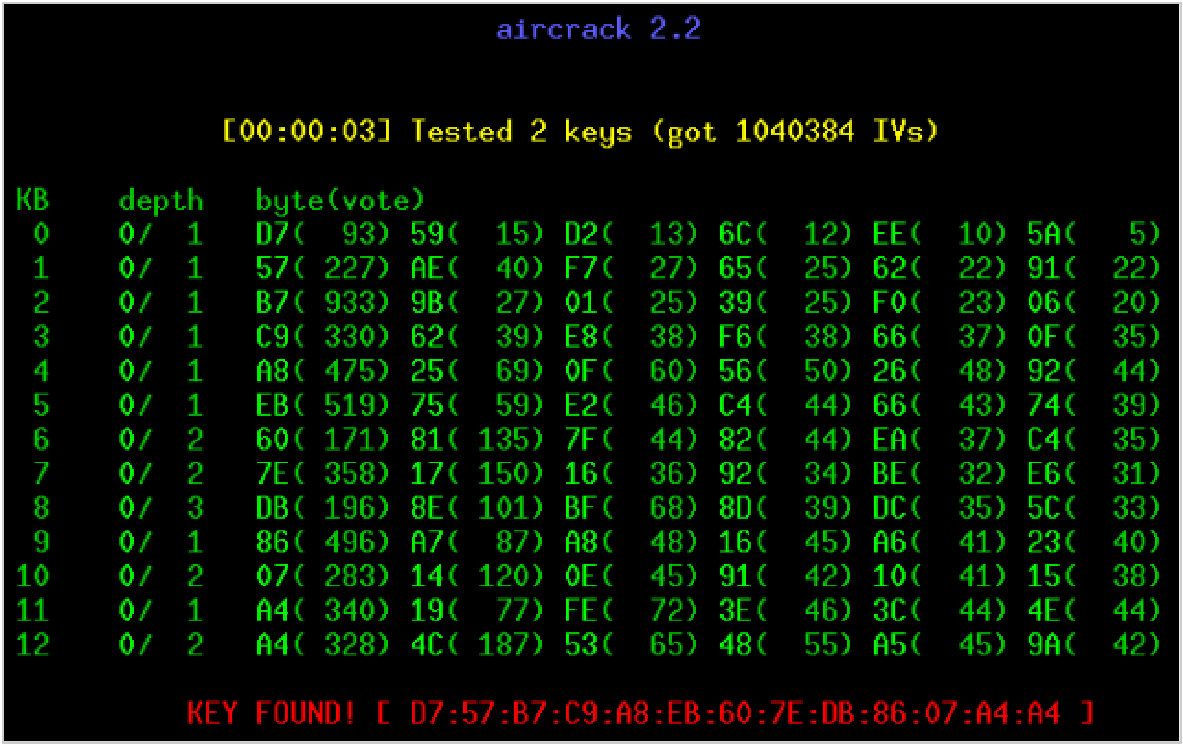
Cracking WEP and WPA Wireless Networks

From Docupedia



```
                          aircrack 2.2


            [00:00:03] Tested 2 keys (got 1040384 IVs)

KB    depth   byte(vote)
 0    0/  1   D7(  93) 59(  15) D2(  13) 6C(  12) EE(  10) 5A(   5)
 1    0/  1   57( 227) AE(  40) F7(  27) 65(  25) 62(  22) 91(  22)
 2    0/  1   B7( 933) 9B(  27) 01(  25) 39(  25) F0(  23) 06(  20)
 3    0/  1   C9( 330) 62(  39) E8(  38) F6(  38) 66(  37) 0F(  35)
 4    0/  1   A8( 475) 25(  69) 0F(  60) 56(  50) 26(  48) 92(  44)
 5    0/  1   EB( 519) 75(  59) E2(  46) C4(  44) 66(  43) 74(  39)
 6    0/  2   60( 171) 81( 135) 7F(  44) 82(  44) EA(  37) C4(  35)
 7    0/  2   7E( 358) 17( 150) 16(  36) 92(  34) BE(  32) E6(  31)
 8    0/  3   DB( 196) 8E( 101) BF(  68) 8D(  39) DC(  35) 5C(  33)
 9    0/  1   86( 496) A7(  87) A8(  48) 16(  45) A6(  41) 23(  40)
10    0/  2   07( 283) 14( 120) 0E(  45) 91(  42) 10(  41) 15(  38)
11    0/  1   A4( 340) 19(  77) FE(  72) 3E(  46) 3C(  44) 4E(  44)
12    0/  2   A4( 328) 4C( 187) 53(  65) 48(  55) A5(  45) 9A(  42)

           KEY FOUND! [ D7:57:B7:C9:A8:EB:60:7E:DB:86:07:A4:A4 ]
```

What else are you gonna do next Friday night? Play Counter Strike?

Written By: Bryan Rite

Shout out to: Jeff :: (www.lucidinteractive.ca) (http://www.lucidinteractive.ca/) for using OSX's Airport to try and generate traffic on our first crack

Also would like to thank Alkaloid Networks (http://www.alkaloid.net/) for support

To all the noobies: Don't call us and asking about how to crack networks.

Like this guy actually did (http://jeffsey.com/files/docupedia-hacking-help.wav)

Date: 11/23/2005

Contents

Overview

This is a good one, let me tell you! There can be so many issues setting up your box to actually get the tools working and i'm not even touching on that, but if you can get everything to work, you'll be cracking wireless networks like a pro in no time.

Disclaimer: I'm not a pro.

Pre-Installation

Checklist

- Tools
  - I've been really, really successful with basically one tool set called AirCrack (http://www.cr0.net:8040/code/network/) . Download that.
  - Kismet (http://www.kismetwireless.net/) is an excellent tool for sniffing out wireless networks as well and could prove useful.
- An encrypted wireless network.
  - We'll be working on WEP encrypted networks as well as static passkey WPA or WPA-PSK

Note: Make sure you can get your card into monitor mode (sometimes called raw monitor or rfmon). **This is VERY important**

WEP Crackin

Theory

A little theory first. WEP is a really crappy and old encryption techinque to secure a wireless connection. A 3-byte vector, called an *Initalization Vector* or *IV*, is prepended onto packets and its based on a pre-shared key that all the authenticated clients know... think of it as the network key you need to authenticate.

Well if its on (almost) *every* packet generated by the client or AP, then if we collect enough of them, like a few hundred thousand, we should be able to dramatically reduce the keyspace to check and brute force becomes a realistic proposition.

A couple of things will cause us some problems.

- If the key is not static, then you'll mix up all your IVs and it'll take forever to decrypt the key.
- Theres no traffic, therefore no packets - we can fix this.
- MAC Address Filtering - we can fix this too.

Setting up your tools

We're gonna need 3 or 4 shells open, we have 5 tools:

- airodump - Grabbing IVs
- aircrack - Cracking the IVs
- airdecap - Decoding captured packets
- airreplay - (My Favourite) Packet injector to attack APs.
- kismet - Network Sniffer, can grab IVs as well.

For a standard WEP hack we'll usally only need airodump, aircrack, and kismet (server and client). If we run into some problems we might have to use airreplay to fiddle about.

I'll leave you to config all these tools up, for the most part they should just be defaults with the exception of kismet.

Finding the Network

First step is we need to find a netork to crack. Start up kismet and start sniffing for APs. Leave it on for a bit so that it can discover all the important information about the networks around. What we want from kismet is:

- Encryption type: Is it WEP 64-bit? 128-bit?
- What channel is it on? Can *greatly* speed up IV collection.
- AP's IP Address
- BSSID
- ESSID

All this info isn't required but the more you have, the more options you have later to crack and sniff. We can get a lot of this from airodump as well but I find the *channel* is important.

Capturing IVs

Alright, we know what we wanna crack, so lets start capturing packets. You can use kismet to capture files but I prefer airodump because it keeps a running count of all the IVs I've captured and I can crack and airodump will automatically update aircrack with new IVs as it finds them.

Note: kimset can interfere with airodump so make sure you close it down before starting airodump.

Airodump is pretty straight forward with its command line looking something like this:

```
./airodump <interface> <output prefix> [channel] [IVs flag]
```

- interface is your wireless interface to use - required.
- output prefix is just the filname it'll prepend, - required.
- channel is the specific channel we'll scan, leave blank or use 0 to channel hop.
- IVs flag is either 0 or 1, depending on whether you want *all* packets logged, or just IVs.

My wireless card is ath0, output prefix i'll use "lucid", the channel we sniffed from kismet is 6, and IVs flag is 1 because we just want IVs. So we run:

```
./airodump ath0 lucid 6 1
```

Airodump will come up with a graph showing us all the APs and their relevant info, as well as client stations connected to any of the APs.

```
BSSID              PWR  Beacons   # Data  CH  MB  ENC   ESSID

00:23:1F:55:04:BC   76    21995   213416   6  54. WEP   hackme

BSSID              STATION            PWR  Packets  Probes

00:23:1F:55:04:BC  00:12:5B:4C:23:27  112     8202  hackme
00:23:1F:55:04:BC  00:12:5B:DA:2F:6A   21     1721  hackme
```

The second line shows us some info about the AP as well as the number of beacons and data packets we've collected from the AP. The two last lines show us two authenticated clients. Where they are connected to and the packets they are sending. We won't use this client info in a straight theory hack but in practice we'll need this info to actively attack the AP.

This step may take a long time or could be very short. It depends how busy the AP is and how many IVs we are collecting. What we are doing is populating a file "lucid.ivs" with all the IV important packet info. Next, we'll feed this to aircrack. To move onto the next step, we'll want at least 100,000 packets (under # Data in airodump) but probably more.

Using IVs to Decrypt the Key

Ok, pretend you have enough IVs now to attempt a crack. Goto a new terminal (without stopping airodump - remember it'll autoupdate as new IVs are found) and we'll start aircrack. It looks something like this:

```
./aircrack [options] <input file>
```

There are a lot of options so you can look them up yourself, i'll be using common ones here that should get you a crack. Our input file is "lucid.ivs", the options we will use are:

- -a 1 : forces a WEP attack mode (2 forces WPA)
- either -b for the bssid or -e for the essid : whichever is easier to type but I like using a BSSID because its more unique.
- -n 64 or -n 128 : WEP key length, omit if not known by now.

So our command will look like:

```
./aircrack -a 1 -b 00:23:1F:55:04:BC -n 128 lucid.ivs
```

and off it goes, resembling the picture from the top. Keep an eye on the Unique IV count as it should increase if airodump is still running. For all intents and purposes you are done. That'll pop open most old wireless routers with some traffic on them.

Anticipated Problems

There are lots of problems that can come up that will make the above fail, or work very slowly.

- No traffic
  - No traffic is being passed, therefore you can't capture any IVs.
  - What we need to do is inject some special packets to trick the AP into broadcasting.
  - Covered below in WEP Attacks
- MAC Address filtering
  - AP is only responding to connected clients. Probably because MAC address filtering is on.
  - Using airodumps screen you can find the MAC address of authenticated users so just change your MAC to theirs and continue on.
  - Using the -m option you can specify aircrack to filter packets by MAC Address, ex. -m 00:12:5B:4C:23:27
- Can't Crack even with tons of IVs
  - Some of the statistical attacks can create false positives and lead you in the wrong direction.
  - Try using -k N (where N=1..17) or -y to vary your attack method.
  - Increase the fudge factor. By default it is at 2, by specifying -f N (where N>=2) will increase your chances of a crack, but take much longer. I find that doubling the previous fudge factor is a nice progression if you are having trouble.
- Still Nothing
  - Find the AP by following the signal strength and ask the admin what the WEP key is.

WPA Crackin

Differences

WPA is an encryption algorithm that takes care of a lot of the vunerablities inherent in WEP. WEP is, by design, flawed. No matter how good or crappy, long or short, your WEP key is, it can be cracked. WPA is different. A WPA key *can* be made good enough to make cracking it unfeasible. WPA is also a little more cracker friendly. By capturing the right type of packets, you can do your cracking offline. This means you only have to be near the AP for a matter of seconds to get what you need. Advantages and disadvantages.

WPA Flavours

WPA basically comes in two flavours RADIUS or PSK. PSK is crackable, RADIUS is not so much.

PSK uses a user defined password to initialize the TKIP, temporal key integrity protocol. There is a password and the user is involved, for the most part that means it is flawed. The TKIP is not really crackable as it is a per-packet key but upon the initialization of the TKIP, like during an authentication, we get the password (well the PMK anyways). A robust dictionary attack will take care of a lot of consumer passwords.

Radius involves physical transferring of the key and encrypted channels blah blah blah, look it up to learn more about it but 90% of commerical APs do not support it, it is more of an enterprise solution then a consumer one.

The Handshake

The WPA handshake was designed to occur over insecure channels and in plaintext so the password is not actually sent across. There are some fancy dancy algorithms in the background that turn it into a primary master key, PMK, and the like but none of that really matters cause the PMK is enough to connect to the network.

The only step we need to do is capture a full authenication handshake from a real client and the AP. This can prove tricky without some packet injection, but if you are lucky to capture a **full** handshake, then you can leave and do the rest of the cracking at home.

We can force an authenication handshake by launching a Deauthentication Attack, but **only** if there is a real client already connected (you can tell in airodump). If there are no connected clients, you're outta luck.

Like for WEP, we want to know the channel the WPA is sitting on, but the airodump command is slightly different. We don't want just IVs so we don't specify an IV flag. This will produce "lucid.cap" instead of "lucid.ivs". Assume WPA is on channel 6 and wireless interface is ath0.

```
./airodump ath0 lucid 6
```

Dictionary Brute Force

The most important part of brute forcing a WPA password is a good dictionary. Check out http://www.openwall.com/wordlists/ for a **'really'** good one. It costs money, but its the biggest and best I've ever seen (40 Million words, no duplicates, one .txt file). There is also a free reduced version from the same site but i'm sure resourceful people can figure out where to get a good dictionary from.

When you have a good dictionary the crack is a simple brute force attack:

```
./aircrack -a 2 -b 00:23:1F:55:04:BC -w /path/to/wordlist
```

Either you'll get it or you won't... depends on the strength of the password and if a dictionary attack can crack it.

Using Aireplay

Aireplay is the fun part. You get to manipulate packets to trick the network into giving you what you want.

WEP Attacks

Attacks used to create more traffic on WEP networks to get more IVs.

ARP Injection

ARP Replay is a classic way of getting more IV traffic from the AP. It is the turtle. Slow but steady and almost always works. We need the BSSID of the AP and the BSSID of an associated client. If there are no clients connected, it is possible to create one with *another* WEP attack explained below: Fake Authentication Attack.

With airodump listening, we attack:

```
./aireplay -3 -b <AP MAC Address> -h <Client MAC Address> ath0
```

Note: The -3 specifys the type of attack (3=ARP Replay).

This will continue to run, and airodump, listening fron another terminal, will pick up any reply IVs.

Interactive Packet Replay

Interactive Packet Reply is quite a bit more advanced and requires capturing packets and constructing your own. It can prove more effective then simple ARP requests but I won't get into packet construction here.

A useful attack you might try is the re-send all data attack, basically you are asking the AP to re-send you everything. This only works if the AP re-encrypts the packets before sending them again (and therefore giving you a new IV). Some APs do, some don't.

```
aireplay -2 -b <AP MAC> -h <Client MAC> -n 100 -p 0841 -c FF:FF:FF:FF:FF:FF ath0
```

Fake Authentication Attack

This attack won't generate any more traffic but it does create an associative client MAC Address useful for the above two attacks. Its definately not as good as having a real, connected client, but you gots to do what you gots to do.

This is done easiest with another machine because we need a new MAC address but if you can manually change your MAC then that'll work too. We'll call your new MAC address "Fake MAC".

Now most APs need clients to reassociate every 30 seconds or so or they think they're disconnected. This is pretty arbitrary but I use it and it has worked but if your Fake MAC gets disconnected, reassociate quicker. We need **both** the essid and bssid and our Fake MAC.

```
./aireplay -1 30 -e '<ESSID>' -a <BSSID> -h <Fake MAC> ath0
```

If successful, you should see something like this:

```
23:47:29  Sending Authentication Request
23:47:29  Authentication successful
23:47:30  Sending Association Request
23:47:30  Association successful :-)
```

Awesome! Now you can use the above two attacks even though there were no clients connected in the first place! If it fails, there may be MAC Address Filtering on so if you really want to use this, you'll have to sniff around until a client provides you with a registered MAC to fake.

WPA Attacks

So far, the only way to really crack WPA is to force a re-authentication of a *valid* client. We need a real, actively connected client to break WPA. You might have to wait a while.

Deauthentication Attack

This is a simple and very effective attack. We just force the connected client to disconnect then we capture the re-connect and authentication, saves time so we don't have to wait for the client to do it themselves (a tad less "waiting outside in the car" creepiness as well). With airodump running in another console, your attack will look something like this:

```
aireplay -0 5 -a <AP MAC> -c <Client MAC> ath0
```

After a few seconds the re-authentication should be complete and we can attempt to Dictionary Brute Force the PMK.

Conclusion

Well thats that. APs crack fairly often but sometimes there is just nothing you can do. *Obviously* you are not allowed to illegally crack other people's wireless connections, this is purely for penetration testing purposes and some fun.

--- Bryan Rite 13:57, 24 Nov 2005 (PST)

Be sure to check out Bryan's Free Travel Photo Blog site Footstops.com (http://www.footstops.com/) . Journals, Maps, Videos, Friends and more, plus all proceeds goto international charities.

Retrieved from "http://docs.lucidinteractive.ca/index.php /Cracking_WEP_and_WPA_Wireless_Networks"

- This page was last modified 16:47, 22 June 2007.