

Re: Using PC as bridge

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2005-08/msg00337.html

- *From:* Chuck <none@xxxxxxxxxxx>
 - *Date:* 3 Aug 2005 20:19:03 -0500
-

On Wed, 3 Aug 2005 15:50:02 -0700, "Koren" <Koren@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

>The university IT staff is aware of the situation. They have only just
>implemented the security scheme, primarily to deal with the student
>accommodation that is in the same building that I live in. (I am a staff
>member). Also, since I am in an Asian country, there are various language and
>cultural barriers associated with trying to explain the issues to them and
>getting them to take it seriously. I (or rather my husband, who is also a
>professor here) notified them of the problem and they are "looking at it",
>but I suspect that they will just tell me that it "can't be done" rather than
>seriously looking for a solution.

>

>The system they have set up means that as soon as you start a browser you
>are taken to a login page where you need to supply a user name and password
>before you can access any Internet resources (including university web
>sites). I don't know about other local network resources (Windows/Netware)
>since my home PC isn't logged in to the local network (and neither will the
>laptops be). The software appears to be from Aruba Networks, since the URL at
>the top begins <https://securelogin.arubanetworks.com>.

>

>I already have firewall software running on my PC, and it is extremely
>unlikely that intruders can get onto our wireless connection for a variety of
>reasons, including physical security of the building surrounds, and that the
>walls are so thick that the connection barely works within our flat let alone
>outside. What other security precautions would I need to take to prevent
>problems?

Koren,

Let's see. A bridge operates at OSI Layer 2 (Data Link), and a Firewall / Router at OSI Layers 3/4 (Network / Transport). I'd question whether anything bridged would even go thru the firewall, so if you have two connections, and you're operating a bridge, that's an open passage from the untrusted network (Internet or WiFi LAN) into the trusted network (your University LAN), and on the WRONG side of the Aruba proxy.

<http://en.wikipedia.org/wiki/OSI_model>

Re: Using PC as bridge

Now the issue of signal strength is really one of security by obscurity, as in there would be lots of stronger signals nearby, so no intruder would ever use mine. You're implying, though, that you have a weak signal, so no intruder would ever see yours. Koren, this is not accurate. Wardrivers use high gain antennas; while your wimpy little stub antenna might barely get you +3db SNR, a wardriver with a high gain parabola might sit in a parking lot a block away and surf with +6db SNR. Please don't confuse yourself, wardrivers don't play by your rules, or use your hardware.

This story illustrates how easy wardriving is.

<<http://nitecruZR.blogspot.com/2005/05/incredibly-stupid-wardriver.html>>

So let's see how this works.

University Network <=(1)=> PC <=(2)=> WiFi Router <-(3)-> Laptops

where <-(n)-> is wireless, and <=(n)=> is Ethernet. You could indeed install a second card in your PC, and make a bridge out of it. But it would, I think, have the security problem that I described above.

What you would want to do is use the WiFi router as a WAP. I've written an article explaining how to do this.

<<http://nitecruZR.blogspot.com/2005/06/file-sharing-on-lan-with-two-routers.html>>

If I was a LAN admin that setup a proxy requiring authentication, I'd certainly not appreciate it to find a bridged connection connecting the protected side of my proxy (my LAN) to the unprotected WiFi environment. And I doubt that I'd be too polite if I did find one. Don't put yourself, or the University network, at risk please.

I do hope, for everybody's sake, that they ARE sweeping their network looking for unauthorised connections. WiFi leaks, like what you're contemplating, are well known threats in the business world, and a whole product line of commercial products, designed to find unauthorised WiFi installations, are available. I wouldn't be too surprised to find that your University LAN admins are taking similar precautions.

This is not to say that I don't think you should have wireless convenience. I do, but what you're proposing, without you knowing the risks, would be very wrong.

Even normal WiFi precautions, which would protect your 2 laptops, and your PC, still won't protect the University LAN IMHO. Please read this article and carefully consider all precautions for YOUR computers.

<<http://nitecruZR.blogspot.com/2005/05/setting-up-wifi-lan-please-protect.html>>

I'm going to do some deeper research into the bridge implications. Please let me know that you have read this, and understand what I said, and whether my ASCII art diagram above is what you're considering. I will get back to you, so please be patient.

Cheers,

Chuck, MS-MVP [Windows – Networking]

<http://nitecruZR.blogspot.com/>

Paranoia is not a problem, when it's a normal response from experience.

My email is AT DOT

actual address pchuck mvps org.

.

• ***Follow-Ups:***

◆ ***Re: Using PC as bridge***

◇ *From:* Koren

• ***References:***

◆ ***Using PC as bridge***

◇ *From:* Koren

◆ ***Re: Using PC as bridge***

◇ *From:* Chuck

◆ ***Re: Using PC as bridge***

◇ *From:* Koren

- Prev by Date: ***Blocking Port 80 with windows firewall***
- Next by Date: ***Re: ICS with XP host, ME client not quite working***
- Previous by thread: ***Re: Using PC as bridge***
- Next by thread: ***Re: Using PC as bridge***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***