

Re: TCP/IP offload: security implications

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-02/0745.html>

From: William P.N. Smith (wpons@compusmiths.com)

Date: 02/27/02

From: William P.N. Smith <wpons@compusmiths.com>

Date: Wed, 27 Feb 2002 16:34:33 -0500

nospam@masoner.net (Richard Masoner) wrote:

>Adaptec and Intel have announced gigabit ethernet cards with full
>TCP/IP protocol offload in hardware. I think offloading TCP/IP from the
>CPU to other hardware makes sense when high wire speeds are involved.
>Not infrequently, however, TCP/IP implementations are found to be
>vulnerable to attack by malformed packets.

While DOS is still a concern, I'd think you'd be even more secure from buffer overrun attacks that generally allow the attacker to run the code of his choice on your machine. [Not that the code couldn't be written to drop executables in the right place in the host's memory using bus master or DMA, but that's certainly a much harder and less likely attack than taking advantage of the usual wellknown MicroSoft vulnerabilities]

--

William Smith wpons@compusmiths.com N1JBJ@amsat.org
ComputerSmiths Consulting, Inc. www.compusmiths.com

- **Next message:** [Bear G: "Re: audit failed writes to read-only file-system?"](#)
- **Previous message:** [Dustin Puryear: "audit failed writes to read-only file-system?"](#)
- **In reply to:** [Richard Masoner: "TCP/IP offload: security implications"](#)
- **Next in thread:** [Dennis C: "Re: TCP/IP offload: security implications"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)