THIRD BRIGADE®
deep security solutions

White paper

Web Application Security: The Overlooked Vulnerabilities

Abstract

Are you adequately protecting the web applications that your business depends on?

Software flaws are rapidly becoming the vulnerabilities of choice to attackers determined to exploit mission critical systems. However, it isn't just vulnerabilities in the web applications that organizations need to be concerned about. Vulnerabilities across the entire enterprise application stack—including web and application servers, databases and operating systems—that form the foundation for web applications, also need to be addressed. Publicity around breaches and regulatory pressures are pushing web application security further in the spotlight. Traditional approaches to web application security, including web application firewalls, and web security modules, can be costly and complex, and do not ultimately protect the entire application stack. Host-based intrusion defense with deep packet inspection is a new approach that addresses the need of organizations to shield vulnerabilities across the entire application stack.

Table of Contents

1. Web Applications: An attractive target 1
2. Web applications are increasingly vulnerable 2
3. Regulations and legislation rule the new security agenda 4
4. Selecting a system to protect web applications....................5
5. Your next steps....................8

1. Web Applications: An attractive target

How do you cost effectively defend web applications from attack? Your organization relies on mission critical business applications that contain sensitive information about customers, business processes and corporate data. Moving away from proprietary client/server applications to web applications gives you a simpler, cost-effective, highly extensible delivery platform. These applications are more than a valuable tool to power your business operations; they are also a valuable and vulnerable target for attackers.

Web applications are increasingly the preferred targets of cyber-criminals looking to profit from identity theft, fraud, corporate espionage, and other illegal activities. The impact of an attack can be significant, and include costly and embarrassing service disruptions, down-time, lost productivity, stolen data, regulatory fines, angry users and irate customers. Beyond preserving the corporate brand, federal and state legislation and industry regulations are now requiring web applications to be better protected.

As you take action to protect web applications in a timely and effective manner, you must balance the need for security with availability, performance and cost-effectiveness. Protecting web applications requires both zero-day protection and rapid response with minimal impact to operations, and must be part of a defense-in-depth plan. Look to host-based intrusion defense systems to provide comprehensive security to proactively protect hosts, applications and sensitive data without impacting performance or changing system architectures.

2. Web applications are increasingly vulnerable

Rapid growth leads to emerging problems

The number of corporate web applications has grown exponentially and most organizations are continuing to add new applications to their operations. With this rapid growth come common security challenges driven by complexity and inconsistency. New awareness into web application vulnerabilities, thanks to organizations such as the Open Web Application Security Project (OWASP), has helped organizations identify application security as a priority. But according to a June, 2006 survey[1], while 70 percent of software developers indicated that their employers emphasize the importance of application security, only 29 percent stated that security was always part of the development process.

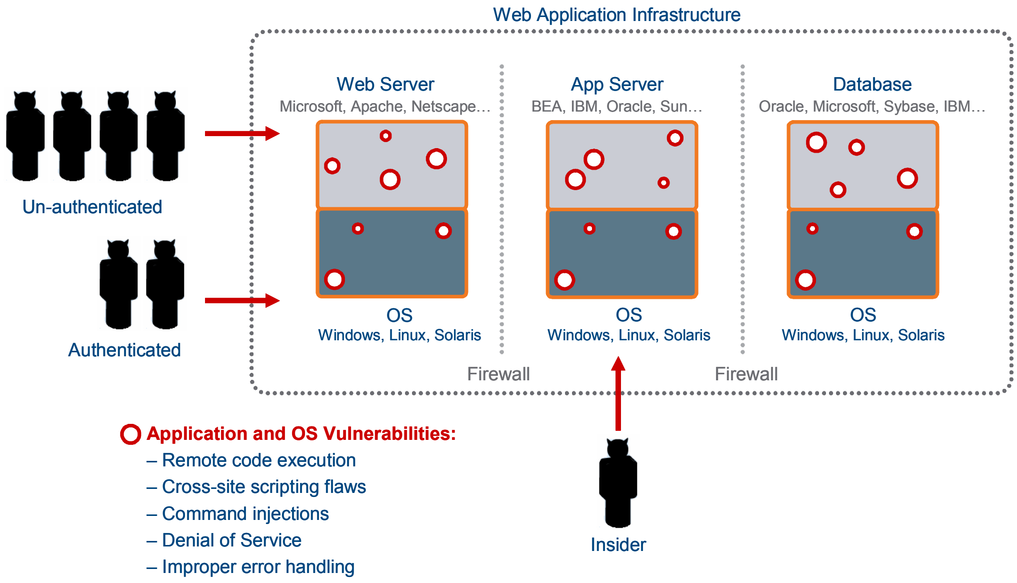
The overlooked vulnerabilities

Unfortunately, it is not just application flaws that are leaving systems vulnerable. In addition to application issues, every web application relies on a large stack of commercial and custom software components. The operating system, web server, database and all the other critical components of this application stack, have vulnerabilities that are regularly being discovered and communicated to friend and foe alike. It is these vulnerabilities that most organizations overlook when they're considering web application security.

The challenge this poses for IT Administrators and security professionals is that regardless of the source of the leak, application code or underlying software, they need to their keep mission critical applications secure.

[1] Symantec, http://www.symantec.com/about/news/release/article.jsp?prid=20060919_01

Figure 1: Typical vulnerability targets in web applications



As noted in Figure 1, threats against applications can come from a variety of sources:

- **Insiders:** A small number of insiders who have the greatest level of access to the overall system and the greatest choice of vulnerabilities that they can exploit;
- **Authenticated Users:** A larger number of authenticated users that can breach a vulnerability anywhere in the application or the first tier of the system;
- **Unauthenticated Users:** Any attacker on the internet able to exploit a flaw in the application authentication mechanism or the web server.

As new vulnerabilities are found, patches become a critical part of managing application security. The process of patch management is complex and difficult to do successfully. Even the most proactive IT team must often reassign critical resources to deploy urgent patches, disrupting normal operations. The time required to patch responsibly lengthens the window of time an attacker has to exploit a specific vulnerability. With thousands of vulnerabilities and patches being announced each year the problem continues to grow. Even organizations with the most efficient patching processes in place can't rely on this alone to protect them from attacks targeting web application vulnerabilities.

Attackers look for the path of least resistance

Today's sophisticated attackers target corporate data for financial and political gain. They know they can more easily exploit vulnerabilities in web application stacks versus trying to defeat well-built network and perimeter security. With myriad numbers of vulnerabilities and many different techniques - including SQL Injection, Cross Site Scripting, Buffer Overflow, Denial of Service

- there is no shortage of options for savvy attackers. In fact there have been over 4,000 vulnerabilities identified in the first 9 months of 2006 and Web flaws made up the three most common.[2]

According to zone-h.org, 45% of attacks make use of vulnerabilities rather than configuration issues or brute force. Attackers are working hard to find and exploit new vulnerabilities in web applications faster then they can be patched. The window of time, from when an attacker identifies a vulnerability to when it is communicated and eventually patched, makes a defense-in-depth strategy critical to prevent a potentially damaging intrusion.

3. Regulations and legislation rule the new security agenda

The drive for compliance is dictating the security agenda for many organizations. As more attackers target web applications, protecting them becomes an essential ingredient in compliance strategies. From the PCI-DSS (Payment Card Industry Data Security Standard) to the data security and breach laws found around the world in countries like Canada and Japan, the European Union and over 20 U.S. states, nearly every organization is rolling out new practices to achieve regulatory compliance and web application security is a critical component of any program. In fact, many regulations such as PCI-DSS are focused on protecting the critical data found in web applications. The proliferation of breach notification legislation highlights one of the primary motivations of attackers: identity theft.

Data Security and Breach Notification Legislation

For companies that do business internationally, nationally or in multiple states, the growing list of data security legislation poses a significant problem. Countries and states often have distinctly different measures spelled out in their data security laws. They each specify different triggers for notifications and set varying requirements on what needs to be disclosed, to whom and when.

Although it’s a good security practice, you can not rely on encryption to protect your business from the potential costs associated with an intrusion. Organizations that were encrypting data to be guaranteed a safe harbor from notifying customers after a breach, are now being faced with new legislation that does not provide automatic “safe harbor” in states like Illinois and Indiana. The application of the various state and potential federal laws depends on the residency of the account holder whose data was compromised, forcing organizations to adopt a “notify all”

[2] Mitre Corp, 09/2006

approach rather than apply separate policies across different customer communities. This makes preventing the breach using host intrusion defense the best approach to compliance.

Breaches are costly. Gartner estimates that organizations can expect a breach to cost them $90 per user for investigation fees, communications, clean up and recovery, customer services, fines, lawsuits and increased security audits.[3] This figure does not account for the damage to the corporate brand and potential market capitalization impacts. In contrast, Gartner estimates that it costs organizations just $16 per user to use data security measures including intrusion prevention, encryption and security audits to prevent a breach.[4]

PCI-DSS

The PCI-DSS provides stringent requirements for the protection of credit card data. Credit card companies collaborated to develop 12 requirements for all merchants or service providers that store, process, or transmit cardholder data, including:

- Requirement 6 : Develop and maintain secure systems and applications
- Requirement 11: Regularly test security systems and processes.

Requirement 6 details the need for proactive monitoring and vulnerability testing of web applications. Organizations can be found non-compliant if they are found to have ongoing application vulnerabilities. Requirement 11 specifically details the use of network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. PCI-DSS has become a best practices guide for organizations outside of the credit card industry because of its clear and specific guidance on web application security.

The pressure to meet regulatory requirements is mounting as is the rate that new vulnerabilities are being discovered. Most regulations do not make any recommendations or prescribe a specific vendor or solution to combat web application vulnerabilities. As organizations face increasing pressure to take action, careful selection of the system that will provide the best protection can be challenging.

4. Selecting a system to protect web applications

Once web application vulnerabilities have been identified, the ultimate solution is to fix the vulnerabilities in the web application source code itself. However, this can put you at risk of an intrusion because application fixes can often require:

[3,5] Gartner, “Online Fraud Solved”, Avivah Liton, June 2006

- Third parties to provide fixes to those components;
- Multiple software components and vendors to support the changes and new versions;
- Specialized expertise to make changes in custom applications;
- Proper vulnerability fixing, testing and software deployment.

Defense-in-depth is a common security strategy that promotes the use of multiple protection techniques to mitigate the risk of one component being compromised or rendered ineffective. Although web applications rely on patch management for protection from software flaws, penetration testing and publicized breaches regularly show that these applications have vulnerabilities that can be readily exploited for extended periods of time.

When vulnerabilities exist and patching is not an immediate option, there are three main types of technologies that can be used as compensating controls to protect web applications.

Option 1: Web Application Firewalls

Web Application Firewalls are network-based devices designed to provide in-depth protection for the web application itself. However, they do not protect against vulnerabilities in operating systems or enterprise software that the web applications depend on. They also present an additional challenge for encrypted traffic as they either require the termination of SSL traffic before it reaches the web application, which limits its protection value within the enterprise, or they require the export and management of all of the private decryption keys. Lastly, although host CPU performance may be unaffected using a web application firewall, there is the cost and complexity of deploying additional hardware and its impact on existing high-availability hardware architectures. This additional hardware does not improve performance or availability, and for a similar capital expenditure both security and performance can be improved using host-based intrusion defense.

Option 2: Web Server security modules (modSecurity, UrlScan)

Web server security modules such as modSecurity for Apache or UrlScan for Microsoft IIS are web server plug-ins that can be deployed on the server itself. These approaches can be used to protect web applications, but like web application firewalls, they do not protect vulnerabilities in operating system or enterprise software that web applications depend on.

A New Option: Host-based Intrusion Defense with Deep Packet Inspection

Host-based intrusion defense systems provide both IDS and IPS capabilities, on the host. Data traffic to and from the web applications is inspected using a high performance, deep packet inspection engine that looks at both packet and payload data for malicious code and other anomalies. Deep packet inspection has been identified by Gartner[5] as a transformational security technology because of its ability to provide fine grained protection directly at the host where it can not be bypassed. The host intrusion defense system then enforces the rules that have been defined: it allows good data to pass through, while blocking data that violates any rule. A truly effective system can also modify the data stream to neutralize potentially malicious traffic.

Host intrusion defense systems can be bi-directional. That is, in addition to inspecting inbound data for malicious code and other anomalies, they can also inspect outbound data. This helps ensure sensitive data doesn't get into the hands of unauthorized users, and supports regulatory requirements.

A host intrusion defense system that uses deep packet inspection can be used to get the best of both worlds: a software-only solution that can protect both web application vulnerabilities, as well as vulnerabilities in the operating system and enterprise software they depend on. With little impact on host performance, they do not require the purchase or deployment of additional hardware to protect critical servers from software vulnerabilities. And by running on the host, it can inspect encrypted traffic without compromising the security value it offers.

Host-based intrusion defense with deep packet inspection gives you:

- Protection, without costly and time consuming application changes
- Automatic protection from new vulnerabilities, so that new patches can be tested and deployed on a scheduled basis, rather than reactively
- Rapid protection against new vulnerabilities through the seamless delivery of new filters.
- Protection that is fully aware of application state, and that can stop attacks like cookie tampering and session hijacking
- Bi-directional protection that stops both malicious incoming attacks and prevents sensitive information leakage

This comprehensive solution to web application security can also provide broad multiplatform support, and be easily used in complex, heterogeneous environments with nominal impacts on performance levels.

[5] Gartner: "Hype Cycle for Infrastructure Protection, 2006"

5. Your next steps

Web applications are increasingly vulnerable and protecting them requires a system that can both ensure compliance today and meet the evolving needs of an organization for tomorrow. To meet the challenge, organizations should continue to be diligent by regularly performing network- and application-level vulnerability scanning and penetration testing. In addition, organizations should select and deploy compensating controls that defend in-depth, provide rapid protection to close the vulnerability gap, with minimal impact on operations. Host-based intrusion defense systems increase security and ensure compliance by stopping attacks before they impact critical web applications, data and hosts.

About Third Brigade®

Third Brigade specializes in providing host intrusion defense systems to government, financial services, health care, telecommunications and other organizations that need to detect and prevent attacks that exploit vulnerabilities in commercial and custom software, including web applications. Third Brigade Deep Security® enables you to create and enforce comprehensive security policies that proactively protect critical applications, sensitive data, and hosts, ensure regulatory compliance, and maximize the performance of your people, processes and hosts. Unlike others, Third Brigade software is not intrusive: it is smaller, faster and simpler. Third Brigade. That's control.

For more information, please visit **www.thirdbrigade.com**, or contact us at:

Corporate Headquarters
40 Hines Road
Suite 200
Ottawa, Ontario, Canada
K2K 2M5
Toll free: +1.866.684.7332
Local: +1.613.599.4505
Fax: +1.613.599.8191

United States Headquarters
11710 Plaza America Drive
Suite 2000
Reston, Virginia, USA
20190
Toll free: +1.866.684.7332
Local: +1.703.903.4479
Fax: +1.613.599.8191

Author Profile

Blake Sutherland, Vice President, Product Management, Third Brigade

Blake is responsible for managing the product life-cycle of Third Brigade's advanced intrusion defense software. He works closely with customers, prospects, partners and industry to understand market requirements, and incorporate them into the product. Prior to joining Third Brigade, Blake was at Entrust, Inc., a leading Internet security company. Blake is a Professional Engineer in the Province of Ontario, as well as a Certified Information Systems Security Professional (CISSP), and holds a Bachelor of Applied Science degree in Engineering Physics from Queen's University.