

IP Security

"Safe sets" for the local stations

Tue, Jun 30, 1992

Introduction

With the addition of IP support for the local stations, the issue of protection from unexpected settings takes on a new dimension. The Internet is a world-wide network; thus it is possible to access the local stations from anywhere on earth. While reading access presents no problem at this time, setting access is not desired. This note discusses a means of restricting setting access to the local stations while allowing unrestricted reading access.

Router blocking

One means of protection would deny IP datagram routing to any local station from outside Fermilab. This would certainly provide protection, but it also denies reading access, since Internet Protocol has no concept of a setting message as we use it in accelerator control. Only higher level layers of the control system protocols recognize the distinction between a request for data and a setting to a device. Use of a router-based scheme may also be inflexible and difficult to maintain.

Trusted host solution

In unix systems, there is a file called `"/etc/hosts.equiv"` that contains a list of nodes that are "trusted" to perform operations that may be denied to other hosts. In the same spirit, the local stations may keep a table of trusted hosts that would be allowed setting access to devices. As the total number of hosts may be large, it may be more convenient to allow access by subnetworks to reduce the size of the table and the processing required to interpret it. A table entry may look like this:

host/net IP address	mask
---------------------	------

When a setting is to be performed in response to an IP-based network message in any of the three device protocols (Classic, D0, Accelerator), the entries in this table are scanned. For each nonzero entry, the source IP address (from the IP header of the setting message) is EOR'd with the host/IP address field and AND'd with the mask field. In this way, entire networks or subnetworks can be represented by a single table entry. Setting access by individual hosts can also be accommodated using a mask of all ones.

Diagnostics

The implementation of setting limitations may provide a chance to include diagnostic information as well. Counts of the number of settings accepted via IP-based access can be kept for the three device protocols supported: Classic, D0 and Accelerator. In addition, the IP source address used by the last such setting and the time-of-day could also be included. Since this is a security issue, one could also keep the last IP address from which a setting was denied, along with the time-of-day that it was attempted. A 64-byte entry for this info:

host/net IP address	mask
—	count-classic
count-D0	count-accelerator
listype #bytes node#	ident-channel/address
data (up to 4 bytes)	IP address accepted
time-of-day of last setting accepted	
count	IP address denied
time-of-day of last setting denied	

Table maintenance

Using the above data structure, it is obvious that only the first two fields are static; the rest are dynamic. It is likely that many local stations will have the same table (static part). This stems from the fact that network access to one local station has always given access to any other. As we download local applications, we can also download the static part of this table. To maintain it and be able to edit the table requires access to the appropriate software development tools such as MPW. Making a change would require the same effort as changing a local application program. The HELPLOOP "text file," providing the prompt text for configuring parameters of local applications, was implemented in this way, although it was installed in only one station, accessible from the rest. Use of group addressing makes it easy to update the table in, for example, all Linac stations at once.