

Securing Enterprise Web Applications for Critical Data Protection and PCI-DSS Compliance

Selecting the Right Technology is Essential in Guarding Against Malicious Attacks

'RAYOSHIMI > 密碼老虎0912 > JOHNSONAMY > TEL2125505672 > MAST
6300929787331 > EXP01/11 > NUMBER0338-2934-051 > BOSTONMA
-TS > PAIEMENTD'HYPOTHÈQUE€2532.90 > DOB09/19/1975 > FAX+
0 > MORTGAGEPAYMENT\$2532.90 > HUOJINZHOU > SSN801-552-09
/ERANGUS > ACCOUNTNUMBER41775310 > LEITHSCOTLAND > VISA5
EXP03/2011 > SECURITYTYCODE > 8439 > 支払¥278733.10 > SPOU
MARGOT > MOBILENO5027742998 > MOBILEALABAMA > FONDAMEN
HIELLESANTACROCE390.30135VENICE > SSN445-09-9388 > PA
33MUG > OTAKENJI > ÅLESUNDMØREOGROMSDALNORWAY > ACCTNUM
02 > SOLOMONSAMUEL > DOB11/12/1988 > PASSWORDDAISEY112
TTIABRIENE > ŽUKAUSKIENĖJANINA > TEL33-04-92-98-78-0
RGENBELGIUM > PAYMENT£1002.00 > SZYMAŃSKI GRAZYNA > OC
電話番号03-3224-9999 > SSN456-92-0993 > TEL40307821 > DI
32093205 > STAVENHOF522KÖLN > EXP09/2011 > SECURITYC

As today's organizations conduct more business over the Internet, Web applications are becoming a key element of their success. Unfortunately, these applications are also being targeted by a growing army of hackers around the world.

Consider these facts from a recent article on malware:

- > SQL injection attacks increased 30-fold from late 2008 to early 2009
- > A major security firm found that a single SQL injection attack had compromised 780,000 Web pages
- > 74% of Web application vulnerabilities disclosed in 2008 were not patched by the end of the year

Web applications provide a tempting target. Many of these applications manage highly sensitive personal, financial, medical or business records that can be illegally sold or otherwise misused for malicious purposes.

A "Borderless" Infrastructure Invites Multiple Threats

By leveraging Internet technology, many organizations today have created a "borderless" IT infrastructure, with applications, networks and data stores connected across environments, both within and outside the enterprise. Web applications reside in a "demilitarized zone," partly within and partly outside the network perimeter.

With this "borderless" infrastructure, information can be easily shared and distributed across the Internet. Unfortunately, so can a wide range of malware, including:

- > SQL injection attacks
- > XSS attacks
- > PHP program access and code injection
- > DoS attempts
- > Modified parameters in a URL request
- > Malicious code injection into Web application requests
- > Tampering with Web application forms
- > Cookie highjacking within Web applications
- > Brute force or dictionary password attacks
- > Data theft, anti-crawl and others

What's more, hackers are using increasingly sophisticated methods of attack to steal or change sensitive data, take control of an entire application or even launch attacks against an organization's clients.

5 6 3 0 0 9 2 9 7 8 7 3 3 1 > E X P 0 1 / 2
T S > D 0 B 0 9 / 1 9 / 1 9 7 5 > F A X 7 1
S N 8 0 1 - 5 5 2 - 0 9 2 1 > M I C H A E L

The following kinds of attacks on Web applications deserve particular attention since they are the most common:

> **PHP file include**

On an unprotected Website, the attacker includes a malicious PHP script called a Web-shell, also known as a PHP shell. The shell enables the attacker to edit, add or delete files on the Web server. Spam programs are often launched through this attack.

> **XSS (cross-site scripting)**

Malicious Web users inject code, such as client-side scripts, into Web pages viewed by other users. This cross-site scripting vulnerability can be used to bypass access controls such as the same origin policy. Vulnerabilities like XSS are used to craft phishing attacks and browser exploits.

> **SQL injection**

SQL query is injected via the input data from the client to the application, accessing sensitive data from the database, executing administration operations on the database (possibly to shut down database management systems), and even issuing commands to the operating system.

> **Denial of Service (DoS)**

This attack is designed to prevent legitimate users from accessing information or services at a Website. The most common type of DoS attack occurs when an attacker “floods” a Website with requests to view a Web page. The server is overwhelmed or errors are triggered so that service is degraded -- with pages loading very slowly -- or the Website itself becomes unavailable.

These kinds of attacks are publicly reported with frequency, and their associated vulnerabilities are often found in commonly used Web software packages. Beyond these are a large set of unique vulnerabilities for custom Web applications, a fact that makes this security problem even more serious.

Compounding this security problem is the fact that many Web-based applications are simply legacy applications that have been “Webified”— made to operate with browsers or similar technology. Their native architecture was never designed for the security requirements of the Internet. Often, two or more applications are combined in a “mashup” that provides a combination of services or access to multiple data stores across systems, platforms and environments. This increases the depth and richness of services provided by Web applications. It also increases the vulnerability of these applications to attack and expands the sensitive data set associated with them.

Finally, organizations must face the burden of compliance. For example, organizations that support credit card transactions over the Internet must fully comply with PCI-DSS requirements. The costs of non-compliance are staggering, with fines of up to \$500,000.

In addition, non-compliance can result in a loss of tier status and an increase in per-transaction interchange rates — or even complete loss of credit card payment acceptance privileges. For most organizations, the latter would actually have a greater financial impact than fines.

Needed: A Layered Approach to Web Application Security

To defend against malware attacks and address compliance requirements, organizations must protect the entire Web application environment. This includes not just Web applications but also:

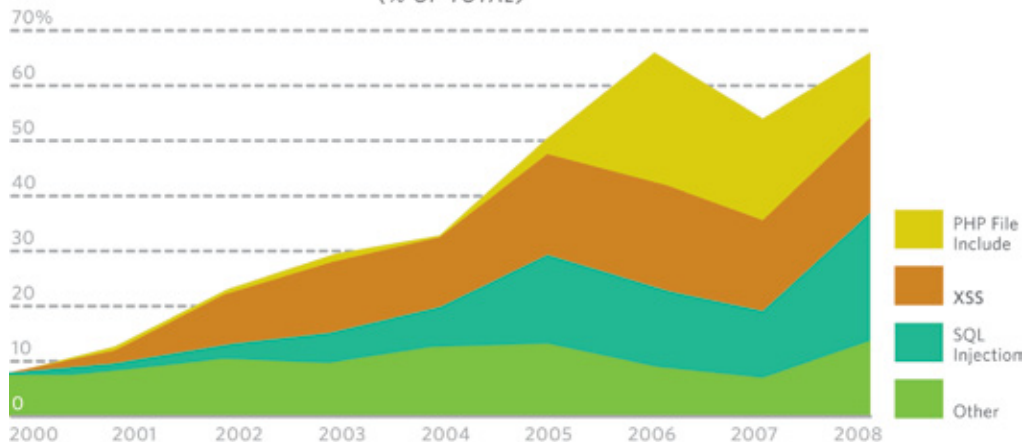
- > The routing, switching and load balancing infrastructure, including the operating systems on each of these devices
- > Web server operating systems
- > Supporting applications for database servers, as well as patch management and database back-up
- > Company and customer data used by the Web applications

Furthermore, Web application filters should detect and exclude all malicious traffic — but not at the expense of false positives or limited traffic flow. At the same time, many Web applications are highly customized, so effective security requires both custom and standard filters. Finally, a Web application security solution should fully address compliance requirements and internal corporate mandates for security and data protection.

In short, a comprehensive, layered approach to security is required that protects applications, operating systems, networks and other areas across the IT infrastructure.

Web Application Vulnerabilities

(% OF TOTAL)



80% of application vulnerabilities that are publicly reported can be traced to three primary types of attacks: PHP file include, XSS and SQL injection. applications.

Why Traditional Web Application Security is Ineffective

Organizations can address Web application security in a number of ways. Some of these approaches have been used for years, and may have been developed when malware attacks were far less numerous and sophisticated than they are today.

> **In-House Code Review and Internal Patches**

Organizations sometimes use in-house IT resources to review, test and harden their Web applications monthly or quarterly in response to security threats. External scans help discover vulnerabilities, but patches must be developed and then tested to determine how they will affect critical systems. The entire process demands significant time and labor, even as new threats are being detected.

In-house resources are actually better suited for regular maintenance tasks such as updating anti-virus software. In addition, security can be low priority for IT departments; many network teams are already overburdened with other tasks and managers cannot cost-justify specialized training in Web application security.

> **WAFs**

WAFs can be tuned to learn acceptable traffic patterns, but WAFs generate high levels of false positives. This can cause network outages or performance problems. As a result, WAFs often operate in a “default permit” mode simply to maintain traffic flow. Obviously this approach can easily compromise security.

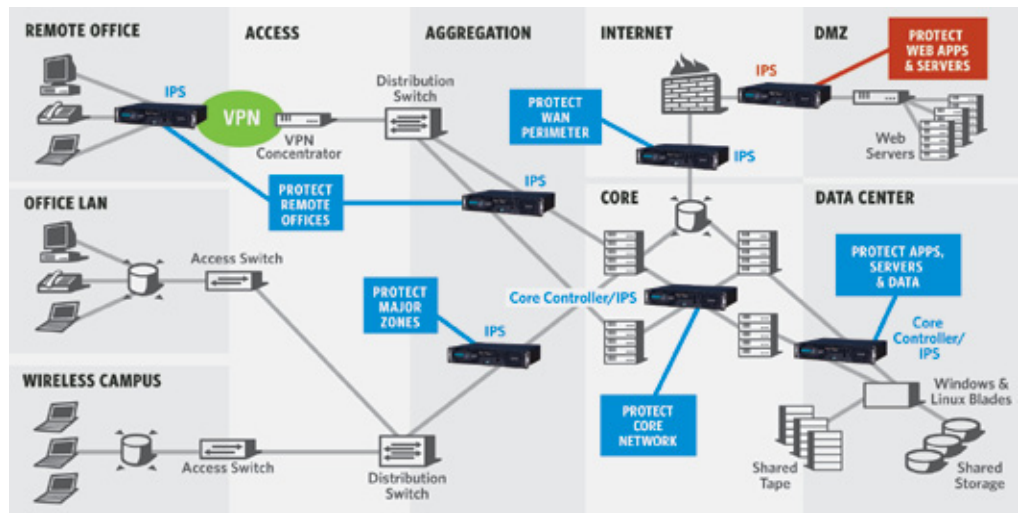
To increase security, some organizations combine WAFs with vulnerability assessment (VA) products, using the VA scanner outputs for filtering. An IPS can also work with VA products, but an IPS solution has the advantage of protecting the base platform – something that a WAF cannot do.

A standard Web application firewall results in constant tuning and a staffing drain to address the discovered vulnerabilities. A layered security approach takes the vulnerability insight provided by the scan and develops specific filters and enforces protection through the TippingPoint IPS, eliminating the burden on IT departments.

“The challenge of implementing a WAF is finding one that ...enforces all the PCI requirements and doesn’t break their application.”

Qualified Security Assessor (QSA) for PCI-DSS

Search Security, May 21, 2008.



Web applications and networks are better protected by a proactive, real-time IPS.

“Using [IPS] technology has pretty much reached the due-diligence level. On PCs you should have software, and on networks you need intrusion-prevention systems.”

John Pescatore, Gartner

Choose the Right IPS for Web Application Security

As an integrated solution, TippingPoint IPS and Web Application Digital Vaccine service help organizations safeguard their Web applications through real-time protection, custom filters and a unique Digital Vaccine service.

TippingPoint Web Application Security with IPS: A Layered, Comprehensive Approach

TippingPoint IPS solution paired with Web Application Digital Vaccine provides a layered, comprehensive approach to Web application security, helping to protect applications, operating systems, networks and other areas. As a proactive approach, the vulnerability insight provided by a Web application scan paired with the IPS analysis of active connections and intercepted attacks in transit, ensures attack traffic never reaches the target. Legitimate traffic passes unhindered through the system at full network speed and with microsecond latency.

5 6 3 0 0 9 2 9 7 8 7 3 3 1 > E X P 0 1 / 2
T S > D O B 0 9 / 1 9 / 1 9 7 5 > F A X 7 1
S N 8 0 1 - 5 5 2 - 0 9 2 1 > M I C H A E L

"If you don't have IPS, you deserve to be hacked."

John Kindervag, Forrester Research

In comparing a layered security approach to WAFs, it should be noted that WAFs require a great deal of tuning to be effective, and this places a constant drain on IT resources and budgets. TippingPoint's layered security approach provides the same custom protection but in a more comprehensive and accurate manner. In addition, a WAF can produce false positives if the tuning is not conducted properly. The tuning itself may end up "breaking" applications, so WAFs are often run in many environments with limited filtering capabilities. In some cases, WAFs are used to simply "tick a box" on a compliance check list.

In contrast, TippingPoint's solutions provide organizations with:

- > Comprehensive protection at multiple levels and attack vectors
- > Greater accuracy with analysis that detects malware while avoiding protection against false positives and false negatives
- > A proactive solution for automatic, real-time enforcement of network policy
- > Multi-gigabit throughput with switch-like latency

Protection: Real-Time Attack Prevention and Response

As packets pass through the TippingPoint IPS, they are fully inspected to determine whether they are legitimate or malicious. This instantaneous form of protection is the most effective means of preventing attacks.

As part of TippingPoint's layered approach for security, TippingPoint IPS performs packet flow inspection through Layer 7 to cleanse Internet and Intranet traffic and eradicate attacks. In addition, researchers working with TippingPoint's Zero Day Initiative (ZDI) provide information about previously un-patched vulnerabilities. While the vendor is being notified about a vulnerability related to one or more of its products, TippingPoint may distribute vulnerability protection filters to its customers' IPS devices through the Digital Vaccine Service.

Custom Filters: Defending Against Custom Vulnerabilities

Custom filters are especially important in Web application security. More often than not, Web applications are custom-built, which means they have custom vulnerabilities that require custom filters.

5 6 3 0 0 9 2 9 7 8 7 3 3 1 > E X P 0 1 / 2
T S > D 0 B 0 9 / 1 9 / 1 9 7 5 > F A X 7 1
S N 8 0 1 - 5 5 2 - 0 9 2 1 > M I C H A E L

To pinpoint these custom vulnerabilities, Web App DV provides an automated, comprehensive vulnerability assessment. The scan uncovers application vulnerabilities as well as site exposure risk. It ranks threat priority and produces graphical, easy-to-understand reports that indicate site security posture by vulnerability and threat exposure.

Based on the vulnerability insight provided by the Web application scan, the TippingPoint security research team develops specific filters for the customer's unique environment. The combination of standard Web application filters and filters written specifically for one-of-a-kind custom applications closes the gap on Web application security.

TippingPoint solutions fully complement regular anti-virus updates and other security maintenance functions performed by in-house IT professionals. These services provide protection between patch cycles and virtually eliminate the need for emergency, ad hoc patching. TippingPoint solutions can also protect legacy applications when the original developers, whether staff or consultants, are no longer available to code, test, fix or otherwise maintain these applications.

Digital Vaccines: for Maximum Security

The Digital Vaccine Service provides packages of filters to TippingPoint customers automatically on a regular weekly release schedule or immediately when critical vulnerabilities emerge. Developed by the TippingPoint DV Labs security research team, these filters are designed to provide organizations with pre-emptive protection against new and zero-day vulnerabilities, including vulnerabilities related to custom Web applications.

TippingPoint Web App DV Meets PCI-DSS Compliance Demands

PCI-DSS includes specific mandates for Web application security, as explained in Requirement 6.6:

For public-facing Web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

- > *Reviewing public-facing Web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes*
- > *Installing a Web-application firewall in front of public-facing Web applications*

TippingPoint addresses these requirements — and more. A comprehensive TippingPoint IPS solution with Web App DV can provide application filters specific to Web application threats, as described above. TippingPoint IPS solutions also help support compliance efforts by protecting infrastructure components, including database applications, VoIP infrastructure, routers, switches, application servers and DNS servers. TippingPoint can even provide a PCI-centric report outlining compliance issues with specific recommendations for filters and other changes.

Choose the Leader in IPS. Choose TippingPoint.

Selecting the right vendor for Web application security and compliance is a critical decision for any organization. TippingPoint is the recognized leader in IPS solutions, with a large and established customer base and acknowledged expertise in the research, development and implementation of IPS solutions. TippingPoint's DV Labs team is the premier security research organization for vulnerability analysis and discovery. The team consists of industry recognized security researchers who apply their cutting-edge engineering, reverse engineering and analysis talents in their daily operations. TippingPoint is also the primary author of the SANS@RISK newsletter, which contains the latest information on new and existing network security vulnerabilities.

For more information about TippingPoint solutions for Web application security, compliance and IPS, contact your TippingPoint representative, or visit www.tippingpoint.com.

Corporate Headquarters:
7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:
Herengracht 466, 2nd Floor
1017 CA Amsterdam
The Netherlands
+31 20 521 0450

Asia Pacific Headquarters:
47 Scotts Road
#11-03 Goldbell Towers
Singapore 228233
+65 6213 5999

Copyright © 3Com Corporation. TippingPoint and Digital Vaccine are registered trademarks of 3Com Corporation or its subsidiaries. All other company and product names may be trademarks of their respective holders. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors which may arise. Specifications and other information in this document may be subject to change without notice. 503218-001 09/09

TippingPoint
www.tippingpoint.com

5 6 3 0 0 9 2 9 7 8
T S > D O B 0 9 / 1
S N 8 0 1 - 5 5 2 -