

How to protect e-mail from prying eyes?

By Martin Bensley

Nobody likes other people reading letters that were not intended for them and thanks to a revamped cypher program on the Internet, reliable e-mail confidentiality is just a mouse click away.

There are several on offer but PGP (Pretty Good Privacy) is the one claimed by its makers to be so sophisticated that even the world's secret services have trouble deciphering it. Indeed, some of them even want it banned from the World Wide Web altogether.

E-mail is a fast, cheap way of communicating, but its nature means the messages are like postcards with no digital envelope to shroud the contents.

A sender might wire something about his employer via the firm's e-mail only to find that the boss has been closely following his correspondence. Or else a sender who happens to be a dissident living under a restrictive regime could find his messages sent abroad being intercepted and read by government agents. The latest version PGP 5.0 for Windows is now available free as shareware through the Internet at a number of locations, thanks to a dedicated band of enthusiasts.

With the consent of PGP's American inventor, Fred Zimmerman, the hackers managed to spirit the program out of the United States despite stringent U.S. legislation forbidding the export of had encryption programs.

The operation exploited a legal loophole which imposes no restrictions on sending abroad the printed version of the source code

although the electronic export of the software or source code is banned.

The encryption source code a version of the software in human-readable as opposed to machine-readable form was published in several volumes and sold in US bookstores. The printed source code soon found its way across the Atlantic and the hackers were busy with their scanners. Tens of thousands of hours went into scanning the 5.0 version.

Now PGP 5 Freeware.exe can be downloaded from the Australian Privacy Home Page <http://210.15.255.14/>. The file contains a long list of other servers, including many in Germany, Eastern Europe and some in Japan. Version 5.0 is much easier to use than its DOS predecessor and there are comprehensive manuals for beginners. PGP operates with the so-called asymmetrical process by which the user generates a public and a secret or private key. Anyone can call up the public key on the Internet but the private one is kept by the recipient only for decoding purposes.

The system is claimed by Zimmerman to be so safe that even the powerful computers used by intelligence agencies could take months or even years to decode a properly generated message. Key size is 1024 bits and experts say such numbers are theoretically safe for between 10 to 20 years even taking into account that computer power is doubling annually. Despite the bold claims, the American cipher guru admits there are some risks. A third unauthorised person could gain access to the communication

line between two e-mail correspondents and try to convince them that a fake public key is the public key of the respective correspondent. In a bid to foil such skullduggery the Internet contains various public key servers where keys can be validated before use.

There are moves in U.S. Congress and in some European states to ban encryption for the masses altogether. Intelligence agencies are worried that by using PGP and other ways of encrypting messages, criminals and extremists could communicate via the Internet untraced. The National Security Agency in the U.S. is lobbying for an agreed standard system where duplicate key codes would have to be logged with the government. In the case of future legislation forbidding encryption a "stealth" version of PGP still at the development stage would make it impossible to prove whether a message had been coded at all. For more information on PGP, its usage and the risk involved see: the independent "International PGP Home Page", located at <http://www.ifi.uio.no/pgp>.

Much of the data here has been compiled and is regularly updated by Stale Schumacher of Finland who helped generate the 5.0 version for use outside the U.S. In addition Keith's U.K. International PGP Home Page at <http://www.iway.co.uk/reality/sunrise/pgp.shtml> offers an excellent overview.

This article was published in the Arab News on 4 November 1997