

Re: wireless router password security

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2008-05/msg00015.html>

- *From:* "Sebastian G." <seppi@xxxxxxxx>
 - *Date:* Mon, 12 May 2008 02:43:43 +0200
-

bz wrote:

"Sebastian G." <seppi@xxxxxxxx> wrote in
<news:68kcijF2sbr7oU1@xxxxxxxxxxxxxx>:

bz wrote:

"Sebastian G." <seppi@xxxxxxxx> wrote in
<news:68jrooF2t4jo8U1@xxxxxxxxxxxxxx>:

bz wrote:

"Kyle T. Jones"
<Email@xxxxxxxxxxxxxxxxxxxxxx>
wrote in
[news:fvvj3k\\$5m\\$1@xxxxxxxx](news:fvvj3k$5m$1@xxxxxxxx):

Sebastian
G. wrote:

Kyle
T.
Jones
wrote:

<http://www.howtodothings.com/computers-internet/hnk-sy-s-wrt54g-router-using-wap-and-wep>

Re: wireless router password security

But
please
omit
the
step
where
disabling
SSID
broadcast.
It
doesn't
change
anything
about
the
security,
doesn't
make
your
network
invisible
at
all,
but
surely
creates
a
lot
of
trouble
with
your
client
accidentally
trying
to
connect
to
someone
else's
network.

Good point.

I don't follow the logic.
Disabling SSID makes it
more difficult for someone
to connect to my wireless
router (WEP turned on
also).

Re: wireless router password security

Actually it makes them easier to accidentally to connect to your network instead of another SSID-disabled network.

HOW? They need to know my router's SSID. It has an SSID, it just doesn't broadcast it.

We're talking about MAC layer connections. First you connect on the MAC layer, eventually guided by a known SSID, and then the connection partners negotiate about the actual connection parameters.

Hmmm. From what I can gather from reading the IEEE 802.11 working doc 80.11 2007.pdf from the IEEE web site, neither one of us has been using the right terminology. It looks like both my router and my laptop network devices are STAs, one(the laptop) is an STA client, the other is an AP(access point) STA. They can be 'associated' or 'disassociated'. "Before a STA is allowed to send a data message via an AP, it shall first become associated with the AP."

And they talk to each other over PHY (the physical layer). "STAs may be hidden from each other".

"IEEE 802.11 is required to look like a wired network to higher layers."

It appears that the SSID is used as part of the associate request at the MAC level.

It is going to take me a while to read through the 1232 pages of the document.

Perhaps you can save me some trouble and tell me how my router STA is supposed to respond to active probing (is that legal in this jurisdiction?) when bulletin broadcasting is turned off and how the wardriver even knows my STA is here.

Even when it doesn't broadcast INVITE requests with the SSID, it still broadcasts Beacon requests to notify its presence on the physical layer. It also responds to Beacon notify requests.

Maybe you should simply try it. Turn off SSID broadcasting, change the default channel to a very specific one, disconnect from the router, fire up NetStumbler and you'll see a No-SSID network on exactly this channel.

Hey, computer owner, I see the following access points. Which one do you want me to establish an association with? [I do NOT see any of the SSIDs that you have previously told me to talk to.]

Re: wireless router password security

Indeed. Since you have no way to differ the routers, you might always connect to the wrong one. The same happens if you set it up to always try them all. Same happens on every little interruption.

And cracking the encryption takes either

1) collecting lots of encrypted transmissions [about a days worth]

or

2) a very lucky guess. [would 'normally' take weeks of guesses to hit.]

Dunno what you're talking about, but I only know WEP and WPA/WPAv2/IEEE 802.11i as the two major techniques. WEP can be broken within some minutes of traffics, or bypassed (by creating a valid (IV, cipher stream) pair to send, but not receive arbitrary packets) within few seconds. The traffic can always be generated by sending out Beacon notification requests.

And IEEE 802.11i or its subsets known as WPA can at most be attacked via a MITM attack on the association setup, which gives you about 30 minutes of pure bruteforcing until the session key is forcefully renewed, and your attempt would have to totally start for a new. Also, how exactly would you bruteforce a random 256 bit key?

Where do I find this in the specs?

Dunno, the analysis documentation of AirCrack is much clearer to read.

If it isn't broadcasting, I would need to send a probe request on each channel asking 'who hears me'? If it is broadcasting, all I need to do is listen for a while [on all channels].

Right.

Yes but that should be at a higher layer, shouldn't it?

It should EMULATE not duplicate.

To emulate Ethernet functionally you have to implement a functionally identical MAC layer, which gives you the required demand for broadcasts.

I would think that it knows its own ID and listens for calls addressed to that ID, properly encrypted, on the proper channel. I would expect it to

Re: wireless router password security

ignore improper calls, those not addressed to it and those not properly encrypted.

Indeed, this is how one might have implemented it if the spec wouldn't require Ethernet MAC layer compatibility.

It is ALWAYS listening for proper calls.

So are the other APs. But you only know that you got the wrong one after trying to decipher his reply. That's why you may permanently hit the wrong one.

I just tried my SMC usb wireless adapter on my laptop but I seem to have problems finding drivers.

Well, you cannot always be as lucky as I was. I bought a random No-Name PCMCIA wlan card, which then turned out to be an AMD PCnet Wireless 800 model based upon the well-known Atheros chipset. You know, the one which was used for the very first WEP hack.

Maybe you're living far away from civilization? Heck, just on my weekly 2hour train+bus tour I can catch hundreds of networks.

They are broadcasting their SSID.

No, about half of them doesn't.

How would you know anything about those that don't?

See above. Beacon request.

I think that deliberately using someone's wireless without their express permission could be expensive. That is regardless of whether they have taken any steps to secure their router.

Re: wireless router password security

Nonsense. In civil law, this is called reasonable expectation of use. If you built a well near a street and some people would start drinking water from it, you couldn't sue them (or at least not successfully). You'd be required to install a sign "No drinking from well without permission", then you could defend.

If my machine is asking your router to establish a connection and it actually does, I can reasonably expect that this was the full intention of its owner. Heck, if it even delivers matching IP addresses via DHCP, this surely must be intentional. After all, if the owner didn't want this access to be public, he would have configured it differently.

Now if somehow it would be likely that I'd notice his internet access has a transfer limit, and intentionally utilize it much beyond this limit, I might get into a little trouble. Unlikely, but possible.

If I were to crack a WEP "encryption", which definitely is a sign of intended privacy, I would become responsible. Though at least in case of WEP, I could successfully argue that the owner has been sloppy to allow such a well-known broken protocols instead of resorting to secure variants (like WPA) and therefore has to pay a certain share of his damage costs out of his own pocket.

.