Limitations of the Approach of Solving a Network's Security Problems with a Firewall

Stefano Zatti, *European Space Agency, ESRIN, Frascati, Italy* (Chair)
Refik Molva, *Ecole EURECOM, Sophia Antipolis, France*
Angelo Tosi, *Price Waterhouse, Zurich, Switzerland*
Gene Tsudik, *Information Sciences Institute, Marina Del Rey, CA USA*
Helmut Kurth, *IABG Munich, Germany*

Abstract

The panel discussion will focus on current usage of firewalls, user expectations, and limitations of today's approach. It will then look into future evolution and possible enhancements of the solutions currently available on the market, that are desirable to strengthen the security of the installations to be protected.

The following topics are likely to be topics of discussion:

- Common uses and configurations of firewalls today
- Firewalls and Beyond
- Common use of firewalls in today's networks
- Limitations of firewalls in today's networks
- Requirements for enhancements to the firewall technology.
- Firewalls and emerging services: WWW, hot Java, Electronic Commerce
- Firewalls and high speed networking: End-to-end argument, ATM, etc.

Introduction

Firewalls are being touted as the ironclad solution for establishing outposts on the Internet and effectively controlling the flow of network traffic crossing administrative network boundaries.

While well-designed firewalls can be successfully deployed for the purpose of tunnelling (securing traffic flowing between a pair firewalls) and controlling in- and out-bound access, there remain some limitations. One of the most notable is the inability of authenticating the origin and contents of incoming traffic whenever this traffic does not originates behind a peer firewall. In other words, firewalls can be fooled by counterfeiting the callers' information.

As an example, consider a Telnet session originating within a private network. The outbound half of the session can be effectively secured and controlled. However, unless the external destination is also protected by a (trusted) peer firewall, the inbound half of the session is fair game for intruders.

It appears -- at least initially -- that the above-illustrated problem is unsolvable...

What's new about new technologies like ATM with respect to firewalls ?

Two points for discussion:

- The possibility to improve security: full fledged, application-level access control can be implemented by integrating security functions into the network control structures of new technologies, like the signalling protocols of ATM. The security functions thus obtained ca be cryptographically strong, contrary to today's packet filters.

- Inherent limitations and new exposures: because of the current trend in high speed networking, the protocols at the network level get leaner and security checks performed "on the fly" become incompatible with the network protocols and the speed requirements. The only possible placement for authentication and access control functions is out of band as part of the network control system. Apart from this limitation, virtual networking functions brought by the new technologies like ATM create new exposures mostly because the physical separations typical of classical network technologies do not exist in the virtual implementations using the new technologies. The best example of this problem is LAN-emulation over ATM, that completely lacks the physical separation of real LANs interconnected by a network-level router. Thus a firewall enforcing access control on the LAN protocols cannot prevent a terminal of a virtual LAN from establishing an unauthorized connection by using the lower level ATM protocols.

Users' view of firewall technologies

- What are the main characteristics of today's market of computer and network security? Firewalls in the framework of a company's security strategy: why does a company need security? Which resources do need what kind of protection, and how can a company choose the most appropriate security level?
- Different users - employees as well as customers - need access to different resources: e.g. marketing people need to promote the company's products to customers; sales representatives need remote access to specific, often sensitive product information. How can network security satisfy all these needs.
- Technical and organizational problems experienced by companies in using firewalls (e.g. configuration management, user interface, human resources planning).
- Problems in using firewalls to secure an already existing network infrastructure.
- How can a company profit of emerging Internet services (Electronic Commerce, WWW advertising, etc.) while controlling its exposure to security risks? User requirements to future firewall technology.