

First off, a brief overview of the RF range of the electromagnetic spectrum.

- ▶ Radio waves have a frequency, hertz, of around 3Hz up to 300GHz
- ▶ The higher the frequency the shorter the wavelength
- ▶ The frequency range is split up using different names
- ▶ e.g Extremely Low Frequency (ELF) up to Extremely High Frequency(EHF)
- ▶ The frequency range is licensed. It is illegal to transmit without a license, except for certain ranges

Radio frequency properties

- ▶ As a simplistic explanation, low frequency radio waves are low bandwidth, high range
- ▶ As frequency increases, the bandwidth increases, but range decreases
- ▶ The variation in range is due to the ability of low frequency signals to effectively 'bounce' off obstacles, including buildings, walls and the ionosphere.
- ▶ Higher frequency signals do not bounce as well and so can be restricted to straight lines
- ▶ Increasing the signal power (measured in watts) can increase the ability to penetrate obstacles, but does not increase the ability to 'bounce'.
- ▶ Signals are broadcast from antennae. These antennae can be directional or omnidirectional

Examples

- ▶ FM broadcasting - VHF 87.5 - 108.0 MHz VHF range
 - ▶ A 100,000 watt signal broadcast in this range might reach up to 240km.
 - ▶ This is limited to around 19 kilobaud
- ▶ Microwave
 - ▶ In the EHF range,
 - ▶ Used as a point to point link with directional antennae for multiplexing phone calls
 - ▶ Set 70km apart for AT&T transmitters
 - ▶ The unlicensed 2.4GHz range is microwave

Radio transmission and jamming

- ▶ Disrupting a radio transmission is a simple concept.
Broadcast noise on the frequency being used
- ▶ If broadcasting on licensed spectrums (without a license), jamming is illegal
- ▶ Frequency hopping is used to try to prevent jamming.
e.g Military radio, Bluetooth



Wireless technologies

We will look at the following technologies in terms of security

- ▶ Wireless LAN - 802.11
- ▶ Bluetooth
- ▶ GSM

802.11 is a range of wireless standards implemented by the IEEE. Relevant 802.11 standards are

- ▶ 802.11b/g/n
- ▶ 802.11i
- ▶ Wireless lan consist of client stations and an Access Point in infrastructure mode
- ▶ Ad-Hoc mode is peer to peer, no AP.
- ▶ A Wlan is identified by its SSID - Service Set IDentifier

802.11 networks use management frames to control communication.

- ▶ Authentication/Deauthentication frame - Open System or Shared key
- ▶ Association/Disassociation/reassociation
- ▶ Beacons
- ▶ Probe Request/Response

Connecting to an AP

A client station locates an Access Point either via a Probe Request or by observing Beacons. Once this is done

- ▶ Client sends an Authentication request
- ▶ AP responds with an Authentication fail or success
- ▶ If successful, client sends an Association request
- ▶ AP sends back an Association Response
- ▶ Depending on the authentication/encryption used there may be more steps then

There are four main 802.11 encryption standards in use

- ▶ None
- ▶ WEP
- ▶ WPA
- ▶ WPA2

Wlan was originally designed to be secured using WEP.
Wired Equivalent Privacy

- ▶ WEP has multiple key sizes, 64, 128 and 256 bits. Initial implementations were limited to 64 bit due to American export restrictions.
- ▶ It uses RC4, a stream cipher
- ▶ The Initialisation Vector is 24 bits, resulting in actual key sizes of 40, 104 and 232 bits

WEP Flaws

WEP has numerous flaws however, making it ineffective.

- ▶ Some practical issues are is that it's optional and it uses a single shared key. No key management system.
- ▶ Brute force attack on 40bit key. Some implementation made this easier
- ▶ Keystream re-use. Authentication requests for shared key make this one easier too.
- ▶ In 2001 Fluhrer, Mantin and Shamir (FMS attack) discovered a flaw in the use of RC4 and 'weak IVs'. Simply listening to enough sent packets allows for cryptanalysis and determination of the key.
- ▶ This took time however, and one solution was to have a set of keys and rotate amongst them.
- ▶ It's possible to generate enough traffic rapidly, using some tricks to obtain the key

<http://www.smallnetbuilder.com/content/view/24244/98/> is a good article describing the process. Images used here are taken from that article.

- ▶ First, find the wireless networks. Kismet for Linux, or Netstumbler for Windows will do this. (There are issues with wireless network cards, the chipset needs to be of a certain type).
- ▶ Kismet will find SSIDs, AP MACs and the MACs of clients

Kismet wlan0

Network List (Autofit)							Info
Name	T	M	Ch	Pkcts	Flags	IP Range	Size
! linksys	A	Y	001	14		0.0.0.0	0B
! starbucks	A	Y	006	1371		0.0.0.0	0B
! thg2	A	Y	001	75		0.0.0.0	0B
! thg	A	Y	003	181		0.0.0.0	37k
! District 24	A	Y	006	139		0.0.0.0	3k
! law	A	N	006	32	U	192.168.0.1	0B
! BFI	A	Y	010	2		0.0.0.0	0B
! 209	A	Y	011	5		0.0.0.0	0B
209	P	N	---	9		0.0.0.0	0B

Info

Nturks
9

Pkcts
1948

Cryptd
121

Weak
0

Noise
4

Discrd
119

Pkts/s
77

Elapsd
00:00:21

Status

Connected to Kismet server version 2005_01_R1 build 200501111115152 on localhost:2501
Found new probed network "209" bssid 00:06:25:1A:05:D2

Battery: AC 100% 10h0m0s

Cracking WEP

Once the target network has been found, the cracking attempt can begin

- ▶ The Aircrack-ng suite of tools contains the latest implementations of the WEP cracks
- ▶ There are several tools to be used. airon-ng, airodump-ng, airreplay-ng, aircrack-ng.
- ▶ The card is put into Monitor mode using airon-ng. Similar to Promiscuous mode on a standard NIC, it listens for all traffic, not just traffic sent to it.
- ▶ Traffic is then recorded using airdump-ng, in a similar manner to tcpdump.

```
10.168.3.113 - PuTTY
CH 7 ][ Elapsed: 9 mins ][ 2007-07-31 15:21

BSSID           PWR Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:06:25:B2:D4:19  50   1336       246   0   5  48  WEP  WEP   OPN  linksys
00:14:6C:B6:64:4A  53   1798         0   0   1  54. WEP  WEP           NETGEAR

BSSID           STATION            PWR  Lost  Packets  Probes
00:06:25:B2:D4:19 00:1A:70:7F:79:F2  39    0     56  linksys
(not associated)  00:16:6F:B1:F7:46  64   78    237  littleharbor,default,Li
```

At this point, the aircrack-ng program can be run on the dump file from airodump, but it will take a long time. We need to generate more traffic.

- ▶ ARP requests are identifiable because of the size of the packet, even when its encrypted. If a captured ARP request is resent, the AP will broadcast it, using a new IV. Sending a flood of ARP Request replays will generate traffic
- ▶ Send a faked Deauth. Client will re-auth, generating more traffic. Obviously a noticeable attack

Aircrack-ng is then run on the recorded IVs and will usually crack the key fairly quickly.

Airreplay-ng

CA645

Gavin O' Gorman

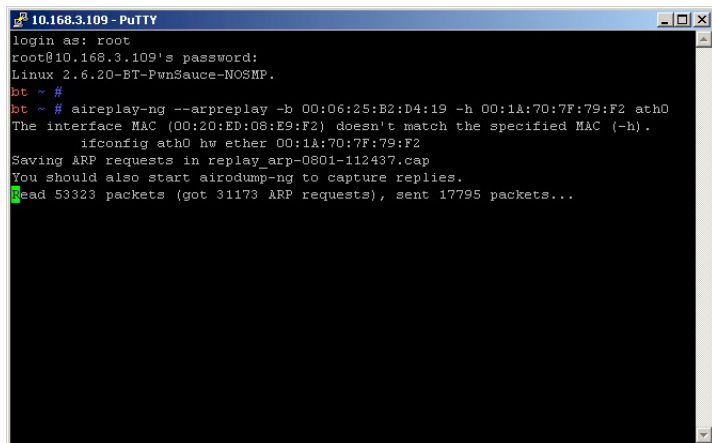
Radio waves

Wireless
Technologies

802.11

Bluetooth

GSM



```
10.168.3.109 - PuTTY
login as: root
root@10.168.3.109's password:
Linux 2.6.20-BT-PwnSauce-NOSMP.
bt ~ #
bt ~ # aireplay-ng --arp-replay -b 00:06:25:B2:D4:19 -h 00:1A:70:7F:79:F2 ath0
The interface MAC (00:20:ED:08:E9:F2) doesn't match the specified MAC (-h).
    ifconfig ath0 hw ether 00:1A:70:7F:79:F2
Saving ARP requests in replay_arp-0801-112437.cap
You should also start airodump-ng to capture replies.
Read 53323 packets (got 31173 ARP requests), sent 17795 packets...
```

Beyond WEP

WEP is clearly broken. Breaking WEP and gaining access to a wireless network is very easy. To maintain backwards compatibility with existing hardware, TKIP was developed.

Temporal Key Integrity Protocol

- ▶ TKIP was partially implemented and named WPA (Wi-Fi Protected Access). It still uses the RC4 stream cipher.
 - ▶ Key mixing function to generate more keys
 - ▶ A sequence counter to prevent replay attacks
 - ▶ A new message integrity code.
- ▶ A full implementation of TKIP was then implemented and call WPA2

WPA2 offers a more comprehensive range of security and keying options.

- ▶ AES is now used instead of RC4
- ▶ Access is controlled with WPA-PSK or 802.1x authentication
 - ▶ WPA-PSK - Pre-shared key. A 256bit key, or 64hex digits, or a passphrase converted into 256 bits.
 - ▶ 802.1x is an architecture to delegate identification/authentication/key management to another service. It allows for integration with a companies authentication systems and for more secure access.

WPA2 does have some vulnerabilities

- ▶ When using a passphrase to generate the key, the phrase is salted with the SSID.
- ▶ As SSIDs tend to be re-used “wifi, home, wlan,work,sales” etc it's possible to build up dictionary attacks
- ▶ The Church of Wifi has a database of 1000 popular SSIDs, with 1,000,000 words giving 40GB of hash tables.
- ▶ It's possible to record traffic on a WPA2 network and then attempt to use this database of hashes to decrypt the data.
- ▶ So passphrases need to be strong !

Additional WIFI Security

CA645

Gavin O' Gorman

Radio waves

Wireless
Technologies

802.11
Bluetooth
GSM

- ▶ MAC filtering can keep out idiots, or workers who bring in personal devices
- ▶ The WIFI network should be firewalled off from the main network.
- ▶ Any access to secure resources should be done via a VPN.
- ▶ When using wifi remotely, definitely use a VPN, or SSH tunnel

- ▶ A short range, Personal Area Network technology
- ▶ Devices come in classes based on transmitter power, 1mw, 2.5mw, 100mw. More power, greater range.
- ▶ Max range is designed to be approximately 100m
- ▶ 2.4Ghz frequency range with Spread Spectrum Frequency Hopping

Bluetooth Security

CA645

Gavin O' Gorman

Radio waves

Wireless
Technologies

802.11

Bluetooth

GSM

- ▶ A bluetooth device can be silent, non-discoverable or discoverable
- ▶ When communicating encryption can be on or off.
- ▶ When devices are pairing, a PIN is used
- ▶ This PIN is used to generate 128bit keys

Bluetooth Vulnerabilities

As Bluetooth is designed for close range communications, one might assume that this offers some security. Someone has to be close enough to you to connect. This is not necessarily the case.



Blue Snarfing attack

- ▶ Connecting to a device and accessing contents such as phonebook, textmessages, photos etc.
- ▶ Applications are bluesnarf and redsnarf but no code is available
- ▶ The attacks are based on flaws in the implementation of the Bluetooth stack on certain phones, not flaws in the actual standard.
- ▶ Such flaws in the phone may also allow access to the AT commands. This give remote control over the phone

Offline PIN Recovery

- ▶ Recording pairing communications between two devices and attempting to brute force the PIN used based. Relies on a short PIN
- ▶ More recent implementations of the attack have been developed, speeding the attack up. Discovering the PIN allows for forging connections from devices
- ▶ Similar attacks can be used to recover encryption keys and so decrypt communicated data.
- ▶ Online PIN attack can attempt to connect to a device using a brute force approach

Eavesdropping

A very simple and invasive attack

- ▶ Most handsfree devices use simple PINs for connection. 0000, or 1234.
- ▶ Using something like the bluetooth rifle, one can easily connect to a handsfree device and listen to conversations.

To secure bluetooth devices is however quite simple. Turn off the bluetooth radio when not using it. Don't use discoverable mode and don't accept file transfers.

GSM mobile phones. Three sets of algorithms are used in GSM networks and devices.

- ▶ The A3 algorithm is used for authentication between a device/network element and a base station. The actual algorithm used is Comp128
- ▶ For encrypting actual voice communications, between the device and base station, the A5 algorithm is used. A5/0, up to A5/3.
- ▶ Key generation is done with the A8 Algorithm

What's broken ?

- ▶ A3 and A8 both use Comp128. Ian Goldberg and David Wagner found that in every implementation they examined, the A8 algorithm had been weakened. The 64bit key had 10 bits set to 0. Comp128 can be broken in less than 1 minute. This means a SIM card can be cloned.
- ▶ A5 has been broken. There are several attacks which require only milliseconds of encrypted voice traffic to extract the key.
- ▶ A5/3 for 3gpp has not been broken as yet.