Does SSL protect you, or is it a condom that is open at both ends?

For the last five or so years, SSL has been paraded as the technology that secures the Internet. All you have to do is look and see the padlock on the bottom of the screen and you can be sure it's safe.

Is it true?

SSL is a technology for providing a secure connection between two places. It provides secure links, or pipes between wherever it starts and wherever it stops.

What it does not do is actually secure any of the data that passes through the pipe, or really know where either end of the pipe actually is. What you can be sure of is that anything put into one end of the pipe is going to come out wherever the other end is.

But surely the data is fully protected? Yes, whilst the data is in the pipe it is protected. Now, assuming – and unfortunately that's what we have to do – that you know for sure where each end of the pipe is, and you are sure that each end is very secure, and you know for certain who is at each end, then you're OK. If any of those is not true then you do have a problem.

My data is SSL protected between the server, and me so why should I worry? Well no one at the server end really knows whom the data is from because they don't know what your identity is. They assume that data arriving through the pipe is right, and that your identity can be presumed from the data, not the other way around. Unfortunately there are hacker attacks that divert your link through their own site, where they can pretend to each end that they are the other entity without either end being the wiser. (This is called a man-in-the-middle attack using web site spoofing.)

Once your information gets to the server it stops being protected and anyone can get to it, at least judging from the fact that hackers target web sites first because that's where they can guarantee to find large quantities of names, addresses, credit card numbers and so on. (Actually, SSL places such a heavy load on computers that they now have other machines doing just the SSL encryption so your data is potentially exposed even before it has a chance to get to the web server, but that's not the point.)

So there's the problem. SSL provides strong protection, but not actually to the data, just the link. You might say it was a condom that protects the pipe.