M.I.T. Laboratory for Computer Science

Request for Comments No. 243
March 24, 1983

Preliminary plans for the M.I.T.-IBM network interconnection project

by Deborah L. Estrin

The objective of this project is to establish a communication link between an M.I.T. local network and an IBM local network that will accommodate experiments with internetwork access-control mechanisms. Such access control mechanisms are needed to support a variety of policy requirements for the inter-organizational network connection.

Neither organization, M.I.T. nor IBM, should be expected to fully specify its policy requirements a priori; nor will these requirements remain static over time. Therefore, in the initial phase of this project we will equip the connection with a basic set of mechanisms, such as authentication, encryption, access checking, and format conversion, and with only limited application-level function, for example mail transfer. After we have successfully implemented this simple, mail-forwarding connection, and have formulated additional policy requirements and control mechanisms, we will extend the application-level functions to include, for example, file transfer and remote login.

1. System Description

1.1. Packet transfer

The IBM and M.I.T. local networks will communicate with one another using the Arpanet Internet Protocol (IP) [6]. M.I.T. and many other academic and government institutions currently use this protocol within their internal networks. Packets from IBM will enter the M.I.T. network via a dedicated port on one of M.I.T.'s multi-protocol gateways. This particular gateway is used primarily for connecting personal computers to the M.I.T. local network; for this reason it is referred to as the PC-gateway[1] [4]. The packets will arrive via a leased telephone line or the public switched telephone network; the former provides a higher level of control and transmission speed while the latter allows sharing of a single port among multiple external sites and is less expensive. A simple, but not yet specified, link-level protocol will be employed on the line between the two half-gateways[2]

The IBM half of the gateway (IBM-hg/w) will consist of an Onyx microcomputer system running Unix version 7. During development and testing, the IBM-hg/w will accept only those packets that are addressed to itself or perhaps to one of the other computers on the IBM local network to which it is connected (i.e., a network located at Cambridge Scientific Center (CSC)). The CSC network is in turn connected to the IBM Corporate Job Network, VNET. After formulation and implementation of suitable access control mechanisms, the IBM-hg/w will also carry message traffic between other IBM sites and M.I.T., via VNET and the CSC network.

IBM will specify the implementation details of the IBM-hg/w, just as M.I.T. will specify the implementation details of its half of the gateway. The decisions made by either organization regarding implementation of its half-gateway should not be of consequence to the the other organization so long as both IBM and M.I.T.: 1) agree upon packet-transfer and mail-format protocols, 2) eventually establish a reliable authentication mechanism, and 3) formulate a satisfactory agreement that insures a commitment on the parts of each party to accept responsibility

---

[1] The PC-g/w is a multi-protocol gateway running "C-Gateway" code on a Digital Equipment Corporation LSI-11.

[2] The link-level protocol will be selected from among the several distinct protocols used within M.I.T. and proposed standards that are used elsewhere.

for the authenticity of packets that exit its network via its half of the gateway[3].

On the M.I.T. side, a Digital Equipment Corporation Vax 11-750 will serve as the site of screening, access checking, format conversion, authentication, etc.; we refer to this machine as the *policy-vax* (see figure). In addition, a lower-level mechanism will authenticate the origin of packet streams incoming to the PC-gateway, before the gateway forwards them to the policy-vax[4]. This mechanism will facilitate sharing of the PC-gateway port among multiple external sites; for example, the PC-g/w may forward traffic from external sites other than IBM to a different policy-screening machine. We will refer to the combined function of the PC-g/w and the policy-vax as the M.I.T. half-gateway (MIT-hg/w).

1.2. Mail Transfer

Once we have established a communications path between the IBM and M.I.T. half-gateways, we will implement a mail-transfer function, including mail-format conversion, authentication, access checking, and other application-level, policy-control functions.

Because of its widespread use, we will use the Arpanet-standard mail format #822 [7] on the link between the half-gateways. The IBM-hg/w will convert incoming mail traffic, which will arrive in 822 format into IBM, internal, mail format; similarly, the IBM-hg/w will convert outgoing mail from IBM internal into 822 format. Because M.I.T. uses 822 format on its internal networks, it will not have to perform any mail format conversion[5].

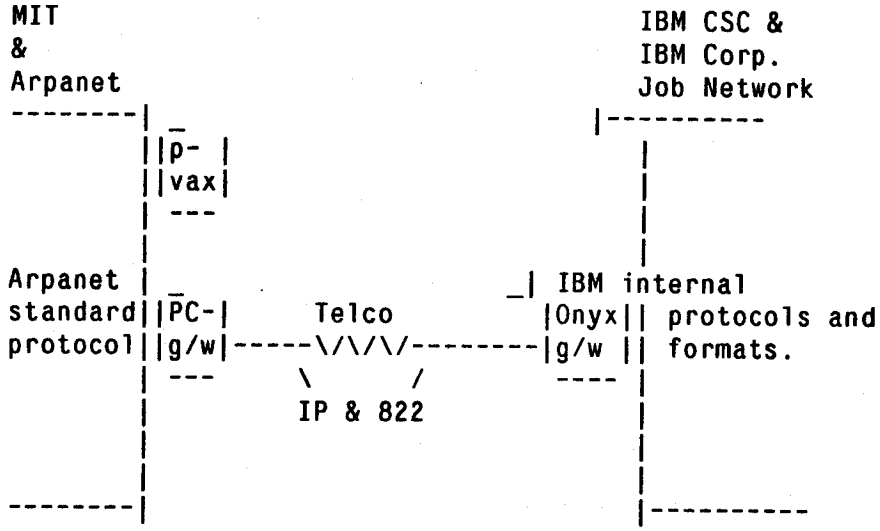
---

[3]The fallibility of the authentication mechanisms make such a commitment necessary. In the commercial and university environments, unlike the military environment, it is acceptable and appropriate to make compromises in the robustness (and proportional cost) of security mechanisms in the presence of contractual agreements.

[4]This link-level, authentication mechanism will be described in a future RFC entitled *Control of telephone line connections to the M.I.T. IP Network.*

[5]In the scenario described above conversion need only take place on the IBM side of the connection because the half-gateways use the same protocols to communicate with one another as are used within M.I.T.. We view this as a non-standard case. A more typical scenario is for both of two interconnecting organizations to convert their internal mail-format into a third format used expressly for communicating between networks, i.e., not necessarily a format used internally by either one of the organizations involved. This scenario allows an organization to implement a single format conversion facility for communication with multiple organizations, provided a standard can be agreed upon; it also avoids the need for either organization to learn the details of the other's internal mail format. In other words, the burden of protocol and format conversion typically would be symmetrical between interconnecting organizations since the inter-network format would be different from the internal formats of either organization.

Figure 1: M.I.T.-IBM local network interconnection



Both the M.I.T. and IBM half-gateways will implement address translation. The M.I.T. policy-vax will translate the indicated recipient's address from that specified by an IBM message originator into the appropriate *user@host* form. Similarly, the IBM-hg/w will translate the address specified by an M.I.T. message originator into the IBM-internal *user host* form. The half-gateways must translate *reply-to* fields of incoming messages into a form compatible with the network to which the incoming message is being delivered (so that any subsequent reply message will be able to find its way back to the network's half-gateway for forwarding).

The half-gateways will use one of two Arpanet protocols for mail transfer, Trivial File Transfer Protocol (TFTP) [12] or Simple Mail Transfer Protocol (SMTP) [9]. TFTP runs on top of a datagram protocol and is somewhat simpler than SMTP which runs on top of a virtual circuit protocol[6]. On the other hand, SMTP provides desirable structures for mail applications that are not provided by TFTP, i.e., special text fields for mail headers. The MIT-hg/w will send mail files into a *public directory* in the IBM-hg/w; by public we mean writable but not readable from external devices. Similarly, the policy-vax will have a public directory for deposit of mail from external sites[7]. The mail file structure will allow differentiation of header and message-contents text.

Both the IBM-hg/w and the M.I.T. policy-vax will encrypt all outgoing mail headers and decrypt all incoming mail headers that are deposited into their respective public directories. The mail will be encrypted using DES; M.I.T. and IBM will establish an off-line protocol for exchanging a number of DES keys, i.e., a floppy-disk-full, for use over the course of a specified period of time, in a specified order. The encryption will serve to protect the contents of the messages from eavesdroppers as it travels between the M.I.T. and IBM networks and, more importantly, it will serve to authenticate the origin of the mail. That is, if the decrypted headers in the M.I.T. policy-vax public directory are intelligible, other than garbage, then the policy-vax will assume that the source of the message contents was the IBM-hg/w, where the DES keys are located; if the messages were put in the public directory by someone other than the IBM-hg/w then the decrypted headers should be unintelligible to the policy-vax, unless the illegitimate party obtained a copy of the DES

---

[6]The datagram protocol is UDP/IP [13]; the virtual circuit protocol is TCP/IP [10].

[7]This is similar to the mechanism used by UUCP based mail communications. The difference lies in the manner in which the public directory contents are filtered, authenticated, etc., before being forwarded to internal users; and in the use of encryption in place of login for authentication.

key currently in use. The Authentication Server Protocol proposed in [8] can be adapted to support this application.

Once a half-gateway has decrypted the mail headers located in its public directory it is free to apply whatever screening or access checking mechanisms it's governing organization, i.e., M.I.T. or IBM, sees fit. For example, on the M.I.T. side, a simple table-lookup of the *to* and *from* fields of the mail header may be used in the early stages of implementation; our study of policy requirements and control mechanisms will provide us with more sophisticated and flexible mechanisms for subsequent stages of this project.

1.3. Future developments

Once we have implemented a basic mail-transfer function between IBM and M.I.T. and we have begun conducting experiments with various access controls, we intend to extend the application-level functions to accommodate: communication between definable subsets of non-CSC, IBM users and non-M.I.T., Arpanet users; additional application-level functions such as file transfer and remote login; and communication between M.I.T. and IBM and other external sites.

In order to extend communication with IBM users to non-M.I.T. Arpanet users, M.I.T. must formulate adequate policy control mechanisms which will allow M.I.T and the Arpanet policy-makers to specify the extent of external access to Arpanet facilities. Similarly, IBM corporate security must review and evaluate its gateway control mechanisms before allowing incoming, external traffic to travel beyond the CSC onto VNET. A primary objective of this study is to investigate the effects of this sort of extension on policy control requirements and mechanisms[8].

We plan to implement additional higher-level protocols such as file transfer (Internet protocol FTP [2]), and remote login (Internet protocol Telnet [11]). More importantly, we will study the policy control requirements for these modes and formulate appropriate access control mechanisms.

If M.I.T. and IBM connect their half-gateways via the public switched telephone network, as opposed to a dedicated leased line, both organizations will be able to accommodate interconnection

---

[8] IBM has already formulated specifications for access control mechanisms in conjunction with interconnection of BITNET [3] and VNET; we hope to contribute to and make use of any relevant developments [1].

with other organizations via these same half-gateways, assuming compatible communication protocols are used. In addition, either organization can use these same facilities to apply security checks to geographically-external, dial-up users, who may or may not be members of the either organization. But, whereas with a dedicated, leased-line connection M.I.T. identified packets originating from IBM based solely on the *from* field of the packet header, with the increase in the number of external parties that will have access to the gateway facilities, and the increase in the communication modes possible, M.I.T., and most probably IBM, will require more robust and flexible identification and authentication mechanisms.

2. Implementation plan

1. Implement IP protocol on IBM-hg/w. The M.I.T.-developed code which runs under UNIX version 6 will be adapted to run on the Onyx under Unix version 7, but will require slight modification of Unix operating system code. In addition, more extensive modification may be needed to adapt the M.I.T. code to the relatively low-speed telephone interface being used for the Onyx gateway, as compared to the high-speed network interface for which the M.I.T. code was written. Select and implement link-level protocol for use between half-gateways. (At this stage M.I.T. will not implement access controls in the PC-g/w, so as to simplify the task of testing the IP implementation.) (Spring 1983)

2. Implement the mail transfer application, encryption scheme, and simple Identification Server on the policy-vax[9]. (Summer 1983)

3. Implement link-level authentication function, e.g., modify PC-g/w to only accept those stream-initiating packets, from the IBM port, that are addressed to the policy-vax. (Summer 1983)

4. Implement mail-format conversion routines and mail-transfer functions on the IBM-hg/w and test mail transfer between the IBM-hg/w and the M.I.T. policy-vax. (Summer 1983)

5. Accept mail from and forward mail to other authorized M.I.T. sites and users, according to filtering-policy controls implemented on the policy-vax. Similarly, connect the IBM-hg/w to the IBM VNET and accept and forward mail from and to other IBM sites in accordance with IBM's policies. (Summer 1983)

---

[9] We will do the necessary programming in "C" because of its transportability.

6. Formulate and Implement access control mechanisms for non-M.I.T. and non-CSC users. Extend communication facilities to non-M.I.T., Arpanet users and non-CSC, IBM users, as deemed appropriate by the organizations involved, i.e., IBM, M.I.T., DCA. (Fall 1983)

7. Experiment with and implement access control mechanisms that are appropriate for extended application-level functions, i.e., file transfer and remote login. (Winter 1984)

References

[1]

Estrin, D.
Examples from IBM of Policy requirements for inter-corporate network interconnection.
Technical Report RFC-244, M.I.T. Laboratory for Computer Science, Computer Systems, March, 1983.

[2]

Postel, J.
File Transfer Protocol.
Technical Report RFC-765, Defense Advanced Research Projects Agency, June, 1980.

[3]

Fuchs, I.
BITNET -- Because it's time.
Perspectives in Computing 2(2), April, 1982.
This journal is published by IBM

[4]

Gramlich, W.
IBM Networking Progress Report.
Technical Report RFC-225, M.I.T. Laboratory for Computer Science, Computer Systems, May, 1982.

[5]

Information Sciences Institute.
Internet Protocol.
Technical Report RFC-760, Defense Advanced Research Projects Agency, January, 1980.

[6]

Information Sciences Institute, University of Southern California.
DOD Standard Internet Protocol.
Technical Report RFC-760, Defense Advanced Research Projects Agency, January, 1980.

[7]

Crocker, D.
Standard for the Format of ARPA Internet Text Messages.
Technical Report RFC-822, Defense Advanced Research Projects Agency, August, 1982.

[8]

Routhier, S.
Authentication Server Protocol.
Technical Report RFC-240, M.I.T. Laboratory for Computer Science, Computer Systems, February, 1983.

[9]

Postel, J.
Simple Mail Transfer Protocol.
Technical Report RFC-788, Defense Advanced Research Projects Agency, November, 1981.

[10]

Information Sciences Institute.
Transmission Control Protocol.
Technical Report RVC-793, Defense Advanced Research Projects Agency, September, 1981.

[11]

Postel, J.
Telnet Protocol Specification.
Technical Report RFC-764, Defense Advanced Research Projects Agency, June, 1980.

[12]

Sollins, K.
Trivial File Transfer Protocol.
Technical Report RFC-783, Defense Advanced Research Projects Agency, June, 1981.

[13]

Postel, J.
User Datagram Protocol.
Technical Report RFC768, Defense Advanced Research Projects Agency, August, 1980.