AIIM

Association for Information and Image Management

1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910
301/587-8202

Centimeter

Inches

MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

1 of 1

SAND94-1213C
Conf-9404145--1

Policies for Implementing Network Firewalls

C. Douglas Brown
Sandia National Laboratories
Albuquerque, New Mexico 87185

Corporate networks are frequently protected by "firewalls" or gateway systems that control access to/from other networks, e.g., the Internet, in order to reduce the network's vulnerability to hackers and other unauthorized access. Firewalls typically limit access to particular network nodes and application protocols, and they often perform special authentication and authorization functions.

One of the difficult issues associated with network firewalls is determining which applications should be permitted through the firewall. For example, many networks permit the exchange of electronic mail with the outside but do not permit file access to be initiated by outside users, as this might allow outside users to access sensitive data or to surreptitiously modify data or programs (e.g., to install Trojan Horse software). However, if access through firewalls is severely restricted, legitimate network users may find it difficult or impossible to collaborate with outside users and to share data. Some of the most serious issues regarding firewalls involve setting policies for firewalls with the goal of achieving an acceptable balance between the need for greater functionality and the associated risks.

Two common firewall implementation techniques, screening routers and application gateways, are discussed below, followed by some common policies implemented by network firewalls.

Screening Routers versus Application Gateways

Firewalls are typically implemented using either a screening router, an application gateway, or a combination of the two. A screening router must be capable of filtering by application; however, this is only possible if the protocol contains a field that uniquely identifies the application. This technique works well with many TCP applications, with which a single TCP port number is associated, but does not work well when application protocol identifiers are dynamically assigned, as is the case with Novell IPX. It is relatively easy for a knowledgeable user on the inside of the firewall to use a TCP port number for an application other than the one for which it was intended; hence, the use of a screening router assumes that users on the inside comply with the network protocol conventions.

An application gateway provides a more robust mechanism for implementing a firewall. In this case, each application protocol must be run on the gateway. Inside users cannot redefine application protocol numbers to implement additional services, since the gateway is processing each of the application protocol messages; hence it is difficult for even an insider to circumvent the firewall protection. Since an application gateway must process each message up through the application protocol, it generally has lower performance than a screening router.

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.

Limiting Access to Specific Network Nodes

The simplest type of firewall can be implemented by a screening router, which uses access control lists to filter packets and allows only specified nodes to communicate. For example, nodes outside the firewall might be permitted to communicate with only one node inside the firewall; that node could be configured to support only certain network applications and could implement robust security mechanisms to protect itself from attack. Other systems inside the firewall would not directly accessible from the outside and would not require the same degree of protection. This simple mechanism provides significant network protection at relatively low cost.

Limiting Access to Specific Network Applications

Most firewalls permit only a few specified network applications to be utilized between systems inside the firewall and those on the outside. Some of the more common application protocols are listed below, along with an discussion of the security concerns associated with each.

- Electronic mail is frequently permitted through firewalls, because in theory it provides limited capabilities--data may only be deposited in a predefined mail file or directory and may not be retrieved. (Of course, the "little extras" provided by the UNIX Sendmail program have been the source of many breakins.)
- File access is one of the capabilities that is not often permitted through firewalls, as it gives an outsider the potential for reading or modifying sensitive data on a corporation's internal network. In some cases, users may be permitted to initiate file transfers from inside the firewall but not from the outside (see discussion below).
- Information services, e.g., gopher, WAIS, and Mosaic, are frequently used to make data publicly available to users on the Internet. Anonymous FTP and NFS used with public read-only data sets provide a similar capability, albeit in a less sophisticated manner. When used to desiminate non-sensitive data to the public, these utilities pose little risk and provide a valuable service.
- Interactive login and remote shell capabilities provide opportunities for outsiders to attack a system in an unrestricted manner; hence, these services pose the highest risk. When permitted through a firewall, these services require robust authentication mechanisms to prevent access by unauthorized users.

Initiation of Services from the Inside Only

Another useful policy is to permit users inside the firewall to access services on the outside but to permit limited access, if any at all, from outside users. In some cases this policy can be enforced by a screening router, but it only works if the application protocol is well-behaved. Many routers can permit or deny connections in a particular direction on specified TCP ports. If the service uses a single well-known port, a screening router can selectively permit the service. On the other hand, if the service uses multiple ports and requires connections in both directions, it may not be possible for a router to permit the service without allowing other unwanted services. An example of this latter type of service is the FTP protocol, in which the client makes the initial connection to the server on a well-known port, but file transfers are initiated by the server on random non-privileged TCP ports (above 1023). Permitting outbound FTP through a firewall requires enabling inbound connections on ports above 1023.

Requiring robust user authentication

When permitting application services through a firewall that provide significant possibilities for attacks from the outside (e.g., interactive login), it is recommended that a robust user authentication mechanism, such as smartcards or Kerberos, be employed. As recent Internet attacks have shown, it is possible for attackers to install network sniffers on one network and capture passwords being used to access another network. Smartcards address this threat by generating a constantly changing password, e.g., a pseudo-random number sequence, that is valid for only a short time. Kerberos accomplishes the same thing by including a time-stamp in its DES-encrypted "ticket". Other similarly robust authentication techniques have been developed or are under development, and all provide a considerable improvement in security over clear-text passwords.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DATE
FILMED
6/14/94

END