

Re: Ethernet cable question.

Source:

<http://www.tech-archive.net/Archive/Vista/microsoft.public.windows.vista.general/2008-09/msg06713.html>

- *From:* wrat@xxxxxxxx (the wharf rat)
 - *Date:* Thu, 25 Sep 2008 04:30:29 +0000 (UTC)
-

In article <#Tu9K7oHJHA.3668@xxxxxxxxxxxxxxxxxxxxxxxx>, Paul Montgumdrop <Paul@xxxxxxxxxxxxxxxx> wrote:

This is stupid, and I know better. I have developed Web HTTPS site solutions on the server and on the client end. If it was so easily breakable as you claim, then a whole lot of transmission of sensitive data would be getting compromised and eavesdropped on. And it would be

With all due respect, you're making a typical mistake. HTTPS *CAN* be secure. HTTPS is NOT forced to be secure merely by virtue of appending an S.

For instance, your browser considers any connection "secured" by some form of SSL to be secure and makes no distinction between 40 bit encryption and 256 bit. If the website is accidentally or on purpose configured to accept 40 or 56 bit you may connect insecurely although you think you are connecting securely. For a discussion of this problem see

<http://www.verisign.com/static/036094.pdf&usg=AFQjCNEZReuU9dor6or5jZusQH52Z-kLCA>

Furthermore, the acceptable ciphers are not all secure. The server may insist – again without notifying the user – that the conversation use an insecure RC4 (for instance) cipher.

And when a person is finished with the bank transactions in a HTTPS session, goes to another site, it's not an HTTPS site, and there person gives up sensitive data over the Internet, then that's falls under the ignorance of the user and is NOT a HTTPS issue on security.

That's exactly the situation that a strong local security policy is meant to protect you from. Someone else tried to use the idea that because the bank conversation is encrypted you don't need to encrypt the link. That's not true, exactly because of the situation you point out.

Re: Ethernet cable question.

And for you to say that some bank site may not be set-up correctly or that the Web site developer(s) who have developed, tested, went through quality assurance testing to ensure the integrity of the site solution and the staff did not know how secure the solution is ridiculous,

Pfffft. Are you telling me that people never make mistakes? Or that insiders never deliberately open holes to exploit for their own purposes? Or that intruders never modify system configurations? These kinds of things happen all the time. A typical example: administrator specifies 256 bit but the product isn't licensed for that level and so falls back to 56. The admin won't even notice until the next security audit because it's not an error and everything looks just fine. (well, she might, if she's good.)

Great Ghu, even classified systems get compromised. Don't you think it could happen at a bank?

particularly at banks. What? Do you think people who hold those positions don't know about the attack vectors and how to prevent them?

To err is human. And you can really foul things up if you're using a computer. You're saying I should trust these unknown people because they work at a bank. Talk about silly.

.

Re: Ethernet cable question.