

RE: Wireless Security for Home Users

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-09/0112.html>

From: Keenan, Scott (scott.keenan@eds.com)

Date: 09/04/02

From: "Keenan, Scott" <scott.keenan@eds.com>

To: "Snow, Corey" <csnow@deltadentalwa.com>, "'Tony Brisco'" <tony_brisco@yahoo.com>

Date: Wed, 4 Sep 2002 16:59:56 -0500

While I don't disagree with Corey's approach, it may be a bit of overkill for most home users to create and/or manage 2 firewalls and a DMZ. Don't get me wrong, this is essentially the same setup I employ at home, but creating, managing and playing with firewalls is also something I do for fun much like Corey's 1/2 mile antenna.

If I were a typical home user with a few PCs for my kids to game on, a laptop or PC for home finance and occasional netsurfing/homework help, I don't think I'd go so far as to install 2 firewalls and segment off traffic from the wireless access points. As with most network security, the level of security needs to be weighed against both the value of the assets to be protected, and the hassles/difficulties inherent in adding layers of security (i.e. if you don't know anything about firewalls, either the expense of buying them or the complexity of building them as Corey suggests may be more trouble than it's worth to just be able to surf the net while sitting on your deck). That said, installing a firewall on the inside of your cable router is a good idea, and should be considered a mandatory security practice for anyone. Most of the "home use" companies like D-link, Netgear and Linksys make decent ones that can also serve as an intro to firewall features such as NAT, PAT, statefull packet inspection, etc. I would recommend ANY and EVERY home user have some sort of firewall between themselves and the internet, even when using dial-up.

Beyond just good home network security practices, specific to wireless I would recommend the following;

- 1) As Corey says, use WEP, 128 bit if possible. In addition, as suggested, investigate additional security features available from the WAP manufacturer. Some are implementing additional WEP features like TKIP (rotating WEP keys), and MIC (Message Integrity Check). If not, then also as suggested, change your WEP keys regularly and often.

- 2) Disable broadcast SSID. Sure the SSID is always transmitted in the clear, so anyone wanting to find it merely has to wait for an exchange between the access point and a client, but most WAP's support disabling broadcasting the SSID to the world. At least this way someone driving up

RE: Wireless Security for Home Users

SecurityFocus BASICS: RE: Wireless Security for Home Users

your street isn't greeted by your WAP saying "hi, here's my SSID, want to join me?" Changing the SSID from the default is slightly helpful. As said, it's always transmitted in the clear, but if you disable broadcast SSID, but never change it from the default, then anyone driving down your street who knows default SSIDs for WAPs would have very little trouble associating to your AP. For example, Cisco's default SSID is tsunami. Everyone knows this (there are webpages that list these, along with default administrator account names and passwords for the various WAP manufacturers), so changing the defaults is always a good idea, if only marginally helpful.

3) Check to see if your access point allows limiting the number of client associations. Some manufacturers allow you to limit the number of clients associated at any given time. So, for example if you have 2 wireless clients, and they maintain a constant connection to the WAP, set this to 2 and no one else can associate to the access point.

4) Along the lines of "additional security features", check to see if your manufacturer allows MAC address filtering. Again, it's easy enough to spoof MAC addresses, but as Corey mentions, why bother trying to break in when someone else down the street is wide open?

5) Depending on your home network complexity, some WAP manufacturers are beginning to support 802.1x EAP, which allows for client authentication via EAP (Extensible Authentication Protocol) enabled RADIUS servers, thus allowing the RADIUS server to authenticate users prior to allowing them onto your network. This assumes you have an EAP enabled RADIUS server, and both the time and inclination to use it.

6) Last, but not least, see if you can adjust your transmit power. Most 802.11b AP's transmit at 100mW max. This of course, allows for the maximum distance for clients attempting to associate with the AP. However, in most cases, particularly in home use, this range far exceeds that necessary. Being able to broadcast 200 feet indoors is useful if your home is 400 ft x 400 ft (that's a bit of an exaggeration, but I'm sure you get the point). Placing an AP in the center of such a house allows 200 feet in all directions (including similar ranges above and below), but if your house isn't that large, then your broadcasting strong signals into the street. Many manufacturers allow the transmit power to be adjusted to lower settings such as 50, 20, 5 and even 1mW. I would suggest lowering the power and then moving around in your house with a wireless laptop, and seeing if you get sufficient coverage in all areas. If so, lower it again, until you find you're losing signal at your most distant client device location. In other words, set the transmit power as low as you can to maintain sufficient coverage inside your home, or intended coverage area, i.e. deck, porch, garage, etc). You may still be beaming signal 50 feet in front of your house, but you may at least stop transmitting to the houses across the street.....you can always wander around outside to see if you can connect from the middle of the street or further also.

Having said all of the above, it doesn't take someone long with tools such as AirSnort to break WEP encryption keys. Currently the security measures

SecurityFocus BASICS: RE: Wireless Security for Home Users

"within wireless" can help prevent casual drive by's or curious neighbors, but by corporate security standards, none of them provide "enterprise class" security. TKIP with frequently rotating WEP key changes help mitigate the threat from all but the most determined hackers, but support for it is only recently beginning to appear in WAPs, so for now most home users are stuck with static WEP. Better than nothing, but you shouldn't rely on it for highly sensitive information. For example, most security plans for large corporations include the use of an IPSEC VPN for encryption between wireless clients and internal networks in addition to network segmentation and isolation within DMZ's as Corey suggests. This allows for the creation of a tunnel between a wireless client device such as a laptop and the corporate intranet, similar to those used for RAS access for years. The user may be at home or on the road, but so long as they're connecting via VPN, they're safe. Many companies are adopting this same approach to WLANs.

Scott

Now for the legal stuff: These are my opinions and suggestions alone, and in no way represent the opinions, advise or positions of my employer.

-----Original Message-----

From: Snow, Corey [mailto:csnow@deltadentalwa.com]

Sent: Wednesday, September 04, 2002 12:54 PM

To: 'Tony Brisco'

Cc: 'security-basics@securityfocus.com'

Subject: RE: Wireless Security for Home Users

Well, I'm not entirely certain what you mean by securing it over cable modem, but the things to do with WLAN connections:

Use WEP. It's not perfect, but it's a heckuva lot better than nothing.

User 128-bit WEP if your equipment supports it. If it doesn't, look into firmware updates from your vendor. Just using WEP will cause about 95% of the casual wardrivers to pass you by; there's always an unencrypted network to snoop just up the street.

Use any vendor-specific security improvements available to you. For example, I believe if you use a 3Com WAP and 3Com client cards, there are some higher-security options than straight WEP available to you. If, like me, you have a different vendor for your client WLAN card than your WAP, you're probably stuck with straight WEP. (do some research as well. Check out the various wireless LAN sites, and google around a bit).

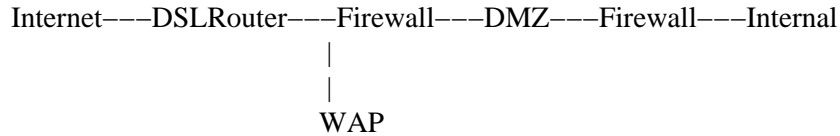
Change your WEP keys on a regular basis. Even if it means typing them in manually. Since this is a home network, you probably don't need to do it for a bunch of machines.

DO NOT, and I repeat: DO NOT put your WAP on your network directly! This is security suicide, and I don't care how many layers of encryption you put on it. If it's directly on your network, you're done for. Put it on a DMZ of

RE: Wireless Security for Home Users

SecurityFocus BASICS: RE: Wireless Security for Home Users

some type, and assume that everything coming from that DMZ is suspect. I have a 3-tier system on my home network, like so:



On my firewall(s), I have some very specific rules about what traffic is allowed in from the segment the WAP point lives on– that is, very, very little. And even that is only enough to establish a more secure connection, which is subject to only very slightly higher privilege levels. I also recommend the use of tools like SSH to add an additional layer of security to your WLAN sessions.

You may not have or need a large system like the one above, but you should definitely keep a WAP off your internal network. Use an old box (even a 486 DX2/66 will do), throw FreeBSD and a couple of old NICs in it, and you've got a nice, cheap firewall.

Remember, nothing prevents someone from associating with a WAP or simply listening to the traffic it broadcasts passively. I have built, just for grins, a directional antenna that lets me use a laptop to pick up and sniff WAP signals from over 1/2 mile away. If I had used more precision tools, I could probably do it from 2 miles. I did this because it amused me. There are people who will do it to attack you. Wireless is cool, but it's major security risk if you don't do it right– and the reason wardriving is so popular is because almost no one does.

Corey M. Snow– csnow@deltadentalwa.com

I don't speak for my employer.

```
> -----Original Message-----
> From: Tony Brisco [mailto:tony\_brisco@yahoo.com]
> Sent: Tuesday, September 03, 2002 9:34 AM
> To: security-basics@securityfocus.com
> Subject: Wireless Security for Home Users
>
>
>
> Hello everyone,
>
> What would be the must do things to secure my home
> wireless connection over cable modem ?
>
> Thanks,
> Tony Brisco.
>
> _____
> Do You Yahoo!?
> Yahoo! Finance – Get real-time stock quotes
```

RE: Wireless Security for Home Users

> <http://finance.yahoo.com>

>

The information contained in this e-mail and subsequent attachments may be privileged, confidential and protected from disclosure. This transmission is intended for the sole use of the individual and entity to whom it is addressed. If you are not the intended recipient, any dissemination, distribution or copying is strictly prohibited. If you think that you have received this message in error, please e-mail the sender at the above e-mail address.
#####

- **Previous message:** [khan rohail: "Denying UDP Scans"](#)
- **Maybe in reply to:** [Tony Brisco: "Wireless Security for Home Users"](#)
- **Next in thread:** [H C: "RE: Wireless Security for Home Users"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)