June 21, 2001

Application vs. Infrastructure Security

Randy Heffner

Catalyst

Analyst collaboration regarding application security

Question

What is the difference between application and infrastructure security?

Answer

When defining technical terms, it is helpful to align the boundaries of a domain with the primary concerns of a particular technical audience. This facilitates communication and clarifies responsibilities. For "application security," it is most useful to define the term in a way that it directly addresses the concerns of enterprise application developers. During design and implementation, a developer's primary concern is to ensure that the application allows users to do only what they are allowed to do. Thus, authentication and authorization are the primary concerns, and administration and audit are important secondary concerns — the application developer must specifically design the application to incorporate these four functions. Of course, the application will not be secure without a secure infrastructure, but developers can (for the most part) rely on the infrastructure team to ensure that network-based attacks do not compromise application integrity.

More specifically, Giga's definition for application security includes Web products, such as **Entegrity** AssureAccess, **Entrust** getAccess, **Netegrity** SiteMinder, **Oblix** NetPoint and **Securant** ClearTrust. It would also include mainframe security managers, such as RACF, ACF2 and Top Secret. These products are central to the issues of application-level authentication and authorization.

Giga's definition of infrastructure security includes firewalls, intrusion detection/prevention, vulnerability assessment and virus scanning (e.g., **Axent**, **ISS**, **KaVaDo**, **Kyberpass**, **Network Associates**, **Qiave Technologies**, **Sanctum**, **Whale Communications**, others). All of these technologies are important for a secure application, but they do not directly affect the design of an enterprise application.

On the line between the two, public key infrastructure (e.g., **Baltimore Technologies**, Entrust, **RSA Security**, **VeriSign**, others) falls into the domain of application security when used for application authentication, encryption, nonrepudiation, etc., and falls into the domain of infrastructure security when used for network authentication, etc.

Why does the distinction matter? Confusion is sometimes caused by different definitions of "application." For example, to an infrastructure person, a Web server is an application, but to an application developer, a Web server is infrastructure. The right definition will facilitate communication and clarify expectations between application and infrastructure teams. Clearly defined boundaries provide a relatively clear set of criteria for placing individual security requirements on either side of the boundary, which provides a way to determine which team should address a given security risk (or whether it requires cooperation between the two). Thus, infrastructure architects can communicate clearly what risks their architecture is designed for and application architects can do the same and there will be efficient layering of the concerns between the two.