Designing a strategy for comprehensive web protection

Contents

Executive summary

In 2000, the United States had nearly 135 million Internet users.[1] As dramatic as that number seemed 10 years ago, the number of Internet users has grown exponentially: as of June 30, 2010, roughly two billion people are using the web.[2] This adoption rate is even more striking given the penetration of Internet use in Australia, Europe and North America, where some 61 percent, 58 percent and 77 percent of the population is connected, respectively.[3] Even other sections of the world that have a lower percentage of web users are rapidly making up ground, with Africa and the Middle East experiencing increases of more than 2,300 percent and 1,800 percent, respectively, in the last 10 years.[4]

This rise and rush to connect has a variety of causes, including the shrinking costs of Internet-capable equipment, the pervasive availability of higher speed wireless connectivity, the integration of cellular voice and data communication devices, and the continuing increase in the value and diversity of services available through the Internet.

As systems and the environments in which they operate become simpler to develop, deploy and use, the world is getting smaller, and people are interacting more than ever. The location of the server or the client is no longer obvious or necessary; we exist in a relatively flat universe, and the barriers are lowering to global communication and global business. We have virtually unprecedented access to information and tools for collaboration.

Web applications power much of this new communication and deliver much of the new and interesting content that attracts this generational wave of new users. Unlike the web pages that first appeared in the mid-1990s, each of which was mainly static and only mildly interactive, today's web-enabled applications are powered by new languages such as Java™ technology, JavaScript, the Adobe® Flash player, XML and Hypertext Preprocessor (PHP). These web-enabled applications have rich, interesting content and can be dynamically altered based on the identity, type or interests of the users who interact with them.

Big opportunities, big risks

This new form of interactivity means real advancement in service and data availability. In the current generation of web interactivity, a user with only a web browser can easily access systems and resources, typically without downloading any new software. Almost any kind of application or service can be driven from connected devices—such as desktops and smart phones. Users are opening their web browsers in increasing numbers to run applications at work, receive and pay bills at home, prepare and file taxes, and manage all kinds of sensitive data, from life savings statements to medical records. In short, new web applications are transforming our experience with the web and the world.

The rise of the Internet and web applications has created whole industries and altered or displaced others. Physical location is losing importance, and disintermediation is creating more direct and substantial relationships for customers and product or service providers. Relationships are much more intimate because customers and business partners can access data and conduct transactions that not long ago were restricted to only employees. As a result, companies can take advantage of new opportunities to collaborate; improve efficiency; and simplify orders, payments, status checking and support.

Few innovations have proven as flexible and valuable as web applications, and while they are extremely powerful, they can also be very vulnerable. The rise in popularity of web applications has led to similarly rapid growth in the demand for developers to create them. Dozens of new products, platforms and frameworks simplify web application development to the point where almost anyone can write one. Unfortunately, the capability to create a secure application, or the capability to review an application for security problems, is not as simple or common. In addition to this skill gap, there are real time-to-market pressures on web application development teams; all too often, applications are rushed to the marketplace without enough focus on security.

The risks of this lack of rigor and concern are enormous because an organization is only as secure as the applications that support it. This white paper discusses the many risks surrounding web applications and their development and reviews the four layers of security an organization should establish to implement a comprehensive web application protection strategy.

Web application security risks are multiplying

Web applications present a number of unique security challenges. One is exposure—because web applications reach millions of users, they also reach millions of potential hackers. Web applications stretch across multiple infrastructure tiers and incorporate many process layers, elements that expose them to a wide range of prospective attackers.

As web applications get more complex, so do their vulnerabilities; as they become more useful and pervasive, they become higher value targets. And cybercriminals are taking note.

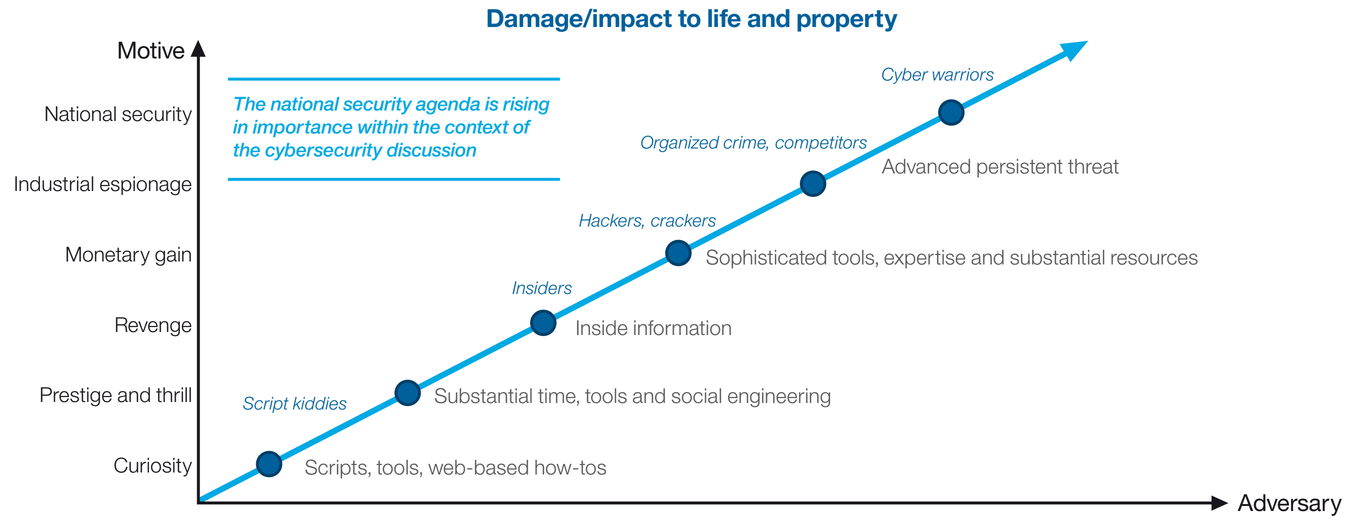


Figure 1: The important information and services accessible through a web-facing application have attracted a new and far more sophisticated adversary. And the motivation for these attacks is changing and maturing from curiosity to financial gain to real espionage. The techniques that hackers employ are also advancing, making them harder to prevent and detect. The arrow represents a rapid rise in the likely overall damage and impact of attacks on applications as a whole.

Public data breaches through web applications are frequent and can result in serious consequences, including lost revenue and business opportunities, revelation of highly confidential or damaging information, brand and reputation erosion, adverse media attention, unwanted scrutiny from consumer advocates, and growing costs to support litigation and compliance.

Consider a few selections in the rich variety of attacks that are available to hackers:

- **Cross-site request forgery (CSRF or XSRF)**—Also known as one-click attack or session riding, this is a type of malicious exploitation of a website where a hacker transmits unauthorized commands from a user whom the website trusts. Unlike cross-site scripting, which abuses a user's trust for a particular site, CSRF capitalizes on the trust that a site has in a user's browser.
- **JavaScript Object Notation (JSON) hijacking**—This kind of attack exploits a subset of the JavaScript programming language. Security concerns about JSON center on the use of a JavaScript interpreter to dynamically execute JSON text as JavaScript, thus exposing a program to an errant or malicious script that an attacker may insert in query text. This is a chief concern when dealing with data retrieved from the Internet.
- **HTTP response splitting**—This is a form of web application vulnerability that results from the failure of the application or its environment to properly sanitize input values. Hackers can use HTTP response splitting to perform cross-site scripting, cross-user defacement, web cache poisoning and similar attacks.

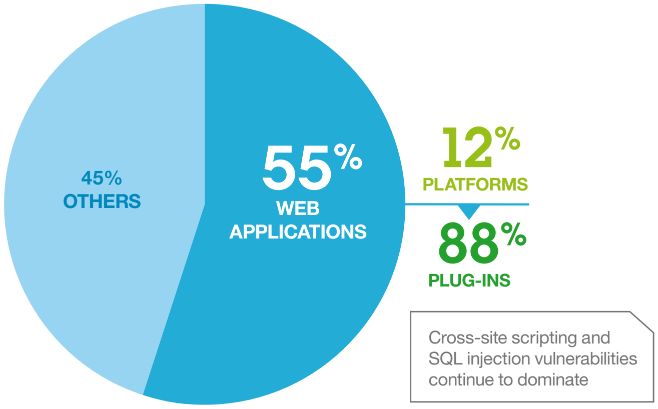
- **SQL injection**—This code injection technique manipulates a security vulnerability that occurs in an application's database layer. The vulnerability is present when user input is insufficiently filtered for characters that can cause actual execution of SQL commands from input fields such as login prompts or when user input is not classified in such a way to prevent inappropriate types of information from being passed on to an application and unexpectedly executed. This more general class of vulnerabilities can occur when one programming or scripting language is embedded inside another.
- **Lightweight Directory Access Protocol (LDAP) injection**—This type of attack exploits LDAP, an application protocol used to query and modify directory services running over TCP/IP, and can execute arbitrary commands such as granting permission to unauthorized queries.
- **XML Path Language (XPath) injection**—This is similar to SQL injection but manipulates XPath, a language for selecting nodes from an XML document. XPath is also used to compute values (strings, numbers or Boolean values) from the content of an XML document.
- **Shell command injection**—This attack inserts malicious code into the shell, or command language interpreter, that executes commands read from a keyboard.
- **Server-side include (SSI) injection**—This inserts malicious code into SSI, a simple server-side scripting language that's used almost exclusively for the web. As its name implies, SSI's primary use is to dynamically include the contents of one file into another when the latter is served by a web server.
- **Cross-site scripting (XSS)**—This type of computer security vulnerability is typically found in web applications that allow code injection by malicious web users into the web pages viewed by other users.
- **Directory traversal (or path traversal)**—This exploits insufficient security validation or sanitization of user-supplied input file names. In this instance, characters that cause the application to execute within other, unexpected areas of the file system are passed through to the file application programming interfaces (APIs).

Prevention is critical

Companies that delay efforts to protect web applications can face substantial consequences. In 2009, the average cost of a data breach in the United States was US$6.75 million,[5] and the probability of a hacker exploiting any given web application can be expected to continue to increase as automated attacks and bots multiply. Recent studies by the IBM X-Force team reveal that in the first half of 2010, web applications accounted for 55 percent of all vulnerability disclosures.[6]

Instead of reaching out to users with malicious code, hackers can now inject it into popular websites and let users come to them. Automated scanners help attackers identify which sites are vulnerable and can be easily infected. Browser plug-ins are particularly susceptible targets of these attacks. According to a recent IBM X-Force team report, in the first half of 2010, plug-ins accounted for 88 percent of disclosed vulnerabilities related to web applications.[7]

Percentage of vulnerability disclosures that affect web applications and web application platforms and their plug-ins



Cross-site scripting and SQL injection vulnerabilities continue to dominate

Figure 2: Attacks on web applications are multiplying, making a comprehensive web protection strategy even more critical for businesses that interact with customers online.[8]

Moreover, if hackers gain access to sensitive information, organizations run the risk of being noncompliant with a host of legislated mandates and other requirements, including the Payment Card Industry Data Security Standard (PCI DSS), which has specific application security requirements. Noncompliance can cost companies monthly fines of hundreds of thousands of dollars.

Existing point security solutions leave gaps

Web applications are the new attack vector for hackers to exploit. Just like with other IT threats, the initial reaction to combat risk is to introduce a point solution for every threat. But existing point security solutions have design limitations:

- Traditional vulnerability scanners scan web servers but not web applications.
- Manual penetration testing is effective but is neither scalable nor focused on remediation.
- Traditional network firewalls offer basic web application protection but don't address the needs of custom web applications.
- Web application firewalls are expensive to purchase and manage; they can be effective but are challenging and time-intensive to properly deploy and tune.
- Most web applications are customized, and it is difficult for web application firewalls to interpret their behavior as either good or bad.

Each of these limitations results in security gaps. The problem is that point solutions weren't designed with web application security requirements in mind.

Security organizations in today's companies demand an integrated solution from a trusted vendor that provides a holistic and cost-effective approach to IT security. For thorough web security, enterprises need comprehensive web protection that fits within a framework of security governance, risk management and compliance.

IBM provides a wide-ranging security framework across key domains that ties back to Control Objectives for Information and related Technology (COBIT) standards. IBM can also deliver and unite professional services, managed services, and hardware and software solutions for each domain. Let's explore the requirements of comprehensive web protection and understand why IBM is in a leadership position to help your company determine and implement a web application security solution that addresses your unique needs.

Layers in a comprehensive web protection strategy

Maximizing web protection involves four layers of security—developing new, security-enabled applications while protecting existing applications; preventing site intrusions with real-time protection; shielding service-oriented architecture (SOA) deployments and XML or other web service traffic; and controlling access to web applications.

To simplify each layer of protection, IBM integrates industry-leading solutions that facilitate comprehensive web protection and that are designed to reduce the risks in web-enabled transactions, websites and web traffic. Let's take a closer look at each of the needed layers.

Develop security-rich, new applications while protecting existing applications

A key first step in enhancing web protection is to identify vulnerabilities in your existing web applications. One of the most cost-efficient ways to do this is to automate the testing process. You need a means to automatically scan applications, identify vulnerabilities and generate reports with intelligent fix recommendations.

To stay ahead of hackers and enable a more secure design, the solution should test not only live web applications but also those in development—throughout their development life cycle. The solution needs to scan and test for common web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification.

To address these requirements, IBM developed IBM Rational® AppScan® Source Edition and IBM Rational AppScan Standard Edition solutions. Rational AppScan Source Edition software analyzes the source code used to build applications, reviews code for issues and errors prior to deployment, and can save you considerable time and money on quality assurance (QA) issues identified later in the cycle. Rational AppScan Source Edition and Standard Edition solutions also share core features that provide application scanning coverage for both new and old web-facing technologies. Rational AppScan tools can assess the following:

- The parsing and execution of JavaScript and Adobe Flash applications
- Asynchronous JavaScript and XML (AJAX) and Adobe Flex technology-related protocols such as JSON, Action Message Format (AMF) and Simple Object Access Protocol (SOAP)
- Elaborate SOA environments
- Custom configuration and reporting capabilities for mashup- and process-driven applications

Because attacks keep evolving, a scanning solution needs constant updates. To help enable Rational AppScan solutions to keep up with and test for the latest exploits and vulnerabilities, IBM research and IBM development teams provide automatic software updates. And because identifying vulnerabilities alone does not make web applications more secure, Rational AppScan software also includes intelligent fix recommendations.

Compliance is critical, and an automated scanning solution should streamline the compliance process. Rational AppScan solutions include more than 40 standard security compliance reports, such as for PCI DSS, ISO 17799 and ISO 27001, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and Basel II recommendations.

After your solution finds application vulnerabilities, your organization needs time to fix them. Your second layer in a comprehensive web protection strategy should be a shield to protect against attacks.

Prevent site intrusions with real-time protection

Good intrusion prevention needs to be web application aware. IBM Proventia® web application security is included in every Proventia intrusion prevention solution. These marketplace-leading solutions for blocking attacks at the network perimeter and server levels now include the protection of a web application firewall. Because of the increasing importance of web applications, IBM delivers the core protection engine of Proventia web application security across its entire Proventia product line.

Four key requirements have guided the IBM Proventia solution design:

- **Proactive prevention**—Instead of auditing attacks and reacting to them, like many web protection solutions do, Proventia web application security helps address and limit primary attack sources.
- **Simplified configuration to enhance security**—You can save time with Proventia web application security because it is configured out of the box with IBM X-Force recommended policies, which are updated automatically. Using a wizard feature, you can more easily build additional security policies that help protect custom web applications.

- **Enhanced compliance**—Proventia web application security addresses PCI requirements for web application protection.
- **Comprehensive protection of a web application firewall**—The firewall is deployed by combining IBM Security Network Intrusion Prevention System (formerly IBM Proventia Network Intrusion Prevention System) with a Secure Sockets Layer (SSL) offloader.

IBM offers Proventia solutions in three form factors to address different deployment requirements. The Security Network Intrusion Prevention System solution provides high-bandwidth web protection for large enterprises with web server farms. The IBM Proventia Network Multi-Function Security solution offers all-in-one remote office or branch office protection with virtual private network (VPN) support. Small offices without a network intrusion prevention system or VPN can use the IBM Proventia Server Intrusion Prevention System solution to decrypt and inspect SSL-encrypted traffic.

Protect SOA deployments and XML and web services traffic

The third layer in a comprehensive web security strategy is to protect SOA deployments and XML and web services traffic, which are often key components of web applications. Yet safeguarding these components requires a different kind of real-time protection than that which would typically suffice to protect web applications. Web services generate high-speed, high-volume traffic; inspecting this type of traffic can easily degrade application performance.

The IBM WebSphere® DataPower® family of appliances features purpose-built, specialized hardware with high-speed, high-volume security inspection capabilities. WebSphere DataPower appliances serve as a security enforcement point for SOA deployments and XML and web services transactions, including encryption, firewall filtering, digital signatures, schema validation, Web Services Security (WS-Security), Web Services Policy (WS-Policy) Framework, Web Services Security Policy Language (WS-SecurityPolicy), XML access control and XPath.

Control access to web applications

To help ensure that only authorized users gain appropriate access to web applications, your authentication and authorization solution should have the following features:

- Centralized authentication, access and audit policies, enabling them to be easily defined and managed
- An established audit and reporting service that collects audit data from multiple enforcement points and across platforms and security applications
- Simplified single sign-on (SSO) options
- Security codes that are separate from application codes
- Fine-grained entitlement and data-level access control

To address these requirements, IBM offers IBM Tivoli® Access Manager and IBM Tivoli Security Policy Manager software. By integrating rigorous access control and identity management capabilities, the Tivoli family of solutions enables appropriate controls for application security, monitoring and management.

Achieve comprehensive web protection

Cost-efficient web protection does not limit opportunity on the web; it is an enabler. It can help your business reduce risk, enhance compliance, protect brand reputation, gain flexibility and reduce long-term security costs by building security into application development.

Leveraging its broad and deep security experience and offerings, IBM can provide a comprehensive strategy to help your business effectively manage web application security. As one of the world's most prolific creators of software and as a security consultant and strategic resource to large, global organizations, IBM informs its solutions with the realities of budgets, schedules and competing priorities. IBM's drive to help clients create web applications that are security rich by design is based on all of these insights and reinforces IBM's position as a valuable adviser and contributor to any security-rich application development effort.

For more information

For more information on how you can take advantage of proven IBM solutions to help safeguard your company's web-based applications, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/application-process.html

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

[1] Computer Industry Almanac, http://www.c-i-a.com/internetusersexec.htm

[2,3,4] Internet World Stats, "Internet Usage Statistics, The Internet Big Picture," http://www.internetworldstats.com/stats.htm

[5] Ponemon Institute, *2009 Annual Study: Cost of a Data Breach*, January 2010.

[6,7,8] IBM, *IBM X-Force 2010 Mid-Year Trend and Risk Report*, August 2010.

© Copyright IBM Corporation 2010

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
December 2010
All Rights Reserved

IBM, the IBM logo, ibm.com, and Rational are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Please Recycle