Wireless Security

Sheetal Joseph
CISSP, CEH
Tech Mahindra
sheetalj@techmahindra.com

OWASP
22nd September 2008

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org

Roadmap

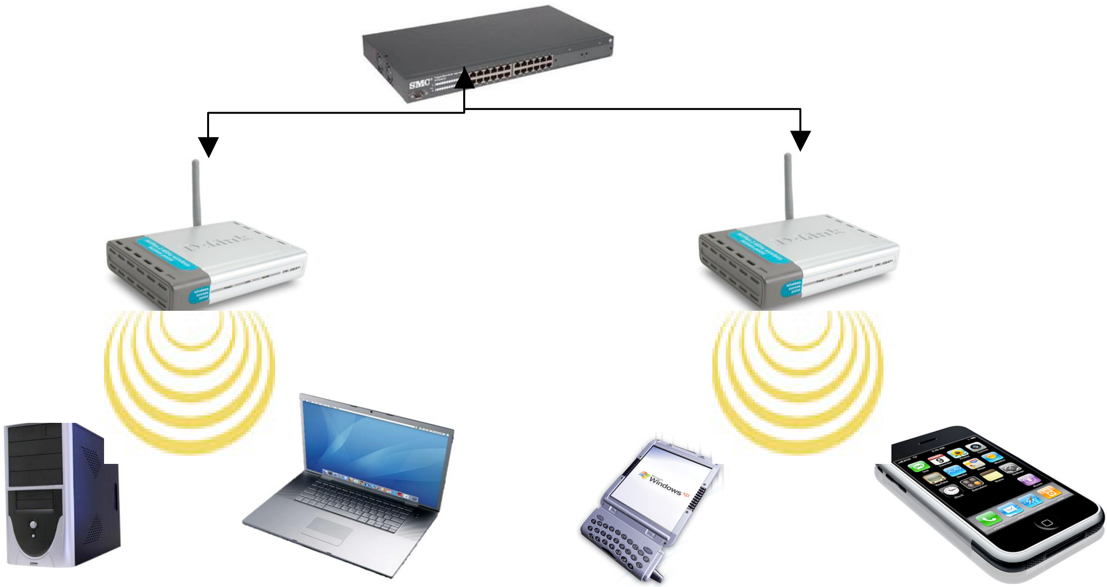
- Wireless Overview
- Wireless Security Standards
- Exploiting Wireless Vulnerabilities
- Wireless Best Practices

Wireless - The World of Convenience!

- User mobility
  - Reduced cost
  - Flexibility and convenience
  - Increase the productivity

- Wireless devices use Radio Frequency (RF) technology to facilitate communication.

- Various types of wireless communication solutions use different frequencies, most regulated by governments.



Wireless Standards

- **802.11b** – Transmits at 2.4 GHz, sends data up to 11 Mbps using direct sequence spread spectrum modulation. 100 -150 feet range
- **802.11a** – Transmits at 5 GHz and send data up to 54 Mbps using orthogonal frequency division multiplexing (OFDM). 50-75 feet range. **Not** interoperable is 802.11b.
- **802.11g** – Combines features of both standards (a,b), 2.4 GHz frequency, 54 Mbps Speed, 100-150 feet range and **is** interoperable with 802.11b.
- **802.11i** – Improves WEP encryption by implementing Wi-Fi Protected Access (WPA2). Data encryption with Advanced Encryption Standard (AES).
- **802.11n** – 600 Mbps speed by adding multiple-input multiple-output (MIMO) and Channel-bonding/40 MHz operation to the physical (PHY) layer, and frame aggregation to the MAC layer. 802.11n uses WPA and WPA2 to secure the network.

Latest Wireless Hacks

- Email sent before the ***Ahmedabad & Delhi bombings*** sent via a hacked ***wireless*** connection

- TJX theft tops 45.6 million card numbers http://www.tjx.com/tjx_message.html

Types of Attacks

- **Identity theft (MAC spoofing)** - Cracker is able to listen in on network traffic and identify the MAC address of a computer and attack after spoofing the same

- **Man-in-the-middle attacks** - Cracker entices clients to log into a computer set up as an AP Once this is done, the hacker connects to a real AP through another wireless card offering a steady flow of traffic.

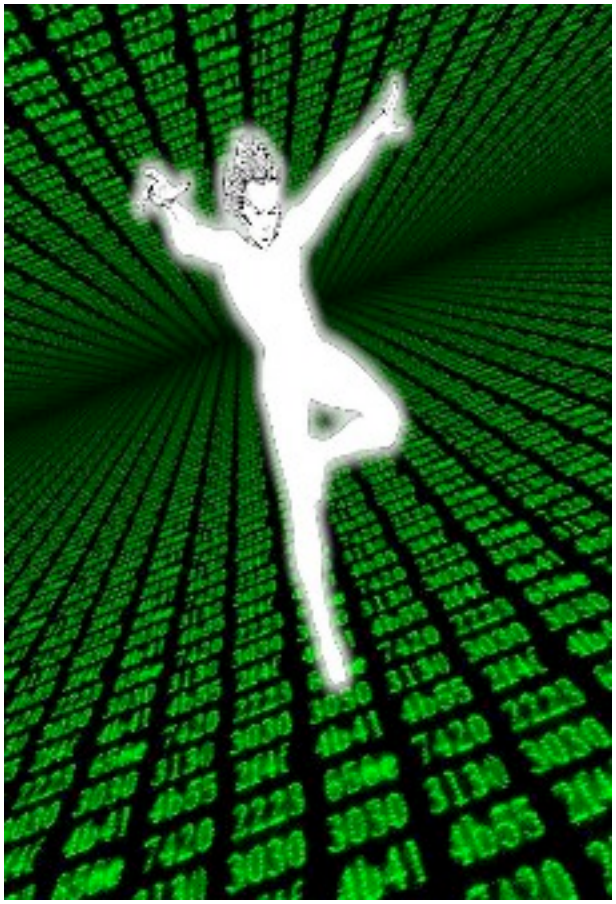
- **Denial of service** - Cracker continually bombards a targeted AP with bogus requests, premature successful connection messages, failure messages, and/or other commands.

Wireless Security Goals

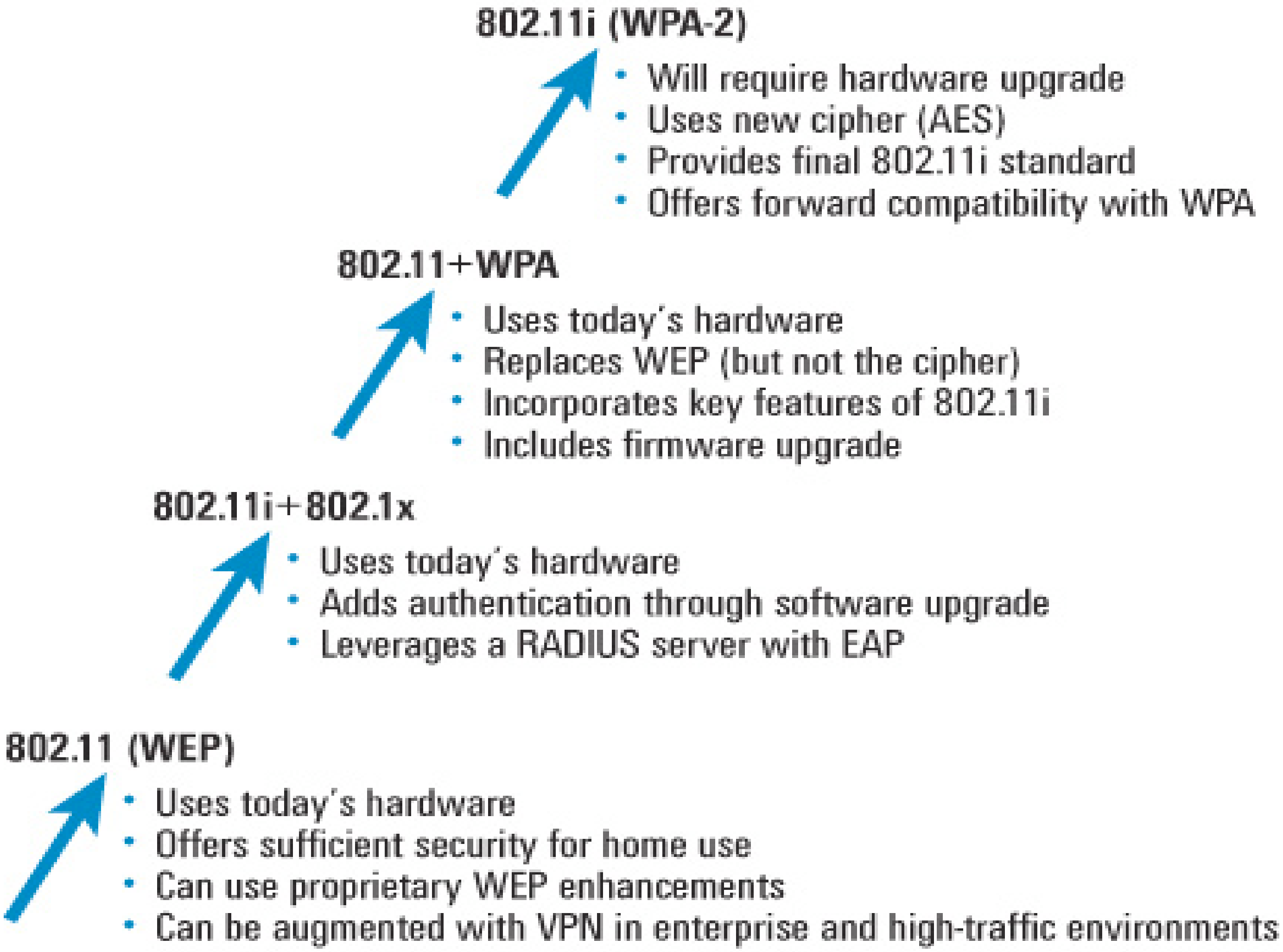
- **Access Control -** Ensure that your wireless infrastructure is not mis-used. This calls for Efficient Key Management

- **Data Integrity -** Ensure that your data packets are not modified in transit.

- **Confidentiality -** Ensure that the contents of your wireless traffic is not learned. Proper Encryption mechanisms need to be implemented.



Wireless Security Standards



802.11i (WPA-2)

- Will require hardware upgrade
- Uses new cipher (AES)
- Provides final 802.11i standard
- Offers forward compatibility with WPA

802.11+WPA

- Uses today's hardware
- Replaces WEP (but not the cipher)
- Incorporates key features of 802.11i
- Includes firmware upgrade

802.11i+802.1x

- Uses today's hardware
- Adds authentication through software upgrade
- Leverages a RADIUS server with EAP

802.11 (WEP)

- Uses today's hardware
- Offers sufficient security for home use
- Can use proprietary WEP enhancements
- Can be augmented with VPN in enterprise and high-traffic environments

Description of WEP Protocol

WEP relies on a **secret key(64 bit/128 bit)** which is shared between the sender and the receiver.

SENDER: Mobile station (eg.Laptop with a wireless ethernet card)

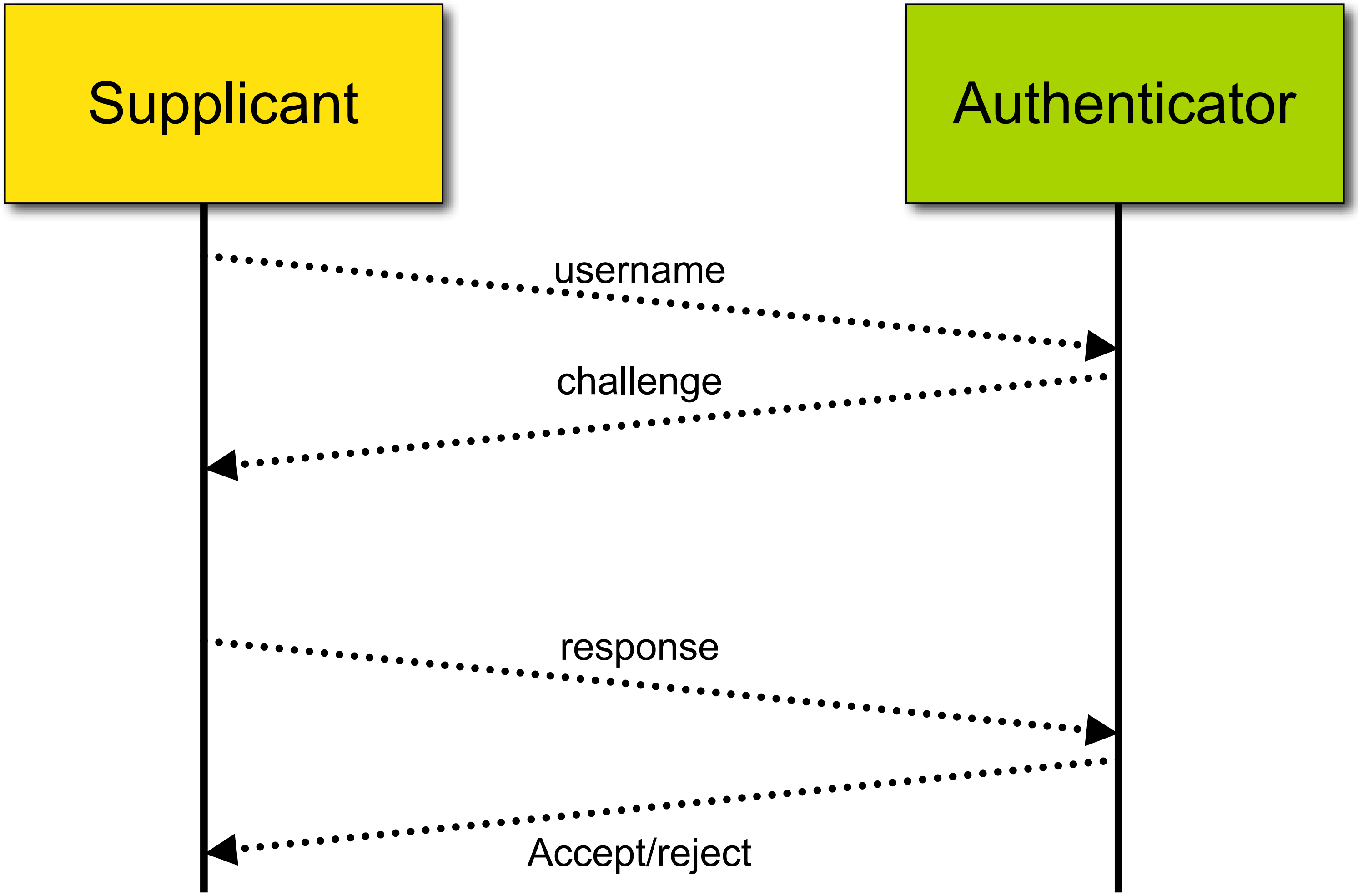
RECEIVER: Access Point (eg. base station)

- **Secret Key** is used to encrypt packets before they are transmitted
- **Integrity Check** is used to ensure packets are not modified in transit.

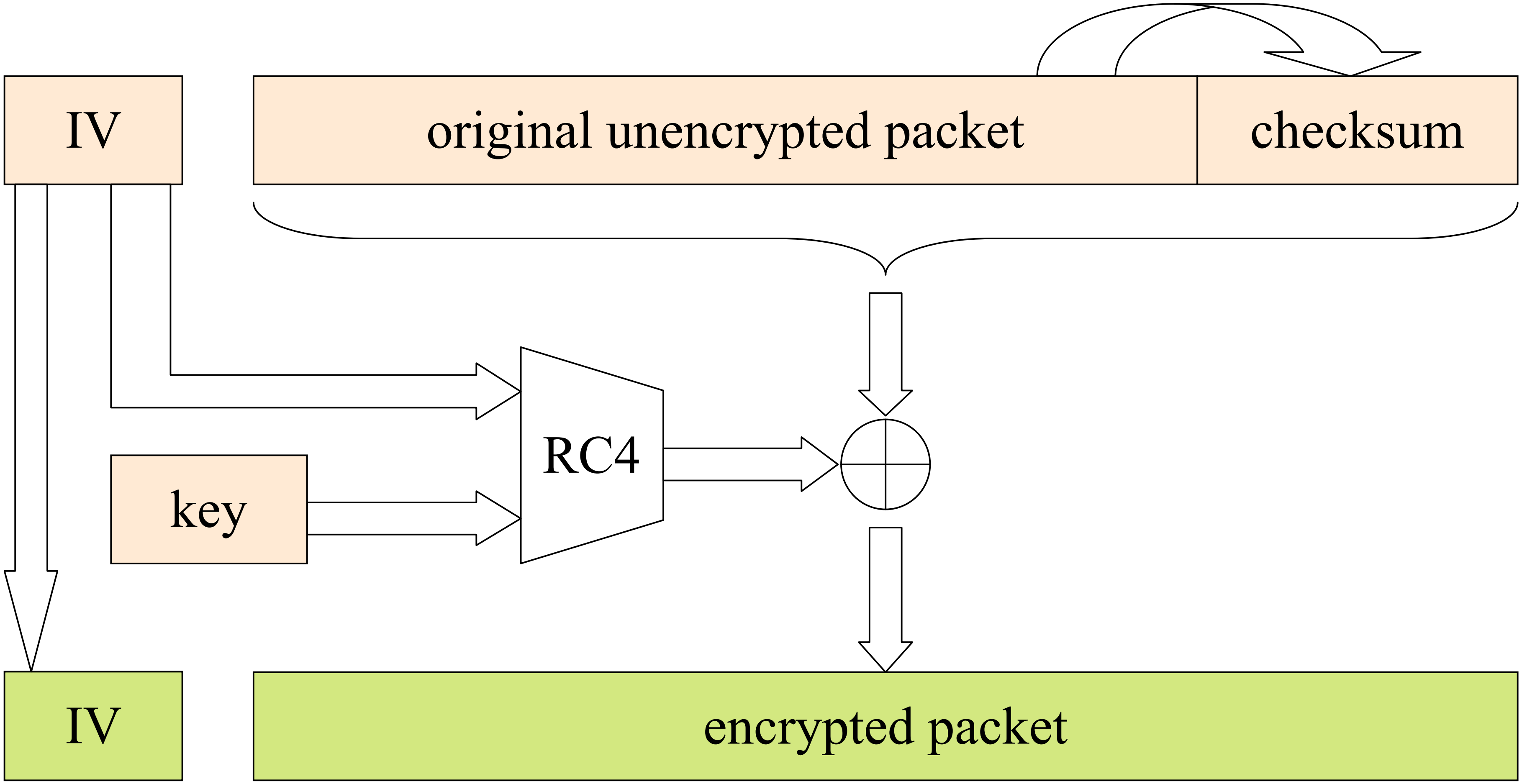
The standard does not discuss how shared key is established

In practice, most installations use a **single key** which is shared between all mobile stations and access points.

CHAP Authentication

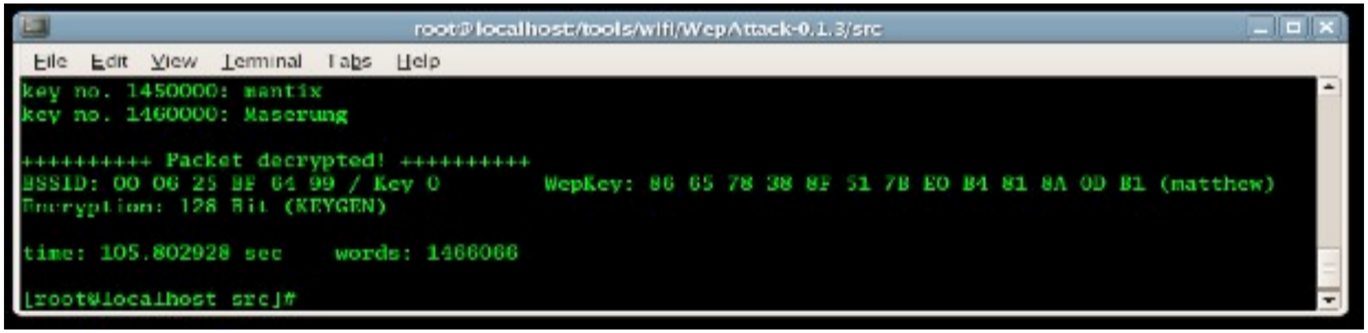


How WEP works



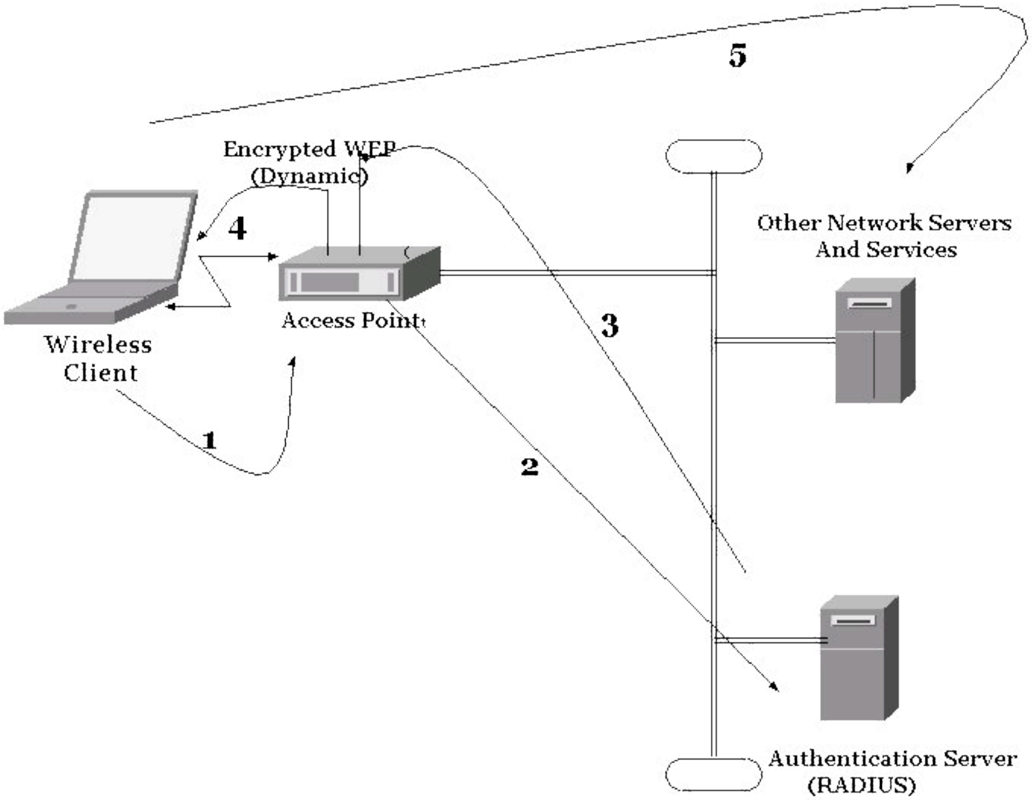
Deficiencies of WEP

- IV is too short and not protected from reuse.
- The per packet key is constructed from the IV, making it susceptible to weak key attacks.
- No effective detection of message tampering (message integrity).
- No built-in provision to update the keys in all wireless clients connected to the access point.
- No protection against message replay.


root@localhost:/tools/wifi/WepAttack-0.1.3/src
File Edit View Terminal Tabs Help

```
key no. 1450000: mantix
key no. 1460000: Maserung

++++++++++ Packet decrypted! ++++++++++
BSSID: 00 06 25 BF 64 99 / Key 0        WepKey: 86 65 78 38 8F 51 7B E0 B4 81 8A 0D B1 (matthew)
Encryption: 128 Bit (KEYGEN)

time: 105.802928 sec     words: 1466066

[root@localhost src]#
```

Radius: An additional layer in the security



WPA (Wi-Fi Protected Access)

- IEEE 802.1X authentication server- LEAP, EAP/TLS, PEAP

  or

  PSK (Pre-Shared Key)

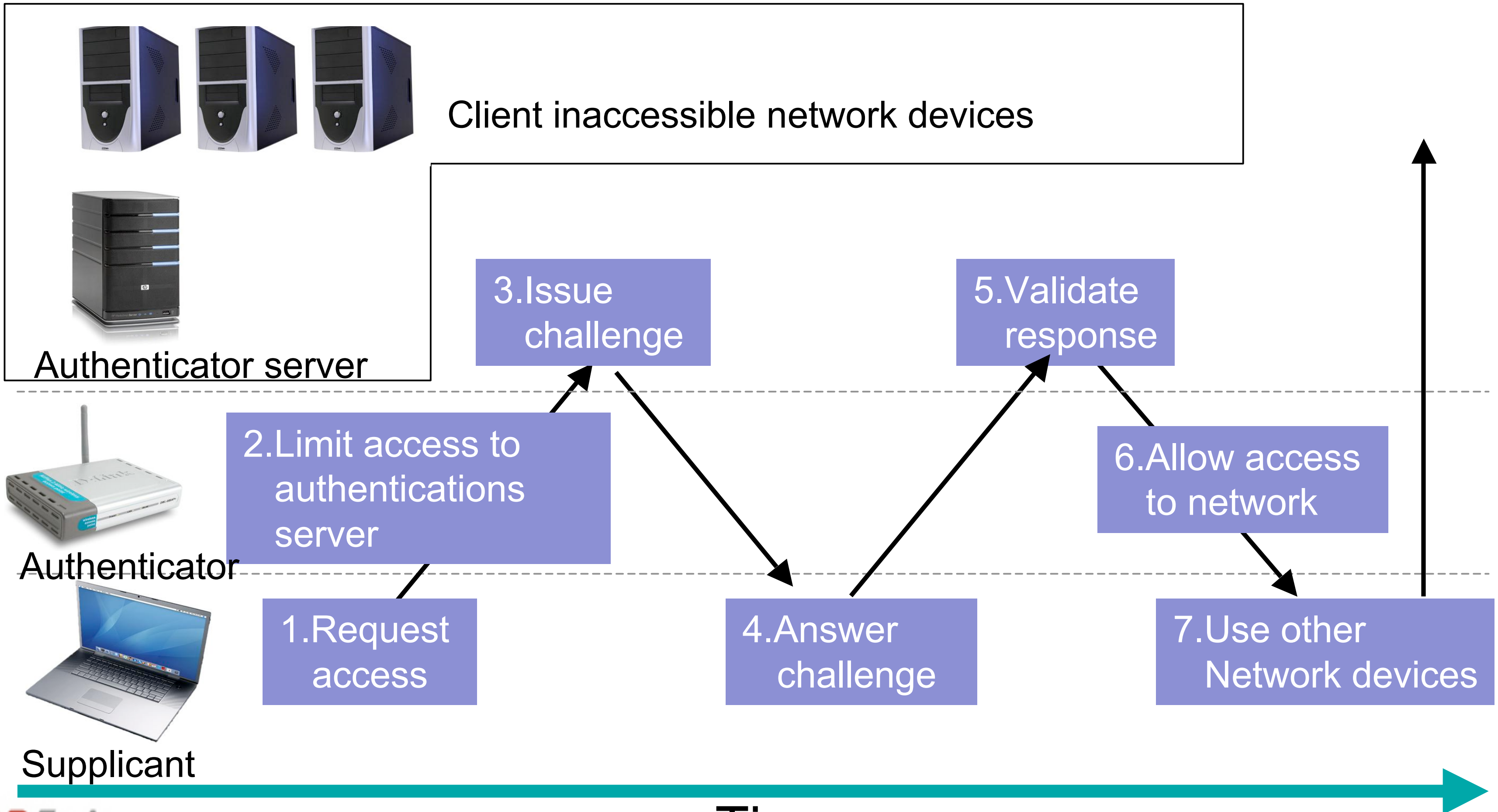
- RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV).

- Temporal Key Integrity Protocol (TKIP)

- Message Integrity Code (MIC) Michael to ensure data Integrity

802.1x

- Port-based access control
- Mutual authentication via authentication server



Client inaccessible network devices
Authenticator server
Authenticator
Supplicant
3.Issue challenge
5.Validate response
2.Limit access to authentications server
6.Allow access to network
1.Request access
4.Answer challenge
7.Use other Network devices
Time

WPA - PSK

- No RADIUS server required

- A Shared secret key is used.

- That PSK is usually generated by combining the WLAN's name (Service Set Identifier, SSID) with a passphrase (an ASCII string, 8-63 characters.)

- A passphrase less than 64 characters can be insecure

- Management is handled on the AP

  - Vulnerable to dictionary attacks

Temporal Key Integrity Protocol

- Fixes the flaw of key reuse in WEP
- Comprised of three parts, guarantees clients different keys
  - 128-bit temporal key, shared by clients and APs
  - MAC of client
  - 48-bit IV describes packet sequence number
- Increments the value of the IV to ensure every frame has a different value
- Changes temporal keys every 10,000 packets
- Uses RC4 like WEP, so only software or firmware upgrade required

Michael Message Integrity Check (MMIC)

- Message Integrity Code (MIC) - 64-bit message calculated using “Michael” algorithm inserted in TKIP packet to detect content alteration
- Message is concatenated with the secret key and the result is hashed
- Protects both data and header
- Implements a frame counter, which discourages replay attacks

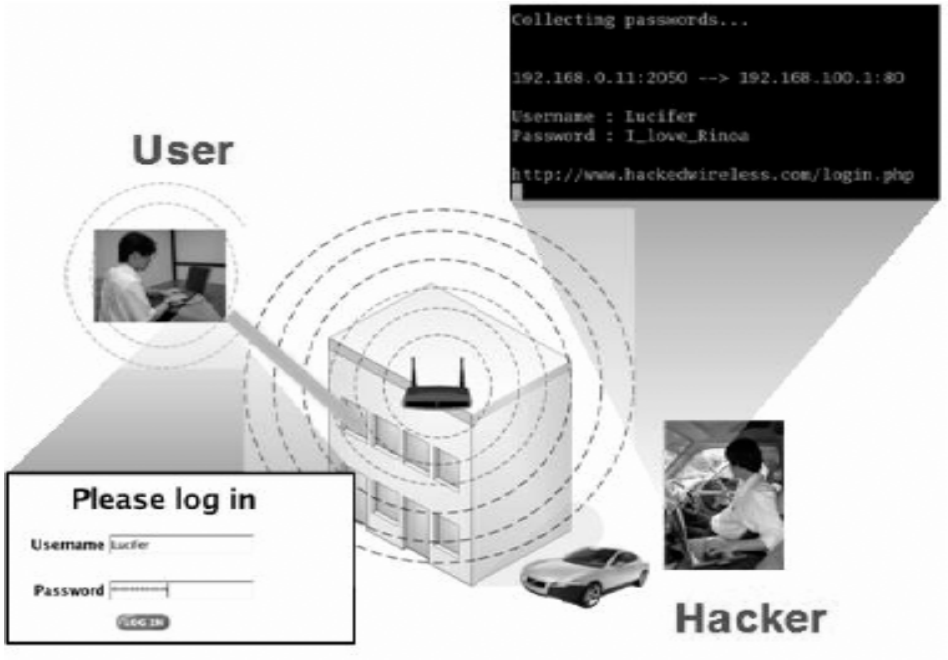
WPA

- Confidentiality: Per-packet keying via TKIP
- Message Authenticity: Michael algorithm
- Access Control and Authentication: IEEE 802.1x -EAP/TLS

Deficiencies of WPA

- **Dictionary Attack on WPA-PSK -** The weak passphrases users typically employ are vulnerable to dictionary attacks.

- **DoS Attacks** - Due to inevitable weaknesses of Michael, TKIP will shut down the network for one minute if two frames are discovered that fail the Michael check after passing all other integrity checks that would have caught noisy frames.



```
Collecting passwords...

192.168.0.11:2050 --> 192.168.100.1:80

Username : Lucifer
Password : I_love_Rinoa

http://www.hackedwireless.com/login.php
```

Please log in

Username Lucifer

Password ********

WPA2 – 802.11i

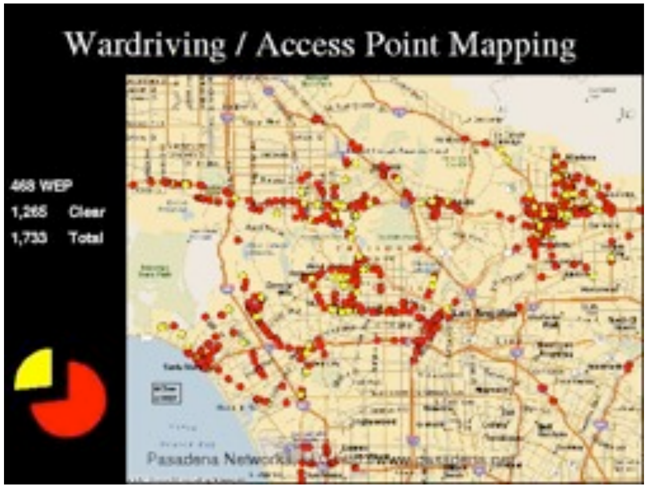
- 802.1x for authentication.
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) to provide confidentiality, integrity and origin authentication.
- AES replaces RC4 w/TKIP

A Comparison

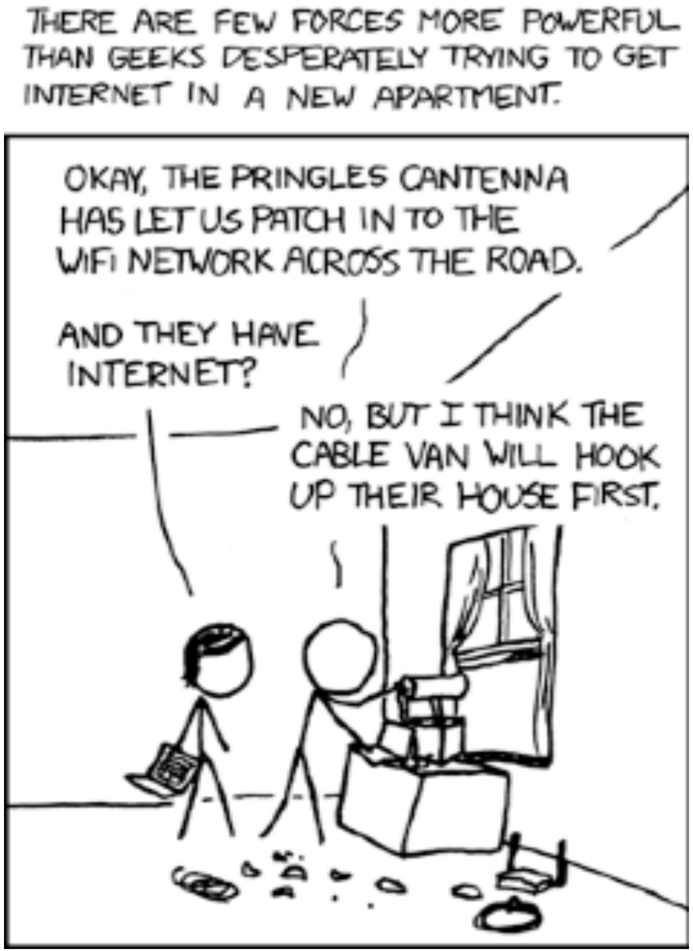
	WEP	**WPA**	**WPA2**
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits	128 bits
Key Life	24 bit IV	48 bit IV	48 bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC - 32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP - Based	EAP - Based

Exploiting Vulnerabilities

1. Locating a wireless network
2. Attaching to the Found Wireless Network
3. Sniffing Wireless Data


Wardriving / Access Point Mapping
468 WEP
1,265 Clear
1,733 Total
Pasadena Networks www.pasadena.net

Locating a wireless network


THERE ARE FEW FORCES MORE POWERFUL THAN GEEKS DESPERATELY TRYING TO GET INTERNET IN A NEW APARTMENT.
OKAY, THE PRINGLES CANTENNA HAS LET US PATCH IN TO THE WIFI NETWORK ACROSS THE ROAD.
AND THEY HAVE INTERNET?
NO, BUT I THINK THE CABLE VAN WILL HOOK UP THEIR HOUSE FIRST.

We need a special holiday to honor the countless kind souls with unsecured networks named 'linksys'.

Source : http://www.xkcd.com
Strip Number: 466

Trivia

- More than 320 wi-fi networks were open and unsafe near
  - Mumbai Airport / Andheri.
  - Major regions of central Mumbai are dominated by Netgear devices.
  - Major western region of Mumbai is dominated by Linksys devices.
  - Thane, surprisingly had over 170 hotspots.

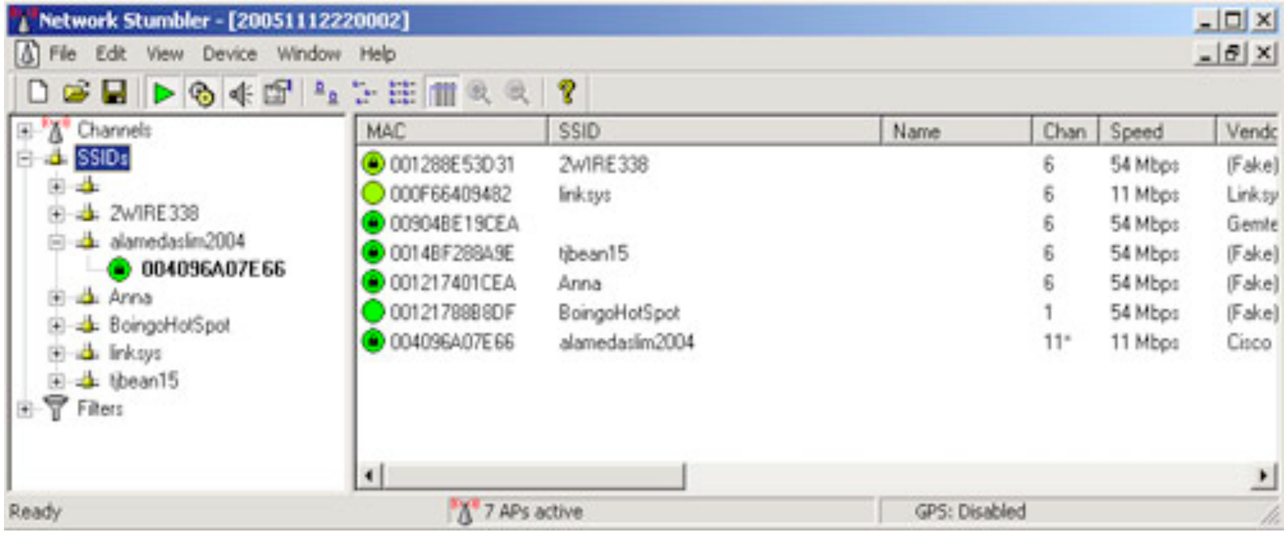
- These were active insecure / open access points / networks.

Ref: http://www.techgoss.com/Story/141S11-Terrorists-exploit-Mumbai-net-security.aspx

Locating a wireless network

There are two tools that are commonly used in this regard:

- **NetStumbler** – This Windows based tool easily finds wireless signals being broadcast within range



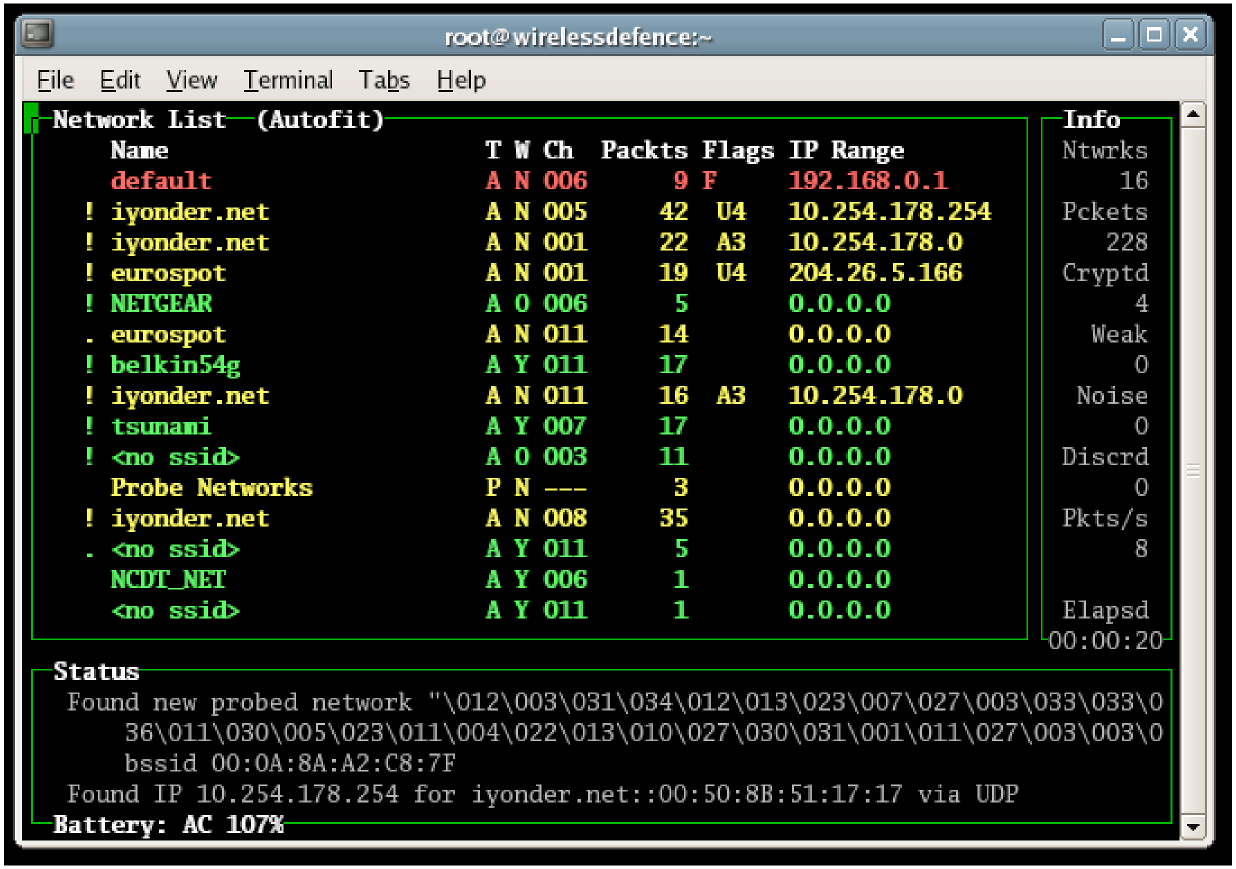
Network Stumbler - [20051112220002]

MAC	SSID	Name	Chan	Speed	Vendo
001288E53D31	2WIRE338		6	54 Mbps	(Fake)
000F66409482	linksys		6	11 Mbps	Linksy
00904BE19CEA			6	54 Mbps	Gemte
0014BF288A9E	tjbean15		6	54 Mbps	(Fake)
001217401CEA	Anna		6	54 Mbps	(Fake)
00121788B8DF	BoingoHotSpot		1	54 Mbps	(Fake)
004096A07E66	alamedaslim2004		11*	11 Mbps	Cisco

Ready 7 APs active GPS: Disabled

Locating a wireless network (contd)

- **Kismet** – Kismet will detect and display SSIDs that are not being broadcast which is very critical in finding wireless networks.

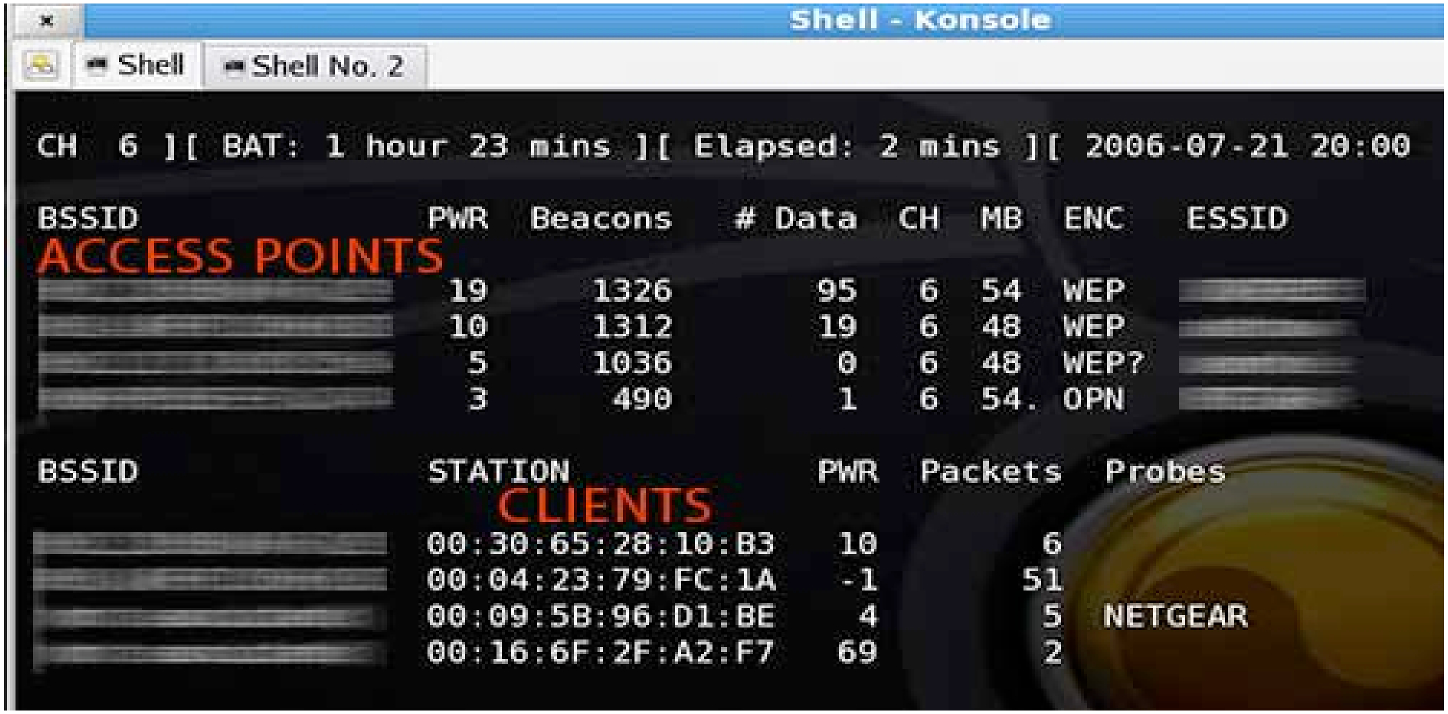


```
Network List (Autofit)                                                    Info
     Name                       T W Ch  Packts Flags IP Range             Ntwrks
     default                    A N 006      9 F     192.168.0.1              16
   ! iyonder.net                A N 005     42  U4   10.254.178.254       Pckets
   ! iyonder.net                A N 001     22  A3   10.254.178.0            228
   ! eurospot                   A N 001     19  U4   204.26.5.166         Cryptd
   ! NETGEAR                    A O 006      5       0.0.0.0                   4
   . eurospot                   A N 011     14       0.0.0.0                Weak
   ! belkin54g                  A Y 011     17       0.0.0.0                   0
   ! iyonder.net                A N 011     16  A3   10.254.178.0          Noise
   ! tsunami                    A Y 007     17       0.0.0.0                   0
   ! <no ssid>                  A O 003     11       0.0.0.0              Discrd
     Probe Networks             P N ---      3       0.0.0.0                   0
   ! iyonder.net                A N 008     35       0.0.0.0              Pkts/s
   . <no ssid>                  A Y 011      5       0.0.0.0                   8
     NCDT_NET                   A Y 006      1       0.0.0.0
     <no ssid>                  A Y 011      1       0.0.0.0              Elapsd
                                                                        00:00:20
Status
 Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\0
     36\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0
     bssid 00:0A:8A:A2:C8:7F
 Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP
Battery: AC 107%
```

Attaching to the Found Wireless Network

If the wireless network is using authentication and/or encryption, you may need one of the following tools.

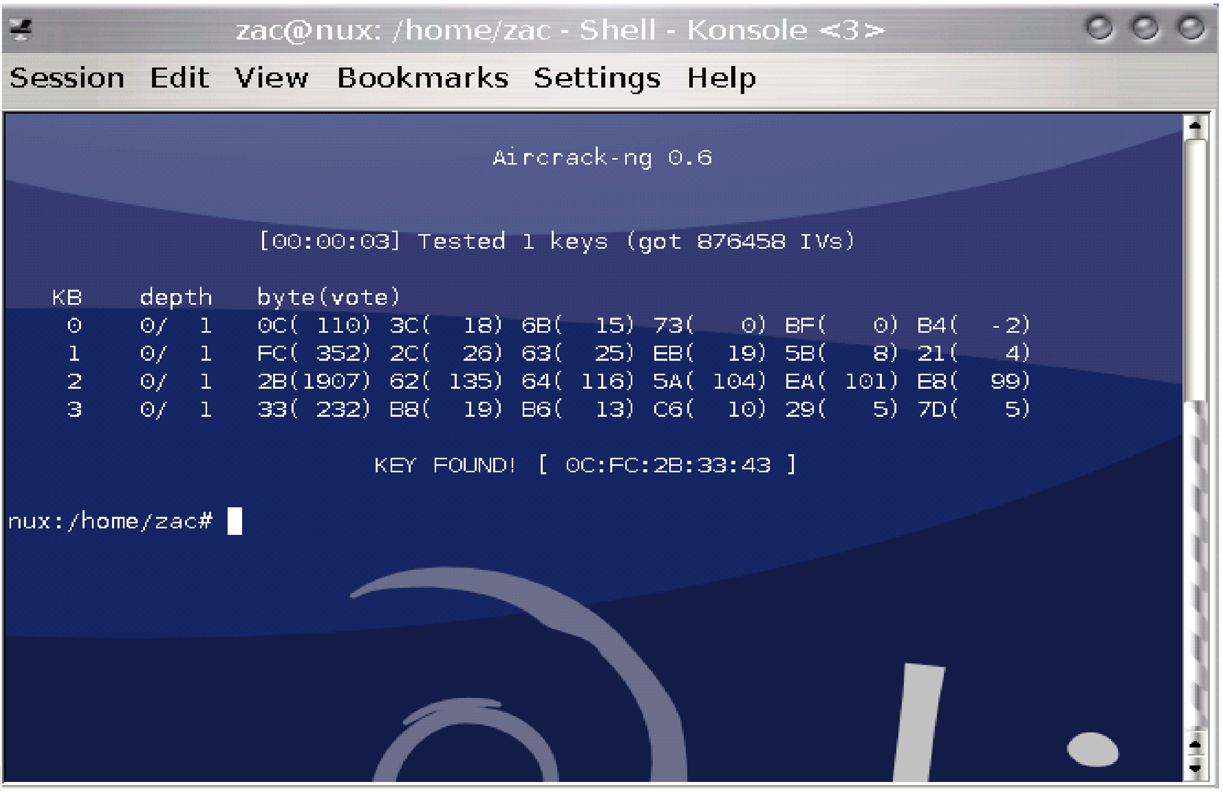
- **Airodump-ng** - packet capture program, collects authentication handshake
- **Aireplay-ng** - de-authenticator /packet injection program



```
 CH  6 ][ BAT: 1 hour 23 mins ][ Elapsed: 2 mins ][ 2006-07-21 20:00

 BSSID              PWR  Beacons   # Data  CH  MB  ENC   ESSID

 [redacted]          19     1326       95   6  54  WEP   [redacted]
 [redacted]          10     1312       19   6  48  WEP   [redacted]
 [redacted]           5     1036        0   6  48  WEP?  [redacted]
 [redacted]           3      490        1   6  54. OPN   [redacted]

 BSSID              STATION            PWR  Packets  Probes

 [redacted]         00:30:65:28:10:B3   10        6
 [redacted]         00:04:23:79:FC:1A   -1       51
 [redacted]         00:09:5B:96:D1:BE    4        5  NETGEAR
 [redacted]         00:16:6F:2F:A2:F7   69        2
```

Attaching to the Found Wireless Network (contd)

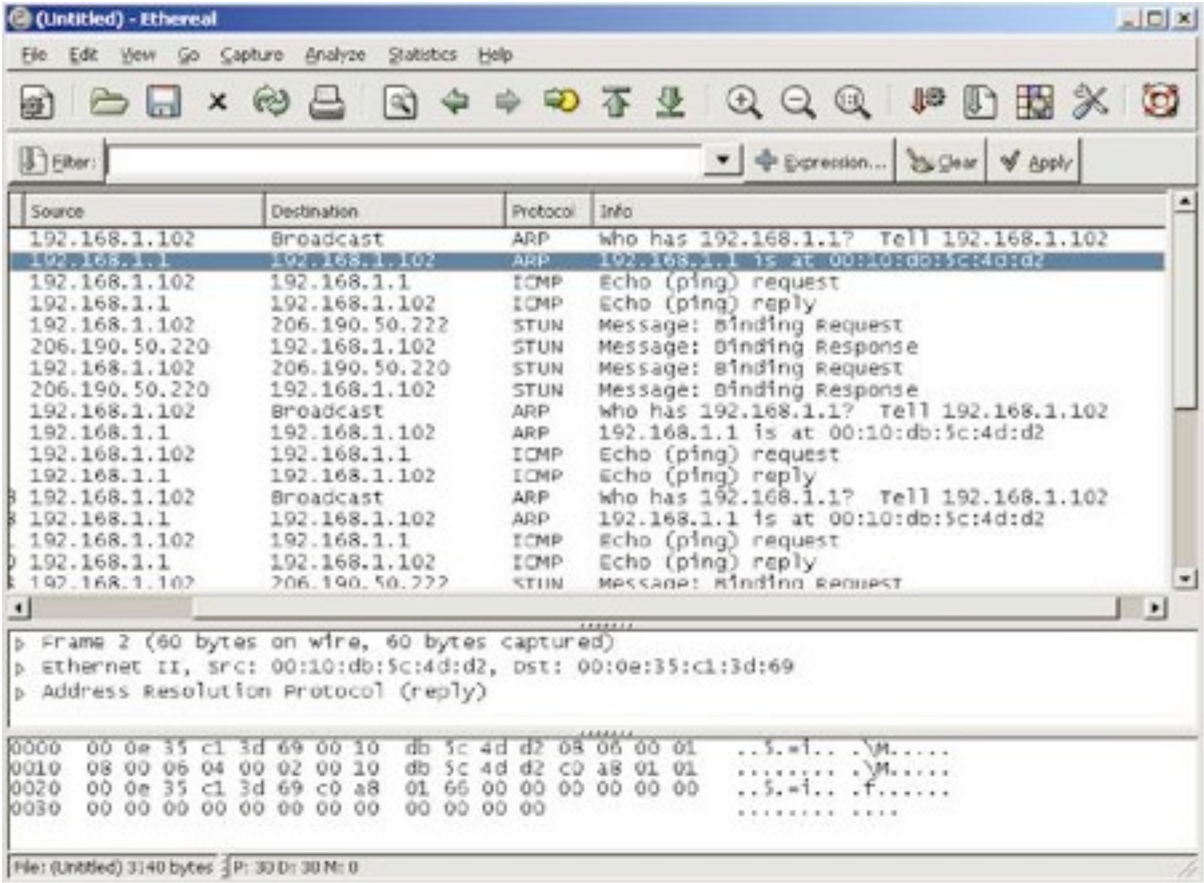
- **CowPatty** – Brute force tool for cracking WPA-PSK..
- **Aircrack-ng** - To crack PSK using authentication handshake
- **Airdecap** - Decrypts WEP/WPA capture files



```
                                 Aircrack-ng 0.6


                  [00:00:03] Tested 1 keys (got 876458 IVs)

    KB    depth   byte(vote)
     0    0/  1   0C( 110) 3C(  18) 6B(  15) 73(   0) BF(   0) B4(  -2)
     1    0/  1   FC( 352) 2C(  26) 63(  25) EB(  19) 5B(   8) 21(   4)
     2    0/  1   2B(1907) 62( 135) 64( 116) 5A( 104) EA( 101) E8(  99)
     3    0/  1   33( 232) B8(  19) B6(  13) C6(  10) 29(   5) 7D(   5)

                        KEY FOUND! [ 0C:FC:2B:33:43 ]

nux:/home/zac# █
```

Sniffing Wireless Data

- **Wireshark** –Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff-out 802.11 management beacons and probes and subsequently could be used as a tool to sniff-out non-broadcast SSIDs.



```
Source             Destination        Protocol  Info
192.168.1.102      Broadcast          ARP       Who has 192.168.1.1?  Tell 192.168.1.102
192.168.1.1        192.168.1.102      ARP       192.168.1.1 is at 00:10:db:5c:4d:d2
192.168.1.102      192.168.1.1        ICMP      Echo (ping) request
192.168.1.1        192.168.1.102      ICMP      Echo (ping) reply
192.168.1.102      206.190.50.222     STUN      Message: Binding Request
206.190.50.220     192.168.1.102      STUN      Message: Binding Response
192.168.1.102      206.190.50.220     STUN      Message: Binding Request
206.190.50.220     192.168.1.102      STUN      Message: Binding Response
192.168.1.102      Broadcast          ARP       Who has 192.168.1.1?  Tell 192.168.1.102
192.168.1.1        192.168.1.102      ARP       192.168.1.1 is at 00:10:db:5c:4d:d2
192.168.1.102      192.168.1.1        ICMP      Echo (ping) request
192.168.1.1        192.168.1.102      ICMP      Echo (ping) reply
192.168.1.102      Broadcast          ARP       Who has 192.168.1.1?  Tell 192.168.1.102
192.168.1.1        192.168.1.102      ARP       192.168.1.1 is at 00:10:db:5c:4d:d2
192.168.1.102      192.168.1.1        ICMP      Echo (ping) request
192.168.1.1        192.168.1.102      ICMP      Echo (ping) reply
192.168.1.102      206.190.50.222     STUN      Message: Binding Request
```

```
▷ Frame 2 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: 00:10:db:5c:4d:d2, Dst: 00:0e:35:c1:3d:69
▷ Address Resolution Protocol (reply)
```

```
0000  00 0e 35 c1 3d 69 00 10  db 5c 4d d2 08 06 00 01   ..5.=i.. .\M.....
0010  08 00 06 04 00 02 00 10  db 5c 4d d2 c0 a8 01 01   ........ .\M.....
0020  00 0e 35 c1 3d 69 c0 a8  01 66 00 00 00 00 00 00   ..5.=i.. .f......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: (Untitled) 3140 bytes P: 30 D: 30 M: 0

Recommendations for Securing Your Home Wireless Network

- Change the router's default passwords.
- Change the SSID name and disable SSID broadcast.
- Setup MAC filters to limit which computers can connect.
- Turn on WPA or WPA2 encryption.
- If you are using WPA-PSK, ensure passphrase is 64 character with no dictionary word.
- Review your wireless logs.
- Watch for upgrades from the manufacturer.
- Practice good computer security.

Recommendations for securing Enterprise Networks

1. Define, monitor and enforce a wireless security policy

- Policy should cover all 802.11 and Bluetooth wireless devices
- Define wireless policies for mobile workers
- Ensure wireless devices are not used until they comply with the wireless security policy

2. Take a complete inventory of all Access Points and 802.11 devices in the airwaves

- Eliminate rogue Access Points and unauthorized user Stations.

Recommendations for securing Enterprise Networks (Contd)

3. Define secure configurations for Access Points and user Stations

- Change default setting
- Disable SSID broadcast
- Turn-off “ad-hoc” mode operation

4. Define acceptable encryption and authentication protocols

- Use strong authentication (802.1x with EAP recommended)
- Use strong encryption with at least 128-bit keys (WPA2, WPA recommended)
- Deploy a layer-3 Virtual Private Network (VPN) for wireless communication

Recommendations for securing Enterprise Networks (Contd)

5. Monitor the airwaves to identify suspicious activity

- Deploy a Wireless Intrusion Detection System (IDS) to identify threats and attacks
- Detect and terminate unauthorized associations in a timely manner
- Monitor wireless assets for policy violations
- Log, analyze, and resolve incidents in a timely manner
- Gather and store wireless activity information for forensic analysis

References

- http://www.ethicalhacker.net/content/view/16/24/
- http://securitytube.net/War-Driving-is-so-2000,-Here-comes-war-shipping-video.aspx
- http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf
- Best Practices for Wireless Network Security and Sarbanes-Oxley compliance - AirDefence
- Wikipedia!

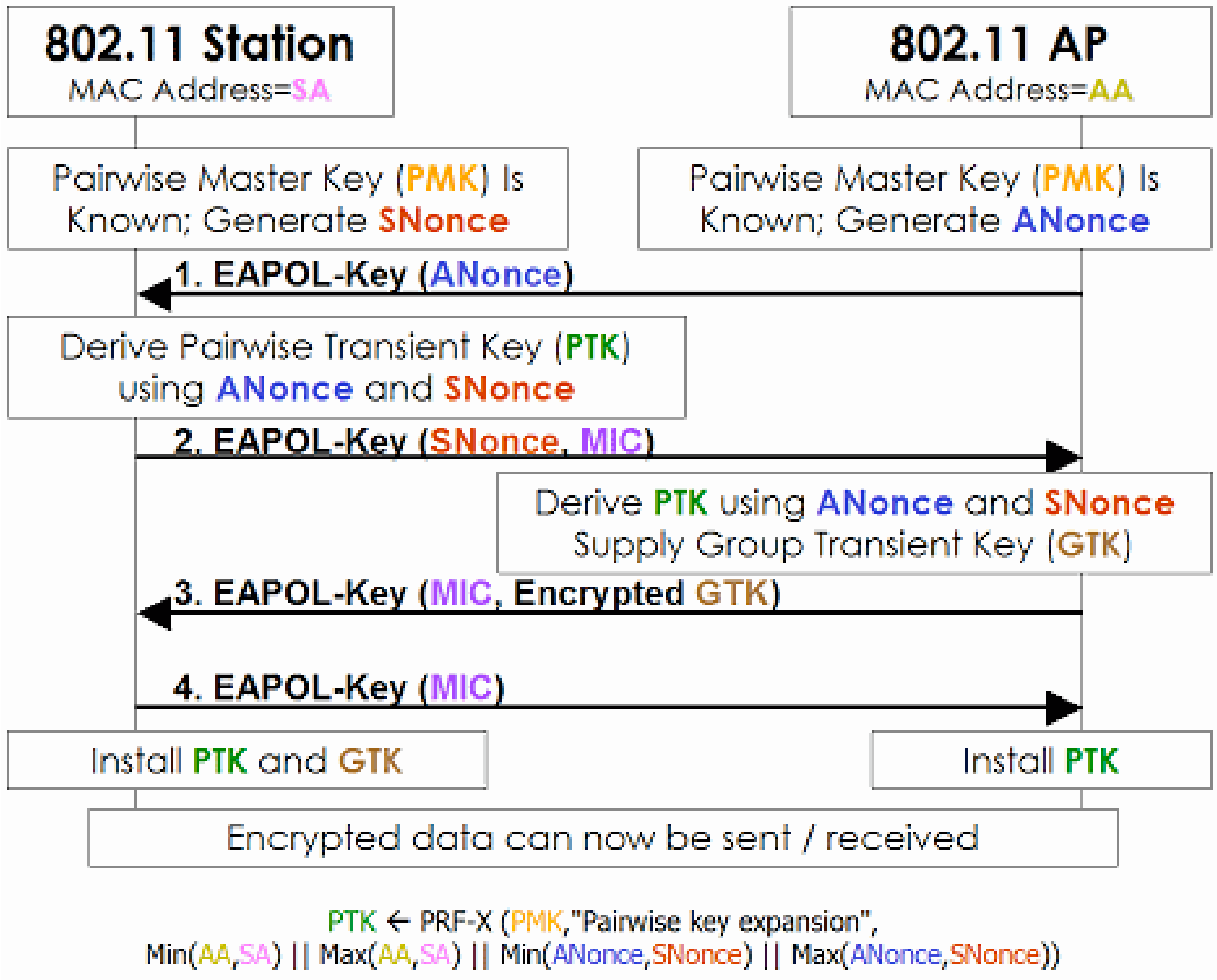
Questions :-?

Thank You!

Types of EAP

- LEAP - Cisco proprietary, uses username/password to authenticate against RADIUS
- TLS - RFC 2716, uses X.509 certificates for authentication on both Supplicant and Authenticator
- TTLS - Developed by Funk Software, Authenticator uses a certificate to identify itself, Supplicant can use username/password
- PEAP - Authenticator uses certificate, Supplicant can use username/password

Four-way Key Handshake



802.11 Station
MAC Address=SA

802.11 AP
MAC Address=AA

Pairwise Master Key (PMK) Is Known; Generate SNonce

Pairwise Master Key (PMK) Is Known; Generate ANonce

1. EAPOL-Key (ANonce)

Derive Pairwise Transient Key (PTK) using ANonce and SNonce

2. EAPOL-Key (SNonce, MIC)

Derive PTK using ANonce and SNonce
Supply Group Transient Key (GTK)

3. EAPOL-Key (MIC, Encrypted GTK)

4. EAPOL-Key (MIC)

Install PTK and GTK

Install PTK

Encrypted data can now be sent / received

PTK ← PRF-X (PMK,"Pairwise key expansion",
Min(AA,SA) || Max(AA,SA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))

OWASP