M.I.T. Laboratory for Computer Science

Request for Comments No. 244
March 24, 1983

Examples from IBM of Policy requirements for inter-corporate network interconnection

by Deborah L. Estrin

This document describes measures taken by IBM to define and implement security requirements on connections between IBM's internal network, VNET, and networks belonging to other organizations. In the first case described below IBM Corporate Security and the IBM users and developers of the interconnection formally defined policy requirements for the gateway design and operation. The second case exemplifies an earlier stage of development in which neither IBM users nor Corporate Security have formalized detailed policy requirements.

1. VNET-BITNET connection

IBM is in the process of implementing a connection between the IBM VNET and a network called BITNET which connects university computing-center computers (primarily IBM machines) throughout the country [1]. IBM-owned computers have been attached to BITNET in the past in connection with joint studies or sponsored research projects, but this project is attempting to implement a controlled connection between the IBM internal *network* and BITNET, not just between an isolated IBM machine and BITNET. The IBM network, VNET, currently connects several hundred nodes world wide.

Initially the connection will support mail and file transfer; in the future IBM may also support remote login. In conjunction with this project corporate security has specified a number of interesting requirements for the connection, some of which are likely to apply to any M.I.T.-IBM connection as well.

The structure of the VNET-BITNET connection is as follows:

~ A *virtual circuit database* in the *BITGATE* (VNET-BITNET gateway) completely specifies which communication functions will be supported between a particular IBM user or host and an outside, i.e., BITNET, user; for example, whether communication will be restricted to mail, or whether file-transfer will also be accommodated.

~ The IBM users, or their system managers, will initialize the BITGATE database. BITNET users will not have control over the specifications entered into the data base on the IBM side except for the ability to accept, reject, or revoke a connection. After an IBM user has specified a communication channel with a BITNET user and the BITNET user has accepted the specification, the BITNET user can initiate sessions (e.g., send mail or transfer files) with that particular IBM user at will, but not necessarily with any other IBM user, and only according to the limitations specified by the IBM user at initialization. The design of this gateway is inherently asymmetric.

~ The BITGATE will log file transfers, including size and user identification; IBM desires the logged information primarily for utilization statistics.

~ IBM's official policy is that it has no interest in looking inside message or file contents.

~ Although gateways or relays exist between BITNET and Usenet and CSNET, it is unclear as to whether or how forwarding will be handled from these 3 networks onto VNET, via BITNET.

~ The BITGATE will permit unrestricted communication between IBM users and all BITNET file-servers without need for prior channel initialization so long as the IBM gateway recognizes the file server as a service machine.

The BITNET operators and IBM agreed that the asymmetry of the BITGATE design met the policy requirements of both organizations. We expect that this solution is not applicable to some interconnection arrangements for which such asymmetry would not meet the needs of both organizations. As part of our inter-organizational networking studies we will investigate more flexible alternatives to this interconnection design.

2. IBM-CSNET

VNET is also connected to CSNET via a computer at the IBM San Jose research laboratories [2]. The CSNET link is a very restricted gateway to VNET; only a few VNET nodes are accessible at this time and VNET management requires individual registration of each user of the link.

A list of "valid" internal IBM users is maintained on the IBM San Jose relay to filter incoming and outgoing traffic. The San Jose relay will forward incoming mail from CSNET to an IBM user if and only if that user's name is on this list; similarly, the relay will forward mail onto CSNET that is generated by an IBM user if and only if that user's name is on the list. As with the BITNET connection, all transactions are logged, but unlike the BITNET connection, there is no restriction as to which CSNET users can be communicated with.

References

[1]

Fuchs, I.
BITNET -- Because it's time.
Perspectives In Computing 2(2), April, 1982.

[2]

Landweber, L., Solomon, M.
Use of Multiple Networks in CSNET.
In *Compcon.* IEEE Computer Society, Spring 1982.