Open Standards – why they are essential

Summary

If you don't pick a solution that not only has a commitment to open standards, but has already implemented them, and can demonstrate interoperability with other users of that standard, then you are betting.

Betting that somehow or other what you are buying is going to take over the world. Betting that everyone else is going suddenly change away from an open standard to a proprietary (lock in) system which they are going to have to pay for. Somehow not very likely.

Introduction

Interoperability has been the bane of most security people's lives. Just ask an X.509 PKI man to show you the scars! Or better still anyone at all from telecomms.

Services have no value at all if the person at the other end does not get the message. And that is just as true for the network people as the security experts. You need open standards if you are ever going to succeed. And standards that work.

You see that doesn't mean the standards can be so open that every implementation can be different. We have had plenty of instances of a standard that is so open that it is wide open to any interpretation a manufacturer feels like – which is proprietary. That happened with V.24, and again with any PKI standard you care to mention.

It isn't enough to waffle on about open standards alone. What you actually need is an open standard where there are a limited number of very clearly described options (profiles) that are implemented reliably and consistently. Because no standard has any value if the guy receiving the message cannot read it, or is given hassle trying to cope because it 'almost' works.

So what is the encryption standard to go for ?

The OpenPGP standard (RFC 2440) is tightly defined and there are many 'middle of the road' implementations (besides the ArticSoft one) that mean you can be confident that the mail will really get through. There are a lot of people out there telling you that their proprietary implementation is much better, but when push comes to shove they are just not going to take over the world.

Reality is that open standards are the way forwards because they can be implemented successfully by all suppliers. Time and time again. And they are going to work. You need certainty over operation, And certainty is given through the fact that the standard has been checked out in serious detail by experts all round the world, any weaknesses in it checked and re-checked, and any errors fixed.

Why bother with open standards ?

Consider, the reason you can read eMail is because of a standard that was originally called USASCII that defined which bit patterns made which characters. Without that, each computer manufacturer did his own thing and everyone was different. And you could not read a file from another manufacturer without doing a complicated conversion from their encoding to yours.

Open standards fixed that problem. And today we have open standards that cover pretty well all the written language formats around the world.

The standard we all rely on for Internet connections, TCP/IP is another open standard. Before it was introduced all the manufacturers had their own ‘standards’ and you don’t get a prize for guessing that none of them worked together.

But the Open Standard eventually displaced the proprietary ones, and life, as they say, returned to normal.

What are the economics of the situation ?

Well, when a market develops, initially all the ‘standards’ are proprietary, where each manufacturer tries to grab the market for themselves. In fact manufacturers might encourage the development of standards in areas where they have patents. Whilst this happens, the suppliers can charge premium prices (and make big profits) because they are the only show you have in town. And they can also charge other suppliers for the privilege of interoperating with them by levying royalties.

In the encryption world, for many years RSA held a patent over the implementation of their algorithm, so if you wanted to use it (commercially) you had to pay whatever they decided to charge. Naturally they were interested in achieving maximum income from a market that they could dominate. This may not have led to the cheapest cost for the customer, if encryption was what they had to do.

Once open standards become implemented, the nature of the market changes, because the element of competition is introduced. Manufacturers are not obliged to license technologies at any price before they can introduce new and innovative implementations for their customers. They are free to compete upon their own skills, instead of being constrained by a proprietary infrastructure that stifles competition by putting an even higher price on innovation. There is no motive for a patent owner to allow innovation in a market they dominate.

Open standards promote commoditization. We see this in other markets. Whether you look at VHS recorders or DVD players we see the effect of a commodity market – greater diversity of choice – lower delivered prices – addition of functionality – feature and function innovation as manufacturers differentiate through innovation rather than through patent or IPR control of a technology.

In fact, there are many arguments to suggest that current IPR controls may actually reduce competition and innovation rather than promote them. Copyright now lasts until 80 years after the death of the last author, so in a software program, it could easily be 100 years before anyone can use that code or layout or appearance again.

So if you don’t have open standards you are more than likely to be paying a premium (that you cannot control) to get the services you are using. This is not good for you economically, because you are looking for the best bang per buck so that your budget goes as far as possible whilst delivering premium product.