Changing environment: new challenges in network security

Satnam Purewal
purewal@ucs.ubc.ca

"The most secure system is unusable, and the most usable is insecure."

—Paulina Borsook, "Seeking Security," *Byte*, May 1993, p. 119.

Before decentralized computing, mainframe computers and computer files were kept in highly secure areas; computing personnel ensured that the data, files and programs were secure, carefully managed and backed up regularly. Use of business application systems was tightly controlled, with access often only permitted from terminals identified with a particular user and specific location. The basis of UBC's mainframe security was identification and authentication.

As UBC left the eighties, the traditional computing environment based on centralized mainframe computer resources was augmented with powerful computer systems administered within individual faculties and departments. Many UBC units have set up their own departmental Local Area Networks (LANs) where computers are connected to each other and to the greater "network of networks" called the Internet. The power of some desktop computers now greatly exceeds what was available only on very large mainframes a few years ago.

The recent phenomenon of distributed databases and applications has introduced a multitude of new challenges in the area of computer security. The UBC Integrated Human Resources Information System (commonly referred to as IHRIS) is an example of distributed technology.

Risks

Today, computers containing valuable and sensitive data are located in easily accessible labs and offices. These computers may be part of departmental LANs that share a transmission medium (wiring). These LANs typically use Ethernet for communication. Because of the nature of how information is broadcast using Ethernet, it is possible for unscrupulous, unauthorized people to monitor data passing over Ethernet cabling or have their machine appear to be a different machine on the network. While it is not easy to do this, if it does occur, it could compromise the security of information or disrupt services.

A LAN presents all the problems and vulnerabilities of its component systems. Connections to other networks increase the physical risks and introduce more subtle, and possibly more dangerous, threats. Separate networks can be totally secure by themselves, but compromise each other when connected to mainframes or other networks. Interconnectivity introduces the potential risk of "break-in" from users physically located at points far distant from UBC.

Analogous to the opportunistic burglar who cruises the neighborhood looking for open windows and doors, an unscrupulous person with access to the Internet can check hundreds of machines for vulnerabilities in a few hours.

(continued next page)

Terms

Ethernet: A protocol for local area networking, originally developed by DEC, Intel and Xerox, later adopted by IEEE as the 802.3 Ethernet standard.

Gateway: Connection of a workstation to a network or system other than an in-house mainframe. This can be to a LAN, a minicomputer, a public network, etc.

LAN (Local Area Network): A LAN is a group of personal computers connected for the purpose of sharing resources. These resources can consist of hardware, such as printers or communication ports, and/or software, such as programs or databases. Usually limited to a moderately sized geographic area such as a single office building.

Router: A device that can decide which of several paths network traffic will follow. Routers forward packets from one network to another, based on network-layer information.

Security: Security in information processing systems consists of providing privacy (confidentiality), integrity (reliability), and availability of information. It utilizes combinations of access control, authentication and encryption, and supplements these with backup.

Telnet: Standard Internet terminal emulation protocol.

TN3270: Terminal emulation software that allows a workstation to appear to an IBM host as a 3270 type terminal.

Workstation: Personal computer connected to a LAN by some means. The personal computers on a given LAN need not be compatible in terms of hardware or software (e.g., IBM and Apple systems). Further, in addition to functioning as LAN workstations, they may also be used stand-alone.

Security challenges *(cont.)*

Responsibility

As information processing is more widely distributed, and as network integration with the campus backbone network continues, administrative information becomes more accessible and, therefore, more vulnerable to unauthorized access, modification or deletion. This has resulted in the inevitable shift of responsibility for computer security to individual computer users and the administrators of departmental networks.

Every department that connects to the administrative mainframe, or stores and processes computerized administrative information locally, shares with University Computing Services (UCS) the responsibility for the security of such information on local computers or networks.

UCS makes every effort to ensure the confidentiality, integrity and availability of all administrative information systems stored and processed by UCS, whether on the mainframe, minicomputers, microcomputers or on LAN servers for which UCS has responsibility.

UCS is subject to security audits by Internal Audit for compliance to standard practices. UBC's Office of Internal Audit is kept informed of departmental LAN installations that process administrative information.

It is a UCS objective to implement a security architecture and to recommend standards and guidelines that will ensure the security of the administrative information assets of the university.

Procedure for minimizing risk

The Task Force on Security of Networked Computing Systems (see article, next page) is currently developing, among other things, UBC's requirements for certifying LANs.

Currently, departmental LANs requiring access are granted authorization to secure administrative systems (i.e. Financial Record System, Student Information System, Alumni/Development System, or the Integrated Human Resource Information System) only if the LAN is recognized as trusted according to the following interim set of recommendations developed by Computing and Communications.

A LAN is trusted when the senior official of the unit owning the LAN (i.e. the dean, department head, director or their designate) signs a Trusted LAN Certification Form thereby taking responsibility that the LAN meets the conditions listed below. It is the senior official's responsibility to ensure that the LAN retains its status as trusted on an ongoing basis.

1. Only registered users who are authorized by the dean, department head or their designate have access to trusted LANs. Each LAN user has signed a Conditions of Use document which is supplied by UCS.
2. A LAN administrator has been appointed by the dean, department head or designate, for each trusted LAN. This person's responsibilities include ensuring that changes to the LAN structure do not compromise network security.
3. The LAN has been implemented as a separate subnet isolated by a router port. Ports on the trusted LAN are not in a public place and will not be left unattended. LAN ports for public use must be on a separate subnet attached to a separate router port.
4. The LANs should be constructed using twisted pair wiring hubs. The hubs must be placed in locked wiring closets. LANs of alternate construction may also be certified, provided the LAN communication medium can be shown to be invulnerable to unauthorized tap.

Consulting services are available from Computing and Communications if assistance is required in assessing security risks of computer networks and implementing appropriate procedures to manage those risks.

For more information or to apply for trusted LAN status, please contact Satnam Purewal at 822-4820 (e-mail **purewal@ucs.ubc.ca**).❑