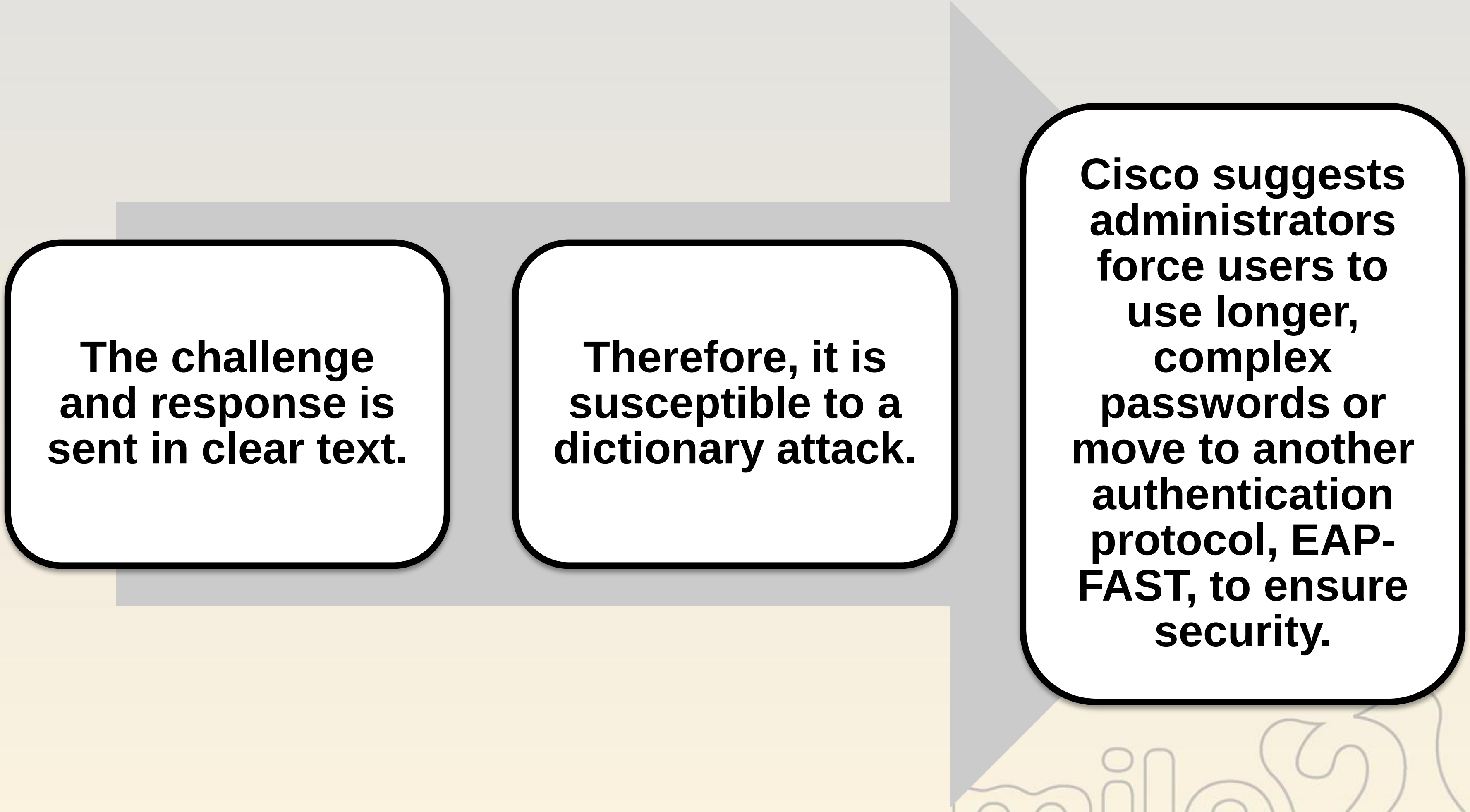
Important features of LEAP

- *Dynamic WEP keys* - LEAP allows for clients to re-authenticate frequently; upon each successful authentication, the clients acquire a new WEP key (with the hope that the WEP keys don't live long enough to be cracked).
- *Mutual authentication* (between a wireless client and a RADIUS server).

LEAP uses a modified version of MS-CHAP

- Authentication protocol in which user credentials are not strongly protected.

LEAP Weaknesses

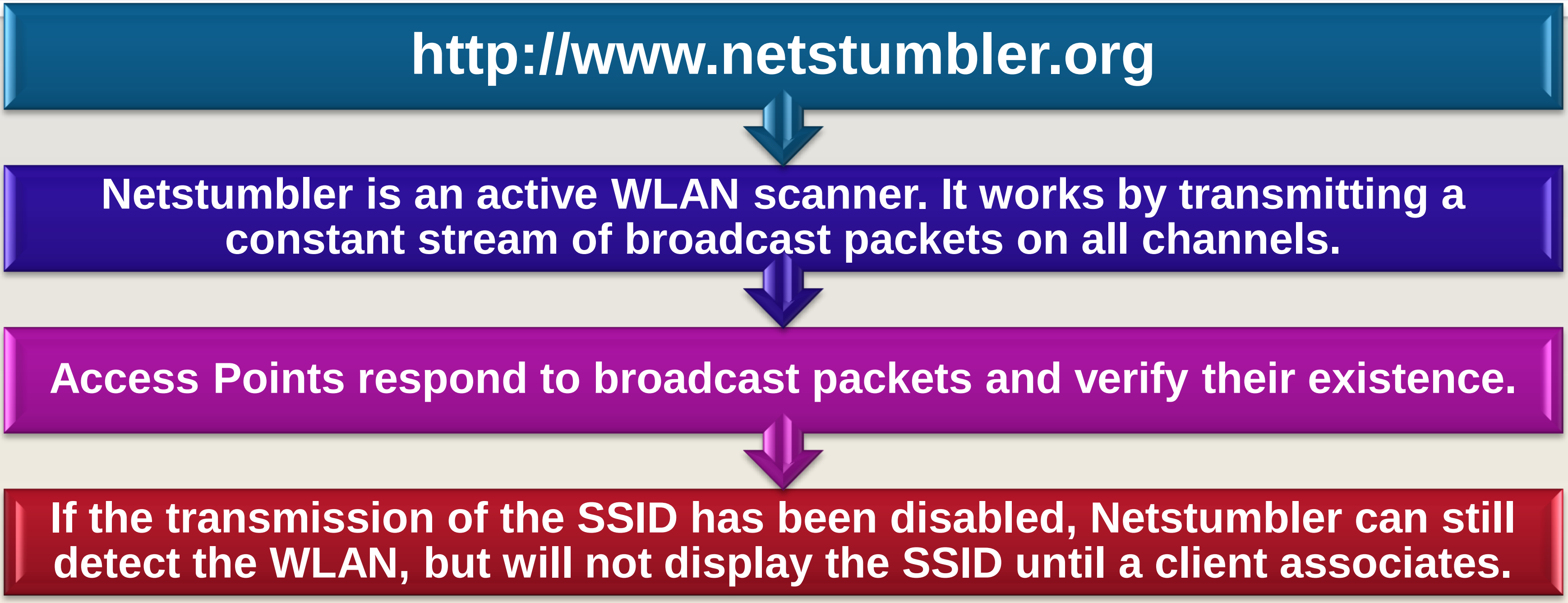


The challenge and response is sent in clear text.

Therefore, it is susceptible to a dictionary attack.

Cisco suggests administrators force users to use longer, complex passwords or move to another authentication protocol, EAP-FAST, to ensure security.

NetStumbler

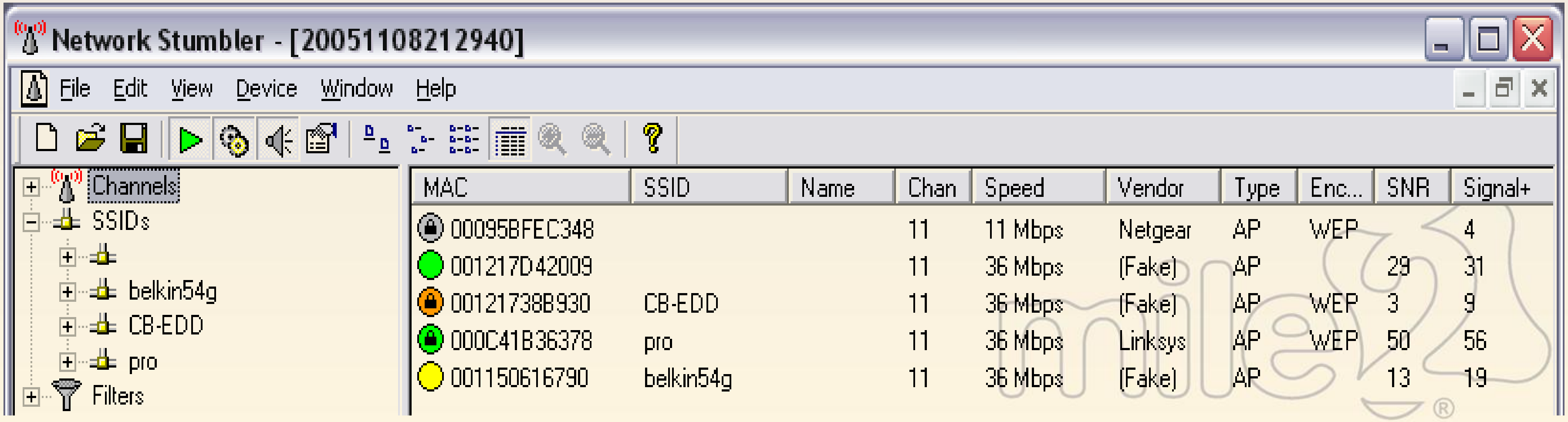


http://www.netstumbler.org

Netstumbler is an active WLAN scanner. It works by transmitting a constant stream of broadcast packets on all channels.

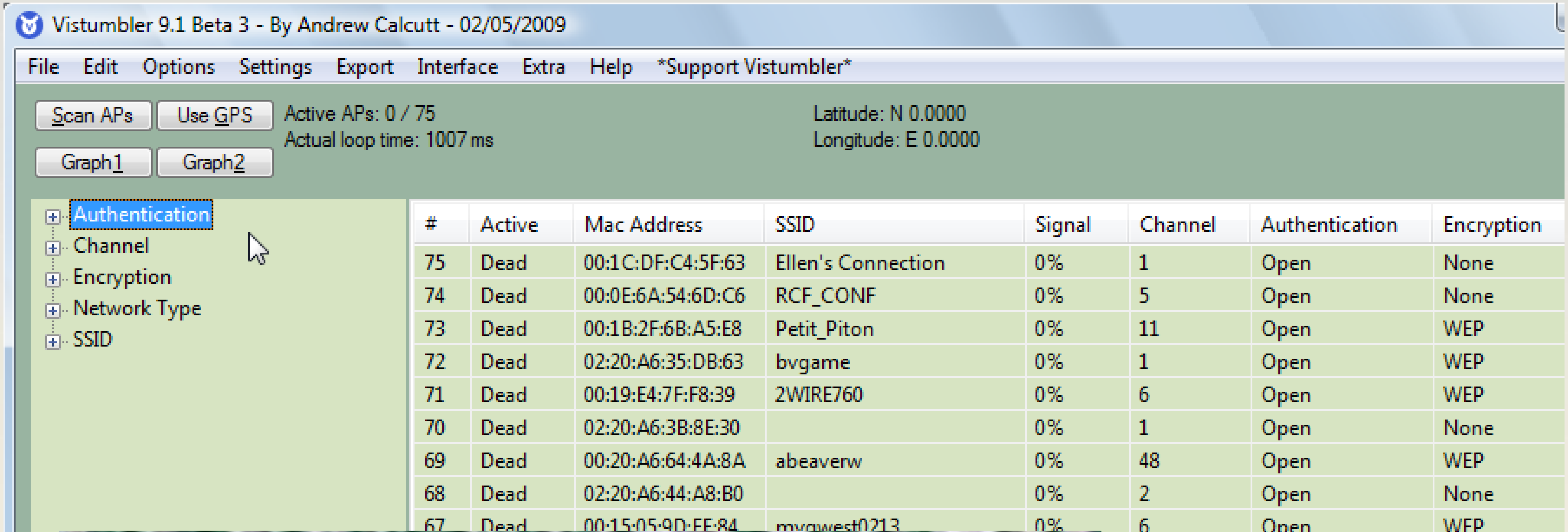
Access Points respond to broadcast packets and verify their existence.

If the transmission of the SSID has been disabled, Netstumbler can still detect the WLAN, but will not display the SSID until a client associates.



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
00095BFEC348			11	11 Mbps	Netgear	AP	WEP		4
001217D42009			11	36 Mbps	(Fake)	AP		29	31
00121738B930	CB-EDD		11	36 Mbps	(Fake)	AP	WEP	3	9
000C41B36378	pro		11	36 Mbps	Linksys	AP	WEP	50	56
001150616790	belkin54g		11	36 Mbps	(Fake)	AP		13	19

Vistumbler

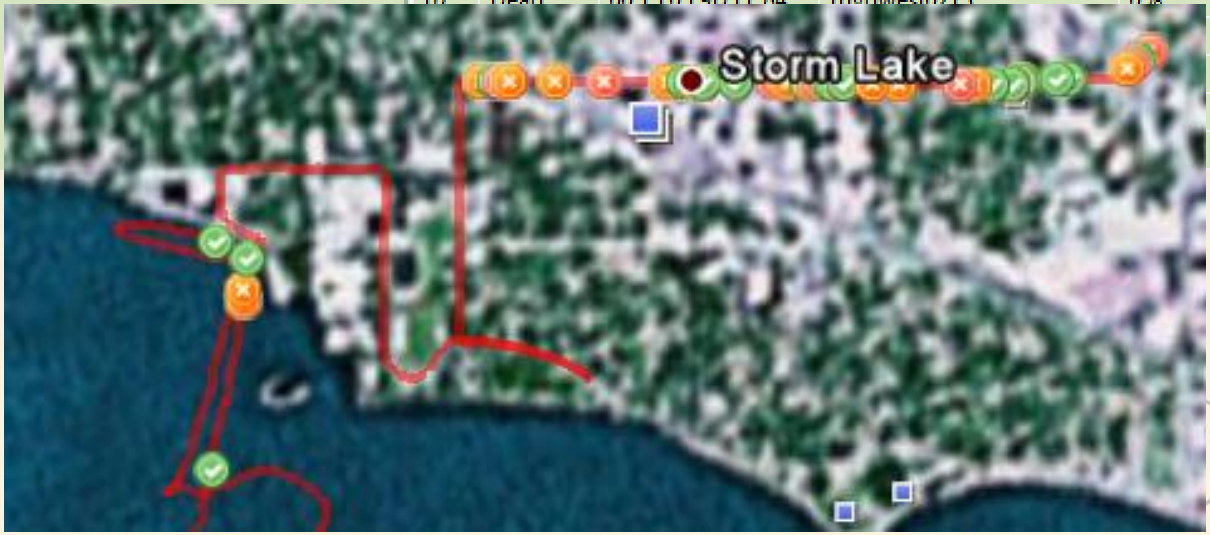


Vistumbler 9.1 Beta 3 - By Andrew Calcutt - 02/05/2009

Active APs: 0 / 75
Actual loop time: 1007 ms

Latitude: N 0.0000
Longitude: E 0.0000

#	Active	Mac Address	SSID	Signal	Channel	Authentication	Encryption
75	Dead	00:1C:DF:C4:5F:63	Ellen's Connection	0%	1	Open	None
74	Dead	00:0E:6A:54:6D:C6	RCF_CONF	0%	5	Open	None
73	Dead	00:1B:2F:6B:A5:E8	Petit_Piton	0%	11	Open	WEP
72	Dead	02:20:A6:35:DB:63	bvgame	0%	1	Open	WEP
71	Dead	00:19:E4:7F:F8:39	2WIRE760	0%	6	Open	WEP
70	Dead	02:20:A6:3B:8E:30		0%	1	Open	None
69	Dead	00:20:A6:64:4A:8A	abeaverw	0%	48	Open	WEP
68	Dead	02:20:A6:44:A8:B0		0%	2	Open	None
67	Dead	00:15:05:9D:FF:84	myqwest0213	0%	6	Open	WEP
					7	Open	None
					6	Open	None
					6	Open	None
					6	WPA-Personal	TKIP

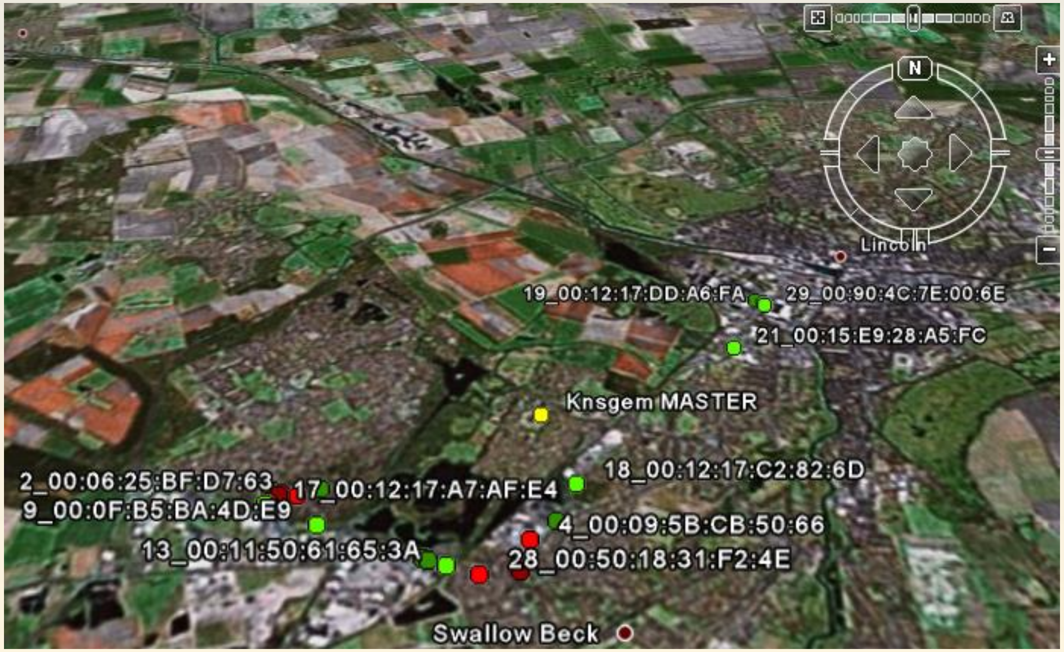


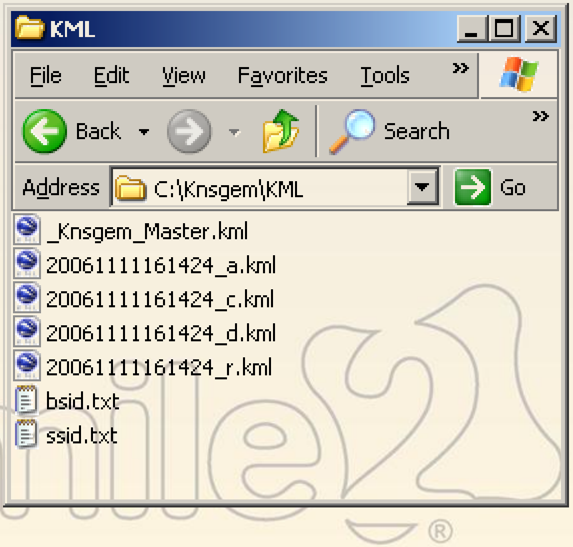
War Driving With KNSGEM

http://www.wirelessdefence.org/Contents/knsgem_main.htm

http://www.rjpi.com/knsgem.htm

You will need Netstumbler, KNSGEM, GPS and Google Earth





Address: C:\Knsgem\KML

_Knsgem_Master.kml
20061111161424_a.kml
20061111161424_c.kml
20061111161424_d.kml
20061111161424_r.kml
bsid.txt
ssid.txt

Tool: Kismet

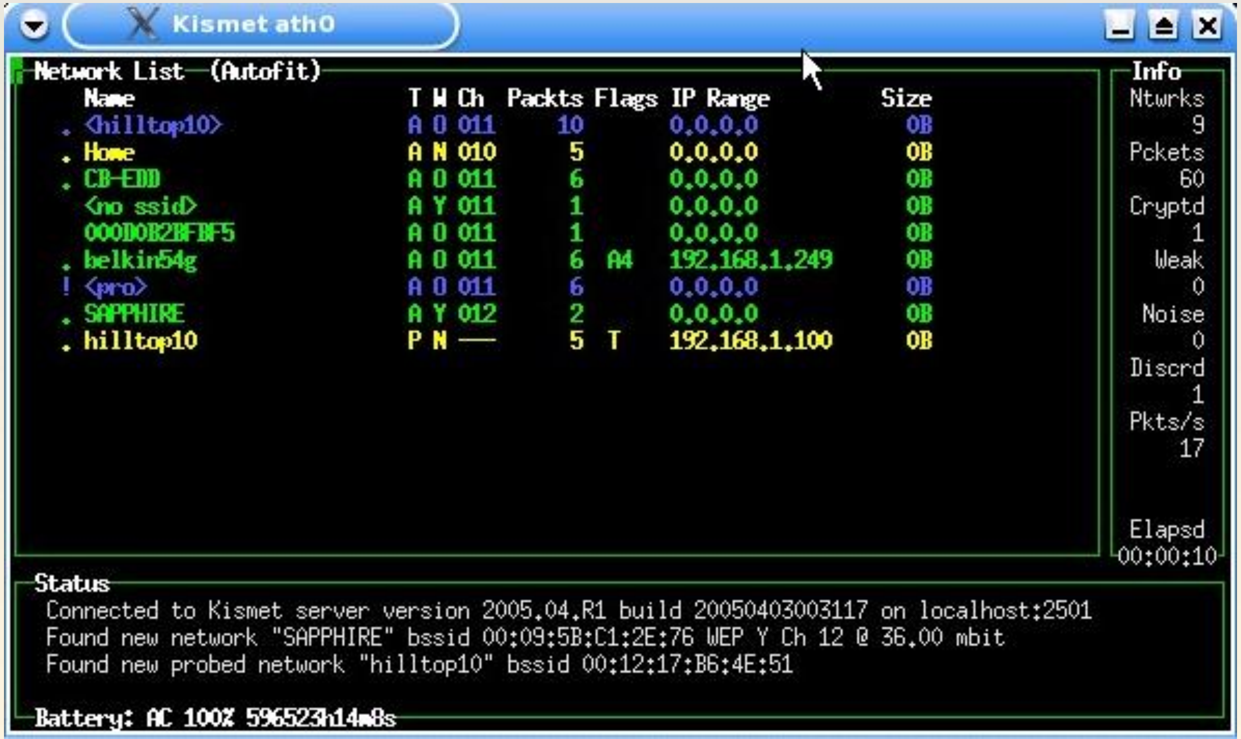
Kismet is an 802.11 wireless network discovery tool and logger.

Any wireless card which is capable of reporting raw packets should work with Kismet.

It is excellent for analyzing a target network.

Kismet will attempt to put the wireless card into promiscuous mode, ready to intercept data not destined for the NIC.

A port has been made to MAC OSX – KisMAC. It incorporates automated passive WEP cracking and WPA dictionary attacks.



```
Network List (Autofit)                                                  Info
     Name                   T W Ch  Packts Flags IP Range       Size    Ntwrks
   . <hilltop10>            A O 011     10       0.0.0.0          0B         9
   . Home                   A N 010      5       0.0.0.0          0B    Pckets
   . CB-EDD                 A O 011      6       0.0.0.0          0B        60
     <no ssid>              A Y 011      1       0.0.0.0          0B    Cryptd
     000D0B2BFBF5           A O 011      1       0.0.0.0          0B         1
   . belkin54g              A O 011      6  A4   192.168.1.249    0B      Weak
   ! <pro>                  A O 011      6       0.0.0.0          0B         0
   . SAPPHIRE               A Y 012      2       0.0.0.0          0B     Noise
   . hilltop10              P N ---      5  T    192.168.1.100    0B         0
                                                                        Discrd
                                                                             1
                                                                        Pkts/s
                                                                            17

                                                                        Elapsd
                                                                      00:00:10
Status
 Connected to Kismet server version 2005.04.R1 build 20050403003117 on localhost:2501
 Found new network "SAPPHIRE" bssid 00:09:5B:C1:2E:76 WEP Y Ch 12 @ 36.00 mbit
 Found new probed network "hilltop10" bssid 00:12:17:B6:4E:51

Battery: AC 100% 596523h14m8s
```

Tool: Aircrack-ng Suite

aircrack-ng

airdecap-ng

aireplay-ng

airmon-ng

airodump-ng

airtun-ng

packetforge-ng

airbase-ng

airdecloak-ng

airdriver-ng

airdrop-ng

airgraph-ng

airolib-ng

airserv-ng

easside-ng

tkiptun-ng

wesside-ng

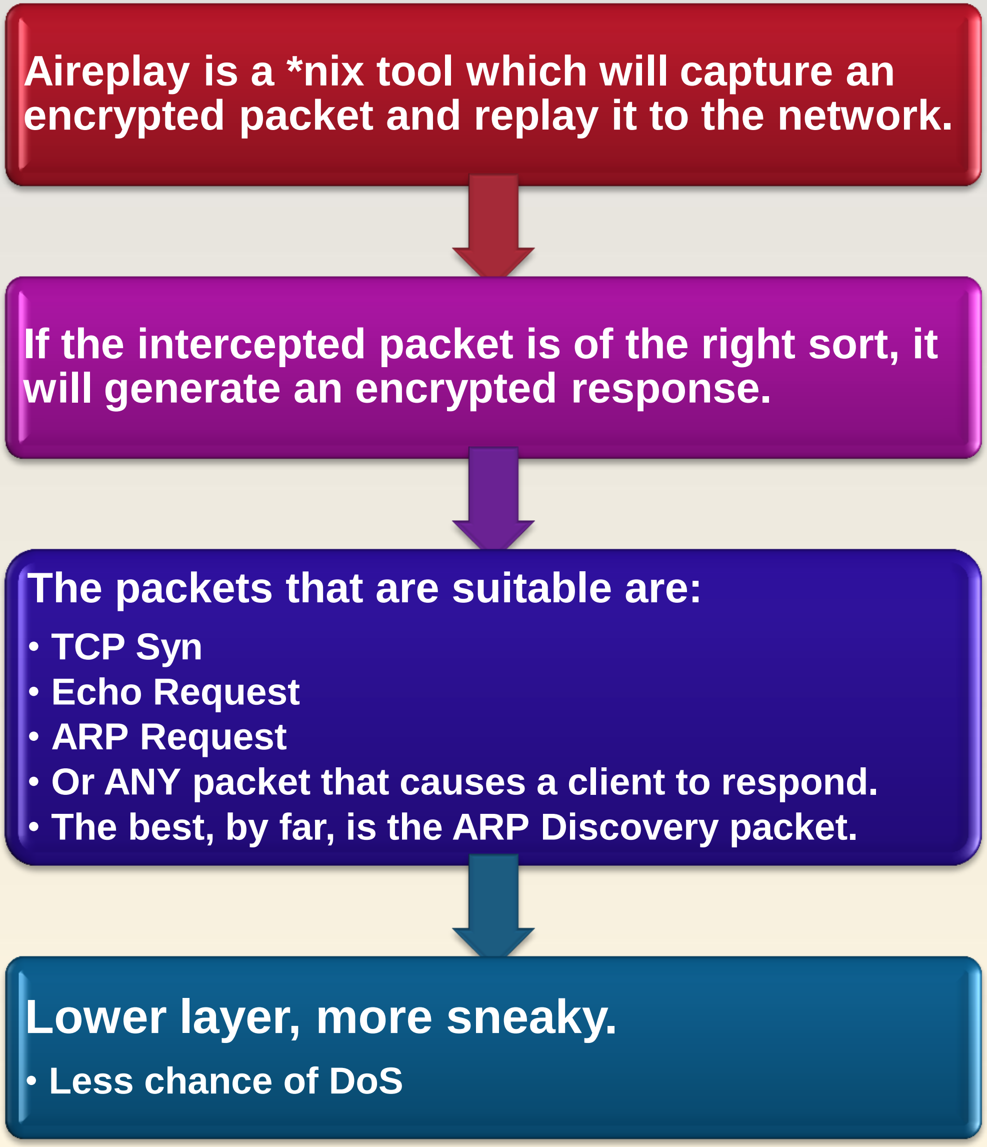
Tool: Airodump-ng

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng.

If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points.

Additionally, airodump-ng writes out a text file containing the details of all access points and clients seen.

Tool: Aireplay



Aireplay is a *nix tool which will capture an encrypted packet and replay it to the network.

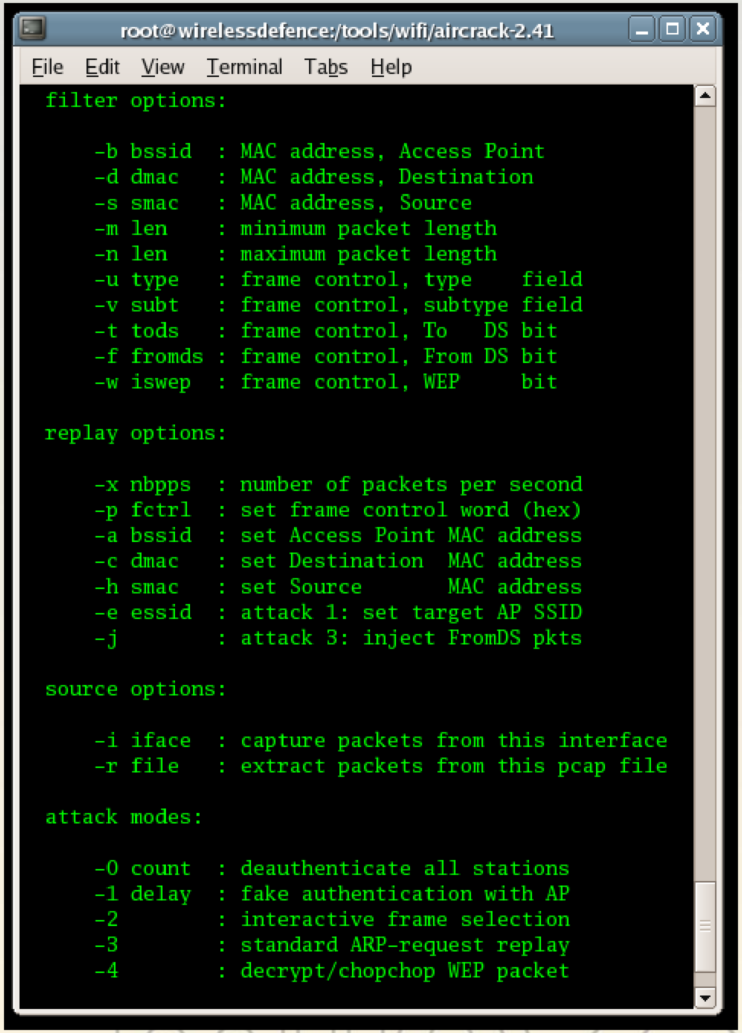
If the intercepted packet is of the right sort, it will generate an encrypted response.

The packets that are suitable are:

- TCP Syn
- Echo Request
- ARP Request
- Or ANY packet that causes a client to respond.
- The best, by far, is the ARP Discovery packet.

Lower layer, more sneaky.

- Less chance of DoS

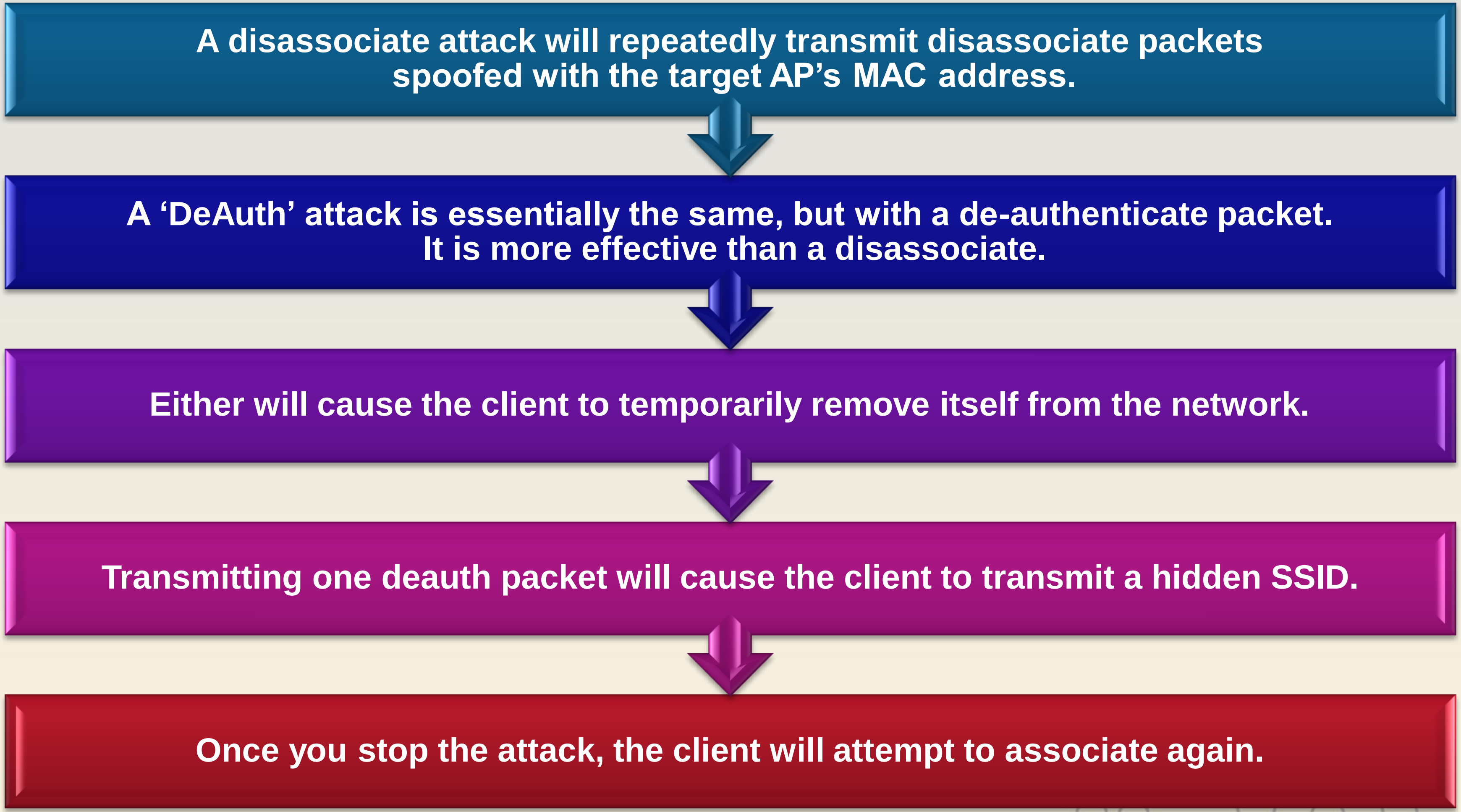


root@wirelessdefence:/tools/wifi/aircrack-2.41
File Edit View Terminal Tabs Help

```
filter options:

    -b bssid  : MAC address, Access Point
    -d dmac   : MAC address, Destination
    -s smac   : MAC address, Source
    -m len    : minimum packet length
    -n len    : maximum packet length
    -u type   : frame control, type    field
    -v subt   : frame control, subtype field
    -t tods   : frame control, To   DS bit
    -f fromds : frame control, From DS bit
    -w iswep  : frame control, WEP     bit

replay options:

    -x nbpps  : number of packets per second
    -p fctrl  : set frame control word (hex)
    -a bssid  : set Access Point MAC address
    -c dmac   : set Destination  MAC address
    -h smac   : set Source       MAC address
    -e essid  : attack 1: set target AP SSID
    -j        : attack 3: inject FromDS pkts

source options:

    -i iface  : capture packets from this interface
    -r file   : extract packets from this pcap file

attack modes:

    -0 count  : deauthenticate all stations
    -1 delay  : fake authentication with AP
    -2        : interactive frame selection
    -3        : standard ARP-request replay
    -4        : decrypt/chopchop WEP packet
```

mile2.com

DOS: Deauth/disassociate attack



A disassociate attack will repeatedly transmit disassociate packets spoofed with the target AP’s MAC address.

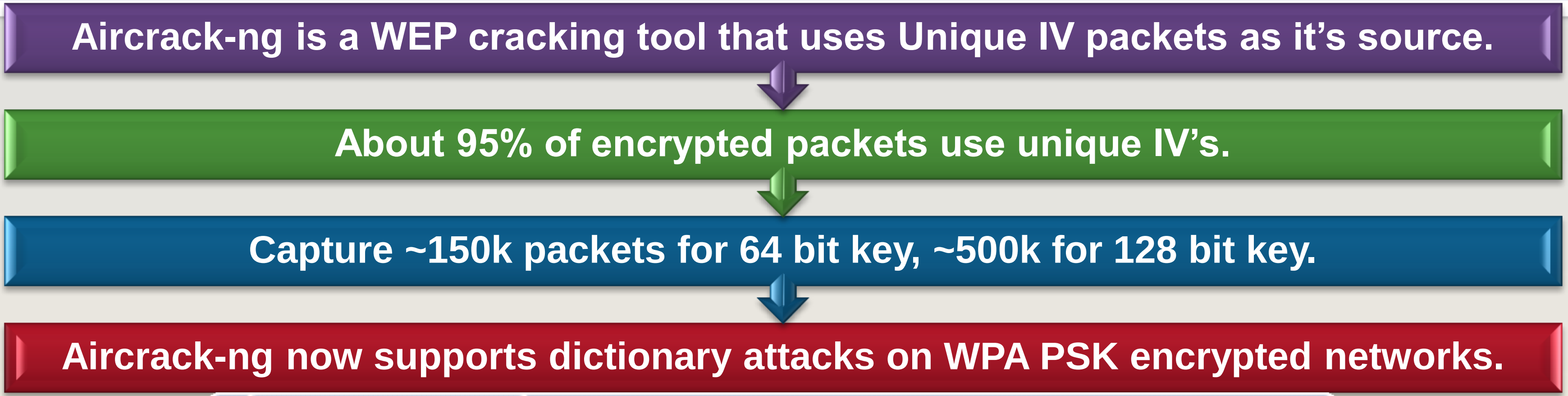
A ‘DeAuth’ attack is essentially the same, but with a de-authenticate packet. It is more effective than a disassociate.

Either will cause the client to temporarily remove itself from the network.

Transmitting one deauth packet will cause the client to transmit a hidden SSID.

Once you stop the attack, the client will attempt to associate again.

Tool: Aircrack-ng

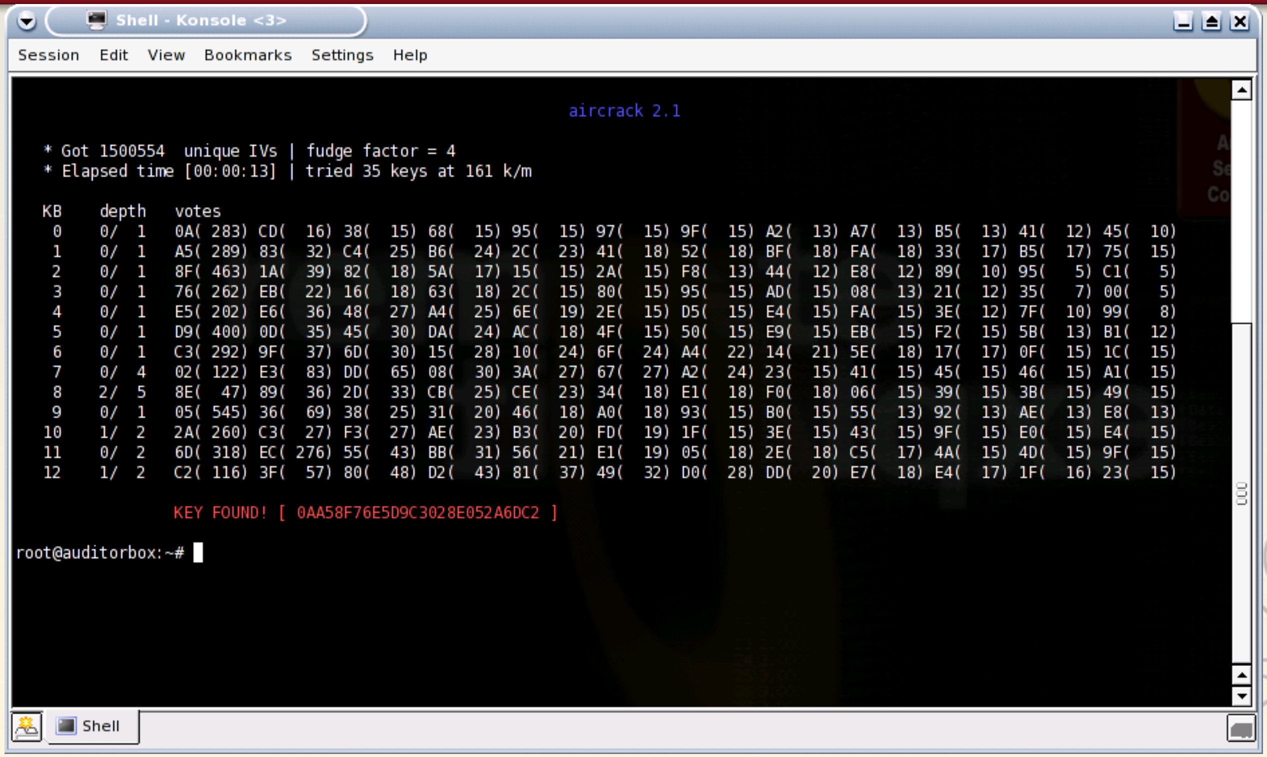


Aircrack-ng is a WEP cracking tool that uses Unique IV packets as it’s source.

About 95% of encrypted packets use unique IV’s.

Capture ~150k packets for 64 bit key, ~500k for 128 bit key.

Aircrack-ng now supports dictionary attacks on WPA PSK encrypted networks.



```
                                              aircrack 2.1

 * Got 1500554  unique IVs | fudge factor = 4
 * Elapsed time [00:00:13] | tried 35 keys at 161 k/m

 KB    depth   votes
  0    0/  1   0A( 283) CD(  16) 38(  15) 68(  15) 95(  15) 97(  15) 9F(  15) A2(  13) A7(  13) B5(  13) 41(  12) 45(  10)
  1    0/  1   A5( 289) 83(  32) C4(  25) B6(  24) 2C(  23) 41(  18) 52(  18) BF(  18) FA(  18) 33(  17) B5(  17) 75(  15)
  2    0/  1   8F( 463) 1A(  39) 82(  18) 5A(  17) 15(  15) 2A(  15) F8(  13) 44(  12) E8(  12) 89(  10) 95(   5) C1(   5)
  3    0/  1   76( 262) EB(  22) 16(  18) 63(  18) 2C(  15) 80(  15) 95(  15) AD(  15) 08(  13) 21(  12) 35(   7) 00(   5)
  4    0/  1   E5( 202) E6(  36) 48(  27) A4(  25) 6E(  19) 2E(  15) D5(  15) E4(  15) FA(  15) 3E(  12) 7F(  10) 99(   8)
  5    0/  1   D9( 400) 0D(  35) 45(  30) DA(  24) AC(  18) 4F(  15) 50(  15) E9(  15) EB(  15) F2(  15) 5B(  13) B1(  12)
  6    0/  1   C3( 292) 9F(  37) 6D(  30) 15(  28) 10(  24) 6F(  24) A4(  22) 14(  21) 5E(  18) 17(  17) 0F(  15) 1C(  15)
  7    0/  4   02( 122) E3(  83) DD(  65) 08(  30) 3A(  27) 67(  27) A2(  24) 23(  15) 41(  15) 45(  15) 46(  15) A1(  15)
  8    2/  5   8E(  47) 89(  36) 2D(  33) CB(  25) CE(  23) 34(  18) E1(  18) F0(  18) 06(  15) 39(  15) 3B(  15) 49(  15)
  9    0/  1   05( 545) 36(  69) 38(  25) 31(  20) 46(  18) A0(  18) 93(  15) B0(  15) 55(  13) 92(  13) AE(  13) E8(  13)
 10    1/  2   2A( 260) C3(  27) F3(  27) AE(  23) B3(  20) FD(  19) 1F(  15) 3E(  15) 43(  15) 9F(  15) E0(  15) E4(  15)
 11    0/  2   6D( 318) EC( 276) 55(  43) BB(  31) 56(  21) E1(  19) 05(  18) 2E(  18) C5(  17) 4A(  15) 4D(  15) 9F(  15)
 12    1/  2   C2( 116) 3F(  57) 80(  48) D2(  43) 81(  37) 49(  32) D0(  28) DD(  20) E7(  18) E4(  17) 1F(  16) 23(  15)

               KEY FOUND! [ 0AA58F76E5D9C3028E052A6DC2 ]

root@auditorbox:~#
```

Attacking WEP

You will need to record the following items from Kismet or Airodump-ng.

- ESSID (network name), BSSID (access point MAC address), Channel number, and a client's MAC address.

Start packet capturing with Airodump-ng.

Start injecting packets using Aireplay-ng.

Perform a Deauthentication / Disassociation attack.

Once 150,000 packets are captured, start cracking a 40-bit WEP key.
A 104-bit WEP key requires 500,000 packets.

Crack the WEP key with Aircrack-ng.

Attacking WPA

You will need to record the following items in Kismet.

- ESSID, BSSID, Channel, and a client's MAC address.

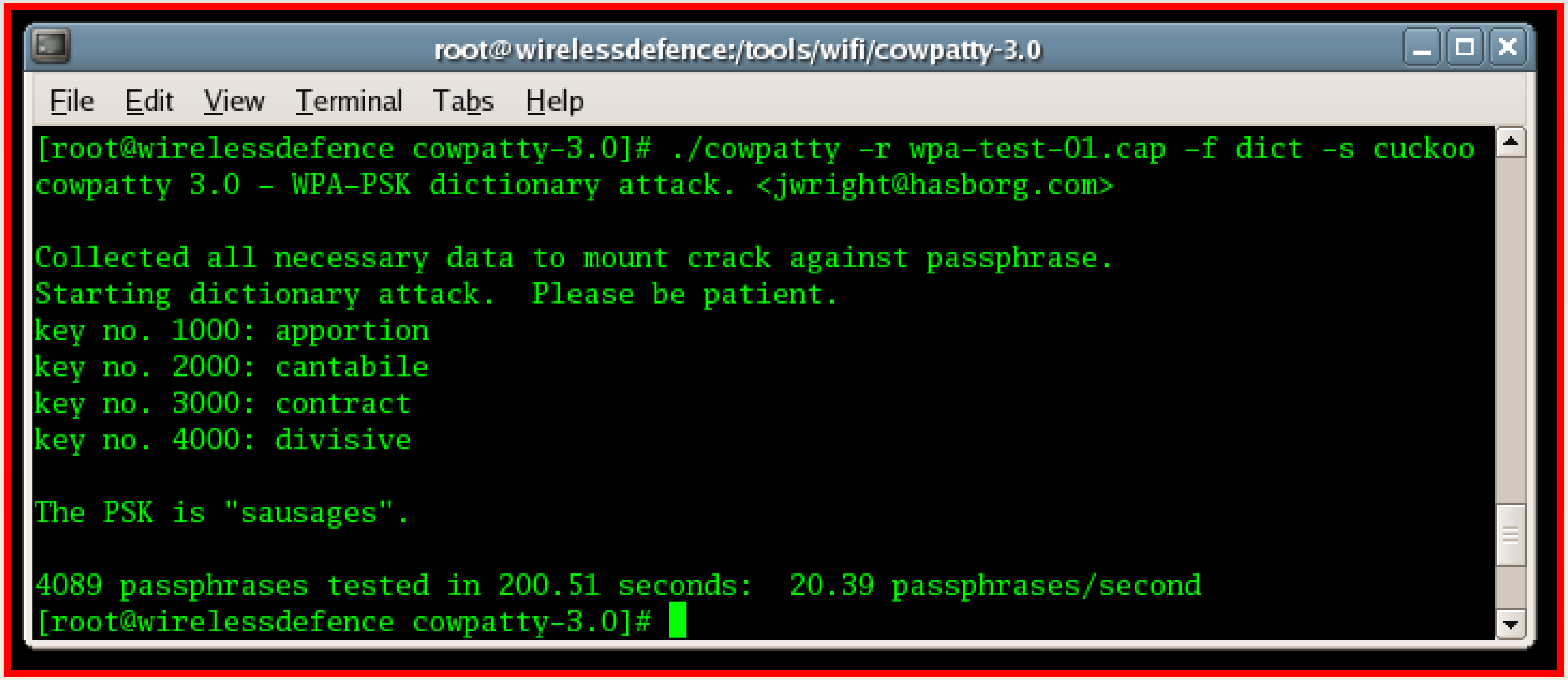
Start packet capturing with Airodump-ng.

Perform a Deauthentication / Disassociation attack.

Once you have captured the complete 4 way handshake, you can perform your dictionary attack using aircrack-ng or you could use coWPAtty.

"coWPAtty is designed to audit the pre-shared key (PSK) selection for WPA networks based on the TKIP protocol." - Joshua Wright.

coWPAtty


root@wirelessdefence:/tools/wifi/cowpatty-3.0
File Edit View Terminal Tabs Help

```
[root@wirelessdefence cowpatty-3.0]# ./cowpatty -r wpa-test-01.cap -f dict -s cuckoo
cowpatty 3.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against passphrase.
Starting dictionary attack.  Please be patient.
key no. 1000: apportion
key no. 2000: cantabile
key no. 3000: contract
key no. 4000: divisive

The PSK is "sausages".

4089 passphrases tested in 200.51 seconds:  20.39 passphrases/second
[root@wirelessdefence cowpatty-3.0]#
```

http://www.wirelessdefence.org/Contents/coWPAttyMain.htm
http://www.willhackforsushi.com/Cowpatty.html

Exploiting Cisco LEAP

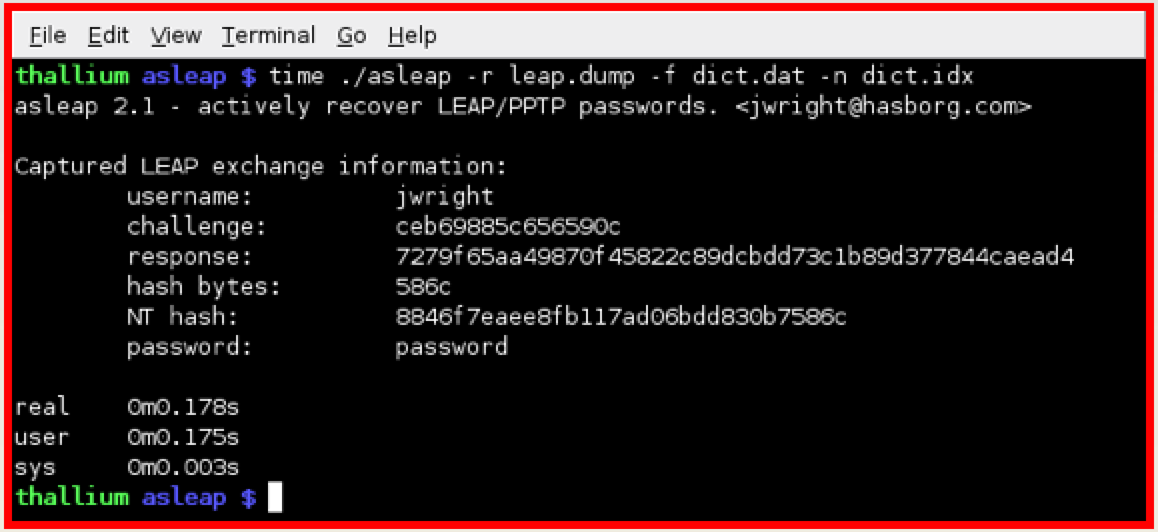
Tools such as asleap, thc-LEAPcracker, anwrap and kisMAC.

As in "asleap behind the wheel".
- Joshua Wright

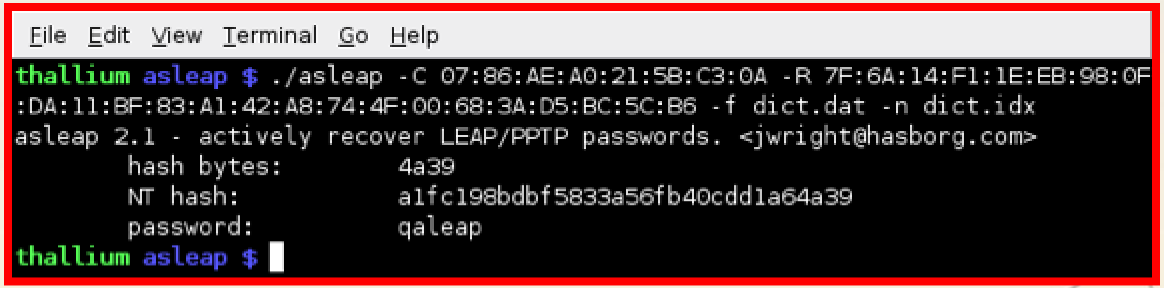
“Within months, some "helpful" person invested their time into generating a cracker tool. Publicizing the threat was a service to everyone, but I leave it as an exercise for readers to determine what satisfaction is obtained by the authors of tools that turn threat into reality and lay waste to millions of dollars of investments.”
"Real 802.11 Security", William Arbaugh and Jon Edney

Laying waste to millions of networks since epoch();

asleap



```
thallium asleap $ time ./asleap -r leap.dump -f dict.dat -n dict.idx
asleap 2.1 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>

Captured LEAP exchange information:
        username:             jwright
        challenge:            ceb69885c656590c
        response:             7279f65aa49870f45822c89dcbdd73c1b89d377844caead4
        hash bytes:           586c
        NT hash:              8846f7eaee8fb117ad06bdd830b7586c
        password:             password

real    0m0.178s
user    0m0.175s
sys     0m0.003s
thallium asleap $
```



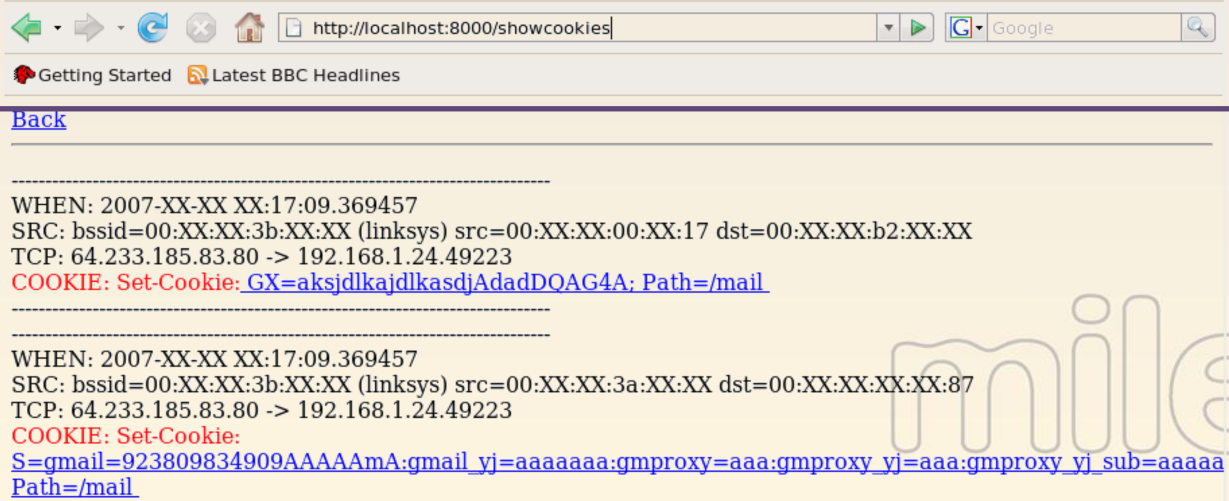
```
thallium asleap $ ./asleap -C 07:86:AE:A0:21:5B:C3:0A -R 7F:6A:14:F1:1E:EB:98:0F
:DA:11:BF:83:A1:42:A8:74:4F:00:68:3A:D5:BC:5C:B6 -f dict.dat -n dict.idx
asleap 2.1 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
        hash bytes:           4a39
        NT hash:              a1fc198bdbf5833a56fb40cdd1a64a39
        password:             qaleap
thallium asleap $
```

http://www.willhackforsushi.com/Asleap.html

WiFiZoo

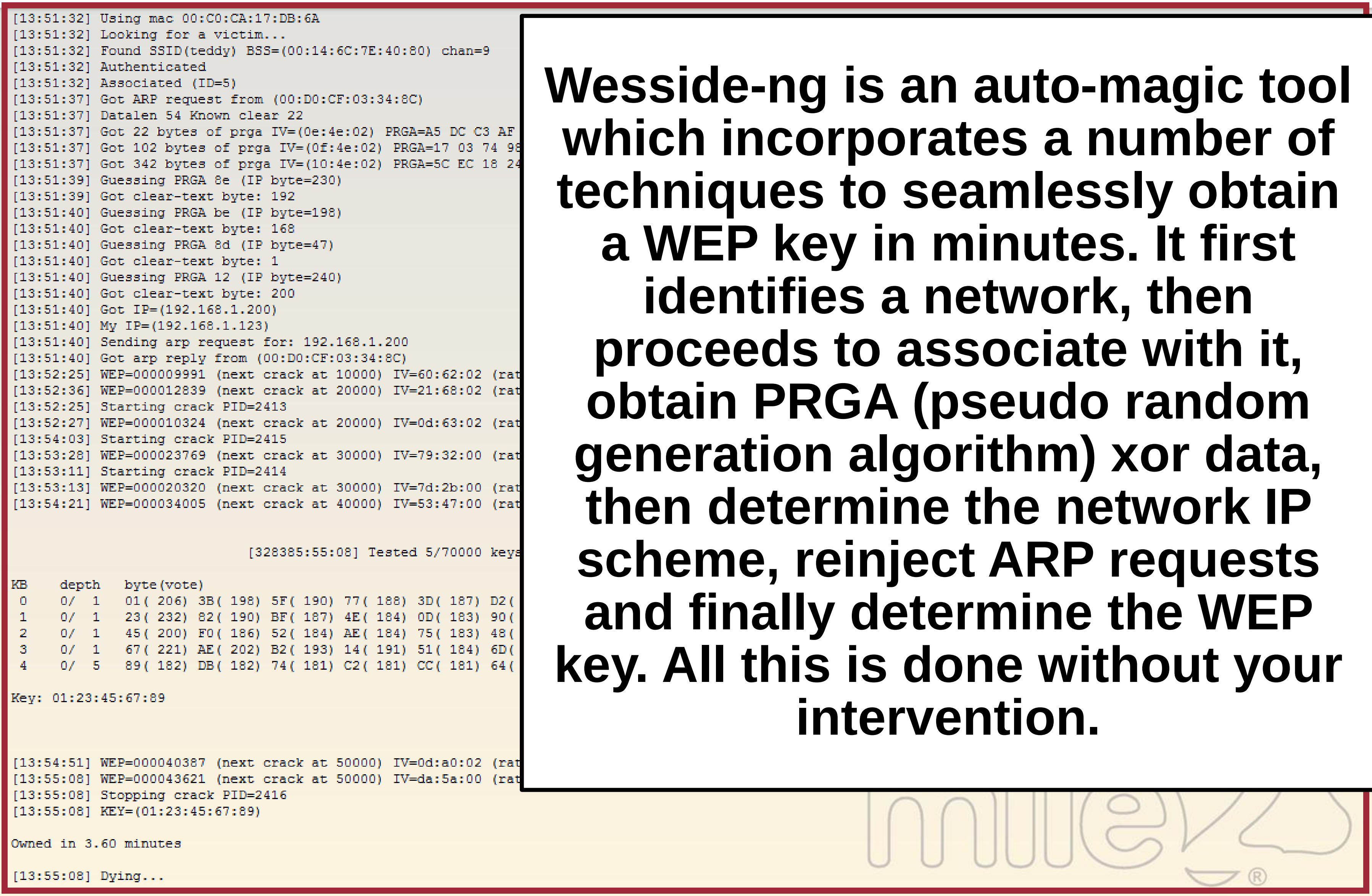
WifiZoo does the following:

- Gathers BSSID
- Gathers list of unique SSIDS
- Gathers the list and graphs which SSIDS are being probed from what sources
- Gathers BSSID client information and outputs it in a file that you can later use with graphviz and get a graph with "802.11 bssids->clients".
- Gathers 'useful' information from unencrypted wifi traffic (ala Ferret,and dsniff, etc); like pop3 credentials, smtp traffic, http cookies/authinfo, msn messages,ftp credentials, telnet network traffic, nbt, etc.
- http://community.corest.com/~hochoa/wifizoo/index.html



```
------------------------------------------------------------------------
WHEN: 2007-XX-XX XX:17:09.369457
SRC: bssid=00:XX:XX:3b:XX:XX (linksys) src=00:XX:XX:00:XX:17 dst=00:XX:XX:b2:XX:XX
TCP: 64.233.185.83.80 -> 192.168.1.24.49223
COOKIE: Set-Cookie: GX=aksjdlkajdlkasdjAdadDQAG4A; Path=/mail
------------------------------------------------------------------------
------------------------------------------------------------------------
WHEN: 2007-XX-XX XX:17:09.369457
SRC: bssid=00:XX:XX:3b:XX:XX (linksys) src=00:XX:XX:3a:XX:XX dst=00:XX:XX:XX:XX:87
TCP: 64.233.185.83.80 -> 192.168.1.24.49223
COOKIE: Set-Cookie:
S=gmail=923809834909AAAAmA:gmail_yj=aaaaaaa:gmproxy=aaa:gmproxy_yj=aaa:gmproxy_yj_sub=aaaaa
Path=/mail
```

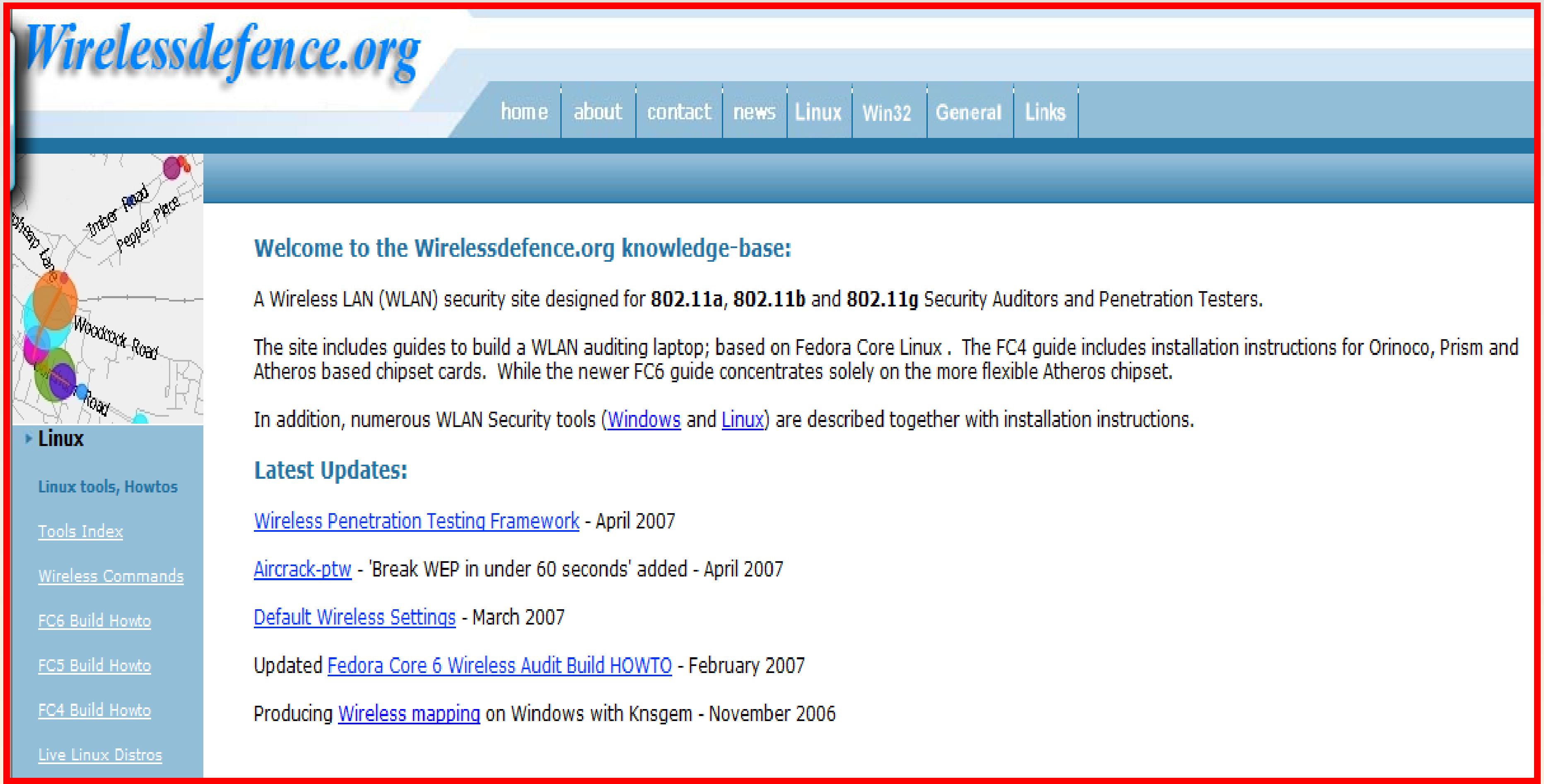
Wesside-ng



```
[13:51:32] Using mac 00:C0:CA:17:DB:6A
[13:51:32] Looking for a victim...
[13:51:32] Found SSID(teddy) BSS=(00:14:6C:7E:40:80) chan=9
[13:51:32] Authenticated
[13:51:32] Associated (ID=5)
[13:51:37] Got ARP request from (00:D0:CF:03:34:8C)
[13:51:37] Datalen 54 Known clear 22
[13:51:37] Got 22 bytes of prga IV=(0e:4e:02) PRGA=A5 DC C3 AF
[13:51:37] Got 102 bytes of prga IV=(0f:4e:02) PRGA=17 03 74 98
[13:51:37] Got 342 bytes of prga IV=(10:4e:02) PRGA=5C EC 18 24
[13:51:39] Guessing PRGA 8e (IP byte=230)
[13:51:39] Got clear-text byte: 192
[13:51:40] Guessing PRGA be (IP byte=198)
[13:51:40] Got clear-text byte: 168
[13:51:40] Guessing PRGA 8d (IP byte=47)
[13:51:40] Got clear-text byte: 1
[13:51:40] Guessing PRGA 12 (IP byte=240)
[13:51:40] Got clear-text byte: 200
[13:51:40] Got IP=(192.168.1.200)
[13:51:40] My IP=(192.168.1.123)
[13:51:40] Sending arp request for: 192.168.1.200
[13:51:40] Got arp reply from (00:D0:CF:03:34:8C)
[13:52:25] WEP=000009991 (next crack at 10000) IV=60:62:02 (rat
[13:52:36] WEP=000012839 (next crack at 20000) IV=21:68:02 (rat
[13:52:25] Starting crack PID=2413
[13:52:27] WEP=000010324 (next crack at 20000) IV=0d:63:02 (rat
[13:54:03] Starting crack PID=2415
[13:53:28] WEP=000023769 (next crack at 30000) IV=79:32:00 (rat
[13:53:11] Starting crack PID=2414
[13:53:13] WEP=000020320 (next crack at 30000) IV=7d:2b:00 (rat
[13:54:21] WEP=000034005 (next crack at 40000) IV=53:47:00 (rat


                               [328385:55:08] Tested 5/70000 keys

KB    depth   byte(vote)
 0    0/  1   01( 206) 3B( 198) 5F( 190) 77( 188) 3D( 187) D2(
 1    0/  1   23( 232) 82( 190) BF( 187) 4E( 184) 0D( 183) 90(
 2    0/  1   45( 200) F0( 186) 52( 184) AE( 184) 75( 183) 48(
 3    0/  1   67( 221) AE( 202) B2( 193) 14( 191) 51( 184) 6D(
 4    0/  5   89( 182) DB( 182) 74( 181) C2( 181) CC( 181) 64(

Key: 01:23:45:67:89



[13:54:51] WEP=000040387 (next crack at 50000) IV=0d:a0:02 (rat
[13:55:08] WEP=000043621 (next crack at 50000) IV=da:5a:00 (rat
[13:55:08] Stopping crack PID=2416
[13:55:08] KEY=(01:23:45:67:89)

Owned in 3.60 minutes

[13:55:08] Dying...
```

Wesside-ng is an auto-magic tool which incorporates a number of techniques to seamlessly obtain a WEP key in minutes. It first identifies a network, then proceeds to associate with it, obtain PRGA (pseudo random generation algorithm) xor data, then determine the network IP scheme, reinject ARP requests and finally determine the WEP key. All this is done without your intervention.

www.wirelessdefence.org



Linux

Linux tools, Howtos

Tools Index

Wireless Commands

FC6 Build Howto

FC5 Build Howto

FC4 Build Howto

Live Linux Distros

Welcome to the Wirelessdefence.org knowledge-base:

A Wireless LAN (WLAN) security site designed for **802.11a**, **802.11b** and **802.11g** Security Auditors and Penetration Testers.

The site includes guides to build a WLAN auditing laptop; based on Fedora Core Linux . The FC4 guide includes installation instructions for Orinoco, Prism and Atheros based chipset cards. While the newer FC6 guide concentrates solely on the more flexible Atheros chipset.

In addition, numerous WLAN Security tools (Windows and Linux) are described together with installation instructions.

Latest Updates:

Wireless Penetration Testing Framework - April 2007

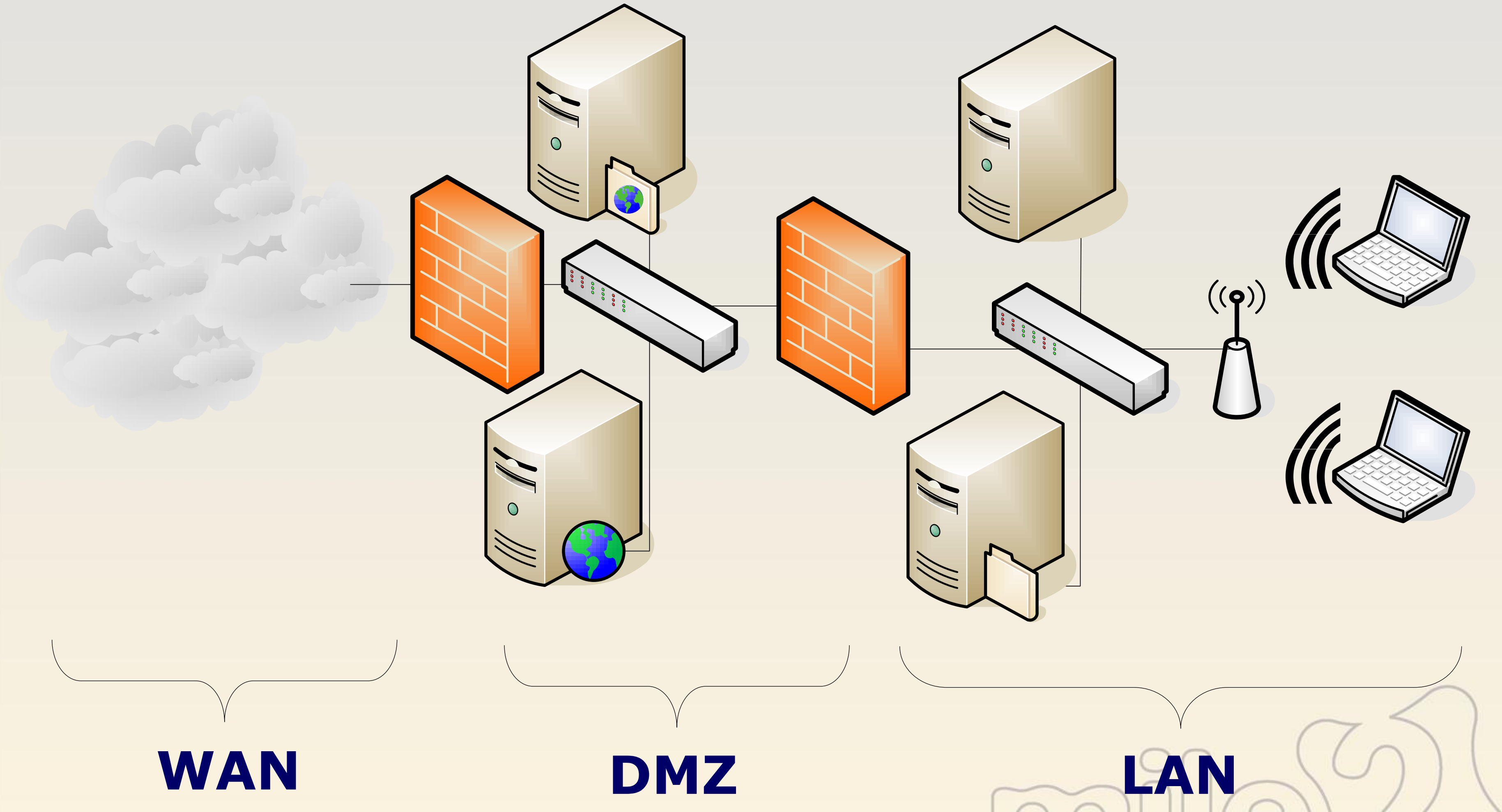
Aircrack-ptw - 'Break WEP in under 60 seconds' added - April 2007

Default Wireless Settings - March 2007

Updated Fedora Core 6 Wireless Audit Build HOWTO - February 2007

Producing Wireless mapping on Windows with Knsgem - November 2006

Typical Wired/Wireless Network



802.1X: EAP Types

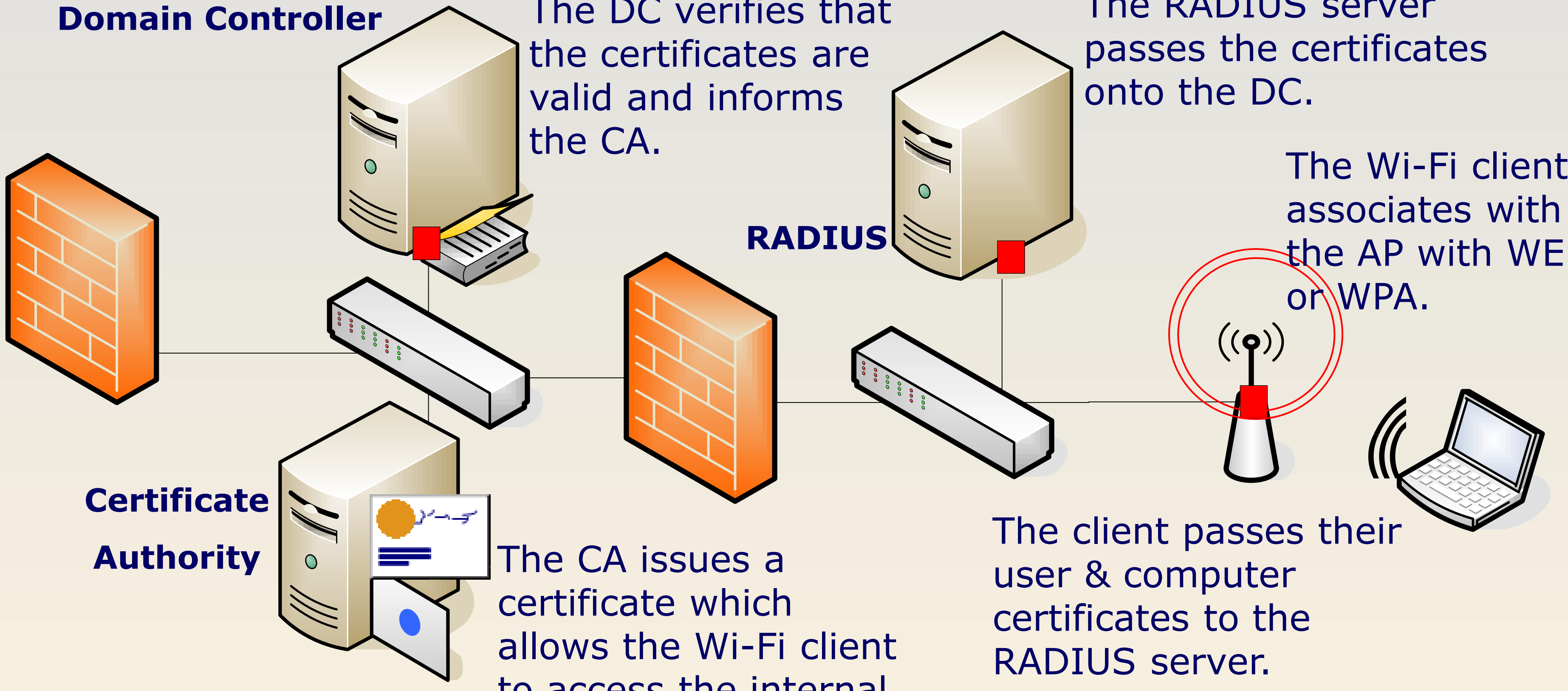
802.1X uses the Extensible Authentication Protocol (EAP) to relay port access requests between WLAN clients (Supplicants), wireless access points (Authenticators), and RADIUS/IAS servers (Authentication Servers).

This will prevent an attacker from accessing the wired network without an authentic logon even if they have broken the encryption key.

EAP Advantages/Disadvantages

	EAP-TLS	EAP-TTLS	PEAP
Server Authentication	Public Key Certificate	Public Key Certificate	Public Key Certificate
Supplicant Authentication	Public Key Certificate or Smart Card Client Certificate Required	CHAP, PAP, MS-CHAP, MS-CHAP(v2), EAP Client Certificate Optional	Any EAP Method Client Certificate Optional
Fast Session Reconnect	No	Yes	Yes
Security Risks	Identity Exposed	MiTM attack, identity hidden in phase 2 but potential exposure in phase 1	MiTM attack, identity hidden in phase 2 but potential exposure in phase 1
Deployment	Difficult	Moderate	Moderate

EAP/TLS Deployment



The DC verifies that the certificates are valid and informs the CA.

The RADIUS server passes the certificates onto the DC.

The Wi-Fi client associates with the AP with WEP or WPA.

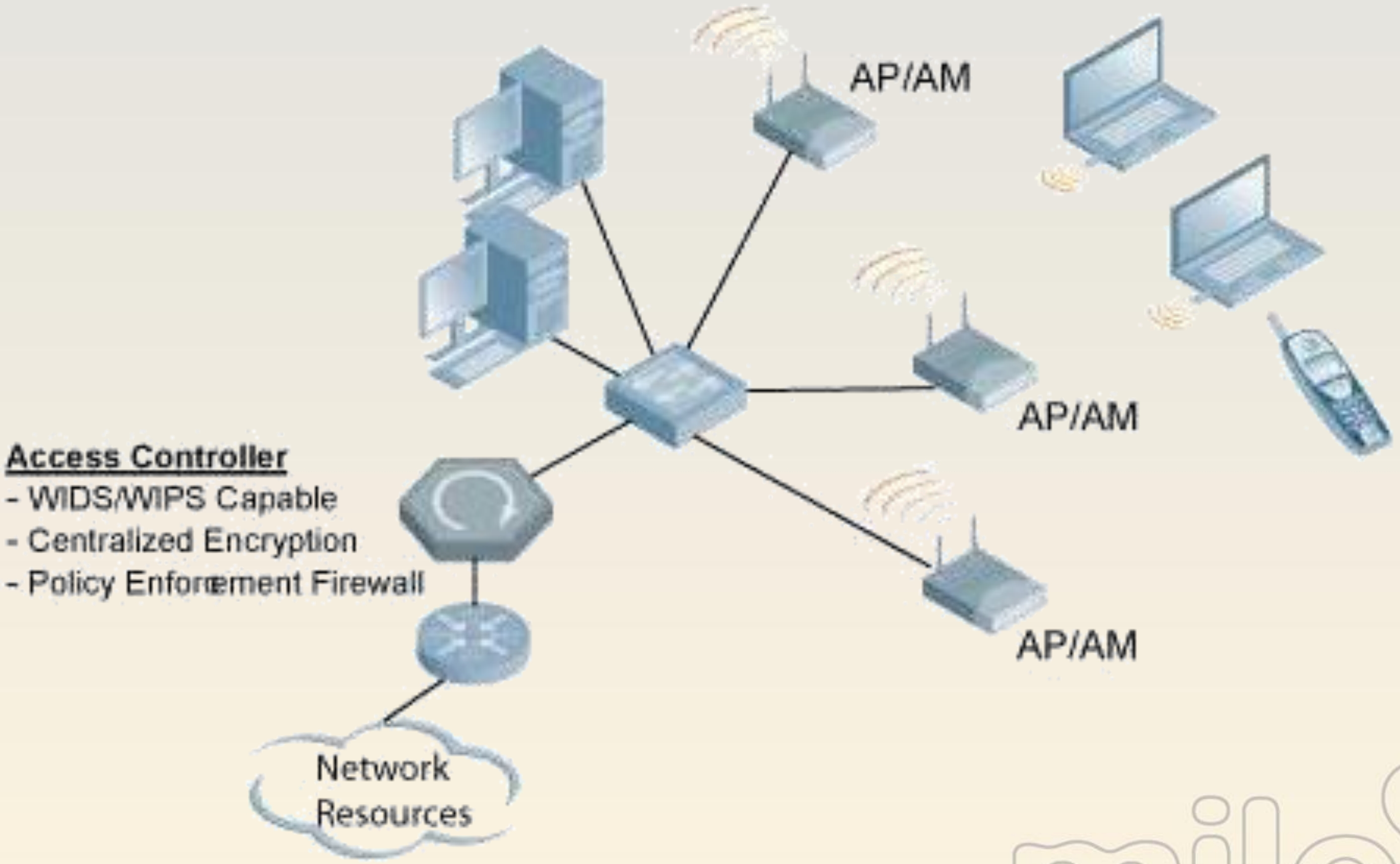
The CA issues a certificate which allows the Wi-Fi client to access the internal LAN.

The client passes their user & computer certificates to the RADIUS server.

Now the client has the required permissions to communicate through the Wi-Fi DMZ firewall.

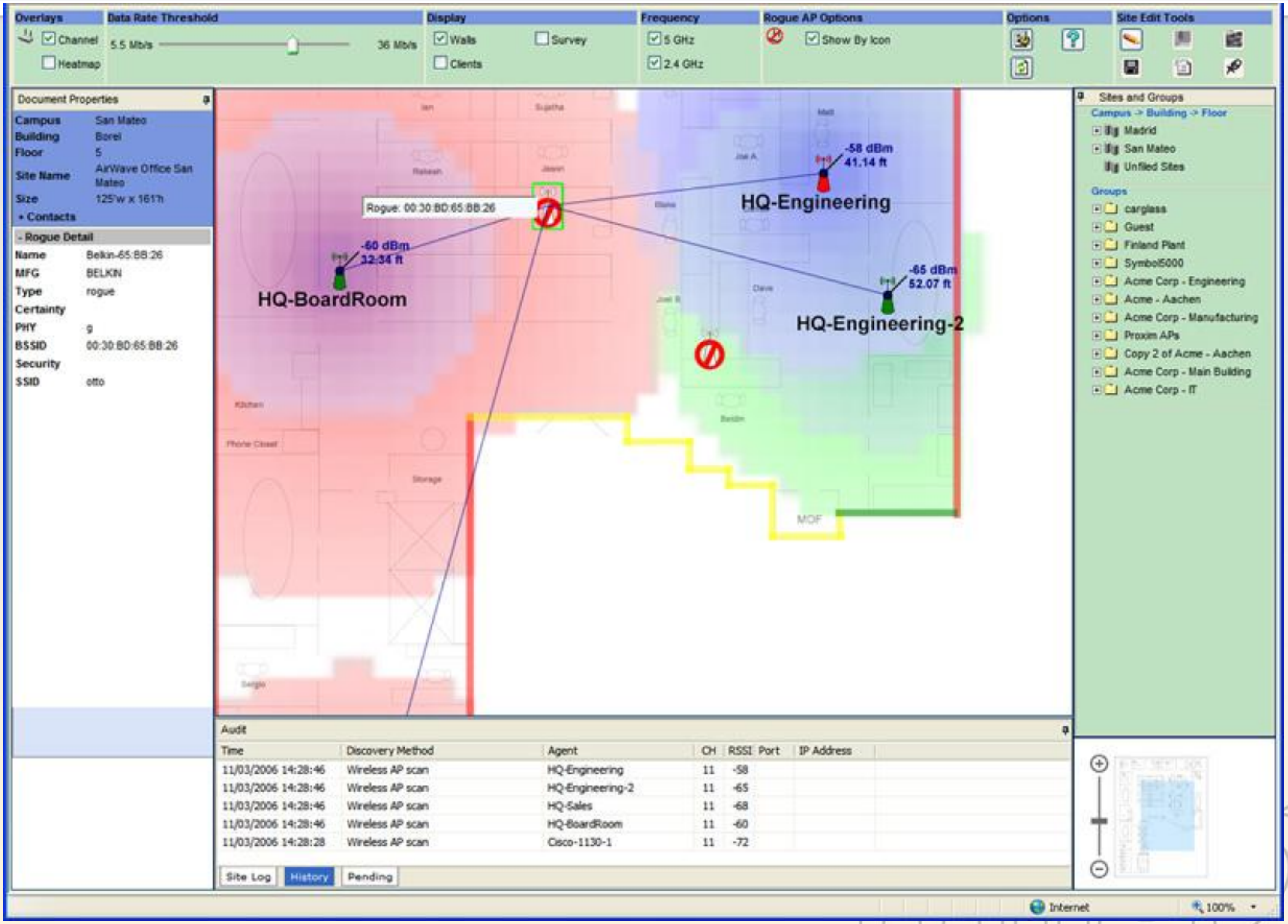
New Age Protection

Aruba – Wireless Intrusion Detection and Prevention



http://www.arubanetworks.com/solutions/use_cases/intrusion_detection.php

RAPIDS Rogue AP Detection Module



Overlays: ☑ Channel ☐ Heatmap

Data Rate Threshold: 5.5 Mb/s – 36 Mb/s

Display: ☑ Walls ☐ Survey ☐ Clients

Frequency: ☑ 5 GHz ☑ 2.4 GHz

Rogue AP Options: ☑ Show By Icon

Options

Site Edit Tools

Document Properties

Campus	San Mateo
Building	Borel
Floor	5
Site Name	AirWave Office San Mateo
Size	125'w x 161'h

• Contacts

- Rogue Detail

Name	Belkin-65:BB:26
MFG	BELKIN
Type	rogue
Certainty	
PHY	g
BSSID	00:30:BD:65:BB:26
Security	
SSID	otto

Sites and Groups

Campus -> Building -> Floor
- Madrid
- San Mateo
- Unfiled Sites

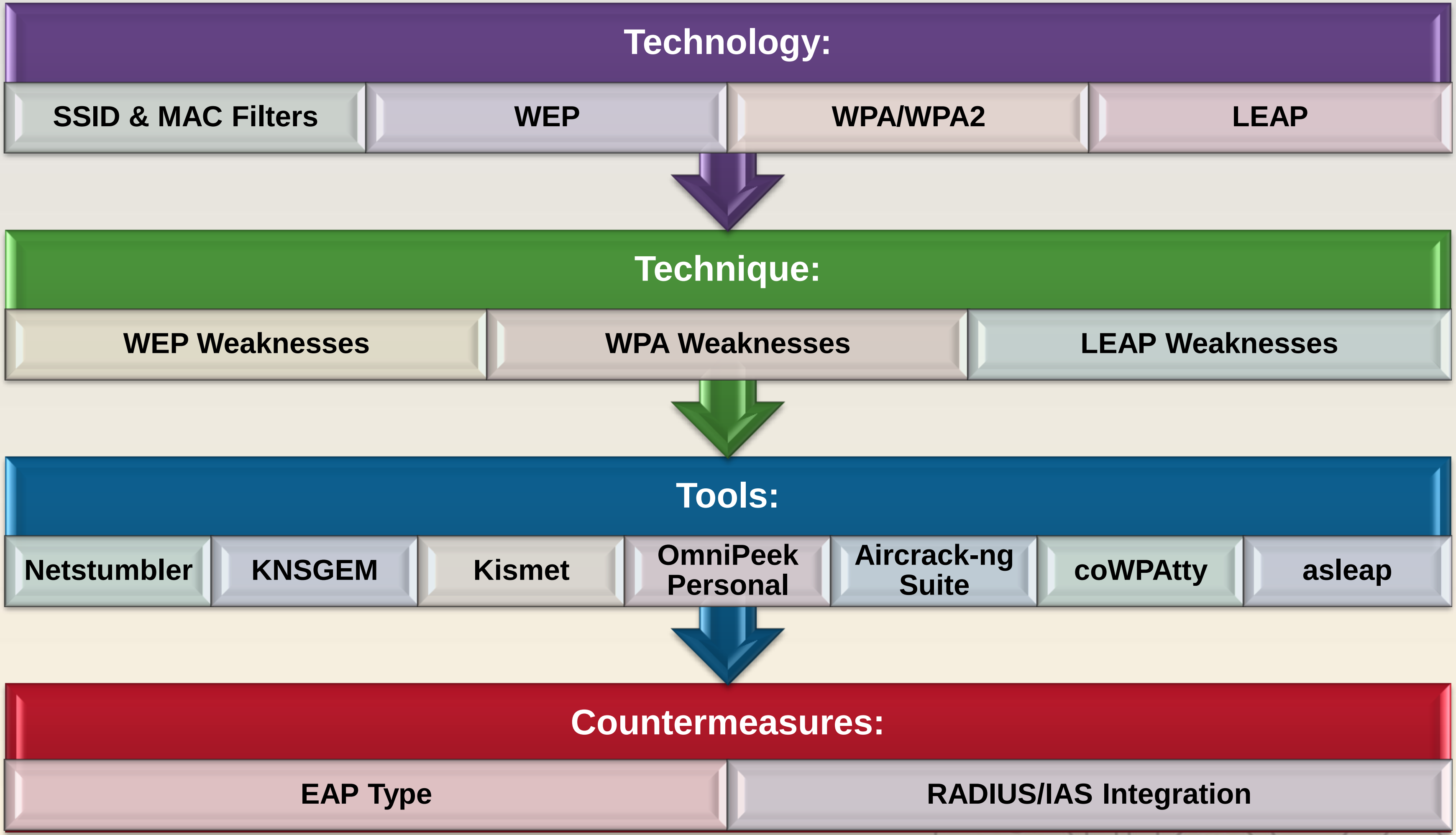
Groups
- cargiass
- Guest
- Finland Plant
- Symbol5000
- Acme Corp - Engineering
- Acme - Aachen
- Acme Corp - Manufacturing
- Proxim APs
- Copy 2 of Acme - Aachen
- Acme Corp - Main Building
- Acme Corp - IT

Audit

Time	Discovery Method	Agent	CH	RSSI	Port	IP Address
11/03/2006 14:28:46	Wireless AP scan	HQ-Engineering	11	-58		
11/03/2006 14:28:46	Wireless AP scan	HQ-Engineering-2	11	-65		
11/03/2006 14:28:46	Wireless AP scan	HQ-Sales	11	-68		
11/03/2006 14:28:46	Wireless AP scan	HQ-BoardRoom	11	-60		
11/03/2006 14:28:28	Wireless AP scan	Cisco-1130-1	11	-72		

http://www.moonblinkwifi.com/pd_rapids.cfm

Review



Technology:

SSID & MAC Filters | WEP | WPA/WPA2 | LEAP

Technique:

WEP Weaknesses | WPA Weaknesses | LEAP Weaknesses

Tools:

Netstumbler | KNSGEM | Kismet | OmniPeek Personal | Aircrack-ng Suite | coWPAtty | asleap

Countermeasures:

EAP Type | RADIUS/IAS Integration

Module 11 Lab
Pen Testing Wireless