Curb e-mail snoops

Did you know that your e-mail is only slightly more secure than that picture postcard you mailed by post? While it's true that not everyone can easily intercept and read your e-mails, the risk exists.

Since we transmit lots of confidential and legally sensitive files via Internet, the risk of illegal interception should set off liability alarms amongst us. What can you do about it? As it happens, you can make your e-mail more secure - at least to the extent that a snooper can't read it - and you can know whether anyone has tampered with it. You also can guarantee that the message you receive from a client or a customer actually came from the person who signed it. Such security issues have become even more vital now that electronically signed e-mail is considered as legal as its paper counterpart.

Beware of 'Sniffer'

What's the likelihood of someone intercepting, reading or tampering with your e-mail? Some Internet experts claim that as much as 25% of electronic mail is scanned by Internet Service Providers (ISPs), company e-mail administrators and hackers who have software that lets them sneak a look at Internet mails.

The most common form of e-mail abuse is electronic eavesdropping, sometimes called sniffing. Don't assume that your password - no matter how long and complex - provides total protection. Apart from hackers, who usually can break a password code, many people have access to your password or can snoop into your mailbox even without it, and all this has to do with the way e-mails are transmitted and stored.

Mubarak Ali

Every organization that has its own e-mail system has a "post-master" with access to your e-mail content. Ditto for the vendor that provides the e-mail function - that is, the ISP.

And if that doesn't shatter your privacy fantasy, consider this: All your transmitted e-mails (sent or received or deleted) end up on digital disks operated by your ISP or your own organization. Even worse: When the message files are removed from your organisation's storage or your ISP's computer, they are moved to separate electronic storage disks as archives and who knows what, if any, security is maintained over this information.

The purpose of the sniffer is to place the network interface (Ethernet adapter) into prosmiscuous mode and by doing so, capture all network traffic. Promiscuous mode refers to that mode where all workstations on a network listen to all traffic, not simply their own.

Sniffer Tools: There are a lot of sniffer tools available on the Net. The four such tools, which I dread most are 'Linsniffer', 'linux_sniffer', 'hunt' and 'sniffit'

The author is a freelance writer. He can be reached at aizan18@rediffmail.com

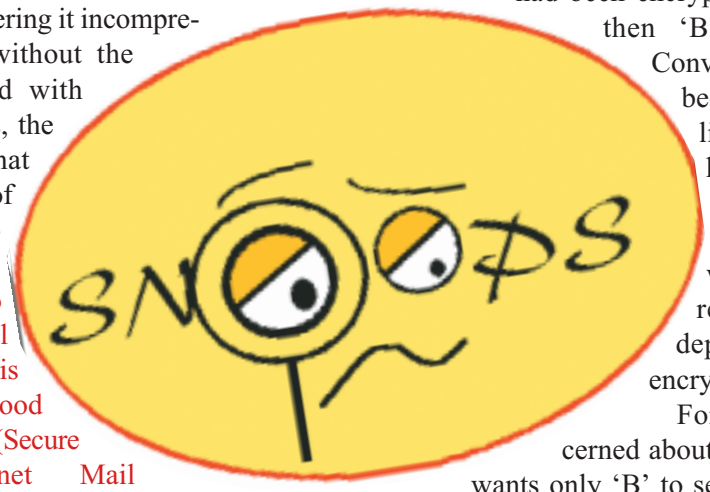
The 'linsniffer' is a simple sniffer whose main purpose is to capture usernames and passwords. The linux_sniffer provides a slightly more detailed view whereas 'hunt' is used when the sniffer is seeking less raw output and more easy-to-read information.

'Hunt' also allows you to specify particular connections you are interested in, rather than having to watch and log everything. It detects already-established connections, offers spoffing tools and active session hijacking too. Sniffit is for the sniffers who need just a little more. It allows them wide latitude to monitor multiple hosts, on different ports, for different packets.

Adopt Encryption, Change Passwords

The simplest way to keep a sniffer at bay is to choose "good" passwords and to keep changing them frequently.

The most common foolproof way to prevent someone from reading your e-mail is to use software to encrypt it, thus rendering it incomprehensible to anyone without the decoder, or key. And with today's fast computers, the process is so quick that you aren't even aware of the time it takes to perform the translation.



There are two major commercial encryption standards is use: PGP (Pretty Good Privacy) and S/MIME (Secure Multipurpose Internet Mail Extensions). PGP is the widely accepted tool. Like a safe-deposit box, it uses two keys - one private and one public - only its keys are complex electronic passwords.

To read a PGP-encrypted message, you need both keys. Private keys or passwords should never be divulged. Public keys, however, which are distributed to all potential e-mail recipients, can be distributed through e-mail, posted on a website or registered with a digital certificate authority.

It's up to users how widely they want their public keys distributed. Most users distribute their public keys to a limited number of people or register one with a digital certificate authority - a firm that operated such services.

Here's an illustration of how a message is sent with PGP security: 'A' wants to send an e-mail to 'B'. So 'A' encrypts his message using either his private key or B's public key. Upon receipt, 'B' decrypts the message using the opposite key - that is, if the message had been encrypted using A's private key, then 'B' uses A's public key. Conversely, if the message had been encrypted using B's public key, then 'B' would use his private key to decrypt the message.

Some Internet experts claim that as much as 25% of electronic mail is scanned by Internet Service Providers, company e-mail administrators and hackers who have software that lets them sneak a look at Internet mails.

Whether you encrypt with your private key or the recipient's public key depends on the reason for encryption.

For example: If 'A' is concerned about confidentiality- that is, he wants only 'B' to see it- then 'A' encrypts the message with B's public key. However, if A is concerned about authentication- that is, assuring B that he, and not an imposer sent the e-mail- then he encrypts the message with his private key, requiring B to open the e-mail with A's public key.

If both confidentiality and authenticity are desired, then 'A' uses the 'double lock' method, i.e. 'A' encrypts his message with both his private key and B's public key. That way, 'A' knows that only 'B' can open the message and 'B' knows for sure that only 'A' sent the message. PGP is available free to non-commercial users. To download it and for more information, we can visit ww.mcafeesecurity.com/us/products/home.htm. PGP is available in a variety of modes for users of various

In India, Safescrypt, Tata Consultancy Services, National Informatics Centre and MTNL are major Certifying Authorities issuing digital signatures. TCS has tied up with ICAI too.

sizes, ranging from standalone PCs to corporate desktop users.

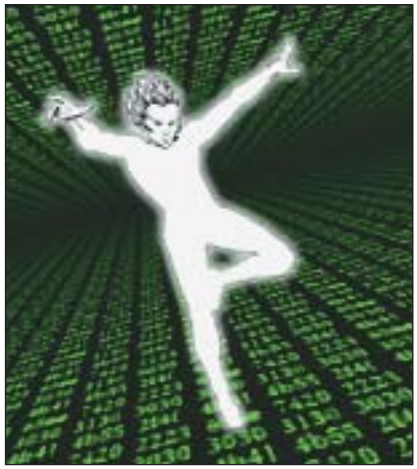
The PGP is relatively easy to install and configure. One advantage of PGP over S/MIME is its acceptance rate. Since PGP is widely used encryption software package, compatibility is hardly ever an issue. Additionally, it can be plugged into the most popular e-mail software applications.

Disadvantage of PGP: If the sender chooses to disseminate the PGP key widely, say, on a website, then there is no way to be sure that an imposter didn't obtain it.

This risk eases if a digital certificate authority is used for user authentication. However, this will of course raise the costs involved.

S/MIME is available free on the Internet and is included in the Netscape Navigator and Microsoft Internet Explorer browser packages. It's available as a plug-in to most e-mail packages.

S/MIME is simple to configure and use - with two major exceptions. S/MIME uses a shorter code for its key, making it easier for a hacker to crack, and S.MIME doesn't rely on public keys; instead it uses third-party authentication relying on digital certificates. These contain the user's name, e-mail address and public key.



As we can see, security is a double-edged sword. While it does provide safety, it also adds to complexity. Like it or not, you can't have one without the other.

Message Tampering

As good as encryption is, it doesn't prevent or detect someone's tampering with the message content during transmission. However, PGP and S/MIME can detect message tampering by using their digital signature features. PGP's digital signature software applies an algorithm (or formula) to the message content that automatically generates a unique code, or digital signature. 'A', who is again sending a message to 'B', appends his private key to the signature and the two are attached to the e-mail. When 'B' receives the e-mail, he first decrypts the digital signature using Bob's pubic key. If signature decryption is successful, he knows the sender is authentic.

Next, 'B' opens the message using A's digital signature and that generates a second algorithm. If the results of both algorithms are the same, 'B' knows the message wasn't tampered with during transmission.

S/MIME digital signatures also apply an algorithm to the message content; the only difference, again, is that the message is "signed" using he digital certificate. 'A' attaches his signature to the e-mail and 'B' compares the digital certificate used to sign the message with that on file, then applies the algorithm and decrypts the message as described above. ■

Get digital signatures from Certifying Authorities

You can buy digital certificates from a third-party digital certificate authority. The IT Act 2000 has authorized the Controller of certifying Authorities (CCA) to issue licenses and regulate the working of Certifying Authorities (CA). The CCA maintains a National Repository of Digital Certificates (NRDC) containing all the certificates issued by the Certifying Authorities in the country.

At present, Safescrypt, Tata Consultancy Services, National Informatics Centre and MTNL are the major Certifying Authorities entrusted with issuing digital signatures. The Tata Consultancy Services has also tied up with the Institute of Chartered Accountants of India. (For more information on Digital Signatures refer an article on page no 402 of the October 2004 issue of *The Chartered Accountant.*