

The SRAD-I Security Layers: A Model for Secure, Rapid Architecture and Design for Infrastructure

By Keith T. Hall
Keith_Hall@sra.com

The Need for a Generalized Security Model

It is possible to argue that an improperly designed and secured enterprise network infrastructure is a primary source of many security incidents. Even if remediation measures are undertaken, many efforts are too high-level, too low-level, too heavily weighted into a single group of security topics. In rapid security architecture and design implementations, it is often a challenge to determine if the security engineering effort was "good enough" to address overall system security amidst the numerous sources of security guidance.

If a simple, clear and concise security model could quickly categorize and describe the various infrastructure-related security functions and interrelationships, then a more balanced security effort is possible. To help address these concerns, this article describes a model similar to the OSI layers of internetworking, but with an enterprise-oriented security focus in mind.

Overview

Figure 1 is broken down into three major sections. The center section comprises the Technical Security layers. The left section in blue forms the Security Operations and Management (O and M) layers and the right section in brown represents the Security Policy and Guidance layers.

Technical Security Layers

There are four network/internetwork layers and four host/node-based layers. The network/internetwork-based layers are the Internetwork, Inter-perimeter, Perimeter, and Interior layers. The four host/node-based layers are the Software Application, Software Operating System, Hardware, and Data-at-Rest layers.

The Network/Internetwork-based Layers

The Internetwork layer represents the backbone interconnectivity that may or may not be under the control of the Enterprise. Only Service Providers owning their own infrastructure will not have this layer as part of their security model. Note that the Internetwork layer represents all infrastructures that are "between networks" and may include Remote Access, Public Switched Telephone Network (PSTN), or other interconnectivity. Although the Enterprise may not exercise control of the Internetwork layer, enforcement measures for the Connection Approval Processes (CAPs), Service-Level Agreements (SLAs), and Interconnection Security Agreements (ISAs) may be appropriate to specify.

The Inter-Perimeter layer describes the security measures between sites, networks, or enclaves as traffic traverses the Internetwork layer. Type I or IPsec encryption devices may be appropriate to specify within this layer.

The Perimeter layer describes the enforcement mechanisms of the site, network or enclave. Typical devices may be Virtual Private Network (VPN) or firewall devices. Perimeters also describe demilitarized zones (DMZs) and mechanisms that determine internal perimeters such as Closed User Groups (CUGs).

The Interior layer defines the security mechanisms present within the system once admitted by the perimeter defense mechanisms. This includes devices such as network-based Intrusion Detection Systems (IDSs), switch-based security mechanisms, and the like.

The Host/Node-based Layers

The Software Application layer describes the security measures taken for all commercial-off-the-shelf (COTS), government-off-the-shelf (GOTS), custom code, mobile code, and freeware/shareware placed within the system. A separate Software Operating System layer captures issues such as patching, version control, and other O/S-related topics. The security measures established for the physical host or node, within or attaching to the infrastructure, are captured in the Hardware layer. Note that both the Hardware and Data-at-Rest layers tie into the physical security aspects of the system. Security measures established for data-at-rest are captured separately from the Hardware layer. This information was separated from Hardware to emphasize the importance of dealing with all forms of data-at-rest coherently as a unit. The Data-at-Rest layer incorporates data-centric security measures. Note that this layer also includes peripherals, removable storage media, or other devices that may be removed from the system infrastructure.

Security Operations and Management (O and M) Layers

There are four basic Security Operations and Management layers: Interfaces, Services (both network and host-based), Alerting and Reporting, and Response. The Security Operations and Management Layers are not intended to describe all possible security O and M functions or the O and M model used, but rather to form a placeholder for the specific linkages between security management and the technical security implementation of the system. The intent is to ensure that the system's O and M interfaces, services, alerting, reporting, and response mechanisms insert basic security functionality for the O and M model selected. The O and M interfaces tie into the technical security layers, to allow the description of secure O and M functions of each layer, if present.

The system implementation provides interfaces from the various technical security layers of the system for either host-based or network-based management services. For example, the perimeter and interior layers may provide Authentication, Authorization, and Accounting (AAA) and various other services to help manage the infrastructure. Host-based services might include Active Directory and other user-facing functions. These services, in turn, provide alerting and reporting information used to trigger a response or initiate another process.

Security Policy and Guidance Layers

There are three Security Policy and Guidance layers that should be addressed: Vendor-Specific, Technical, and Organizational. The intent is to ensure that for each technical security layer, all three guidance and policy sources should be examined for applicability. At the highest levels, all security policy should either directly and indirectly trace back to the organization's mission requirements. For this reason, security policy should never detract from or be inconsistent with organizational mission requirements. Note that government laws, government regulations, organizational security policies, and established security policy standards may all contribute to underlying organizational requirements.

The next policy and guidance layer is the Technical layer. This is where "best practices" and basic security principles implement the organizational security intent. The general technical rules that must be implemented upon vendor-specific hardware and software are also established. For example, "least-privilege" access principles and meta-data tagging requirements are implemented on vendor-specific software to implement the organizational intent to restrict information flows. This layer is also intended to address any gaps in guidance between the organizational and vendor-specific documentation in the other layers.

Fundamentally, the technical implementation of the system is based upon vendor-specific products. For this reason, the bridge from the technical system implementation into security policy should take into account the vendor-specific capabilities and limitations. The Vendor-Specific layer refers to the product-specific, low-level security considerations necessary to implement the higher-level technical security policy and guidance. Examples include the vendor's product usage and employment guidance to ensure the product is properly configured to achieve the intended security result. The vendor may also have developed the hardware or software with established standards, evaluation criteria, or formal certifications that are of security interest.

Mapping to Other Models

SRAD-I is intended to co-exist with or integrate into many architectural and design frameworks. For example, the orange text and arrows represent one possible mapping to the high-level IATF framework to provide additional organization and structure for its various subcomponents.

Similarly, the ITIL framework may integrate with the Security Operations and Management layers to link security into the various service management and customer support functions. SRAD-I provides a placeholder for the host and node security relationship supporting the ITIL

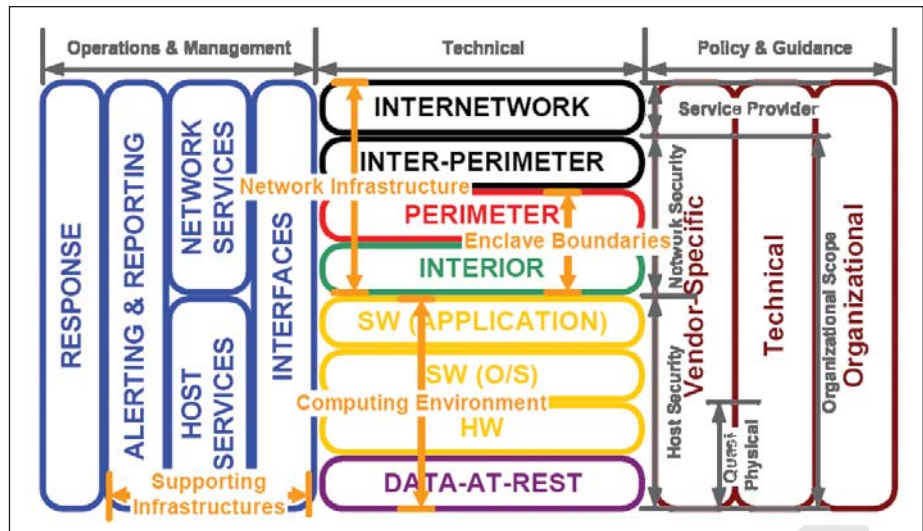


Figure 1: Three Layers of Security

functions and provides a placeholder for the information feeds into those same components.

The SRAD-I Security Layers are also suitable as a Table of Contents (ToC) skeleton for document development or as a Security Engineering framework for an Enterprise Architecture (EA) knowledge management tool. Note that every layer may be further characterized, broken down into detailed subcomponents, or described via low-level guidance. The model is highly flexible and intended to allow the insertion of details as appropriate for the system.

Summary

Although many sources of security guidance, frameworks, models, and techniques exist, a simplified and easy method to address the security layers within a system is still a useful tool. The SRAD-I Security Layer model is intended to provide a quick means of characterizing, classifying, and clarifying, with a tailorable level of detail, the security layers present within many system infrastructures, but without excessive complexity and detail.

Keith T Hall, MBA, BSEE, is a Senior Member of the Professional Staff with SRA International, Inc. He holds current certifications as an INFOSEC Professional (NSTISSI 4011 Std.) and Senior System Manager (CNSSI 4012 Std.), CISSP, CCIP, CCSP, CCDP, CCDA, CCNA, IAM, IEM.