by Hugh Long, C.Tech

NETWORK SECURITY SOLUTIONS TO PROTECT YOUR INFORMATION

NETWORK SECURITY CONSISTS OF MEASURES taken to protect information assets from unauthorized disclosure, modification or destruction, either accidental or intentional, or the inability to process that information. Many of you will have your own ideas of what security is, but there is no one answer. The problem is this: network and, fundamentally, information security is a ratio of the benefits derived from a protected system, to the cost of achieving that protection. The difficulty lies in finding a balance.

As the flow of information increases at an unprecedented rate, the risk of information falling into the wrong hands or being corrupted or altered en route also increases. Such information could be proprietary business plans or product designs. Nine years ago, a U.S. Justice Department survey reported that "the average take for today's computer thief is $883,279, compared to only $6,100 for an old-fashioned bank robber". One can only wonder what the average take is today.

First steps in implementing network security

As an organization concerned with the security of your information you may want to:

1. Assess security threats by performing a security audit, then establish a security policy (legally required in the U.S. by the Computer Security Act, 1987).
2. Evaluate risks and costs by performing a qualitative and quantitative risk analysis.

After you have identified and evaluated potential areas of risk, you should be ready to choose methods of implementing various levels of security measures.

Forms of security

Security solutions can be divided into three categories: access rights management, hardware and software solutions.

❑ Access rights management (ARM) can be further divided into physical access control and hierarchical access control. Physical access control is the control of access to actual hardware, typically provided by a locked room or equipment cabinet. Hierarchical access control dictates varying levels of access to system information. For example, the CEO might be granted access to most company files, while the co-op student may only have access to files on his or her own personal computer (PC). ARM also helps mitigate equipment theft and accidental power interruption, etc.

After you have identified and evaluated potential areas of risk, you should be ready to choose methods of implementing various levels of security measures.

❑ Hardware solutions are numerous and range from simple devices like dongles to high-tech encryption systems. Dongles are small devices that plug into the parallel port of a PC or terminal and contain a unique ID code which must be read by the computer prior to granting access. Dongles are most often used to control software circulation. Random key generators are popular. They are used to generate a new key or sequence of characters every 30 to 60 seconds and are kept in sync with the host system. A buffer of four to five keys is kept in case the generator gets slightly out of sync. This key is in effect a password generator and is only about the size of a credit card.

Some companies choose inline encryption systems, at a cost of between $1,500 and $15,000 on average. These are usually used in conjunction with random key generators which help set up the initial stream of communications by providing a common key. After a common key has been established the encryption system encrypts all outgoing data which is decrypted on the recipient's end.

❑ Software security can be divided into access control and file protection. Access control is familiar to many of us as a login sequence. A user enters an identification number and password. This procedure is used as much for accounting purposes as it is for security. File protection can be as simple as adding a password to a file or can entail full file encryption. Many packages such as WordPerfect offer encryption and password protection, but beware, the algorithms used are not usually difficult to break for a serious hacker. For those interested in further reading, a quick search of the world wide web will yield a wealth of publications and interest groups.

References:

- Hendry, M., Practical Computer Network Security. Norwood, MA: Artech House, 1995
- Fites, P., Kratz, M., Information Systems Security. New York, NY: Van Nostrand Reinhold, 1993
- Madron, T., Network Security in the 90s—Issues and solutions for managers. Toronto, Ont: John Wiley & Sons, Inc., 1992

Hugh Long is a Senior Consultant at Cadence Design Systems, Inc. He can be reached at 613-828-5626 or hlong@cadence.ca. Cadence is a supplier of software tools and professional services used to accelerate and manage the design of semi-conductors, and computer systems.