SSL – does it provide the security that users believe?

SSL (secure sockets layer) is the security technology everyone uses to ensure that their web connections are secure. An SSL connection is symbolized by a padlock icon in the right-hand side of the taskbar and a URL that starts with 'https', the 's' standing for a secure http connection. What trust, however, should users associate with SSL?

Confidentiality

SSL uses a method known as public key authentication in order to provide the confidential link between the server and the client computer. This can be a very strong and effective method. It allows you to establish a strong confidential link between a server and a client without either knowing about the other beforehand. And that's where the problems really begin.

Public key authentication works where each end of a connection can independently check that the other end is real. It's the same idea as getting a cheque from someone you don't know and calling their bank to see if it's OK. That's why it doesn't really work. If it was going to work, the server would have to be able to find out if the client key really belonged to them or not – and it can't. In our bank example, it's like having a cheque without the bank name on it or the customer name the bank knows you by so that you can't even ask the question. In fact if that happened you probably wouldn't accept the cheque!

As a result, the server can't tell if a hacker has diverted you via their own site and is playing a 'man-in-the-middle' attack where the hacker gets to see all the data going both ways.

Usually the server uses an identification that has been approved by one of the companies whose information is stored inside your browser. That's why at the client end it all seems fine. There is just the minor problem that you can't actually tell if the identity is still valid because there's no way in the current system to do that.

Not surprisingly, there is nothing happening that allows the server to link the information arriving at it with the actual user of the client PC. It is always assumed that the information comes from there but you can't prove it.

Is the padlock real?

Although the SSL padlock has been on the bottom of the screen for a while now, only the most adventurous have tried doing things like clicking on it. If you did you might be in for a surprise.

The first thing is that you can't tell if the padlock is genuine. After all, anyone can write a padlock to that point on the screen, it's not a special protected area of some kind. So seeing the padlock appear needn't mean a secure connection is actually in place.

If you do click on it you should see the web site address for the site of the server that purchased the certificate being used. You should compare this with the web site address shown in your browser tool bar. It is important to read it carefully since you are the one doing the checking, there is nothing automated about the comparison.

What needs to change?

Several things need to change before you should feel comfortable using SSL.

1) Getting enough functionality onto the client system to be able to sign and encrypt actual data instead of trying to make secure connections to places you don't know.

2) Providing clients with the ability to check that certificates sent from servers are still genuine (check to see if they have been revoked) automatically. Then users can be sure that no man-in-the-middle can read the information they send, and that the server they are dealing with is for real.

3) The client needs an identity that can be authenticated by the server (this does not have to mean that users need to go out and buy a certificate, the server site may provide them with a suitable certificate as a separate process).

4) Automating this whole process so that the user does not have to click on the padlock icon to find out if the security is real.