

Re: wireless network interception

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-09/0704.html>

From: Duane Arnold (*NotMe_at_NotMe.com*)

Date: 09/19/04

Date: Sun, 19 Sep 2004 01:18:32 GMT

spoking@bellsouth.net (spokin) wrote in
news:cb8310a2.0409181203.6079598b@posting.google.com:

- > *Ok, all you wireless security freaks, I need your help – educate me.*
- >
- > *Question 1: given a wireless router with WEP encryption, can an*
- > *outside machine intercept a signal from a network machines WITHOUT*
- > *getting the router to recognize it (the interceptor) in some fashion?*

WEP can be cracked and that's why there is WAP.

- >
- > *Question 2: If eavesdropping is actually taking place, is there some*
- > *way to DETECT that it is happening? How?*

Maybe, I don't know and maybe you should limit how many wireless computers are on the network. Maybe, you should have one machine that is a wired connection, which is more secure than wireless, if you're concerned.

- >
- > *Question 3: If isp account hijacking were taking place thru my router,*
- > *to spam or whatever, shouldn't i be able to see their connection in*
- > *the router log?*

If you have a router that shows outbound connections, you'll be able to see everything going outbound or inbound to the router. You may need a log viewer to see the logs for more than one day of traffic.

- >
- >
- >
- > *My setup is a wireless router as my DHCP server, with DSL connection*
- > *on the other side. All machines on local network run software*
- > *firewalls, base ip address range has been customized, password for the*
- > *router is strong, and I run WEP. But I think my questions are generic*
- > *enough that this detail won't matter.*

comp.security.firewalls: Re: wireless network interception

The DHCP would help you detect if some other machine was not part of your network got an IP and that prevented one of your machines from getting a DHCP IP. But that would be based on the number of DHCP IP(s) that can be issued is the number of computers wired or wireless that can physically connect to the network. If you have 3 machines total, then total number of DHCP IP(s) that should be issued is 3. If it's 10 then someone else could get an IP. Hey, it's better than nothing. And besides, if one wanted to get an IP, they could always use one of the router's static IP (s).

If you're that concerned about it, then use the router's wireless MAC Filtering feature, if it's got it, which only allows a wireless connection to your router based on the MAC of the wireless NIC that could connect to the router.

There is also wireless IDS systems as well, if you're that concerend.

Duane :)