

From Perimeter Security to Database Security: Protecting the Crown Jewels

By Aaron Newman

A modern-day visitor to the Tower of London will notice that, although the ancient fortress is surrounded by thick stone walls and heavy medieval gates, its most modern and elaborate security system can be found where it counts the most: in the Jewel House, where Britain's priceless crown jewels are kept. Increasingly, security and database professionals are taking a similar approach as they strive to protect their organizations' crown jewels: their data assets. Network security is moving away from protecting the perimeter of the network to protecting data at the source.

The reason for the change is simple: perimeter security no longer works in today's environment. Today, not just employees, but also external partners and customers need access to enterprise data, so databases can no longer simply be hidden behind a firewall. Of course, as databases become more exposed to the Internet, it is imperative that they be properly secured from outside threats and attacks. Securing databases involves not only establishing a strong policy, but also establishing adequate access controls.

But how does an organization go about "protecting data at the source?" First, it is imperative that security and database professionals see through the marketplace confusion, determine the actual risks, and investigate what can be done about the situation.

The truth is that most databases are configured in such a way that they can be broken into relatively easily. However, databases can be properly secured if organizations can only get the information required to do it and take the proper lockdown procedures. They also need to act quickly; the tide has turned in the battle for network security, and by most accounts, the good guys are losing.

Not Your Father's Database

Today, applications and databases are often distributed in geographically-dispersed business units to meet local needs, and are increasingly made available to suppliers, customers and business partners in order to conduct business over the Web. But with this increased access comes increased risk. Many of the new threats take advantage of the fact that today's databases are not mere repositories for information, but robust development environments that allow developers—and intruders—to carry out complex functions within the database.

In one common form of attack, such as a SQL injection, an intruder uses the SQL database-access language to insert malware designed to infiltrate, corrupt or gain illegitimate access to the database. Another common attack is the buffer overflow, in which an authorized user inserts more data into a buffer (temporary storage area) than the buffer was designed to hold. The extra data can corrupt the legitimate data in the

buffer, or in adjoining areas of memory, or contain instructions that allow illegitimate access to information.

Other threats come from application worms, which are automated, self-propagating attacks on the custom code written for many Web applications. Application worms take advantage of publicly available Web indexes to find sites to attack, and to determine how best to attack them.

Examples of application and database attacks are not hard to find. In 2005 alone, more than a dozen breaches have been publicized across a range of corporate, government and educational institutions, affecting more than 1,000,000 consumers. This represents a dramatic leap from the prior year—and there are no signs that the risks are subsiding.

Getting Your Jewel House in Order

Most large organizations have already installed antivirus software, firewalls and even intrusion detection systems to protect their networks and host operating systems. Though these defensive tools do a good job of protecting their servers and networks, they are not designed to detect application-level attacks or to stop such threats before damage is done.

By comparison, enterprise-class applications have received relatively little attention from security personnel on the assumption that they are protected by firewalls and other defenses at the network perimeter. These essential applications and databases — containing the enterprise's most valuable assets—are left largely unprotected. It is as if the Tower of London had all its gates and Yeoman Warders guarding every entrance, but no vault for the crown jewels.

Although a critical component of a layered defense, firewalls cannot detect or stop the new class of threats now being directed at applications and databases. Intrusion detection systems perform only passive monitoring and after-the-fact forensics—they cannot prevent attacks. Indeed, the Gartner Group recently highlighted the limitations of these measures:

"...most organizations have learned that perimeter firewalls, antivirus software, and intrusion detection systems are not enough to protect them from cyber attack. Attacks have moved to the application level, circumventing network-based firewalls. Worms propagate so quickly that signature-based antivirus protection is useless. Intrusion detection systems do not provide protection, only faster notification that your security has failed. The ideal form of protection requires hardened, locked-down server and desktop configurations..."¹

Organizations need to bring the same level of protection to applications and databases that they apply to servers and networks, with solutions that can automatically detect and respond to application-level threats in real time. These solutions also need to be granular enough to permit access to customers and business partners while keeping attackers out.

The Weapons of the New War

For a proven application-layer security framework, look no further than the methodology organizations have already successfully applied at the network and host operating system levels. Just as at the host and the network perimeters, application-aware security solutions must provide vulnerability assessment, real-time intrusion protection and audit, and encryption. To achieve these goals, such application-level tools must provide:


- ▲ **Audit/Proactive Hardening:** The system must audit the status and configuration of all application components and perform security tests and proactive hardening of such components while producing detailed security audit reports before and after application deployment. It must also ensure all current patches have been installed, default passwords have been changed, and recommended security configurations have been implemented. As with the network and host OS, assessing the vulnerability of application components helps an enterprise proactively minimize risk and gauge ongoing compliance with its security policies.
- ▲ **Real-Time Protection:** Given today's rapidly propagating threats and the time needed to deploy patches, organizations require real-time protection to complement the proactive hardening provided by ongoing vulnerability assessments. The growing threat from "zero-day" attacks points up the need for behavioral-based intrusion prevention systems that can detect, and block, application-level attacks for which there is no known signature to scan, nor any patch to apply.
- ▲ **Encryption:** Organizations need the ability to encrypt the most sensitive data as a "last line of defense," even if the database itself is compromised, without incurring the overhead or complexity of encrypting the entire production database. Selective encryption also prevents unauthorized access to data by legitimate users. For example, a database administrator needs administrative access to the application in order to grant, revoke or change users' access rights, but should not be able to see, change or copy the actual information in the database, such as customers' credit card numbers. Any such encryption solution must be transparent to the application components it protects, meaning that the encryption will still function, even as needed changes are made to individual components.
- ▲ **Internal and External Protection:** The system must detect and protect against application or database attacks from inside as well as outside the firewall. Many organizations focus their security attention on attacks from outside the organization and believe that a secure perimeter will eliminate most threats. But Gartner, Inc. estimates that 70 percent of security incidents that cause loss (rather than mere annoyance) to organizations involve insiders.
- ▲ **Multi-Tier Protection:** It is necessary to protect against attacks against any tier of the IT infrastructure, including the Web front-end, the application and middleware, and the back-end database. Intruders are increasingly creating "blended" attacks that might use a port scan to find a way into a Web front-end, a password dictionary attack to gain illegal access to an application, and a SQL injection attack against the database itself.
- ▲ **Enterprise-Class Infrastructure:** The system must have a unified scanning infrastructure that works in a common fashion and provides the same capabilities within each tier of the application

environment. As organizations move towards flexible, service-based IT architectures, applications may run on any number of tiers (or platforms) throughout the enterprise. The number and nature of tiers on which an application depends may change unpredictably as business or technical needs change. Organizations cannot afford to pay skilled personnel to monitor multiple security scanning tools, nor can their networks afford the bandwidth it takes for those scanners to look for threats and report their results. Just as with network and host-level security tools, organizations need scalable, enterprise-class application security tools that can grow to meet their future needs.

- ▲ **Distributed Management/Centralized Reporting:** Organizations need the ability to delegate the responsibility for, and the work involved in, monitoring and managing application and database security across geographies or business units, while providing for centralized reporting of audit results. Modern businesses outsource more work than ever to consultants, contractors, or business partners such as distributors or contract manufacturers. An application-level security system must be flexible enough to delegate responsibility to such outside entities for keeping their portion of shared information systems secure. Even within a single organization, multiple business units, divisions or geographies must cooperate in—and take responsibility for—keeping data secure. At the same time, however, the security infrastructure must provide a single, centralized security audit to provide for centralized accountability and enforcement of security processes.

Summary

Applications and databases form the core of an organization's IT infrastructure. Without the business processes they support and the data they hold, the business cannot function. Yet applications and databases have been disturbingly neglected within the enterprise compared to the security provided for networks and servers.

Organizations that understand the importance of their applications and databases recognize the need for proactive, dynamic tools that can find and stop attacks on applications and databases before they cripple the enterprise. Fortunately, hard-earned experience securing the network provides a ready-made blueprint for an effective approach to securing enterprise applications: vulnerability assessments, real-time intrusion protection and audit, and encryption at the application layer. It's the best to ensure that the crown jewels remain safely in the kingdom for years to come. 

Aaron Newman is Co-Founder and the Chief Technology Officer of Application Security, Inc. (AppSecInc). In his current role, Aaron is responsible for defining the overall AppSecInc product vision. Widely regarded as one of the world's foremost database security experts, Aaron is the co-author of the Oracle Security Handbook, printed by Oracle Press. Visit www.appsecinc.com for more information.

¹ M. Nicolett, J. Pescatore, Gartner Group, "Security Demands Drive Shift to Vulnerability Management" November 2003