Electronic mail and privacy

More and more physicians are relying on the Internet to communicate and seek information, but increasing use can bring increasing danger. The major risks involve e-mail, security threats associated with the World Wide Web and computer viruses.

E-mail is revolutionizing interpersonal communication, but e-mail programs do not protect the contents of a message from unauthorized readers. I've already warned that sending e-mail over the Internet provides as much privacy as sending a postcard through the mail: anyone who is sufficiently motivated can intercept and read your correspondence. Consequently, although e-mail may be used for routine communications, personal information or particularly sensitive patient information should never be sent via unencrypted e-mail.

To provide privacy, Netscape Communicator and Internet Explorer 4.0, two popular Internet suites due for release this summer, incorporate public-key encryption, an easy-to-use encoding and decoding utility that encrypts messages and provides a digital signature that positively verifies the originator.

Encryption for Dummies!

To better understand public-key encryption, think of the decoder rings that used to come in cereal boxes. Using the ring, a message could be encoded into an unintelligible string of characters or numbers, rendering it safe from prying eyes. Once a message had been encoded, only those with an identical decoder ring could extract the real message. This scheme, which uses identical keys to encrypt and decrypt, is called secret-key cryptography.

On the Internet, it is difficult to distribute secret keys. With the decoder ring, a secure channel could be established by delivering rings to those with whom you wished to communicate. This may work if your correspondent lives down the street, but it is not practical for secure, global communication via the Internet. Unfortunately, the fact that e-mail can be intercepted by anyone also means that anyone can eavesdrop on attempts to establish a secure key.

To solve this problem, Whitfield Diffie and Martin Hellmann developed public-key encryption in 1976. It eliminated the need for secure distribution of secret keys by using 2 separate keys: a public one that is freely distributed and a private one that is guarded carefully in your computer.

Let's say you have installed Netscape Communicator or Microsoft Outlook Express and wish to send me a secure message. Your first step would be to obtain my public key from a key server, which is an Internet directory of public keys, or by having me send the key to you as an e-mail attachment. Once a message that is intended for me is encrypted with my public key, I become the only person who can decrypt it with my private key.

Digital signatures

Public-key encryption also provides a digital signature, which provides additional security. Upon receipt of the message, my e-mail program conducts a quick calculation based on the actual message, your public key and the enclosed digital signature. If the result of this calculation holds, then the digital signature is valid according to my e-mail program. If there has been any attempt to alter the message by someone who does not have access to your private key, the calculation fails and the message is suspect.

Public-key encryption serves 2 essential functions for physicians:

- It protects the privacy of sensitive information.
- It provides a way to verify that a message is genuine by checking the digital signature against the sender's public key.

In a future column I will look beyond e-mail and consider security on the World Wide Web. — *Warren Lampitt*, information systems manager, Gretmar Communications (**warren@gretmar.com**).

Highlights from *CMA Online*

Reform of the health care system is proceeding at breakneck speed and few physicians will be affected more than family doctors. To help them ask the right questions about primary care reform, the CMA is creating an evaluation toolbox. Phase I of the project has been completed and phase II is under way. The overall project plan is now on our Web site at **www.cma.ca/canmed/projects/toolbox** [English] and **www.cma.ca/canmed/projects/toolbox/index_f.htm** [French].