SSL – a false sense of security?

One of the greatest errors you can ever make is to believe your own PR. The IT security industry may be in danger of doing just that, by issuing what, at best, should be described as contradictory or highly confused statements.

The battle is on right now to give users confidence in the security of the Internet and the reliability of the businesses you contact over it.

Some interesting claims published by bodies describing themselves as Certification Authorities (or server certificate suppliers) make confused reading:

- server certificates ensure your customers are dealing with the correct web site
- server certificates prevent web spoofing
- server certificates ensure user's credit card details are safe
- the padlock icon means that you can communicate securely with your customers

Let us consider these merely as matters of technical fact.

On February 2nd 2002 Dartmouth College (USA) published an academic report which can be found in www.cs.dartmouth.edu/~pkilab/ that states quite clearly, "There is no single part of the browser window that cannot be spoofed." Previously Princeton University had published an academic report
www.cs.princeton.edu/sip/pub/spoofing.html
that came to similar conclusions.

Even if the academics were completely wrong (and there has been no reported litigation, take-down notices or other actions so far to stop them publishing), just consider the following:

- it is a commonly accepted practice to issue server certificates with wild cards – that is that the character * may be one or more other characters (A-Z, a-z, 0-9 and so on)
- certificates on their own prevent nothing at all – just as critical are practices, procedures, methods and techniques by which the keys are protected, by which information is protected and by which customers are protected
- it is reported that ISPs offering SSL services to their customers do so using a single SSL key for the ISP. If this is so, then it is anyone's guess as to which site is actually being contacted by the user
- the padlock icon, on its own, has no more meaning than any other icon

However, do not knock SSL. It has provided one of the few real means of protecting information traveling across the Internet, and has been immensely successful within the constraints of how it has been implemented in an architecture that does not provide it with adequate security information.

So if the absolute security of SSL is open to question, what other mechanisms are there that are technically defensible?

Elsewhere, we see an increasing number of self regulation sites promoting customer assurance by displaying their logos on web sites. These look to be extremely worthy ventures. They correspond to trade bodies verifying the conduct of members and checking that they behave properly. However, some may be following the SSL lead by suggesting that sites displaying their logo can be relied upon absolutely.

Well, if Dartmouth are right then they are wrong. It's rather difficult to get round that point. Some state that you cannot copy their logo and misuse it. That claim needs some careful interpretation. Almost anything that's displayed on the PC can be copied. If the PrtSc key doesn't capture it so that your picture publishing package can manipulate it, you might have to take a photograph (digital, hopefully) and then paste that in. Mathews' Law of Computing says, "If it's processed on an ordinary PC it can be copied."

Others tell you to click on the logo to get full verification. Again, if Dartmouth are right then they are wrong. Once you have spoofed one item you can just as easily spoof another.

So what can actually be done?

The flaw in all the current methods is that they actually exclude the user from the process(es). The user has to accept blindly whatever the computer says at all times without any independent means of checking anything. This is the ideal environment for the hacker and spoofer. The user needs software, running in his own machine, independent of all the merchants, that can tell him what his eyes are unable to – because he cannot see what happens inside the computer.

As Dartmouth identified, he needs something that can check where he is really connected to and where information is really coming from. He needs to be warned if things don't stack up. He needs to be told, interactively, when information may have been altered or appears to be false. He also needs to be much more aware of when web sites are operating securely, and when they are not but should be. That applies to whole sites, not just a few SSL or SHTTP pages here and there. By the time he gets to a secure session it may be too late! Static methods are flawed. (Whoever heard of a car where you had to check for warnings by clicking on icons on the dashboard?)

ArticSoft, an Internet fraud prevention company provides free software that ensures the whole process of genuine trust. Web sites are able to link their identity to every page they publish and users are able to see them checked as they arrive – not just live in hope. ArticSoft automatically provides the user with an alert when a web site page has been altered or where it is not coming from the real site. Users know instantly if something has gone wrong, before they put credit card or personal details into the system. They can print out a copy of the proof of source if a transaction is important.

ArticSoft, used in conjunction with logo schemes and/or SSL gives web sites and users confidence of who they are really dealing with and users confidence that their personal information can only be going to the place they want – nowhere else.