



## WEP Cracking, the FBI Way

WEP cracking usually takes hours. Lots of hours, depending on the amount of traffic on the access point. A few months ago, two FBI agents demonstrated how they were able to crack a WEP enabled access point within a couple of minutes. 3 minutes to be exact. This is unbelievable when compared to, say 3 days of work. Here is how they did it, and how you can do it. You may need to know your way with each and every of these tools to get this done. You can ask Google for that. Anyway, if you are familiar with them, just do as follows :

- Run Kismet to find your target network. Get the SSID and the channel.
- Run Airodump and start capturing data.
- With Aireplay, start replaying a packet on the target network. (You can find a 'good packet' by looking at the BSSID MAC on Kismet and comparing it to the captured packet's BSSID MAC).
- Watch as Airodump goes crazy with new IVs. Thanks to Aireplay.
- Stop Airodump when you have about 1,000 IVs.
- Run Aircrack on the captured file.
- You should see the WEP key in front of you now.

The software runs on Linux, they are all available on the **Knoppix Linux Live CD**. And finally, I think you should always use a combination of 2 or more security features. As for what you need, get **Aircrack** (Includes Airodump, Aireplay, Aircrack and optional Airdecap for decrypting WEP/WPA capture files) and get **Kismet**.

Update: Kismet for Windows (**Kiswin32**) is available now.

SPONSORED LINKS

**Saturday, June 4th, 2005**

---

## Possibly related stuff

- No related posts
- 

## 45 Responses to “WEP Cracking, the FBI Way”

- **Wayne D. Berg** Says:

WOW, this really works. Any illegalities I should be aware of when cracking WEP encryption in my hobby? Is it illegal to crack someone's code?

**January 23rd, 2006**

- **primary0** Says:

think of it as lock picking. if its ur lock - no problem. if it is someone else's, u need permission and it wud be illegal otherwise i suppose.

**January 23rd, 2006**

- **Joe B** Says:

Going to test it when i have some time on the WEPS in my work offices if it can be cracked that easily I will stop using wep and move to other encryptions all together.

**March 8th, 2006**

- **h4x0r** Says:

Any chance of Aircrack comming out for PC?

**June 28th, 2006**

- **Dave N** Says:

WPA and WPA2 is crackable as well (but a lot harder). There is no real secure wireless network. WEP is sufficient for home use, but not for corporate use.

**June 28th, 2006**

- **Dave N** Says:

Aircrack is out for PC, but aireplay does not work for the PC due to drivers.

**June 28th, 2006**

- **Geeks Are Sexy] Tech. News** Says:

Yeah, cracking WEP has never been easier.

Just go on youtube and do a search for WEP cracking, you'll end up on a couple of video presentation about what you just posted.

Even WPA isn't safe anymore now...

**June 28th, 2006**

- **shawn m** Says:

It's not sufficient to say WPA and WPA2 are "a lot harder" to crack. With sufficiently strong keys, it would take current computers millions of years to crack via brute force.

I also disagree that WEP is sufficient for home use. All your on-link banking may be secured via SSL, but your email and all your surfing is easily accessible. Someone snooping would know what banks you deal with, what companies you buy from, and even know when to expect deliveries if they pick up shipping confirmations sent in email. If you live in a sparsely populated area, it's low risk. If you live in a dense neighborhood or apartment building, you should just assume someone is trying to get to your network and lock it down tightly.

**June 28th, 2006**

- **Mark** Says:

Well, It made the front page of digg. WEP is officialy dead.

I, a 14 year old kid with linux, can compramise your home network in 3 minutes.

**June 28th, 2006**

- **stephengilroy[dot]com » Blog Archive » WEP Cracking, the FBI Way** Says:

[...] Cheers to you, Stephenread  
more | digg story [...]

**June 28th, 2006**

- **Thermopyae » Blog Archive » Hacking WLAN in 3 Minutes.** Says:

[...] About a year ago the FBI demonstrated how they can hack a wireless WEP encrypted network in three minutes, prior to this I it would take hours! Today I found an article which gives you step by step intructions on how to do it, but you will need to run linux! [...]

**June 28th, 2006**

- **Stork** Says:

WPA is safe if you put a nice juicy password such as

”

```
+26]RkW\>mjk>D$BM9S1s28DN2E.*rw@_Zya!"Bl]JBs,3)VF;EHA7.t!04`IT5
```

”

But WPA will be audited if everyone uses their passwords as  
” macintosh ”

So please, If you have a neighbor who uses WEP, be a good neighbor and crack it and use a nice program such as airpwn(which is on auditor) to remind them that they could lose a poop-load of valuable information if they don't get a WPA router.

**June 28th, 2006**

- **The bandito** Says:

Just tell your router not to accept connections from anything but your approved MAC addresses. Is there any way around that?

**June 28th, 2006**

- **dibbs online** Says:

1000 IV's is not enough, even the aircrack docco says this.

**June 28th, 2006**

- o **ardos** Says:

you can spoof mac address so thats  
i not a way around the problem

**June 28th, 2006**

- o **Matt** Says:

Bandito:

Once you've cracked the WEP key,  
just sniff enough packets and pull  
out which MAC addresses ARE  
allowed, then spoof. Bingo.

**June 28th, 2006**

- o **stone** Says:

Spoofing MAC addresses is actually  
pretty easy...

**June 28th, 2006**

- o **Rob** Says:

@bandito - First, you can often  
override the MAC address to be  
anything you want, so you could  
simply take one of the approved  
MAC addresses if you want to  
connect through the network. This  
would probably only work when the  
other computer is off though.

Second, if you only want to monitor  
traffic, then you don't need to  
connect, you just have to sit there  
and listen to the traffic going by.

**June 28th, 2006**

- o **Interiot** Says:

@Dave N

Wireless networks \*can\* be secure,  
you just have to run a wrapper like  
SSH+SOCKS or IPSec over them.

**June 28th, 2006**

- o **Stephen** Says:

I find myself rather suprised that  
people are still using WEP when  
WPA-PSK is so easily available and  
easy to configure. If you use a 20  
character password minimum w/  
alphanumerics and such - which you  
can keep written down in case you

forget, and which will already be saved on your computers anyway - then WPA-PSK is virtually impregnable. It's ridiculously simple to migrate to WPA, and if you're using WEP, you should've switched years ago.

Heck, just use Mac Address filtering if you're really worried.

cmd prompt: ipconfig /all  
and pop that mac addy into your router.

**June 28th, 2006**

- o **makingfunofh4x0r** Says:

omglol111!!!111  
some idiot named h4x0r needs aircrack on a pc... your not h4x0r your n00bx0r

**June 28th, 2006**

- o **AlbanyWiFi.com » Blog Archive » WEP Cracking, the FBI Way** Says:

[...]  
[www.primary0.com/2005/06/04/wep-cracking-the-fbi-way/](http://www.primary0.com/2005/06/04/wep-cracking-the-fbi-way/)  
[...]

**June 28th, 2006**

- o **RE: To bandito** Says:

RE: The bandito  
yes, there is an easy way around it, you simply wait for an authorized client to use the network and grab thier mac address and simply spoof your mac to be thiers

**June 28th, 2006**

- o **Don** Says:

What kind of wireless card(s) did you use for your auditing?

**June 28th, 2006**

- o **rych** Says:

not all drivers are compatible airodump.

**June 28th, 2006**

- o **Killagoat** Says:

With a combination of hidden SSID and MAC authentication you're about 20x more secure than using WEP. The cheap wal-mart linksys routers can do this and I've not yet been able to find a way to get around it.

**June 28th, 2006**

o **Jack** Says:

Well - I run AES encryption with a long [ > 60 letter password] - is that safe?

**June 28th, 2006**

o **thru9** Says:

anytime soon for Max X?

**June 28th, 2006**

o **marticus** Says:

"Just tell your router not to accept connections from anything but your approved MAC addresses. Is there any way around that?"

once someone figures out the MAC address of any on your network they can simple use a MAC "spoofer" that will allow them to access the network hosting your MAC address.

So, no.

**June 28th, 2006**

o **Fred** Says:

This is just for n00bs ... you can't crack a WEP with 1000 IVs. You probably need 400000 or even 600000 IVs!!!

What the FBI did in his demo, was confusing/disconnecting Windows workstations by sending them deauth packets to be sure to create more traffic. The more traffic you have, the more IVs you can get.

Everybody can write down what he thinks ... everybody should what he writes down ... because I'm sure God is a 3m high guy.

**June 28th, 2006**

- **Aryss Ska'Hara** Says:

So, if that's your private network - disable SSID broadcasting. Those, who need to know SSID will know it from you.

**June 28th, 2006**

- **Tom Wright** Says:

@Aryss Ska'Hara  
Disabling SSID broadcasting won't help (although it will reduce your power usage) because traffic can still be sniffed when it goes between legitimate clients and the node. They will inform the brat next door of your SSID making the whole exercise pointless.

**June 28th, 2006**

- **thewebguy** Says:

Matt:

I was going to ask if something like that was possible. I used MAC filtering instead of any encryption recently thinking it might be faster (and it would be fun to piss off people in my apartment complex trying to piggy back because they didn't see a required password, HAH)

It ended up not being so great.

**June 28th, 2006**

- **Jason's Random Tech Stuff » WEP Cracking, the FBI Way** Says:

[...] WEP cracking usually takes hours. Lots of hours, depending on the amount of traffic on the access point. A few months ago, two FBI agents demonstrated how they were able to crack a WEP enabled access point within a couple of minutes. 3 minutes to be exact.read more | digg story [...]

**June 28th, 2006**

- **误入世界 » links for 2006-06-28** Says:

[...] pwtb » WEP Cracking, the FBI Way (tags: web crack) [...]

**June 28th, 2006**

- **adam** Says:

I'm a fan of the SecurityNow podcast (Steve Gibson and Leo Laporte) and well, Steve has a page at [grc.com/password](http://grc.com/password) that creates long passwords. It's pretty nifty for generating long, secure passwords.

**June 29th, 2006**

- **误入世界 » links for 2006-06-29** Says:

[...] pwtb » WEP Cracking, the FBI Way (tags: web crack) [...]

**June 29th, 2006**

- **Init (){ Ririn.toString(); } :: WEP Cracking, the FBI Way :: June :: 2006** Says:

[...] U can check the details here [...]

**June 29th, 2006**

- **otro blog m♦s » Unos cuantos de seguridad inform♦tica** Says:

[...] Y un par m♦s sobre WiFi: Cracking WEP and WPA Wireless Networks y WEP Cracking, the FBI Way. [...]

**July 4th, 2006**

- **EveryDigg » Blog Archive » WEP Cracking, the FBI Way** Says:

[...] WEP cracking usually takes hours. Lots of hours, depending on the amount of traffic on the access point. A few months ago, two FBI agents demonstrated how they were able to crack a WEP enabled access point within a couple of minutes. 3 minutes to be exact.[read more | digg story](#) [...]

**July 8th, 2006**

- **kalyank.net » Blog Archive » WEP Cracking, the FBI Way** Says:

[...] [source] WEP cracking usually takes hours. Lots of hours, depending on the amount of traffic on the access point. A few months ago, two FBI agents demonstrated how they were able to crack a WEP enabled access point within a couple of minutes. 3 minutes to be exact. This is unbelievable when compared to, say 3 days of work. Here is how they did it, and how you can do it. You may need to know your way

with each and every of these tools to get this done. You can ask Google for that. Anyway, if you are familiar with them, just do as follows : [...]

**July 16th, 2006**

o **cw** Says:

I figure that for a home network, WPA2 personal AES PSK with the longest key you can create, non-broadcasting SSID, MAC filters and DHCP turned off, no AP management from the wifi side, no WAN management, disable uPnP, is about the best you can do, unless you want to go with a RADIUS server (my attempts at building openradius on one of my OpenBSD boxes was a mess, so I've not played with that). Tweaking (increasing) some of the timeout values for beaconing might cause a joyrider to miss the network if using wellenreiter. Seems with tools like karma and all the hostap based apps that impersonate an AP that there are many ways to own a wifi net/host. At work we run an 802.11b/g net on a non-routed 10.x.x.x VLAN that's isolated from the main network via an IPSEC VPN that requires auth from the central credential store. It's also got a feature that won't allow the clients to talk with one another even at layer 2 (helps mitigate or stop ARP trix for MitM and spoofing). Once someone authenticates their profile allocates which IP pool they use. From there, unless the Cisco ACS server applies a downloadable ACL, the VPN user is on the internal network and unfortunately the Cisco client doesn't seem to have any remediation or NAC-based checks so you have unprotected/compromised endpoints.

I'm sure there is some way to break the security but so far it's resisted my attempts to pentest it.

**September 15th, 2006**

o **michael** Says:

I'm going to try this tonight, if it works ill warn my neighbour (im not sad) btw, im frm New Zealand any one else? or just U.S.A?

**September 28th, 2006**◦ **Bob** Says:

Yeah brute forcing WPA might take eternity, but the truth of the matter is when its your dogs name "fluffy" with numbers 12 or 21 after such name to equal the min characters of 8 (fluffy12), I can assure you that brute force takes no more than 20 minutes when adding min number strings to the end of your lists. Thats the sad truth behind 80% of wireless network users password schemes.

**November 9th, 2006**◦ **aneel** Says:

Some tips on aircrack-ng command line. Aircrack never seems to end even in 20 million years ahead

**December 6th, 2006****Leave a Reply**

Name (required)

Mail (will not be published) (required)

Website

## 10 Most Popular Posts

- o WEP Cracking, the FBI Way
- o Geek vs Nerd
- o Mega Yachts - Pelorus and Carinthia VII
- o Command and Conquer 3 (Tiberium Wars) Screenshots
- o Enlightenment DR17 on Fedora Core 4
- o The Golden Ratio and the Marquardt Mask (1:1.618)
- o Courier and Postfix with MySQL on Fedora Core
- o Perl MSN Sniffer
- o World's Most Expensive Coffee: Kopi Luwak
- o The True Furqan, The Fake Quran

## Explore

blogging code culture **else**  
 gaming hardware **internet** linux  
**maldives** music science  
 software

## Search

o

## About

- o About Me
- o Contact

## Feeds

- o Entries RSS
- o Comments RSS

## Recent Comments

- o eXpo on Internet Cats  
*"hehe the last two pics are the best :P..."*
- o moyameehaa on Internet Cats  
*"this is a kewl one u must see...."*
- o subcorpus on Internet Cats  
*"thats a lot of cats ... hehe ....."*
- o anon on Internet Cats  
*"fuck man , your wierd..."*
- o n3m6 on Internet Cats  
*"in your blog spamming your comments..."*
- o haha on The True Furqan, The Fake Quran  
*"nobody knows the truth...."*
- o subcorpus on Resolution?  
*"amen!..."*

## Credits

- o WordPress
- o UrbanGiraffe
- o Shazeen Samad Photography