Payoff

Large organizations must be able to communicate with external suppliers, partners, and customers. Implementation of bidirectional E-mail and file transfers, however, may pose a significant security threat to the organization's internal systems. This article describes a network architecture for securing external communications that has been successfully implemented at Lockheed Missiles and Space Co. This architecture employs security mechanisms, referred to as a firewall, which protects internal trusted systems from external networks. The firewall model is supported by a thorough set of technical and administrative support policies and procedures.

Introduction

Today more than ever before, computer and network security officers are expected to accommodate external network connectivity requirements to optimize the company's competitive edge, reduce networking and computing costs, and enhance productivity. In addition, it is assumed that multivendor network environments will support integrated security solutions and protection and control mechanisms across the enterprise. It is particularly challenging because vendor-provided integrated security and network control solutions are not available today.

Security officers and network and systems support personnel more often than not must implement internally developed and maintained code to enhance vendor products while integrating additional hardware and software control mechanisms. The result, which may offer enhanced security controls and allow increased external connectivity, is often cumbersome to administer, introduces additional risk to the system, and is difficult to troubleshoot and maintain.

This article presents an external network policy and architecture developed at Lockheed Missiles and Space Co., which allows worldwide connectivity through external networking and Internet communications. It describes an architecture that establishes generic concepts and rule sets that facilitate the management of external network connections. This policy is designed to accommodate growth and change in technology as well as new requirements for connectivity and network capability. It is cost-effective in its use of inexpensive communications methods and maintains consistency with the company's overall computer and network security architecture. Finally, the policy supports a layered security software control architecture that promotes uniformity and flexibility across networks, computer systems, and applications.

External Connectivity Requirements

As is the case with most government contractors, Lockheed must be able to communicate with external contract and proposal team partners. Connections often involve companies who are competitors on one contract or proposal effort and teaming partners on others. More often than not, these network connections require the ability to communicate over bidirectional E-mail and bidirectional file transfer and the establishment of interactive sessions from outside the company network.

The requirement is further complicated by the need to isolate the project or proposal network from each individual company's internal network. The communications and networking requirements are frequently heterogeneous in nature, and in most cases, the customer dictates the hardware, software, and protocols used to establish and support the
system and network connectivity. Because the content of the projects are often very sensitive, a high degree of security, audit, and integrity are required.

In addition to being a manufacturer, Lockheed is also a research and development company. Research scientists and engineers have long requested the ability to use the high-powered capabilities of Internet, the US government’s major research network, from internal company systems and networks. Internet's global network provides access to a vast collection of decentralized networks, bulletin board systems, and communications.

Providing a framework to accommodate these requirements posed a great challenge to both the security and networking departments. The main goals in developing a network policy to meet these requirements were to maintain complete control from within the company, to ensure authentication and identification from all external sources accessing the company's internal network, and to establish a single physically protected and controlled access point. This required a three-tiered approach involving the development and implementation of a computer and network security architecture—a foreign-node firewall model—and a thorough set of technical and administrative support policies and procedures.

The Network Security Architecture

The security architecture is a set of rules governing the implementation, protection, and management of external network connections. The foreign-node firewall model shown in Exhibit 1 provides a graphic representation of the architecture. It is supported through written policies and procedures establishing approval processes, levels of service, and functionality, hardware and software control mechanisms, and integration methods across the enterprise.

Foreign Node Firewall Model

The external network security architecture establishes a firewall to isolate the internal company network from the outside world. The foreign-node firewall model contains three basic elements: an internal company network of trusted and approved systems, the external world, consisting of all non-company controlled networks and systems, and its most secure element, a firewall composed of front-end hardware and software control mechanisms that separate the internal and external systems. It is assumed that any external network is hostile.

The model ultimately places the responsibility for security and the implementation and maintenance of control mechanisms in the hands of the company's own employees. The architecture supports the company's computer and network security policy, which strives to fully exploit technical and communication resources with minimal impact to the business process.

An Internal Partnership of Trusted Systems

To become a player in the trusted network of an internal company, the system or network must be professionally managed. This guarantees auditability and adherence to all corporate and company computer and network security requirements. The security controls must be minimally implemented at the government-defined C2 level. This can be achieved with an access control software product, the internal capabilities of the operating system and its supporting software, or custom-developed software systems. The systems manager must provide the results of a recent risk assessment, which must be conducted every two years according to company policy. If changes to the system, network, or application configuration occur within the two-year period, a new assessment must be completed and the identified exposures or security vulnerabilities corrected.
The system cannot maintain its own inbound dial-up modems unless it adheres to the company policy and product standards for dial-up access control mechanisms. In addition, the system cannot be connected to an external network, except through the firewall managed by the IS and network security group.

Compliance agreements, approvals, and audit records are kept up to date on all interconnected internal computer systems. Qualification and certification of trusted host status is not trivial, nor is the expectation to comply with all of the organization's computer and network security requirements. This process requires a partnership among internal networked company systems to create and open internal computing and network environment. Authorized users are free to navigate throughout this trusted environment without limitation to services and capability. Access to one system increases the potential for attempted access to any or all of the interconnected systems on the internal network.

The Dial-Up Access Control Management System

The foreign node firewall model supports unlimited dial-up access when used in conjunction with a corporate-approved dial-up access control management system using challenge-response technology for user authentication. This provides two of the three established methods of authentication; something the user has (the challenge-response device) and something the user knows (the pin number and log-on ID). The one-time-only password also ensures that passwords will not be captured and reused over the net by someone masquerading as an authorized user.

The dial-up access control management system is also compliant with the government-approved C2-level security rating. It has been configured to duplicate the security control mechanisms and policies implemented on the trusted host systems. It also displays a no-trespassing banner when an attempt is made to connect across the firewall.

The External Network Firewall

The firewall architecture also supports external network connections, including Internet, when used with the dial-up access control management system and a front-end firewall router (as shown in Exhibit 2). The router must support restrictive access control lists (ACLs) to filter out unauthorized addresses and levels of Internet protocol capability (e.g., finger).

Firewall Control Mechanisms

The control methodology relies on Transmission Control Protocol/Internet Protocol (TCP/IP) architecture and its internal addressing and protocol components. The router becomes the external filter, and the dial-up access control management system provides for secure individual authentication through the implementation of smart-card technology using challenge-response devices.

While providing for external network communications outside the firewall, this architecture places some limitations on capability. Electronic mail—Internet's Simple Mail Transfer Protocol (SMTP)—is permitted in both directions. To further safeguard the internal company network, the Internet mail is routed through a mail server functioning as a control node; this process is transparent to the users.

File transfer (using the Internet File Transfer Protocol (FTP)) and remote interactive access (using the Internet Telnet function) are permitted when initiated from within the firewall. These functions are also permitted from outside the firewall, when a challenge-response device is used through an approved dial-up access control management system and router.
Attempts have been made to limit the number of internal company systems with direct Internet access and node authorization. To qualify for approval, a strict security and control criterion must be adhered to and the applicant system must demonstrate that it is a professionally managed mainframe system and compliant with computer and network security requirements. (Specifications are outlined in the company technical and administrative guidelines.) Connections are approved by upper management and the computer and network security group.

Users who reside on systems that are not approved as Internet nodes may make use of Internet mail through the company Internet domain mail server; routing is automatic. To use outbound File Transfer Protocol or Telnet, the user must log on to an authorized Internet node. Although this is somewhat inconvenient, it is necessary to limit entries in the router to guarantee timely throughput and ensure security. Router access controls depend on the TCP/IP client using a TCP/IP source port number greater than 1023 and sending to specific destination ports for various Transmission Control Protocol services.

The use of UNIX REMOTE commands is severely restricted over the Internet and outside the firewall system. Until a secure method can be built internally or purchased from an outside vendor, Lockheed will continue to deny these requests.

Physical Controls

On a case-by-case basis, external full-function network connections are approved. Security controls are implemented by means of an A/B physical network control switch or physical detachment from the internal company network. These connections are limited, periodically reviewed for ongoing connectivity requirements, and closely monitored and audited. In addition, a separate router may be implemented at approved distributed nodes but must be configured and managed by the central computer and network security group.

Audit and Intrusion Detection

Use of audit and intrusion detection mechanisms contributes to the overall security of this architecture. Both the router and the dial-up access control management system provide access and violation records. An internally developed system integrates these records to provide analytical data for use in detecting unauthorized access attempts. Plans include the incorporation of knowledge-based systems to integrate additional network and system access violation functions with an overall enterprisewide audit system. Visualization systems will also be implemented to highlight unauthorized activities in large volumes of audit information.

The dial-up access control management system also has an intrusion detection system built in to monitor access attempts and violations. Acceptable violation thresholds are keyed into the software, and an alarm system pages the dial-up system security administrator when potential intrusion events occur.

The computer and network security group subscribes to Computer Emergency Response Team/Coordination Center (CERT/CC) and Computer Incident Advisory Capability (CIAC), which routinely monitor and publish computer and network security alerts, problems, and fixes. Computer Emergency Response Team warnings are routinely distributed to all network and system managers, and policies and procedures are in place to disconnect from the Internet or any external network in the event of a suspected problem or intrusion. The security group routinely practices system shutdown procedures to disconnect the external network.
Dial-Up Access

Company policy prohibits the use of dial-up access directly into a personal computer or local area network (LAN) unless it is routed through the centrally managed dial-up access control system or implements remote dial-up controls through an approved system. Use of the centrally controlled dial-up access control management system has allowed safe non-TCP/IP LAN-to-LAN connections outside the company network. These connections are limited to bidirectional mail. Following authentication through the dial-up access control management system, the mail is routed to a secure mail server for further filtering on addresses or LAN server serial numbers.

Security Organization and Decision Making

The security architecture cannot be effectively implemented without the continuing support of senior management. To achieve these goals, it is necessary to have the support of an overall corporate computer and network security infrastructure. This infrastructure must be thoroughly understood and supported by all levels of management and personnel. It should be a corporatwide board, coordinated and facilitated at the corporate level with full participation of each subordinate company.

At Lockheed, a computer and network security board is chaired by a manager reporting directly to the corporate chief information officer. Its mission, functions, and responsibilities are defined through the corporation's highest-level policy document. The corporation is organized across lines of business, and each group of its companies forms a subset board. Within these boards, each individual company has its own computer and network security organization with full participation and representation within the overall infrastructure. Chairpersons, representing both the classified and the unclassified areas of network and computer security, attend meetings and facilitate bidirectional and lateral communications to ensure the success of the infrastructure. The board establishes enterprisewide computer and network security policies, approves external network connections, and integrates solutions and standards to support new technologies and communications capabilities.

This structure supports the application of additional or more restrictive data and resource protection requirements. This is an iterative process in which requirements are typically generated from the operating companies at the bottom levels of the organizational structure and solutions and policies are devised and agreed on throughout the organization and ultimately by the board and senior management.

The Risk and Protection Model

The risk and protection model shown in Exhibit 3 supplements the firewall model, providing a framework for risk assessment, design, and implementation of technical control mechanisms and the development of protection policies and procedures. This model was developed in accordance with the philosophy that access controls should be layered, that the smallest percentage of intrusion attempts occur at the external layer, that access control mechanisms should be provided at each layer, and that the greatest potential for loss occurs within the circle or layers. Of particular concern are the protection and control of privilege and the detection of intrusion at all layers.

Risk and Protection Model: Layers of Defense

The risk and protection model is intended to facilitate management and end-user communications and understanding of the overall objectives of the company computer and
network security architecture across the enterprise. It also supports the integration of new technologies and control mechanisms within the framework of the existing architecture.

**Handling Diverse Protocols**

Lockheed supports a heterogeneous computer, network, and communications environment. In addition, specific platforms and products are contractually dictated by the customer. This has evolved to a complex and highly integrated technical environment.

This architecture is based on the TCP/IP protocols. Although TCP/IP is supported as a standard by leading vendors, it is not fully integrated into their proprietary network protocols. This includes Digital Equipment Corp.'s DECnet, IBM Corp.'s System Network Architecture, and Tandem Computer, Inc.'s Expand, all of which are widely used at Lockheed. Many of its contract customers and partners prefer or even mandate the use of these protocols.

The foreign node firewall model is sufficiently flexible to support a diverse set of protocols, as can be demonstrated by examining the implementation of Digital Equipment Corporation Security Gate, a VAX/VMS Decnet product. Exhibit 4 shows how this product can be integrated within the existing firewall model. Digital Equipment Corporation Security Gate, which resides on a VAX workstation, duplicates the function of the TCP/IP foreign node router system. When combined with an approved dial-up access control management system implemented at the VAX/VMS host, it provides for individual authentication using standard and approved challenge-response device. The VAX/VMS system is also physically secured and protected to the same level as the dial-up access control management and the foreign node router system.

**DEC Security Gate**

Communications filtering is provided by node, circuit, date and time, and Decnet object or task. Full audit capabilities are also provided.

Although Lockheed succeeded in integrating external network support for Decnet, this was not true for IBM's System Network Architecture and Tandem's Expand networks. Because the foreign-node firewall architecture relies on the capabilities of TCP/IP, the layered approach must be used for non-TCP/IP network protocols. A layered approach is implemented for both Tandem and IBM through the use of operating system internal software controls, security controls within the software security package, software controls within the network software and session managers, and when available, through the database management system and application-level security controls. External network connectivity for these environments is limited to bidirectional E-mail and data transfer only. Restrictions and controls are provided through the combination of security software controls at the various levels and within each product. An integrated audit system has been implemented to provide for auditing and monitoring across systems, products, and applications.

Exhibit 5 illustrates a Tandem implementation combining the integrated control capabilities of the operating system, network software, security software products, and application level controls. Because Tandem supported only a limited implementation of TCP/IP at the time of this implementation, the firewall router could not be used to filter addresses or limit inbound functions.

**Layered Security in a Tandem Network Environment**
Full-function Tandem-to-Tandem, process-to-process communications were required. A network hardware A/B switch provided full-function Tandem networking capabilities across the foreign node network when the network was fully disconnected from the internal company network. This restriction required coordination and scheduling between external and internal nodes for processing times. The external connection stayed up most of the time for application programming development, and the internal connection was used only intermittently for batch file transfer. (This restricted approach is not feasible when full-function bidirectional network communications are required simultaneously. For additional protection and control, Tandem's Expand network security software supports network passwords, which can be used to control network access, define resources available across the network, and ensure outbound communications only. Tandem's Safeguard security software product supports the use of access control lists to control access to specific resources.

Implementation Issues

Because of the nature of the aerospace and defense business, it was difficult to convince Lockheed's management that it should provide bidirectional external network capabilities and that the technical control mechanisms, audit, and administrative policies and procedures were adequate to maintain the high-level of system and information integrity previously guaranteed by denying external network connections. It has been challenging to maintain trained network and security technicians who understand both the risks and control objectives. Time and effort were needed to automate the installation, maintenance, and audit of the router access control lists. However, once the foreign node firewall architecture was accepted and implemented, the greatest challenge was to accommodate the growing number of access requests in a timely manner and accurately forecast hardware growth requirements.

Conclusion

In summary, the firewall architecture has enabled Lockheed to respond in a timely manner to customer requests for external network connections. It is now possible to communicate in a secure manner with contract partners and external networks and to effectively and simultaneously share and isolate internal networks from external network partners. Lockheed is also able to exploit the worldwide research resources available through the Internet. The approval cycle is also reduced because the firewall model itself was initially approved by all levels of the corporate computer and network security organizations. Additional implementations of the model are approved at the individual company level rather than at a higher corporate level, thereby decreasing the paperwork and authorizations required.

Author Biographies

Lynda L. McGhie

Lynda L. McGhie supervises a group of fifteen programmers, computer and network analysts, and security administrators at Lockheed Missiles and Space Co. in Sunnyvale, CA. McGhie has worked for over twelve years in computing and network security; her current specialization is the development and implementation of security architectures to ensure security integration and integrity across complex, heterogeneous enterprise systems.