IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB12235

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter XIII

The Demilitarized Zone as an Information Protection Network

Jack J. Murphy, EDS and Dexisive Inc., USA

Abstract

This chapter presents some basic concepts for the design, implementation, and management of a network-based enterprise boundary protection mechanism. The reader should not expect to see a complete security solution from the material presented in this chapter. The concepts presented here must be combined with host and application security mechanisms, as well as procedural and administrative mechanisms. The chapter will provide an explanation of some of the security concepts involved before explaining how an information protection network *(IPN) enables collaboration and information exchange between the enterprise and external entities on the public Internet. Finally, specific technologies needed to implement an IPN will be discussed.*

Defense-in-Depth Approach

Information protection requires an in-depth risk-based approach involving network, host, and application security, which together constitute a defense-in-depth approach to information protection. Like armies defending a nation's capital, this approach has multiple layers of defense, beginning with the front line. The *demilitarized zone* (DMZ) for an enterprise corresponds to the front line of a defense-in-depth strategy, providing network-layer security from untrusted networks via an intermediary perimeter network charged with granting or denying external access to hosts and ports within the enterprise network. Hosts on the enterprise network must employ a second line of defense in the event that the network protection mechanisms are defeated or exploited for nefarious purposes while configured to permit access for legitimate use. Finally, applications on host machines protect access to enterprise information and can be thought of as the final layer of defense. Network defense mechanisms protect against attacks directed at network vulnerabilities, while host and application security mechanisms protect against host and application vulnerabilities, respectively.

The network/host/application layers can be configured in complex ways to enhance security. The network layer itself may employ diverse technologies, another dimension of defense-in-depth, to mitigate exploits against a specific technology. For example, *transmission control protocol/internet protocol* (TCP/IP) (Layer 4/3) security mechanisms may be supplemented by *virtual local area network* (VLAN) (Layer 2) security mechanisms. Diverse technologies protecting against a specific threat or vulnerability can be effective. However, redundant technologies could create a false sense of security. The subtle distinction between technological diversity and technological redundancy must be thoughtfully evaluated.

Such an approach requires an analysis of the threats to security, the vulnerabilities that may exist in networks, hosts, and applications used by the enterprise, and the value of information and processing capability to the enterprise or to threat agents outside the enterprise. Risk can be loosely modeled as the product of threat, vulnerability, and value (Risk = threat x vulnerability x value), where threat and vulnerability are real numbers in intervals (0, t) and (0, v) respectively, and value is measured in dollars, also in some interval ($0, $n). Each site must determine the risk (value of the information it is responsible for protecting, the threats, and the vulnerabilities) and the countermeasures required.

Among security professionals there is no universally agreed set of "best practices" for securing the IT components of an enterprise. However, few would argue that, at a minimum, the enterprise should have a written security policy that serves to guide the operation and evolution of the security components of the enterprise IT infrastructure. One approach that has proven successful is to establish a set of core principles. These principles should be universal (widely understood and agreeable), comprehensive (covering a broad collection of threats and vulnerabilities), and fundamental (not subject to or dependant on rapidly changing technologies or threats).

Table 1 identifies four core principles and 19 prescriptive policy statements supporting the core principles. The culture of the enterprise will determine whether this set needs modification. The information protection network referred to in several of these policy statements is the technical security component providing boundary protection. As described in greater detail in the next section, the IPN supports these four core principles.

A comprehensive enterprise security program includes technical mechanisms and operational practices, procedures, and processes. Technical mechanisms include things such as firewalls, intrusion detection, access control lists, and filtering routers. Operational practices, procedures, and processes include things such as security training, independent audits, security policies, and configuration management.