Popular Threads on Solosez

Wireless Network Security

Based on the recent thread about the Wi-Fi signal thief being arrested, I started thinking about wireless network security. Isn't there a way to limit which remote computers can access your network? I have a vague recollection that you can program the network only to accept a code generated by a specific remote computer.

I'm about to set up my wireless network, so this information about be helpful.

Scott, Los Angeles, California

Yes. You can tell the wireless network which MAC addresses to allow to connect. The MAC address is a serial number type indicator on the network interfaces of computers to be connected to the network. You also want to have encryption enabled.

And no, nothing is perfect.

Mike Phillips, Cary, North Carolina

And you want to disable SSID broadcast.

Mike Riddle, Papillion, Nebraska

Yes, but, some wireless cards will show reception of a signal but not show the SSID. If it is not protected, you can still connect to it.

Mike Phillips, Cary, North Carolina

You should do both. And also you should change the default name of the SSID. (E.g., the default for my Linksys is "Linksys". I've changed it to something else.)

Searching the archives will bring up a virtual treatise on this, I believe by Ross Kodner. IIRC correctly, his message was that none of the security options you can take are foolproof, including encryption; but the more of the security options that you invoke the less likely your system will be compromised by someone other than a real pro -- like the NSA.
Andy Simpson, Christiansted, St. Croix, U.S. Virgin Islands

Mike already answered your question and gave you another pointer. If you go to my website's download page at http://www.lawofficetech.com/technical_downs.htm you can find articles and presentations on Mobile Lawyering and Protecting your computer from Security threats.

Nerino J. Petro, Jr. Loves Park, Illinois

Agreed. A "layered" defense involves SSID disabled, MAC address filtering, and encryption.

Mike Riddle, Papillion, Nebraska

That's why I like wire!

Mike Phillips, Cary, North Carolina

I hate to be a killjoy here but I do not recommend any wireless network for practicing law. I was an engineer for many years before becoming a lawyer, and rest assured there is someone out there that can and will defeat whatever security measures you put into place. If you do not believe me, take a look at some of the recent highly publicized hack jobs that have been done to major companies with the most intense security. I venture to guess that most companies who get broken into do not even report the break-ins due to the negative publicity.

When you go wireless, you are not only using radio frequency's to broadcast whatever is happening in your network, but you are also giving a sophisticated hacker the ability to enter your network, and do what they do. With wireless they can simply sit outside of your office in their car.

For every encryption method that exists, there is also someone out there that knows the key to de-encrypting the data.

At least on a wire network, you can limit your data somewhat, that is unless you have your network tied into the internet via a router.

Norman G. Fernandez, California

Is your router TEMPEST certified?

My point is that every technology is vulnerable. Heard of "black bag" jobs?

So the question becomes not "what is perfect" but rather "how much is enough?", considering that deliberate attacks are themselves serious crimes. So what is the nature of what you are protecting, and "how much

is enough?"

Mike Riddle, Papillion, Nebraska

You can limit access by MAC address. MAC addresses are unique for each specific piece of hardware that connects to the network. I have mine set up to only allow my laptop (the only computer I have that has wireless capability). However, keep in mind there are ways to clone a mac address (Linksys in fact allows this for sharing one ip address for multiple computers, though I'm not sure how feasible it would be for some random person to discover this mac address of your computer if it isn't even the cloned MAC address used for connecting to the external internet).

Additionally you can use WEP or WPA encryption. WEP generates the security code for you, either automatically or based on a phrase you type in. WPA allows you to type in any combination of characters you want for the security code. (at least this is the case with my Linksys router, I don't know if the determination of the code varies from brand to brand or not as I'm just speaking from personal experience).

I use both a filter on the MAC address and encryption personally.

Lesley Hoenig, Illinois

It would be real easy: http://www.ethereal.com/

That's why MAC filtering provides a false sense of security, in my humble opinion. I could get past a MAC filter on an active network in about 2 minutes.

Eric

Do you want to see how easy it is to look into someone's network? Do a Google search for sniffer.

With this software, or hardware device, you can look at everything that is going on in an entire network!

Norman Fernandez, California

Here is another package that will even re-assemble the data for you
http://www.effetech.com/

Norman Fernandez, California

The same is true for wired networks. If you want to so cautious, we really

ought to all cancel our ISP subscriptions. There is no logical reason for drawing the line at wireless connections. Respectfully, I'd rather have a tight wireless network than a wired network comprised of exploited workstations and rootkitted servers, the latter of which I see quite a bit.

Eric

You asked for it Eric, you got it. Go ahead and read here:
http://airsnort.shmoo.com/ also look here:
http://sourceforge.net/projects/wepcrack

With this software, you can not only assemble "lost" encryption keys, you can do it with a wireless device. People with this software can get into your wireless network and defeat your encryption.

Also read here: http://www.drizzle.com/%7Eaboba/IEEE/rc4_ksaproc.pdf

Anyone can download the software Eric.

Now read a copy of this report on how our own government is having problems with wireless security Eric:
http://www.netstumbler.com/2005/06/27/
feds_beset_by_wireless_security_problems/

Here is another article that talks about the unique issues related to wireless LANs Eric:
http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html

Do you need more? Do you want to risk your client's confidentiality or all of your data by broadcasting your data via radio frequencies, or allowing a hacker to penetrate your network with a wireless laptop equipped with the latest encryption software?

There are also devices out there than will detect the presence of a wireless LAN. At least with wire, you are not broadcasting your network out to the world line a cordless phone. Wired networks are much more secure than non-wired networks for this reason, not that I am saying wired networks that are connected to the internet are totally secure by any means!!

Enough said, time to get back to work.

Norman Fernandez, California

Sorry Eric, one of the government problems links did not work, try this one: http://searchmobilecomputing.techtarget.com/
originalContent/0,289142,sid40_gci1097219,00.html

Norman Fernandez, California

Excellent! A real discussion. This is exciting. Here is my response.

Airsnort, kisment, etc., only work on WEP devices. WEP has a documented flaw in the implementation of IV packets. This was not a flaw in the WEP protocol itself, but rather a flaw in the implementation of the protocol. Vendors became aware of this flaw in 2001, and fixed it with a firmware upgrade. Thus, WEP is not insecure and is not susceptible to attack via Airsnort/kismet/whatever as long as the AP has firmware newer than 2001. And WPA is totally insulated from the tools you cite.

See http://www.oreillynet.com/cs/user/view/cs_msg/26023 for more info.

So how many people do you know using WEP on AP's with firmware older than 2001?

:Now read a copy of this report on how our own government is :having problems with wireless security Eric:

:http://www.netstumbler.com/2005/06/27/feds_beset_by_wireless_security_problems/

The above URL you give is lacking on any facts at all. It's pretty vacuous. So I'll move on.
:Here is another article that talks about the unique issues :related to wireless LANs Eric:
:http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html :

The above URL shows an article that lists "Seven Security Problems of 802.11 Wireless."

Those 7 are:

Problem #1: Easy Access Problem #2: "Rogue" Access Points Problem #3: Unauthorized Use of Service Problem #4: Service and Performance Constraints Problem #5: MAC Spoofing and Session Hijacking Problem #6: Traffic Analysis and Eavesdropping Problem #7: Higher Level Attacks

The problem is that this article was written in 2002, and is discussing the work of IETF task groups from 2001. That is well before WPA was introduced in 2003. WPA does per packet authentication, which is exactly what your article says is needed.

All of the seven problems above are obviated by not broadcasting the SSID, setting up WPA (non-pre-shared key), or WEP plus Kerberos, turning off DHCP, etc.

So no part of the discussion in these 7 sections supports your assertion that:

"When you go wireless, you are not only using radio frequency's to broadcast whatever is happening in your network, but you are also giving a sophisticated hacker the ability to enter :your network, and do what they do."

:Do you need more?

Yes.

:There are also devices out there than will detect the presence :of a wireless LAN. At least with wire, you are not :broadcasting your network out to the world line a cordless :phone. Wired networks are much more secure than non-wired :networks for this reason, not that I am saying wired networks :that are connected to the internet are totally secure by any means!! :

There are also devices that will detect and read what your flatscreen monitor or CRT is displaying. If I had one of these devices, I could park in front of your office and read what is on your screen. So are you going to stop using a computer now?

Wireless is "secure," and does not pose any unreasonable risks to client confidences.

Eric

I would add that turning off DHCP is another step to be taken to protect the network.

Also, set your subnet to an esoteric non-routable addressing scheme is another excellent move to make. E.g., instead of the hackneyed 192.168.0.x, use 172.16.x.x.

Eric

Here is my original post: I hate to be a killjoy here but I do not recommend any wireless network for practicing law. I was an engineer for many years before becoming a lawyer, and rest assured there is someone out there that can and will defeat whatever security measures you put into place. If you do not believe me, take a look at some of the recent highly publicized hack jobs that have been done to major companies with the most intense security. I venture to guess that most companies who get broken into do not even report the break-ins due to the negative publicity.

When you go wireless, you are not only using radio frequency's to broadcast whatever is happening in your network, but you are also giving a sophisticated hacker the ability to enter your network, and do what they do. With wireless they can simply sit outside of your office in their car.

For every encryption method that exists, there is also someone out there that knows the key to de-encrypting the data.

At least on a wire network, you can limit your data somewhat, that is unless you have your network tied into the internet via a router.

Now Eric, you challenged me to provide proof to back up my above statements. I provided links to hacker and de-encryption software, articles about wireless weaknesses etc., you countered that the links were dated.

Here is an article that was written on June 17th 2005, by wireless LAN experts. Notice the last 6 paragraphs or so of the article. If this does not support my position and opinion, I do not know what else to tell you.
http://www.newsfactor.com/news/
Wi-Fi-Security-Wakes-Up-to-Reality/
story.xhtm l?story_id=101009U6CKHZ

If you run your law office on a wireless network, you are subjecting yourself to security risks that a wired network does not have.

You seem to disagree with every expert that has written on the subject.

Norman G. Fernandez, California

I offered a point for point response to your post. In turn, you think I said only that your link was dated. I don't see any use in offering substantive rebuttals if you aren't going to address them. I could go through the new article you cite, line by line, but I'm afraid your mind is already made up, so I won't.

Eric

So it is your position that wireless internet is 100% safe and secure, and that wireless is more secure than non-wireless? You challenged my original post by saying that I should back it up with evidence, which I did. I stand by my original post.

I will not be using wireless internet anytime soon in my firm. For me, the benefit of wireless internet is substantially outweighed by the risk of harm if a hacker does get into my network by using an air sniffer or other device.

Obviously, you stand by your position, and I stand by my position. Let's agree to disagree. You may have the last word if you like. I am getting ready for a trial. The discussion has been fun.

Norman Fernandez, California

You didn't offer any good evidence. I pointed out the reasons why, and you totally skated over them. What am I supposed to do? Get on top of my house and start jumping up and down?

My position is that wireless networks do not post an unacceptable risk to client confidences, when used responsibly.

By "responsibly," I mean take the security precautions discussed by Mike P., myself, and others.

I think if you read the articles you cite, understand what exactly is being

said, and put it in context, we should mostly agree.

As one more example, the premise of the 2005 article you cite was two-fold: first, that not all enterprises can afford to upgrade every single wireless device, so therefore there is insecurity.

Well duh--if you can't afford to upgrade your products, then you are going to be less secure: this is true for wired networks as well.

Second, it made the point you are making: "The truth is that wireless technology in general has an inherent weakness not shared by a wired network: A physical barrier can't protect wireless."

Who can argue with that point? If that is your only point, then you are correct. However, I don't think that point means that a wireless network is "insecure."

There is no such thing as "secure": there are only degrees of risk.

What I'm saying is you take proper precaution, then the wireless world does not present unacceptable risk, even from an ethics point of view.

Eric

If someone wants to get into your network, with time and some luck, they will so long as you access the outside world. NO system, wired or wireless that has outside access is 100% secure. The chances of someone using a sniffer to get into your network are pretty remote. I don't know the office setup...stand alone building, office tower, etc. If you're in a tower, the chances of having your signal detected more than one office suite away are pretty small.

Having said all this, you're obviously free to do whatever you want in setting up your network. Just don't think that because you're doing it the wired way you're inherently more secure than wireless

Tom Simchak, Houston, Texas

I have a business client who has a fail-safe never-been-able-to-be-broken ocular and thumbprint security product that encrypts email and documents and systems if someone wants to contact me off line to contact him. I don't know his marketing rationale but one division has already proven to DOD its abilities..... Reta McKannan

---

I know there has been some heated debate about whether a Wireless Network can be truly secure. Let's set that aside from the time being. Or, as the great peacemaker Rodney King once said, can't we all just get along?

I've just installed my DLink DI 624 wireless router. So far, so good. The notebook is seeing the internet with a very strong signal. How do I set up the network so only the notebook's MAC address can access it? In other words, how can I exclude all wireless connections except my notebook's MAC address?

Thanks for your help.

Scott

That should be an option somewhere inside the DLink DI 624 configuration pages.

Mike Riddle, Papillion, Nebraska

I've found that. Now, how do I find the MAC address for my notebook?

Scott

Start > Run > cmd

At C: prompt, enter "ipconfig /all"

Eric

Open a DOS box type the word GETMAC and hit enter. You should see what you want.

Bruce L. Dorner, Londonderry, New Hampshire

Progress being made!

I've found the MAC addresses for both the desktop and the notebook. I've configured the D-Link router to only accept those MAC addresses. Next question...

When I go to the available wireless networks screen on my notebook, I see three listed. Two are likely my neighbors, and show low signal strength. The third is my network. It shows five bars. It also indicates, however, that my network is "unsecured."

Given that I've limited the D-Link to two MAC addresses, I'm guessing the "unsecured" notation means that though the network may be unsecured (i.e., no encryption or other security measures), unless the computer has one of the two allowed MAC addresses, it won't be able to access the network. Am I correct on that one?

Thanks for your help.

Scott Barer

The "unsecured' means you have WEP or WPA (encryption) turned off. Turn WPA on, or WEP if you must, choose preshared key, and choose as LONG A PASSPHRASE AS IS POSSIBLE. And don't make it a dictionary word. Once you turn on encryption, it will show as "secured."

Eric -----

Turn it over. 

Most notebooks have the MAC address on a label underneath. If you're using a plug-in WiFi card, look on the card.

Mike Riddle, Papillion, Nebraska

Yebbut: MAC addresses can be spoofed. Radio links can be sniffed. You still need to implement encryption on the wireless link and you should (if DLink allows) suppress SSID broadcast. Think of it as three layers of security, none perfect, but better with each layer that's added.

Mike Riddle, Papillion, Nebraska

------ You should be aware that the DI 624 may have a problem with sporadic disconnects when working on the internet. I recently experienced this at home and am replacing mine. I hope to get a full refund from DLink since I just installed the router.

Gene Thompson, Pampa, Texas

Back to Popular Threads