

Re: [fw-wiz] home net security (was Re: 802.11b and IPSec)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-06/0107.html>

From: Paul Robertson (*proberts_at_patriot.net*)

Date: 06/15/03

To: Bennett Todd <bet@rahul.net>

Date: Sun, 15 Jun 2003 08:46:06 -0400 (EDT)

On Tue, 10 Jun 2003, Bennett Todd wrote:

> *I don't know the answer to the question you ask. If I wanted to hunt*

I got lots of answers, I'll write up a summary in the next week or so...

> *If you don't mind, though, I think it'd be valuable to expand the*

> *discussion to a more general analysis of security for home nets.*

I think that's valuable...

> *Now obviously a home net can be anything. There are undoubtedly*

> *maniacs who have beowlf clusters doing hotly proprietary financial*

> *modelling or whatever, with Special Needs. But they aren't typical.*

I think that much, much worse is the user who doesn't know what the value of data on their home network is— or who underestimates it. Heck, the CIA had a Director who took classified home to his PC, the rest of us have much less strict environments, and have to deal with the outcome..

> *Let's fantasize that the typical home net has 802.11b; it has one*

> *or more workstations on it, which being pure clients are easy to*

> *harden (hardening hosts is only hard when you need to offer network*

> *services from those hosts).*

I'm not sure that assumption is valid, many home networks have 2 or 3 clients on them— some of which may be doing things like serving music files, participating in P2P networks, etc. In a typical home environment, it's only easy to enforce a security policy if there's one person using the machines, or one predominately computer-literate person, otherwise, it's as political and bad as any other network, maybe worse...

> *As I see it, the one hard-to-address aspect of home net security is*

> *preventing drive-by wireless users from committing offenses on the*

> *internet through your access.*

Firewall-Wizards: Re: [fw-wiz] home net security (was Re: 802.11b and IPSec)

That's one of the three main reasons I want to enforce IPSec on the WLAN side of things...

- > *While it's weak protection, I think wiring down the DHCP with an*
- > *enumerated list of MAC addr is decent protection. Not perfect, of*
- > *course, but it'll cut out casual*