

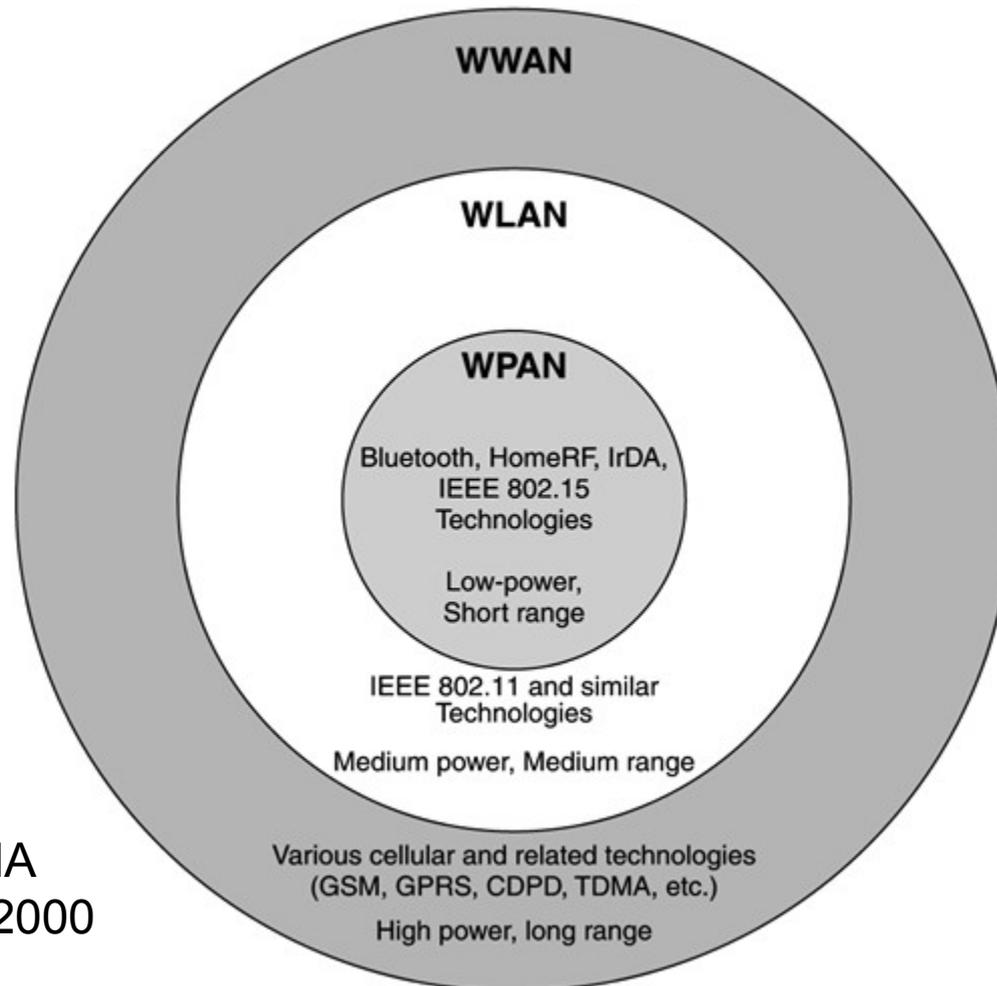


# The golden age of hacking

War Driving

War Dialing

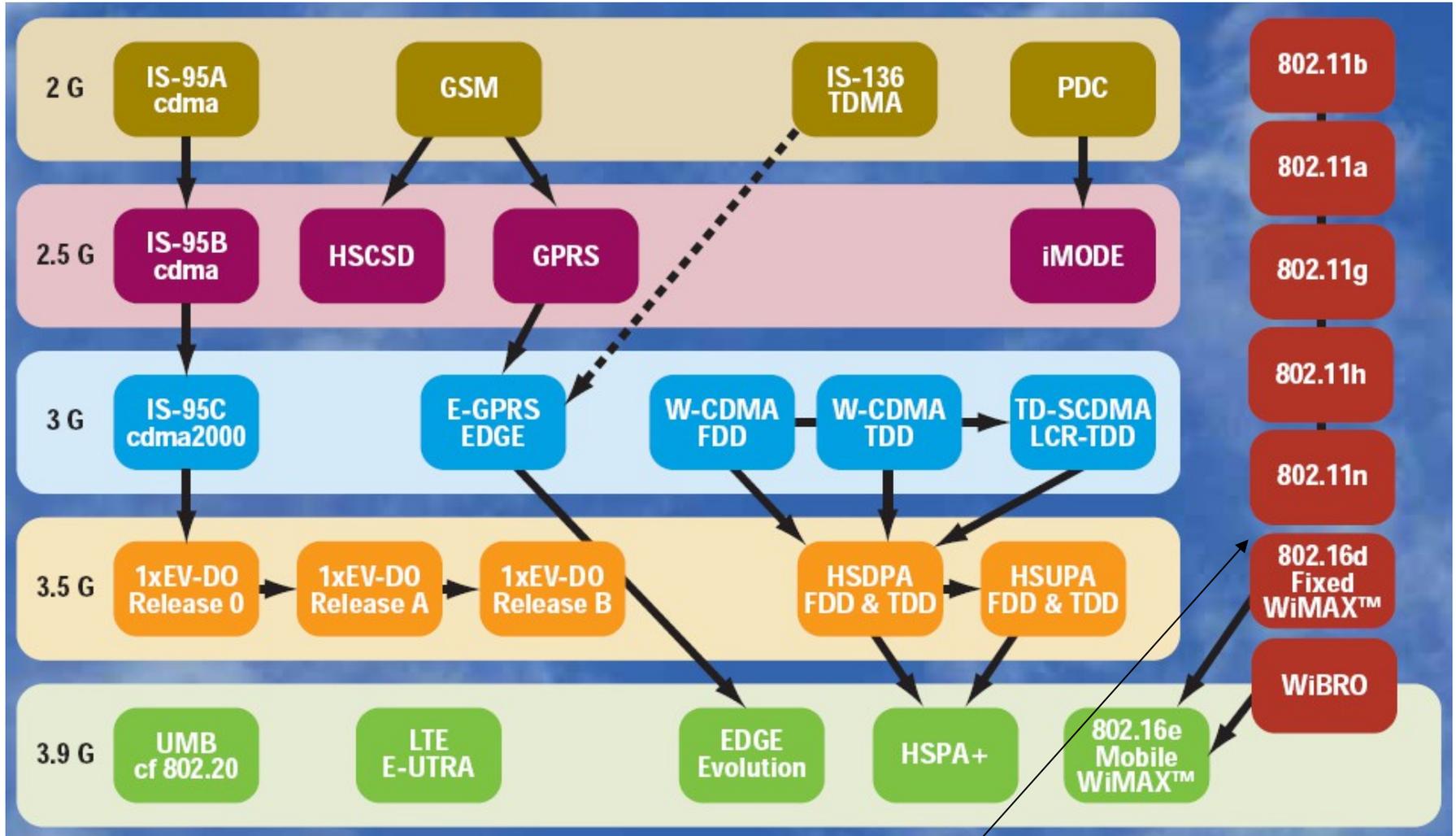
# An overview of modern wireless networks



3G { W-CDMA  
CDMA 2000

4G { WiMAX  
LTE

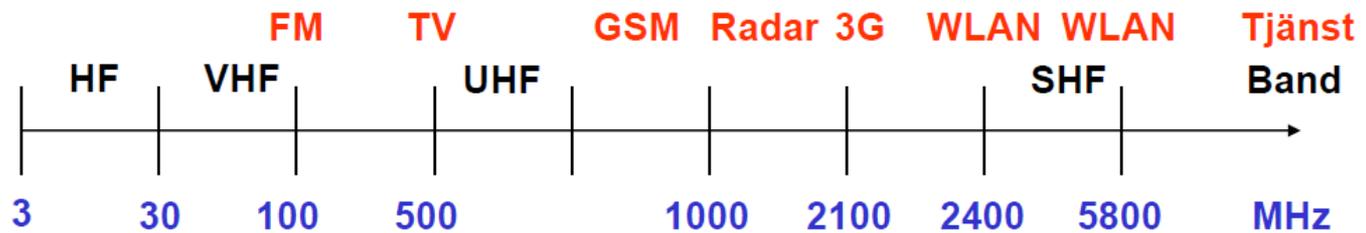
# Evolution of wireless protocols



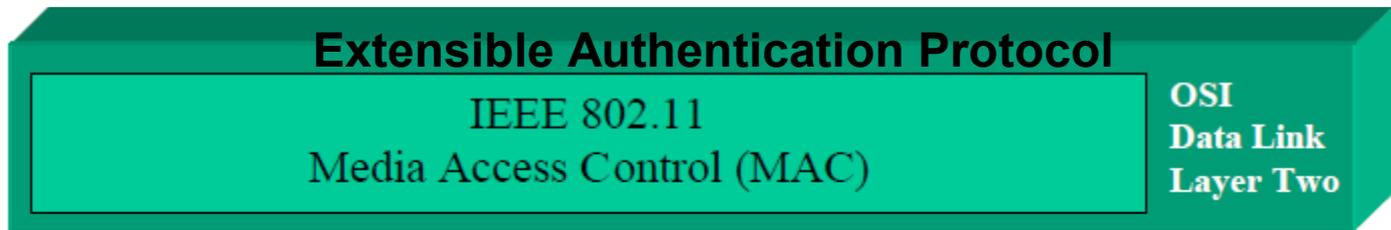
[http://en.wikipedia.org/wiki/IEEE\\_802.11ac](http://en.wikipedia.org/wiki/IEEE_802.11ac)

# OSI model according to IEEE 802.11

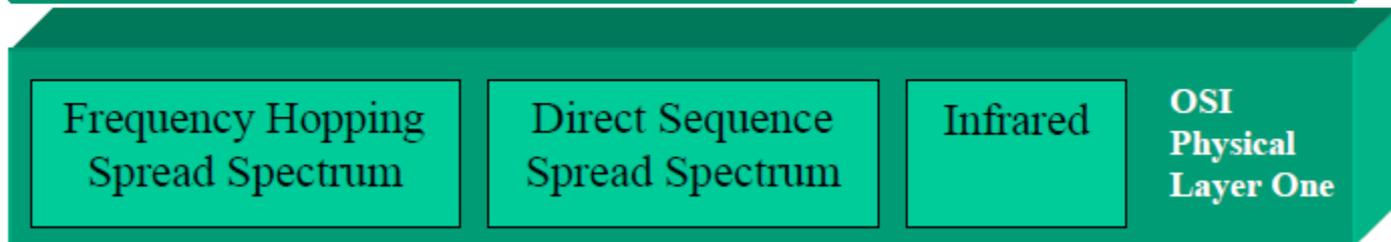
- The MAC layer provides a set of services e.g. data transfer, association, re-association, authentication, privacy, and power management that control the communications between the wireless stations (STA) and access points (AP) over a shared medium
- 802.11a/g/n/ac uses OFDM (Orthogonal Frequency-Division Multiplexing)
  - Same as in ADSL, VDSL, WiMAX, DVB-T(2), LTE etc...



EAP



OFDM



# Worlds largest hotspots 😊

- War Driving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes
- Laptop setup (could also be a PDA)
  - A laptop computer
  - A wireless network interface card (NIC) Card
  - An external antenna
  - A pigtail to connect the external antenna to the wireless NIC
  - A handheld global positioning system (GPS) unit
  - A GPS data cable
  - A War Driving software program
  - A cigarette lighter or AC adapter power inverter
- Mobile phone with built in GPS and Wi-Fi
  - A War Driving software program, no additional equipment needed!



# NIC:s, software etc.

[http://www.aircrack-ng.org/doku.php?id=compatibility\\_drivers](http://www.aircrack-ng.org/doku.php?id=compatibility_drivers)

- ESSID (Extended Service Set Identifier)
  - Default: Netgear, Linksys, Belkin, Dlink etc.
- BSSID (Basic Service Set Identifier)
  - MAC address of the AP or client
- Before purchasing a wireless card, you should determine the software and configuration you plan to use
- Chipset software support
  - Atheros, Ralink, RTL818\*...
  - AirPcap (Windows)
- External antenna?
- Connectors?
- Support for rfmon/monitor mode (passive/sniff scan with no AP connection)
  - rfmon/monitor mode = promiscuous mode ++ (listen on all WLANs)
  - Linux ok
  - Windows - usually not



**USB works in VMware!**

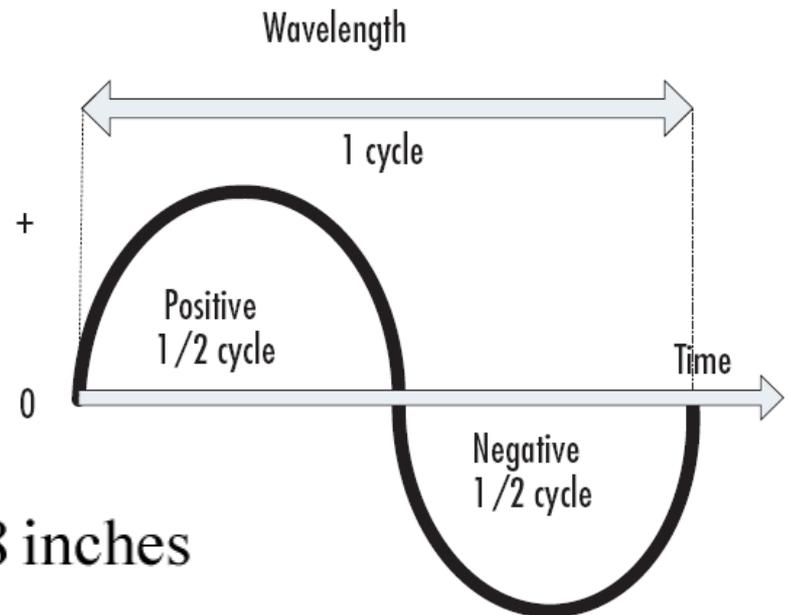
# RF (Radio Frequency)

- There are 11 channels used in the U.S. and Canada and 13 channels in Europe on the 2.4 GHz spectrum starting with Channel 1 at 2.412 GHz and incremented by 0.005 GHz (5 MHz) for each channel
- The Relationship of Wavelength and Cycle with a Radio Wave

$$\lambda = \frac{300,000 \text{ km/s}}{f}$$

- $\lambda$  = wavelength in meters
- $f$  = frequency in kilohertz
- For 2.45 GHz - 802.11g

$$\lambda = \frac{0.3}{2.45} = 0.124\text{m} = 12.4\text{cm} = 4.88 \text{ inches}$$



# RF Terminology 1

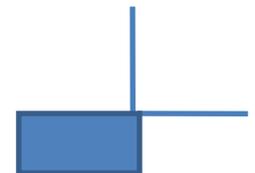
- Radio Signal
  - RF wave that has been changed to carry some information, modulated
    - Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread, Spectrum (FHSS), Orthogonal Frequency-Division Multiplexing (OFDM) etc.
- Noise
  - Is the measurement of how many stray RF signals are in the same frequency area
- Noise Floor
  - The level of background RF noise, *typical* noise floor for 802.11b/g signals is usually about -90 dBm to -100 dBm
- RSSI (Received Signal Strength Indication)
  - 0 to RSSI\_Max (-100 to -50 dBm) , or just Signal Strength

# RF Terminology 2

- Decibels (radio waves)
  - Magnitude of power decrease over distance
  - Ratio of power levels is used – Bel, dB (1/10 Bel)
- The equation for decibels is:
$$\text{dB} = 10 * \log_{10}(p)$$
  - where  $p = \text{the power reference}$
- Usually for wireless it (p) is to one milliWatt (mW) (1/1000 Watt)
$$\text{dBm} = 10 * \log_{10}(1 \text{ mw})$$
- A radio transmitting a 0 dBm signal sends with  $p = 1\text{mW}$ , 10 dBm sends 10 mW and 20 dBm sends 100 mW ... 30 dBm sends with?  
-20 dBm sends with?
- It is typical to see negative numbers to show decibels of a received signal which represent a gradual loss, or *attenuation* of a signal
- Positive numbers indicate a signal addition or *gain*

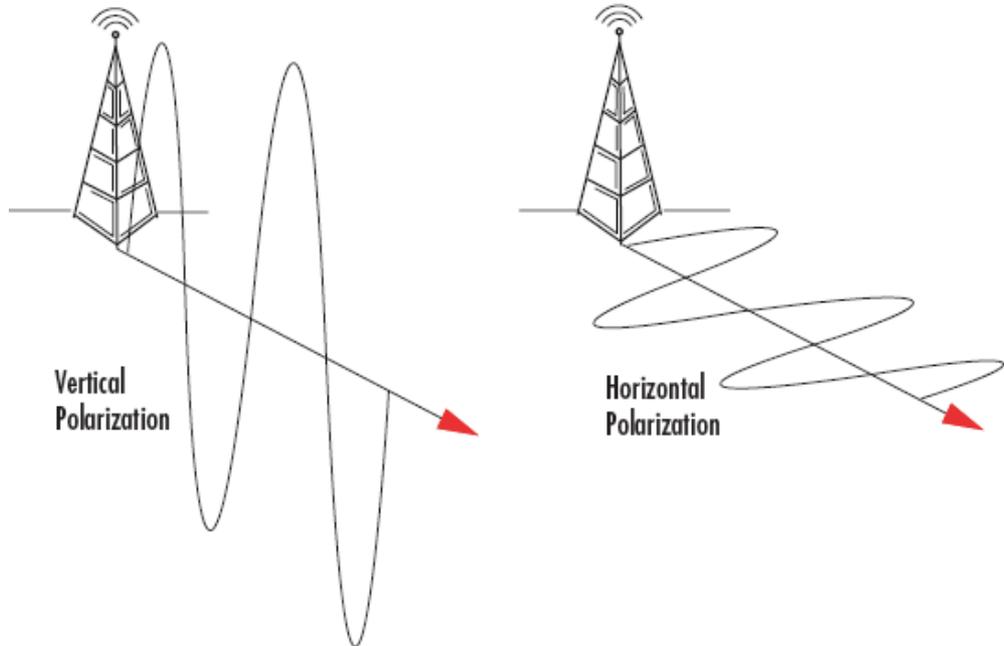
# RF Terminology 3

- Signal strength - typical AP
  - 100 – 500 mW (20 - 27 dBm)
- Signal strength - typical Client Adapter
  - 30 – 200 mW (13 - 23 dBm)
- Estimated loss
  - Plasterboard (gipsskiva) at 4 dBm, brick wall at 8 dBm, and concrete wall at 10 - 15 dBm
- $S - N = \text{SNR}$  (Signal-to-Noise Ratio)
  - S is Signal Strength in dBm and N is Noise in dBm
  - Ex: Wi-Fi HW shows a signal of -82dBm and a noise floor of -96dBm which gives  $\text{SNR} = 14\text{dBm}$  (-82dBm - -96dBm)
- Multipath (reflections)
  - Can be good and bad (out of sync gives interference)
  - MIMO (Multiple Input Multiple Output) - interference as advantage
- Diversity
  - Equipment got more than one antenna - uses the one with best signal minimize multi-path fading



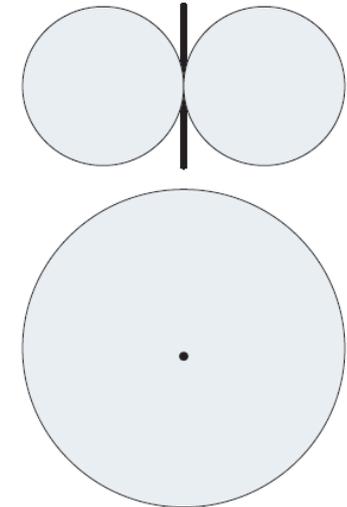
# RF Terminology 4

- Impedance (usually 50 ohm)
  - Is the electrical load on an antenna circuit, wrong ohm ( $\Omega$ ) can give high attenuation (dämpning) which kills the signal
  - Cables and other components
- Polarization
  - Vertical is most common



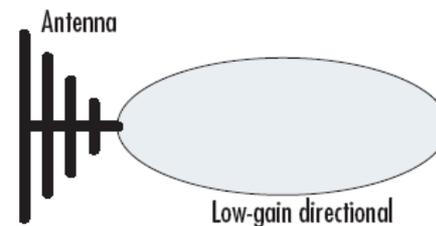
# Passive antenna types

- Gain in
  - dBi (isotropic), dBd (dipole)
  - $\text{dBd} = \text{dBi} - 2,15 \text{ dB}$
- Omnidirectional antennas
  - Typical 4 - 5 dBi
- Directional antennas
  - Grid, typical 21 - 24 dBi
  - Panel
  - Pringles 😊
- Yagi
  - Typical 10 - 17 dBi
- Non-distorting the waveform
  - RF Amplifiers
  - Attenuators (reduce power)

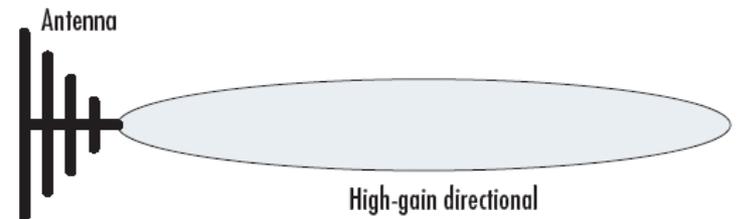


Omnidirectional  
Signal Pattern as  
seen from the  
side.

Omnidirectional  
Signal Pattern as  
seen from above.



Low-gain directional



High-gain directional

The pattern is usually the same when viewed from both the top and the sides .

# Wireless Penetration Testing Tools

- Aircrack-ng - <http://www.aircrack-ng.org>
- AirPcap – CACE/Riverbed Technology - <http://www.cacetech.com/>
  - The ONLY equipment that works in Windows!
- List with Wi-Fi attacks and tools (Wireless attacks, A to Z)
- [http://searchsecurity.techtarget.com/generic/0,295582,sid14\\_gci1167611,00.html](http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1167611,00.html)
- <http://wirelessdefence.org>
- A bit outdated below! **2011:** <http://www.tech-faq.com/wi-fi-software-tools.html>

Tool	Functionality	Operating System(s)	Link
Kismet	WLAN Discovery	Linux	<a href="http://www.kismetwireless.net">www.kismetwireless.net</a>
NetStumbler	WLAN Discovery	Windows	<a href="http://www.stumbler.net">www.stumbler.net</a>
Kismac	WLAN Discover, Full Suite of Penetration Test Tools	MAC OS	<a href="http://kismac.de">http://kismac.de</a>
AirSnort	WEP Cracker, WLAN Discovery	Linux/Windows	<a href="http://airsnort.shmoo.com">http://airsnort.shmoo.com</a>
WEPCrack	WEP Cracker	Linux (Windows with Cygwin)	<a href="http://wepcrack.sourceforge.net">http://wepcrack.sourceforge.net</a>
AirCrack Suite	WEP Cracker, Packet Generator	Linux	<a href="http://www.personalwireless.org/tools/aircrack">www.personalwireless.org/tools/aircrack</a>
Asleap	LEAP Cracker	Linux	<a href="http://asleap.sourceforge.net">http://asleap.sourceforge.net</a>
CoWPAtty	WPA Cracker	Linux	<a href="http://www.personalwireless.org/tools/cowpatty">www.personalwireless.org/tools/cowpatty</a>

# Understanding WLAN Vulnerabilities

- Vulnerabilities can be broken down into two basic types
  - Vulnerabilities due to poor configuration
  - Vulnerabilities due to poor encryption

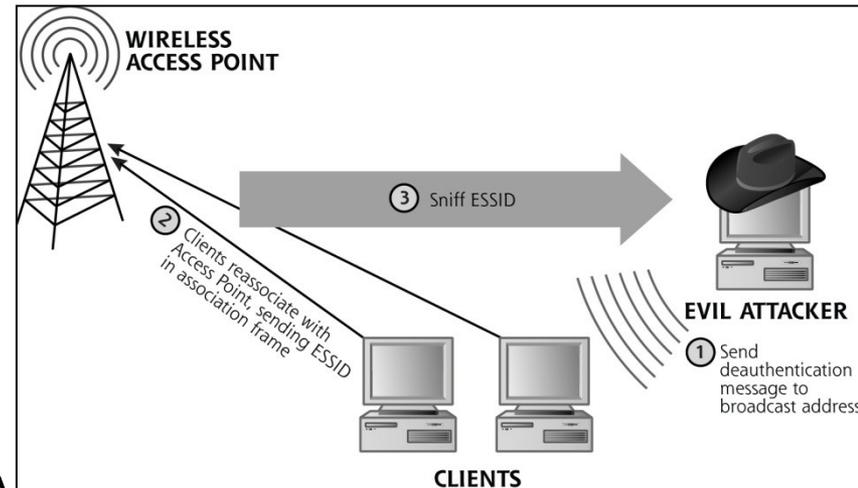
- Attacks usually use one of these three techniques

- Active scanning
- Passive scanning
- Forcing deauthentication

- Pen-testing WLAN

- Target Identification

- ESSID : Name of the WLAN
- BSSID : MAC address of AP or STA
- Probing with ESSID "Any" makes most of the APs answer with their ESSID
- AP:s sends beacon packets every 100 ms with ESSID in clear text



# Active scanning (any probe) with Netstumbler

- Superseded by inSSIDer
  - <http://www.inssider.com/>

The screenshot shows the Network Stumbler interface with the following table of detected access points:

MAC	SSID	Chan	Vendor	Type	Enc...	Signal+	Noise-	SNR+
00022D1F51E0	monkeycheesepants	7	Proxim (Agere) ORINOCO	AP	WEP	-88	-93	5
004096472A13	MSTWN	11	Cisco	AP	WEP	-77	-97	13
0040965840D7	MSTWN	11	Cisco	AP	WEP	-84	-97	12
00409648B990	MSTWN	11	Cisco	AP	WEP	-82	-98	11
00022D37AB0D	Murmur Net	1	Proxim (Agere) ORINOCO	AP		-86	-95	8
002078000499	n3ur0m	6	Runtop	AP		-72	-90	5
0002A52E5268	Neurohub1	10	Compaq	AP		-70	-97	24
00508B991462	NextWave	6	Compaq	AP		-80	-81	1
0040965A857E	nsu_universal_acc...	6	Cisco	AP		-86	-96	9
00409641264A	nyc	3	Cisco	AP	WEP	-84	-97	10
00045A0C53D5	nyc840w	9	Linksys	AP	WEP	-95	-96	1
00022D2A3C2E	NYC_LAB	6	Proxim (Agere) ORINOCO	AP	WEP	-43	-98	48
00022D38ED85	nylink	1	Proxim (Agere) ORINOCO	AP		-87	-95	6
00409640C8F2	NYSIFnet	6	Cisco	AP		-70	-96	24
00409645358D	NYUMobileNet	11	Cisco	AP	WEP	-88	-92	4
0030651CABBF	Office	1	Apple	AP	WEP	-76	-96	18
00022D0F8EAC	Ohh La La Network	1	Proxim (Agere) ORINOCO	AP	WEP	-78	-99	17
00601D23C89A	Op59w6ys	3	Proxim (Agere/WaveLAN)	AP		-83	-96	9
00601D23C200	Op59w6ys	3	Proxim (Agere/WaveLAN)	AP		-79	-99	16
0030651C69CE	oport	1	Apple	AP	WEP	-81	-96	14
0030A809A5F1	OptecInc	10	Delta (Netgear)	AP		-76	-99	13
00409629236D	oven	3	Cisco	AP		-82	-96	12
0030A80A8758	PANACEA	1	Delta (Netgear)	AP	WEP	-88	-94	6

Filters let the user focus on access points with specific characteristics

Here are the SSIDs that I harvested

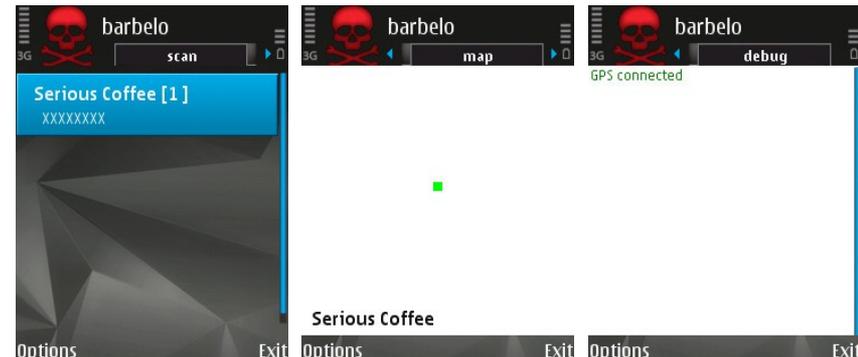
Note that about 40% of access points I discovered used WEP

Here is the strangest SSID I've ever found

I logged 455 access points in 1 hour

# Active scanning with old mobile phone

- Barbelo and gpsd under Symbian S60v3(v5)
  - <http://darkircop.org/barbelo/> (unfortunately bugs)
  - <http://wiki.nomi.cz/gpsd:start> (also turn your phone into BT GPS)
- Kisgearth (Perl script - Kismet XML > KML)
  - More than 1 AP in Wi-Fi network log
  - å, ä, ö and comma (',') must be converted to US standard ','
  - <http://mytty.org/kisgearth/>
- Other wardriving apps for Windows Mobile 6.x etc.
  - AiroMap (<http://blogs.wefrag.com/divide/airosuite/>)
  - <http://www.wardrive.net/wardriving/tools/>
- View KML with Google Earth



# View in Google Earth

The screenshot displays the Google Earth interface with a satellite view of a residential complex. Numerous Wi-Fi network names are overlaid on the map, including: NETGEAR, AirLink89300, 2f4bac, belkin54g, Laadin's network!, vandrarhem2, tudou, BTOpenzonelite, NETGEAR vandrarhem3, Belkin\_G\_Plus\_MIMO\_ED0ECA, vandrarhem4, Chen's new Family, Sheila\_Yau kloker, FRANK\$TAYO, and Ipredia. A detailed information window for the 'Ipredia' network is open on the right side, showing the following details:

**Ipredia**

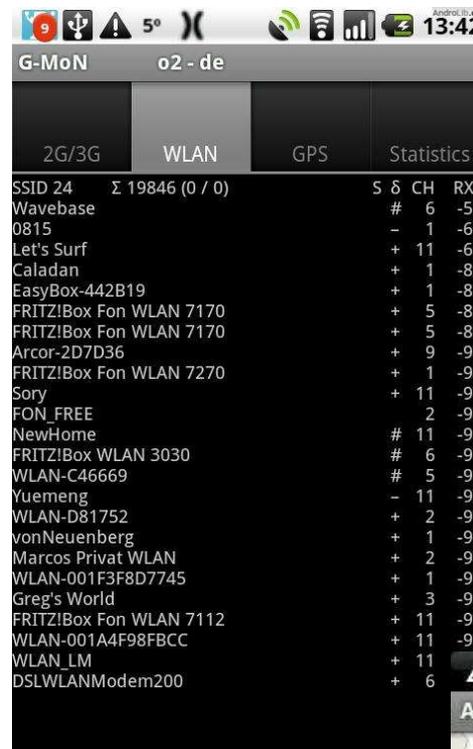
- Number: 5
- SSID: Ipredia
- BSSID: 00:11:50:AF:2F:F6
- Channel: 11
- Encrypted: false
- Carrier: IEEE 802.11b
- Cloaked: false
- Datasize: 0
- Maxseenrate: 0
- Firsttime: Sat Apr 18 15:52:54 2009
- Lasttime: Sat Apr 18 15:53:22 2009
- Type: infrastructure
- Maxrate: 0.0

Generated with KisGearth 0.01f  
Website: <http://mytv.org/kisgearth/>  
Växebeskrivning: Lit

At the bottom of the window, the coordinates are displayed: lat 60.492428° long. 15.403087° höjd 148 m. The bottom right corner shows the Google logo and the text "© 2009".

# Active scanning with Android phone

- Android apps (there is a lot!)
- Most support KML, export etc.
- Wardrive, Wigle WiFi, WiFi Scanner
- Scout, G-MoN, WlanPollution
- Antennas (Cell-ID)
- Penetrate (Crack)
- ...



# Passive scanning (rfmon/monitor mode)

- **Handheld - Wellenreiter II**
  - <http://www.vanille-media.de/site/index.php/projects/wellenreiter-ii>
- **Hotspotter**
  - <http://www.wirelessdefence.org/Contents/hotspotter.htm>
- **Wicrawl (plugin support)**
  - <http://midnightresearch.com/projects/wicrawl/>
- **Airscanner Mobile Sniffer**
  - <http://www.airscanner.com/>

## Packet Sniffer



Net/Station	#	MAC
vanille	0	
		00:04:76:60:4F:5A
	11	00:60:1D:FD:2D:98
	678	00:50:18:05:4A:A0

SSID	BSSID	Time	Packets	Plugin	Event	Timestamp	Encryption	Power	Channel
wi-foo	00:12:17:28:15:5b	0	0	Internet Speed Check	have-internet	3-7-2006 13:8:7	WEP	0	10
Frog	00:0f:66:95:a0:bd	0	0	iwconfig	association	3-7-2006 13:9:12	None	0	01
linksys	00:06:25:54:a6:c1	0	0	DHCP	associated	3-7-2006 13:8:38	None	0	01

Output

```
[:] Found no new APs in discovery, I'll wait a bit more...  
(last count [3] new count [3])  
[:] Found no new APs in discovery, I'll wait a bit more...  
(last count [3] new count [3])  
[:] Found no new APs in discovery, I'll wait a bit more...  
(last count [3] new count [3])  
[:] Found no new APs in discovery, I'll wait a bit more...  
(last count [3] new count [3])  
Stop was pressed  
Killing child [24879]  
Child [24879] dead  
Discovery and plugin-engine finished
```

# Passive scanning with

- Also used to capture data when forcing deauthentication

```
dragorn@gir.lan.nerv-un.net:/home/dragorn
```

Network List—(Autofit)								Info
Name	T	W	Ch	Pkts	Flags	Data	Clnt	
p@thf1nd3r	A	Y	06	171		70	35	Ntwrks 105
<no ssid>	A	N	05	1		0	0	Pkts 1258
KrullNet1	A	Y	06	27		0	0	Cryptd 104
<b>linksys</b>	<b>A</b>	<b>N</b>	<b>06</b>	<b>81</b>	<b>FU4</b>	<b>8</b>	<b>2</b>	Weak 0
marley	A	N	06	312		17	1	Noise 289
<no ssid>	D	N	--	20	A2	20	18	Discrd 289
! PARMAS	A	N	07	30		0	0	Pkts/s 50
<no ssid>	A	Y	06	1		0	0	
GRXWirelessNetwork	A	Y	06	2		0	0	
! SECMAS	A	N	07	13		0	0	
<no ssid>	D	N	--	1	A4	1	66	
! <Lucent Outdoor Router>	0	N	--	267		267	1	

Elapsd  
000027

```
Status
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
Found IP 159.139.120.13 for <no ssid>::00:B0:D0:DE:60:E3 via TCP
Battery: AC charging 100% 0h0m0s
```

# Cain and CACE AirPcap USB dongle

The image displays the main interface of Cain and CACE software. The top menu bar includes File, View, Configure, Tools, and Help. Below the menu is a toolbar with various icons for network analysis. The main window is titled "VMware Virtual Ethernet Adapter" and shows a selected device: "Device\NPF\_{758D4F89-8FDD-4364-81F6-9EC5EDBE0F2F}". An "Active Scan" button is visible to the right of the device selection.

On the left side, there are several configuration panels:

- AirPcap:** Driver version: not installed; Current channel: (empty).
- Lock on channel:** (empty dropdown).
- Capture WEP IVs to dump.ivs file:** Checked; Buttons: Analyze, Delete, Save As.
- WEP Injection:**  ARP Requests; TxRate (Mbps): 2.
- WPA-PSK Auths:**  Send to Cracker.

The main display area is a table with the following columns: BSSID, Last seen, Vendor, Signal, SSID, Enc, Mode, Channel, Rates (Mbps), Packets, Unique WEP IVs. The table is currently empty.

An inset window is open in the foreground, showing a list of hash types and a table with columns: 802.11 Capture File, Size, Type, Note.

- IKE-PSK Hashes (0)
- MSSQL Hashes (0)
- MySQL Hashes (0)
- Oracle Hashes (0)
- Oracle TNS Hashes (0)
- SIP Hashes (0)
- 802.11 Captures (0)
- WPA-PSK Hashes (0)
- WPA-PSK Auth (0)
- CHAP Hashes (0)

The table in the inset window is empty. The URL <http://www.oxid.it> is visible at the bottom of both windows.

# War Driving Defenses

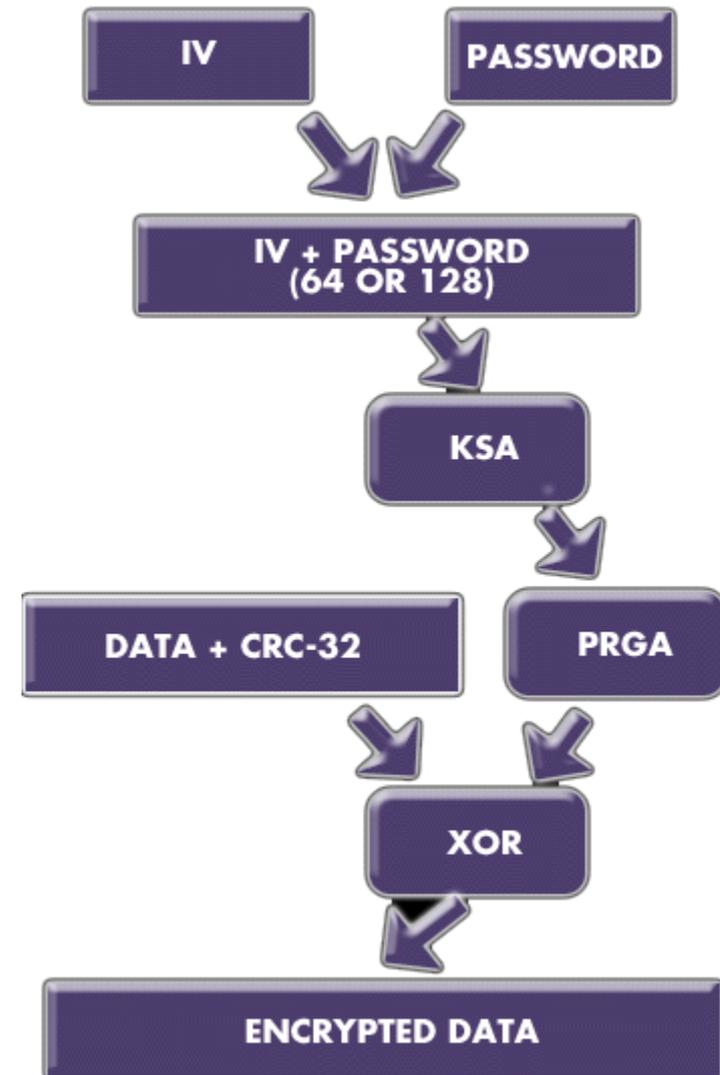
- Set non informative ESSID in AP and an unique name
- Set AP to ignore probe requests that do not contain ESSID and omit ESSID in beacon packets
- Set AP to filter out MAC-addresses that are unknown
  - Mac MakeUp (Windows)
  - ifconfig [if] hw ether [mac address] (Unix)
- Wired Equivalent Privacy (WEP)
  - Protocol is broken – not recommended to use
  - FMS (Fluhrer, Mantin, and Shamir)/KoreK attack method - 2001
  - PTW (Pyshkin, Tews, Weinmann) attack method - 2007
- WiFi Protected Access (WPA)
  - WPA implements a subset of 802.11i (WPA2) but uses RC4 instead of AES cipher
  - WPA/WPA2-PSK
    - Short passphrase (less than 21 characters) is vulnerable to a dictionary attack  
<http://seclists.org/isn/2003/Nov/0021.html>

**Offensive Security: WPA Rainbow Tables, 49 million word dictionary**

- <http://www.offensive-security.com/wpa-tables/>

# WEP (Wired Equivalent Privacy)

- IVs (initialization vectors) used with stream cipher RC4
  - IV produce a unique stream independent from other streams produced by the same encryption key
- RC4 uses the key to initialize a state machine via Key Scheduling Algorithm (KSA)
  - Then continuously modifies the state and generates a new byte of the key-stream from the new state
- RC4 XOR-encrypts one byte at a time with the key-stream output from Pseudo Random Generation Algorithm (PRGA)
  - <http://en.wikipedia.org/wiki/RC4>
  - [http://en.wikipedia.org/wiki/Wired\\_Equivalent\\_Privacy](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy)



# WEP key reuse

- Many packets contain well known fields at well known locations
  - E.g. header fields in IP and ARP etc.
- RC4 64 bit seed is created by concatenating a 40 bit shared secret (10 hex characters) with a 24 bit initialization vector (IV)
- A family of  $2^{24}$  keys for each shared secret
- Keys are cycled for each packet
  - Frames can be lost and stream ciphers do not deal with missing bits, so the stream must be reset with each packet
  - Therefore, a new IV is sent in the clear with each packet
- IV is only 24 bits, the time to repeat IV's (and thus keys) with high probability is very short
  - 50% probability of getting some IV reuse after using 4096 IV's
  - 99% likely that you get IV re-use after 12430 frames or 1 or 2 seconds of operation at 11 Mbps

# Aircrack-ng

<http://www.aircrack-ng.org/doku.php?id=aircrack-ng>

- Knowing two of key stream, plain-text, and cipher-text lets you easily compute the third

- Reusing a key value is a really, really bad idea.  
A well known fact for RC4

XOR	Input 1	Input 2	Output
	0	0	0
	0	1	1
	1	0	1
	1	1	0

- FMS/KoreK chopchop attack method

- When enough IVs are captured incorporate various statistical attacks to discover the WEP key and use these in combination with brute forcing
- [http://en.wikipedia.org/wiki/Fluhrer,\\_Mantin,\\_and\\_Shamir\\_attack](http://en.wikipedia.org/wiki/Fluhrer,_Mantin,_and_Shamir_attack)
- [http://www.aircrack-ng.org/doku.php?id=korek\\_chopchop](http://www.aircrack-ng.org/doku.php?id=korek_chopchop)

- PTW attack

- Builds upon Andreas Klein work which in turn works on FMS/KoreK work
  - <http://eprint.iacr.org/2007/120>
- Fewer data packets/IVs are needed but is limited to only ARP
- <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>

- For cracking WPA/WPA2 PSK, a dictionary method is preferred



# WPA/WPA2-PSK

- Elcomsoft Wireless Security Auditor
- Pyrit (Python), backtrack support
  - <http://code.google.com/p/pyrit/>
- Only wordlist or hash chain attack make sense!
- Algorithm – the PMK (Pair-wise Master Key) may be pre-computed

1 Generate PMK:  $PMK = PBKDF2(PSK, SSID, SSID\_Len, 4096, 256)$

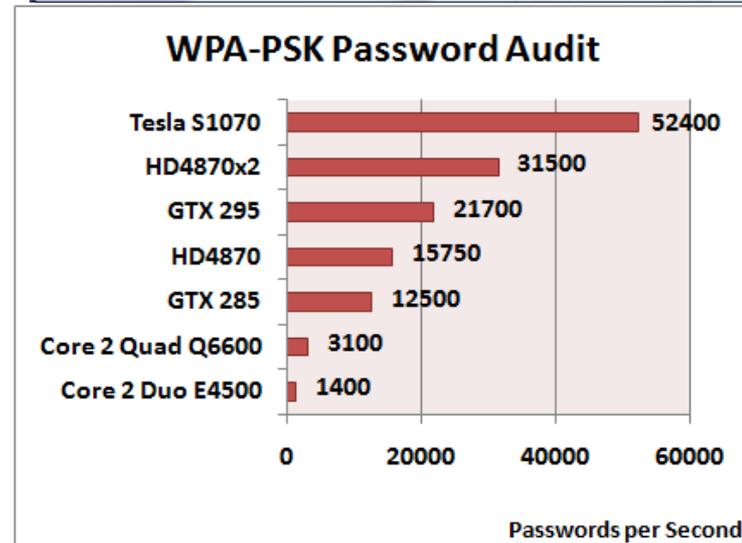
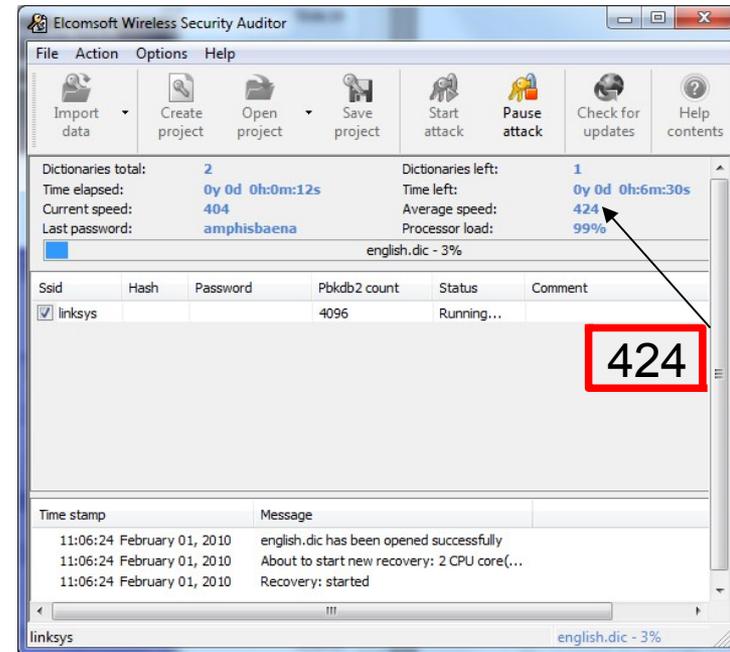
2 Generate PTK:  $PTK = sha1\_prf(PMK, PKM\_Len, Pairwise\ key\ expansion, data, sizeof(data))$   
 where data is composed of: LowerMac, HigherMac, LowerNonce, HigherNonce

- MAC of client and AP (packet 3)
- AP nonce (packet 3)
- Client nonce (packet 2)

PTK is captured with aircrack-ng

3 Generate the MIC:  
 TKIP:  $MIC = hmac\_md5(key, 16, data);$   
 AES:  $MIC = hmac\_sha1(key, 16, data);$

4 Compare computed MIC with captured MIC from packet 4



# Possible offline extraction of PMKs

- Pre-Shared Key (PSK): 8-63 printable ASCII characters (keyspace 96)
- Note! You may not need the PSK, try use the PMK hash directly in config?
- PMK = 32 bytes (256 bits), PBKDF2 = HMAC-SHA1, iterated 4096 times
  - Generate a PMK hash: <http://www.wireshark.org/tools/wpa-psk.html>
- PMKs are in Windows XP encrypted and decrypted with the DPAPI CryptProtectData and CryptUnprotectData functions, ex. WZCook (Aircrack-ng)
  - <http://msdn.microsoft.com/en-us/library/ms706987%28VS.85%29.aspx>
- The registry/file location of PMKs storage where the Interface GUID represents the wireless network card
  - Windows XP: SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\[Interface GUID]
  - Windows Vista/7: stored in the file system in a .xml file (keyMaterial element), under C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\[Interface GUID]
- Starting from Windows 7, Microsoft changed the encryption and hashing algorithms that are used by the Windows Data Protection (DPAPI) system
- In Linux the PMK is usually stored in some wpa\_supplicant config file

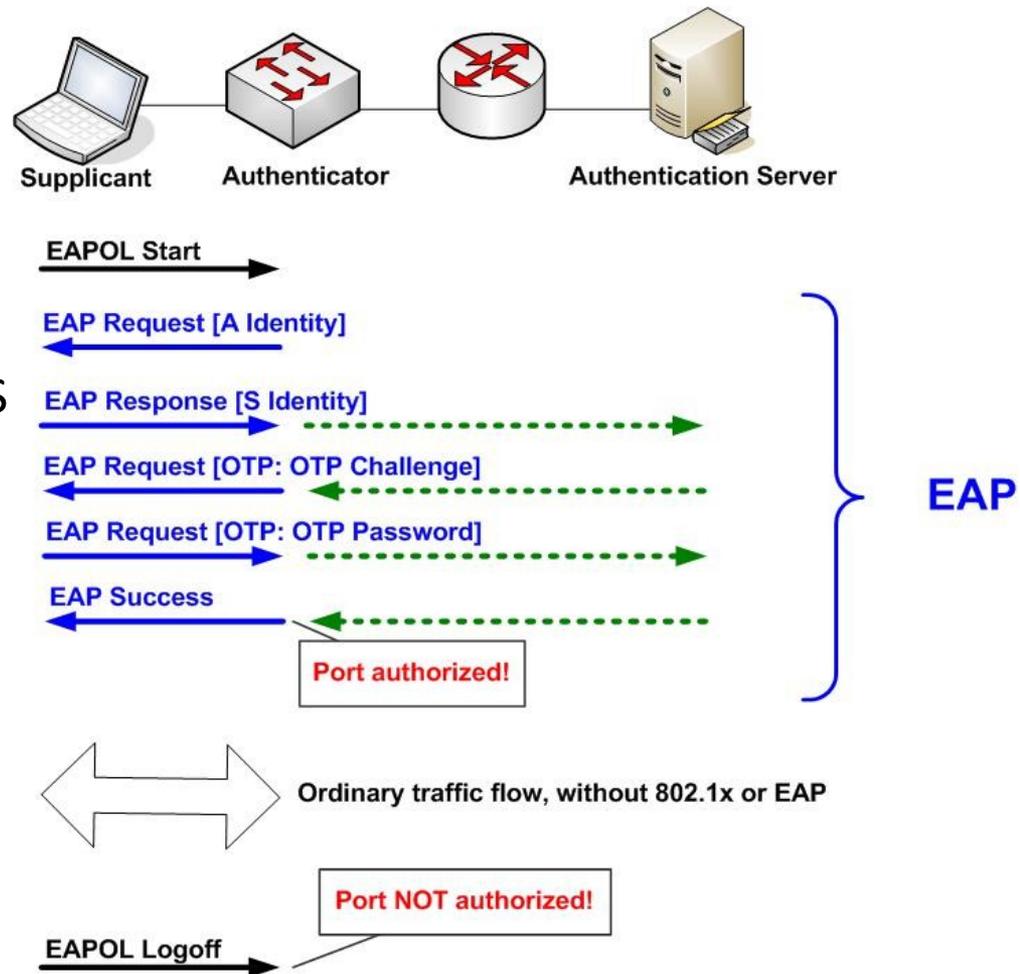
# 802.11i architecture

- WPA2 = 802.11i also called RSN(Robust Security Network)
- The 802.11i architecture contains the following components
  - 802.1X for authentication (entailing the use of EAP and an authentication server)
    - <http://en.wikipedia.org/wiki/802.1x>
  - AES-based CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), to provide confidentiality, integrity and origin authentication
    - Replaces TKIP (Temporal Key Integrity Protocol)
  - [http://en.wikipedia.org/wiki/IEEE\\_802.11i](http://en.wikipedia.org/wiki/IEEE_802.11i)
- EAP is an authentication framework, not a specific authentication mechanism
  - There are about 40 different EAP methods for authentication
    - EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA, PEAP, LEAP, EAP-TTLS... EAP-PSK
  - EAP (Extensible Authentication Protocol) methods and messages provide authentication and a secure PMK (Pair-wise Master Key) between STA and AP
  - If EAP is embedded in 802.1x it is called EAPOL (EAP Over LANs)
    - The PMK/PTK is used for the wireless encryption session which uses TKIP or CCMP
    - [http://en.wikipedia.org/wiki/Extensible\\_Authentication\\_Protocol](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol)

# General EAP authentication

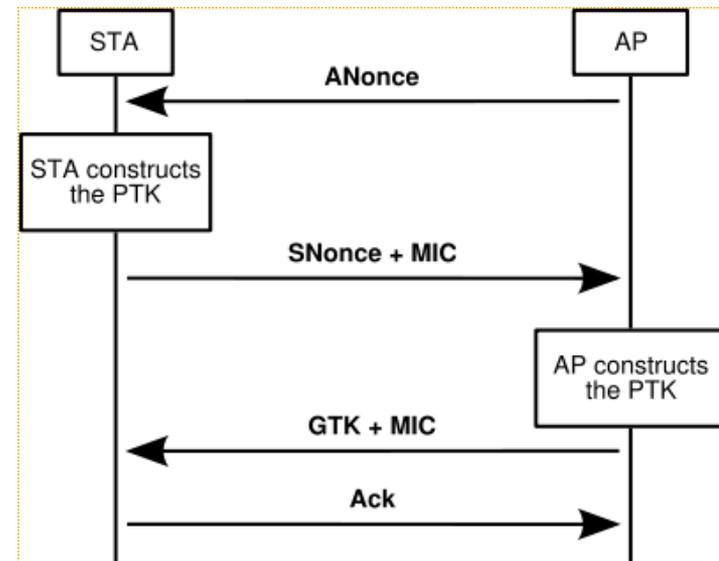
<http://www.netcraftsmen.net/welcher/papers/dot1x.html>

- Encapsulation of EAP Over LANs
  - 802.1X EAPOL
  - Layer 2 wrapper to transport EAP information
- EAPOL start is only used if the supplicant initiates the exchange
- Green dotted lines show RADIUS (AS) messages
- EAP-OTP (One Time Password)
- EAP-PSK = OTP
  - If passphrase is 256 bit, PMK = passphrase, else
  - PMK = PBKDF2(passphrase, ssid, ssidLength, 4096, 256)
  - Hashed 4096 times



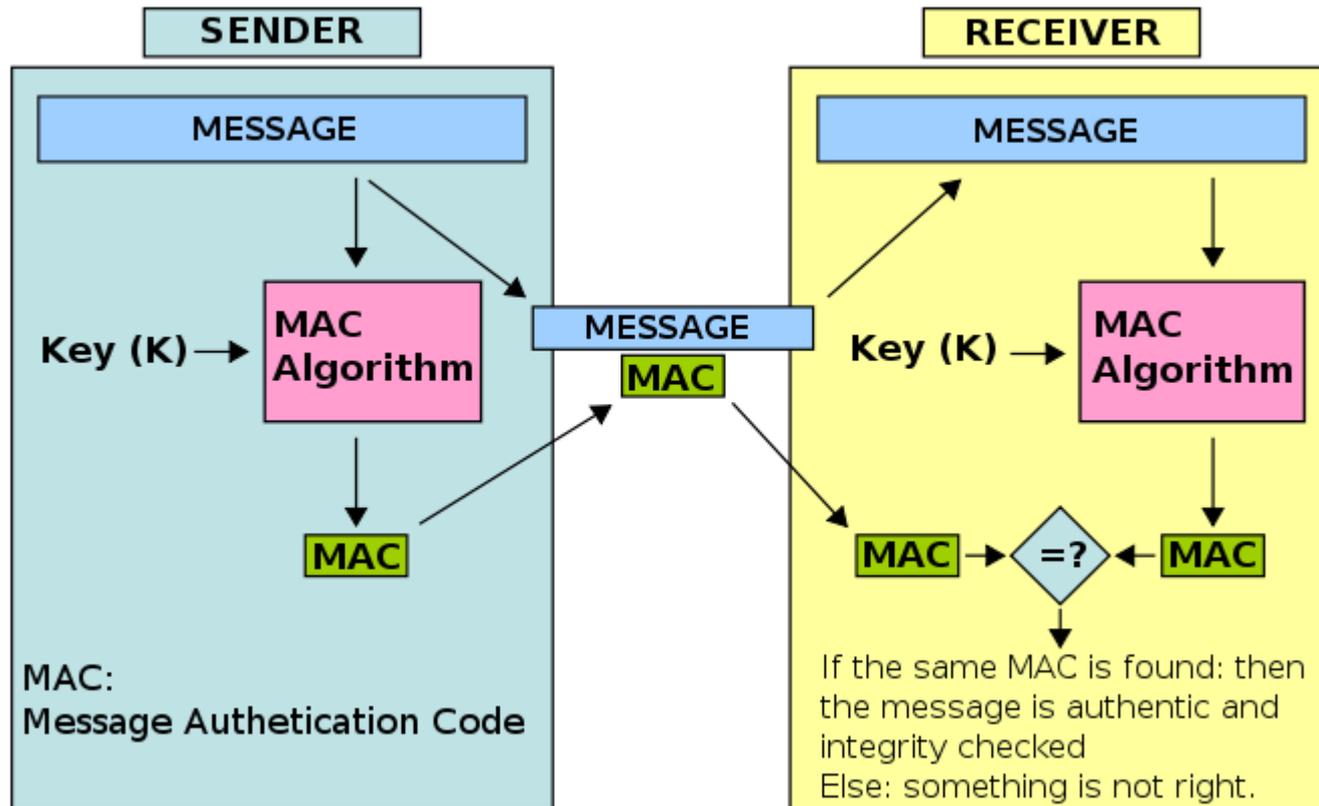
# 802.11i Encryption key distribution

- The earlier 802.1x EAP exchange has provided the shared secret key PMK (Pair-wise Master Key) Note! If it is WPA2-PSK we already know it.
  - This key is however designed to last the entire session and should be exposed as little as possible
- Therefore the four-way handshake is used to establish another key called the PTK (Pair-wise Transient Key)
  - The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address and STA MAC address
  - The product is then put through a cryptographic hash function
  - The handshake also yields the GTK (Group Temporal Key), used to decrypt multicast and broadcast traffic
  - **Nonce** stands for: number or bit string used only once
  - **MIC** = Message Integrity Code
  - All the messages are sent as EAPOL-Key frames
  - [http://en.wikipedia.org/wiki/IEEE\\_802.11i](http://en.wikipedia.org/wiki/IEEE_802.11i)



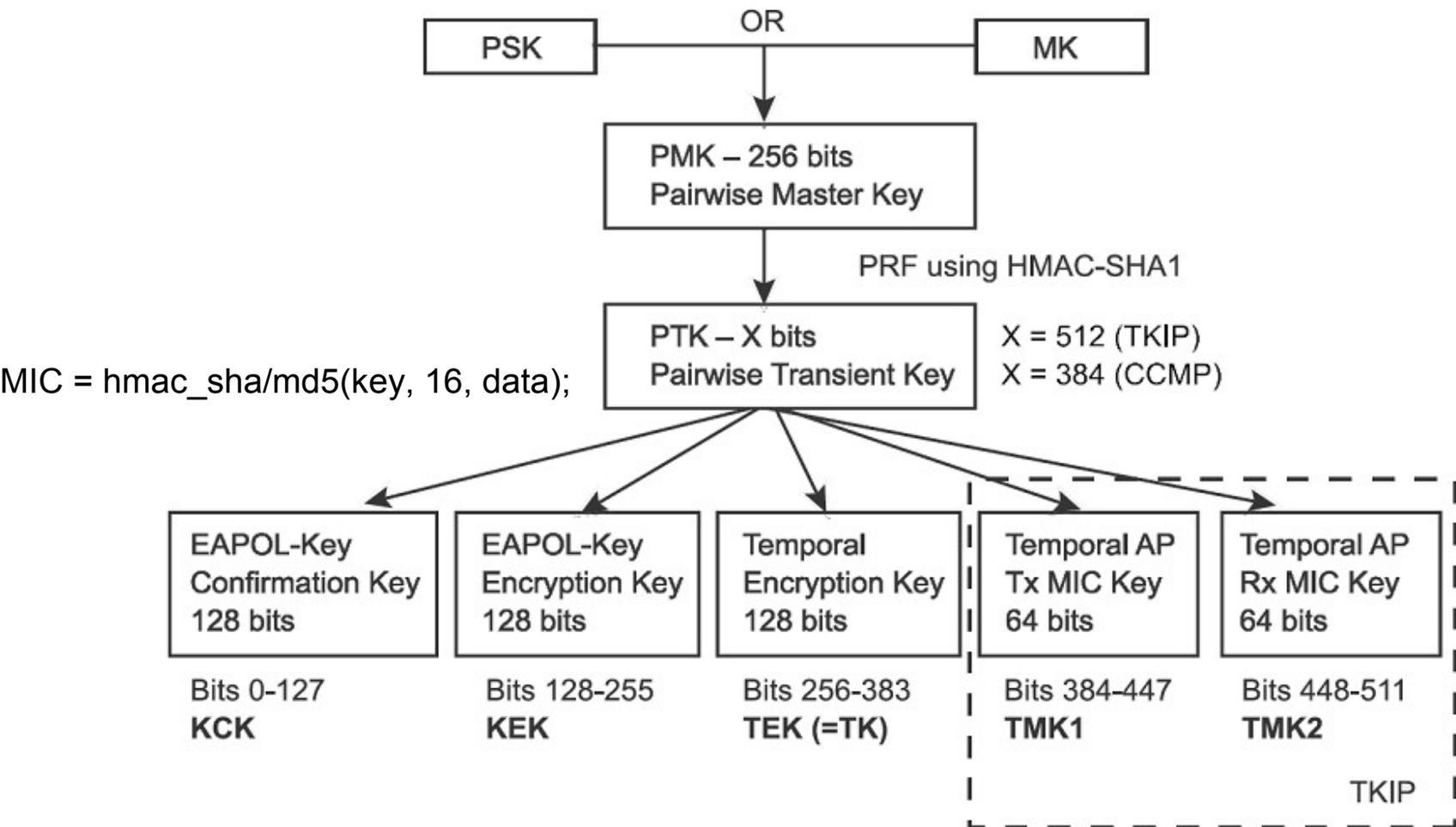
# MAC

- (H)MAC = (Hash-based) Message Authentication Code
  - <http://en.wikipedia.org/wiki/HMAC>
  - [http://en.wikipedia.org/wiki/Message\\_authentication\\_code](http://en.wikipedia.org/wiki/Message_authentication_code)



# MIC and the hierarchy of keys

- The KCK (Key Confirmation Key) is used for computing the MIC (Message Integrity Code)
- If computed MIC is equal to eavesdropped MIC we can calculate the PSK/MK



# RADIUS, VPN and defense

- Remote Authentication Dial-In User Service (RADIUS)
  - AAA (Authentication, Authorization and Accounting)
  - Centralized client/server approach
  - Uses a shared secret that never is sent over the net
  - Flexible authentication with PAP, CHAP, LDAP etc.
  - Uses UDP port 1812
  - FreeRADIUS <http://www.freeradius.org>
- VPN
  - PPTP and L2TP
  - IPsec
  - OpenVPN (SSL/TLS based)
- IDS (Intrusion Detection System)
- Physical defense (Faraday cage) or turn down transmit power



# War Dialing

- Looking for modems in all the **right** places
  - Remote access lines
  - Often weak protection
- Automated dialers
  - Feed with recon data
- TCH-Scan 2.0
  - Full featured
  - <http://freeworld.thc.org/welcome/>
- If inside you really are inside!
- Defenses
  - Modem policy
  - Dial out only
  - Find the modems before the attacker



```
MS-DOS Prompt - THC-SCAN
8 x 12
TIME          STATISTIC
Start >> 16:49:50  Done : 2
Now >> 16:51:25   To Do : 8
ETA >> 16:56:58
Timeout >> 2/50  Dials/H: 114
Rings >> 0/6    Carrier: 0
                Tones : 0
                UMB : 0
                Voice : 0
                Custom: 0
                Busy : 0
                Others: 2
                2ndary : 0
FOUND!
MODEM WINDOW
ATH
OK
ATDT7511027
NO CARRIER
ATH
OK
ATDT7511021
* FINAL *      THC-SCAN v2.00  (c) 1996.98 by van Hauser/THC  * FINAL *
```

# WiFi Definitions 1

Term Name ▲	Definition
802.11	A group of wireless networking standards defined by the Institute of Electrical and Electronics Engineers (IEEE) and commonly referred to as Wi-Fi or WLAN.
802.11a	A Wi-Fi network standard that describes radio transmissions in the 5.0-5.8GHz frequency range and with data rates of up to 54Mbps.
802.11b	A Wi-Fi network standard that describes radio transmissions in the 2.4GHz frequency range and with data rates of up to 11Mbps.
802.11g	A Wi-Fi network standard that describes radio transmissions in the 2.4GHz frequency range and with data rates of up to 54Mbps.
802.11i	An IEEE standard that specifies AES or TKIP encryption and 802.1X authentication for securing Wi-Fi networks. It supersedes the previous WEP specification from the original 802.11 standard that was found to be easily compromised.
802.11n	A yet-to-be-released, next generation Wi-Fi network standard that describes radio transmissions in both the 2.4GHz and 5.0-5.8GHz frequency ranges and with data rates of up to 600Mbps.
802.1x	An IEEE standard for port-based network access control, providing for the authentication of users attempting to access a network. It is specified by the IEEE 802.11i standard and the Wi-Fi Alliance WPA and WPA2 certifications for implementing Wi-Fi security. It is typically operated in conjunction with a RADIUS server.
Access Point	A Wi-Fi device (typically with 1 or 2 radios) that connects wireless devices/users to another (typically wired) network. Commonly abbreviated as AP.
Ad Hoc	A Wi-Fi network connection method that does not require an access point (base station). Using this mode, Wi-Fi devices such as laptops or gaming stations can connect directly to each other.

# WiFi Definitions 2

Ad Hoc	A Wi-Fi network connection method that does not require an access point (base station). Using this mode, Wi-Fi devices such as laptops or gaming stations can connect directly to each other.
AES (Advanced Encryption Standard)	The preferred encryption algorithm for use in wireless LANs today. It provides government-grade encryption and can be used with both WPA and WPA2 Wi-Fi security.
BSSID (Basic Service Set Identifier)	The MAC address of the Access Point.
CCMP (Counter Mode with Cipher Block Chaining with Message Authentication Code)	An encryption protocol defined by IEEE 802.11i. It is used in conjunction with the AES encryption algorithm and is part of both WPA and WPA2 Wi-Fi security.
Channel	A frequency band, identified by a unique number, used for Wi-Fi communication. Each channel supports independent communication from any other channel. Wi-Fi channels are 20MHz wide in 802.11a/b/g networks, and can be either 20MHz or 40MHz in 802.11n networks.
dBm	A logarithmic unit of measure for milliwatts of power, used in Wi-Fi to measure the strength of a signal. Several examples of the conversion from dBm to milliwatts: 0 dBm = 1 milliwatt; 10dBm = 10 milliwatts; 20dBm = 100 milliwatts; -10dBm = 0.1 milliwatts.
MAC Address (Media Access Control Address)	A quasi-unique address value used to identify network adapters that follow different communication standards. In Wi-Fi (as well as Ethernet and other standards), MAC addresses are six bytes (48 bits) in length.
PSK (Pre-shared Key)	An encryption key shared between and common to the access point and client. It is used in WPA and WPA2 security.
RADIUS (Remote Authentication Dial In User Service)	An AAA (Authentication, Authorization and Accounting) protocol for controlling user access to a wired or wireless network.

# WiFi Definitions 3

Roaming	The ability for a mobile wireless station to transparently change its connection between access points as it moves throughout a wireless network.
RSSI (Receive Signal Strength Indication)	The strength of the Wi-Fi signal as measured by the receiver of the signal. The larger the signal strength, the better the connection. RSSI is usually expressed in dBm or as a numerical percentage. The translation of dBm to percentage is: -100dBm = 0% and -50dBm = 100%, with each dBm accounting for 2% in between. A "good" Wi-Fi signal is typically considered to be -70dBm or greater (keep in mind negative numbers, so -60dBm is greater than -70dBm for example).
Signal Strength	See RSSI.
SSID (Service Set Identifier)	A unique name that identifies a wireless LAN and that differentiates it from others. All access points and clients attempting to connect to a specific WLAN must use the same SSID.
TKIP (Temporal Key Exchange Protocol)	An encryption protocol defined by 802.11i as an enhancement to WEP. Both WPA and WPA2 Wi-Fi security allow for the use of TKIP encryption.
WEP (Wired Equivalency Protocol)	The original encryption protocol defined for 802.11 wireless LANs by the IEEE. WEP encryption is easily cracked and is not recommended for implementing Wi-Fi security today.
WEP-104	WEP with 104 bit master encryption key.
WEP-40	WEP with 40 bit master encryption key.
Wi-Fi	A term developed by the Wi-Fi Alliance to describe wireless local area network (WLAN) products that are based on the IEEE 802.11 standards.
Wi-Fi Alliance	Industry organization that certifies 802.11a/b/g/n products for interoperability.
WPA (Wireless Protected Access)	The original Wi-Fi Alliance certification of 802.11i security for wireless LANs. It provides good Wi-Fi security but was introduced as an interim option before WPA2 was released.
WPA2 (Wireless Protected Access 2)	The second generation Wi-Fi Alliance certification of 802.11i security for wireless LANs. Use of WPA2 is considered best practice for implementing Wi-Fi security today.