Encryption the key to message security

IN MY OPINION

SATNAM PUREWAL

Secret codes. Enigmatic messages. Undercover officers. Spies. Espionage. Sounds like a Hollywood movie — or does it?

Today's businesses are facing magnified risks. Business information is a valuable commodity.

It needs to be protected at all times — not only at its storage location but also when it is transmitted within an organization or to external parties.

Any business that is concerned with espionage, tampering or confidentiality knows the risks related to information increase with the integration of computers into business.

Almost every business card these days has an e-mail address. Internet e-mail is now one of the preferred methods of communication, but it may be the least safe. It should never be considered secure.

An e-mail goes through many checkpoints before reaching its destination and anywhere along the way it could be read by an unethical system administrator or a hacker.

Always assume that someone other than the intended recipient will be reading your correspondence.

Almost all businesses have local area networks or access to the Internet. When entering user-IDs or passwords on any network, there is a risk that a sniffer (network traffic analyzer) has been installed by an unauthorized individual.

Using this tool, a person may be able to view user-IDs, passwords and any other confidential information being exchanged. Remember that if you are on any network computer, your communications with any other system can be tapped.

This risk is no longer limited to governments or international corporations: it concerns anyone worried about privacy. There are confidential files and databases on most servers, workstations and laptops.

If someone does gain unauthorized access, what will the impact be on the business and its reputation if critical information is read or distributed?

Laptops are stolen from cars, offices, and hotel rooms. Confidential information should not be kept on a laptop if it is not encrypted.

Securing electronic commerce is a huge issue. Many organizations feel that doing business on the Internet is risky, yet more and more businesses are increasing their Internet profile every day.

There is little you cannot buy via the Internet, but for electronic commerce to prosper on the Internet consumer confidence needs to increase.

This can only be achieved through visibly improved security. Consumers want assurance that, when doing business on the Internet, their credit-card liability is limited and their privacy is not affected.

Encrypted communication cannot be easily understood when "sniffed" by network analyzers. Encryption can reduce risks for businesses and individuals, adding a significant layer of security.

Encryption is a way of scrambling or coding information using a secret key and can be decoded only by using a corresponding key.

If you can decrypt the message, you know it was not tampered with and you know the true identity of the sender. With more and more people impersonating others on the Internet (known as "spoofing"), this is becoming an important security feature.

Like many electronic solutions, the impact of whether you need to encrypt all transmitted information must be carefully assessed. The benefits must be weighed against the costs.

The bottom line, however, is that by using well-designed and well-implemented encryption techniques, businesses can secure information travelling beyond the personal computer.

There is no doubt that encryption greatly improves the ability to perform commercial transactions securely.

In my opinion, electronic commerce will only flourish when encryption becomes the accepted standard.

Satnam Purewal, CISSP, is a security consultant for Deloitte & Touche in Vancouver. She can be reached at (604) 640-3080, or by e-mail at spurewal@dttus.com.