Confidential E-Mail Communication

- Authentification and Encryption -

Ernst F. Hefter, E-R-D = English-Russian-German Language Services
Birmingham [valya.hine@e-r-d.net] – Lobenfeld / Heidelberg [ernst.hefter@e-r-d.net] Internet: http://www.e-r-d.net/

[Published in the Newsletter of the Consultancy Group of the IOP: NL26, July 2002; pp. 6-7]

Via ordinary e-mail you've just received a confidential message from your new client discussing the details of his most promising project, a project shaping his future and securing your income for a good while. You play a most important role in its key sections. Naturally, you've signed a confidentiality agreement with a high penalty in case...

If it's really a project of international importance then both of you should be aware of the fact that under the given circumstances the confidentiality agreement isn't worth the paper it is written on. Apologies! I do not want to indicate that *you* might commit a breach of such an agreement.

Let us assume that it really *is* an important project of global significance. Well, then you can almost bet that after the exchange of the first (or first few) e-mails the respective departments of most of the secret services of the civilized world – including your American cousins and European friends – will have copies of these e-mails in their files. And they will follow the further correspondence of such an important project with great interest. The closeness of the contact that these services keep with trade and industry of their home countries is a geographical variable. Yet, with a really important project you can be almost (the "almost" is needed since you will presumably never be able to prove it) sure that one or more of the competitors of your client will be informed in due time – and in addition to these services there are the "small" guys, the hackers.

Besides, talking about ordinary e-mail: How can you be sure that the e-mail message received is the same as the one dispatched? That the message really comes from the person given as the sender – not from the famous "man in the middle"? You can't be sure that ordinary e-mail has not been altered and that it is from whom it appears to be from.

Speculations? Maybe. But have a look at the web site of the DTI (www.dti.gov.uk), say. In one of their brochures ("Information Security and the Internet"; URN: 00/1391; pdf-format) you find statements like:

> "Here is a summary of the realities:
> The Internet is inherently insecure...
> A company using the Internet is responsible for the security of its own ... information.
> ...
> Companies cannot control the route which a message will take when it crosses the Internet...
> It is possible for messages to be read or modified.
> ...
> Unless properly encrypted, credit card payments can be intercepted and manipulated or stolen...."

The DTI – as one of many good sources of information on security and related topics – provides a good number of leaflets, information brochures etc. on the subject. But you have to download, or order them, to read them and to implement the necessary procedures...

However, the main problem is acquired carelessness (with regard to electronic media in particular and information in general). I trust that you lock the door of your house when you leave – even for a short walk round the corner. And your car? Don't you lock it automatically too? But how carefully do you protect your main asset, information?

The ordinary business person / manager will not be able to check the route his e-mail took. He will never see the relevant data! He might not know about their existence. From actual experience and from TV films he should know what might happen with a telephone conversation or an (ordinary un encrypted) fax. He is far less likely to realize that similar pitfalls surround his "confidential" e-mail.

So, how can I ensure authentication of my e-mail? – By applying an electronic signature every time you send an e-mail. Thus you make sure that the recipient has a chance to verify your

signature, to prove that it has been sent by the person specified therein and that the information has not been modified. The first point is well known from traditional paper communication. The second point is new. A signed paper document may be forged by adding information on the paper above the signature. That's not possible with electronically signed e-mail or files. You *can* check whether they were tampered.

How can I ensure confidentiality of my e-mail? – Use adequate encryption to "scramble" the text so that unauthorized readers will not be able to make sense of your message.

What software should I use for signing and encrypting? – The response of your lawyer or tax advisor to a seemingly simple question will often be "it depends". The same applies here. It depends in the first place on the costs arising from a fraud, from a breach of confidentiality. And don't trust encryption software simply because *you* can't decrypt the material yourself; to a specialist it may be a trifle. I think open source software is not a bad option. Everybody knows the method and algorithm, a lot of professionals have tried to break the code, and its "strength" is well established. It's the same with the front door of your house: it only has to serve its ordinary purpose – not withstand explosives and the like...

You think you don't need stuff like electronic signatures and encryption? You don't really mind whether all received e-mail is intact? There are no risks and losses involved as far as your electronic communications are concerned? Maybe. Or is it simply that you are not aware of the risks (as indicated by research published by the DTI)? Even if your assessment is correct today, the situation may be very different tomorrow. Why not make preparations for tomorrow?

With procedures that may have a great effect (like signing and encrypting e-mail) it is to my mind most important to build up a habit – just like locking your house / car. And for that purpose any decent software should do. In such a manner I am training myself and the people I can influence. We use software that is available free of charge for personal use or with a rather cheap licence for businesses. It is Pretty Good Privacy (PGP) by Phil Zimmermann. According to the currently available (non-classified) public information it is extremely secure in spite of the export regulations of its country of origin, the USA. Comparing the role of such a program with the function of the front door of your home or business premises, the implication is that you may safely use it for safe-guarding the precious stones / business assets you normally deal with.

As far as we are concerned, we stated explicitly in our old terms of business that we are not obliged to use means of communication that are safer than the ones our partners use when sending us their messages (including documents). Just now we are updating this document. We intend to stress the point and to offer our partners authenticated and secure electronic communications using PGP. In an internal trust center we are already offering them certification of keys to be used.

Presently we try to get all our members of staff and communication partners to add electronic signatures to all their private and business e-mails. The aim of the exercise is the building up the habit of automatically doing it. Once that has been accomplished to a good degree, all communications will have to be encrypted – at least within the organization and with its closest partners.

There are also solutions that automatically sign / encrypt the messages when they are sent. To my simple mind they have significant shortcomings:

(1) The user will soon "forget" about the need to be careful.
(2) He will never make it a habit to sign / encrypt messages.
(3) If the system happens to fail (or is corrupted / put out of action by chance / hackers) then the ordinary user will not take notice of that fact and continue to act as if all security measures were in place.

If you store your client's personal or confidential data on your computer then it is again encryption that can help to safeguard them. No need for it? Maybe, but you should consider having a look at the Data Protection Act (1998). It requires that information held on people is safeguarded adequately.