Security can be simple and secure

It was interesting to read the press release given by Phil Dunkelberger, CEO of the newly formed PGP Corporation, saying, "You are faced with the situation where usability is traded off against security--the more usable something is, the less secure it is." But why must security be difficult to use in order to be secure? Well the reality is that it doesn't! However, if you wanted to believe the press release then you could be forgiven for mistakenly believing that it must be so.

Let us use some logic here to analyze the thinking. If it were true, then anything that is simple to use cannot be secure. The fact of the matter (as the lawyers would say) is that it is not essential to make something difficult to use in order to make it secure. Rather the opposite.

There is no reason at all why something MUST be difficult to use for it to be safe and secure. Look no further than your automobile vendor. Do you suppose that they make cars more difficult to use so that they are more secure? Get real!

So why have we got this strange idea of` "No pain, no gain?"

The basic problem seems to start with the IS security community themselves. In order to achieve recognition they have to carve out their own niche that demonstrates how important they are (and why you should pay their costs). To make yourself important in a technical subject you have to be difficult to understand so that people cannot readily question what you do or why you do it. To reinforce that notion you make people learn all about your own ideas (worship at your shrine) so that they become true believers.

Quite frankly, if you can't understand what someone is telling you, the problem is with them, not with you. That is not to say that the subject of IS security is not complex. But so is the subject of how car tires are safe, and few, if any of us know (or really care) how they are made - providing they perform.

So that's the acid test. Can the person using the security system make it work without too much difficulty? Well, according to the pundits of the security industry, apparently not. It seems that the average user (or senior executive) can't use security products because they are just too difficult. Well they probably haven't tried products from ArticSoft which take the mystery out of security.

Certainly the 'Public Key Infrastructure' which was supposed to solve all our Internet security problems is very complicated. It is particularly complex if you look at the web sites of VeriSign or RSA. It would be a lot simpler if they talked in plain English instead of 'Pompous Techspeak'. Perhaps that is one of the reasons why it seems just too difficult to use.

If you want to talk to someone on the phone you need their phone number. So if you want to speak to someone with privacy you need their public cryptographic key (phone number?). That's all there is to it. If you don't happen to know their number or have it in your diary (keystore, wallet, or whatever it's called) then you either get them to tell you (send it by e-mail) what it is, or you look it up in a Directory if there happens to be one handy.

If you want to send something that's really 'private' you're hardly going to do that with someone you don't actually know. That would be really silly. You only ever send secrets to people you actually know! And a secret is hardly going to be sent to 'everybody' because that's an oxymoron (a contradiction in terms according to the Oxford English Dictionary). So there's little point having a 'solution' to a problem you don't actually have.

So where does that leave us? Well, security products only have to be complex if the designers make them so. You see, that's the issue. Whilst there are too many people who think that users should 'take responsibility' for security by making what are, in reality, arbitrary choices (what algorithm, key length, password length, quality of mother's maiden name, smart card and so on) then security will continue to wander in the wilderness.

It is a simple matter of making the presentation of security to the user much simpler by hiding the complexity and using 'best of breed' methods so that the user can make useful business decisions such as who to send secrets to, secure in the knowledge (as with the car tire) that the technical 'stuff' has been dealt with by people who know what they are doing.

As a final thought, if you want your computer to be totally secure, then the easiest approach is probably to bury it underground encased in concrete. Plenty of pundits will tell you that you should not use a system that is not totally secure. Follow that kind of advice and you will be unable to travel, live in a house, eat or maybe even breathe. We all know that security has to be good enough provided that it's the best that's available without being impossible to use.