Authentication – who's site is it really?

If you go to the site of the UK e-Envoy (www.e-envoy.gov.uk) you will learn a lot of really useful information about how the UK government is approaching the question of how to identify the people they are dealing with whilst out in the wilds of the Internet.

The site has published a large of papers addressing government policy, (www.e-envoy.gov.uk/publications/consult_index.htm) giving the UK government's views on how they intend to address many of the security questions raised when trying to do 'business' over the Internet. The original papers were provided early in 2001, public comments were submitted by February 2001 (I'm sorry, like me you've missed the opportunity) and revised papers were published in December 2001.

One of the documents I found helpful lists all the comments made during the public consultation process and the response of the e-Envoy's office.

Apart from the usual axe-grinder questions about how this would help sell more of a particular manufacturer's product, or what issues there were for public privacy, there were more than a few comments about the problems of authentication.

What on earth is that all about? Well, (maybe not) obviously, when the UK government is doing something with citizens/customers over the Internet, it thinks it would be a jolly good idea if it knew who it is dealing with at the other end. So much so, in fact, that there is discussion on levels of authentication and identification and what you should be thinking about, as a government department, when deciding the levels that you require from the people accessing your systems over the web before letting them in. This kind of discussion is well informed and any business looking at Internet authentication should read it carefully and consider how much of what is said would apply to them and their own business requirements.

There are many issues in the business of authentication, and methods by which it is achieved, that are worth discussing at some length, but that is not the topic of this paper and they are not considered here.

The point of this paper, and the discussion so far, as was pointed out in the public comments, is that whilst there was an enormous amount of material contained in the advice about authentication of the citizen/customer coming into the government system, there was nothing at all about how that user could authenticate the government web sites.

And that set me to thinking. Is there a difficulty about authenticating web sites. Obviously, if it make senses for the government to insist that people using its services have to be authenticated, those people should know precisely who or what in government they are dealing with?

The problem seems to be that when it comes to verifying things like site credentials, the average PC is currently about as much help as a paperweight. Whilst the technology is technically available, nothing has been implemented in the operating systems PC desktops that proactively helps the user check out the web site they are connecting to.

When you visit many web sites you will see lots of logos telling you what good folk they are and how well the sites are designed – and, to be honest, they're right. But they don't have any positive way of proving to the user that they really are who they say. Sadly, tools exist that allow anyone (they're not just for hackers!) to download an entire web site automatically. So without some form of active protection, it is very hard indeed to realize that you are not connected to the web site you think.

Something has to be done about getting some realistic level of confidence into otherwise unproven web sites. (It doesn't matter how confident the web site owner is that their content is fine, it's a matter of the customer having the ability to check it for themselves. Anyway, with web pages cached all round the world, the attack doesn't have to take place on the originator's web site, it could be anywhere.)

The UK government says, quite rightly, that authentication should require different levels of protection depending upon the sensitivity of the information being dealt with, at least in the eyes of the citizen/customer? Remember, it's important for government to do this to protect it, so it must be just as important for everyone else.

Applying that logic to web sites and portals, it seems to me that we are being asked to prove our identities to them to fairly stringent levels, and they are giving precisely nothing back in return. Now that may be seen as rattling a few cages, but if you think about it, the Internet is supposed to be a two way street. So why is it that the web sites and portals expect us as customers to take everything on 'trust' whilst they insist on strange cookies, credentials, ID/password and so on?

Well the answer is given earlier in this paper. It's because they don't have anything on the desktop sorting it out, and hardly anyone seems to be willing to break the mould and do an Adobe or a PKzip in the desktop security world. If that doesn't happen, let's hope we're not waiting for miracles from manufacturers. Thus far, their commitment to security has been less than totally convincing, and on that track record and any change would parallel the results of a famous journey on the road to Damascus. I suspect that few in the industry, let alone in the public, would have enormous confidence in a group of suppliers that have so successfully gained a poor reputation for placing any priority on security.

Perhaps companies like ArticSoft will help us to take the high road and give citizens/customers the kind of security that they should expect from web sites. If that doesn't happen, then we should be asking serious questions of governments and commerce who have done nothing to justify why we should have so much confidence in them on the Internet.