



Security PS is the Midwest's Leading Independent Application and Network Security Consulting Firm.

We offer services in the following areas:

- Web Application Security Assessments
- Network Security Assessments
- Source Code Security Reviews
- Password Compliance and Analysis
- Training
- Vulnerability Testing and Management
- Security Compliance
- And much more...

The Roots of Application Security

*Kris L. Drent,
Chief Technology Officer*

After conducting hundreds of application security assessments, it is not difficult to identify strong correlations between highly secure applications and the practices that are used to build them. Currently, there is a strong emphasis on the need for application security assessments and testing in the business world. While this is a positive sign of increasing awareness of application risk, this awareness seems to focus almost solely on conducting post-development assessments.

Here is where we find a gap that, if resolved, can save businesses a significant amount of money and effort in the form of

increased efficiency and reduced operational risk. Assessments are a fundamental necessity for identifying and managing risk of an application. But by that definition, these efforts are normally conducted on applications that have already been built and do not reduce the number of security problems built into the application during development. This approach tends to promote the dangerously common "build it first, secure it later" mentality that can make security appear to be a very high-cost and painful check box on the deployment checklist.

Our experience shows that by considering and applying se-

curity practices earlier in the Software Development Life Cycle, fewer security flaws and exposed vulnerabilities reach the testing and deployment phases. Software giants like Microsoft and Oracle also agree and have recent results that prove this is not a just theory but an approach that significantly reduces risk and provides a strong return on investment for application security efforts. The alternative is developing an application that, after being built, is diagnosed with a large number of vulnerabilities or systemic security problems that require a significant re-write of code or even a re-design effort. At the risk of stating

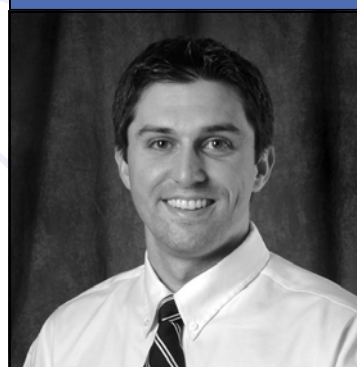
(Continued on page 4)

Consultant on the Rise: Tom Stripling

Tom Stripling got a strong education in computer sciences at Stanford University- but not all of it was in the classroom. When he caught his roommate on his computer bypassing the then limited Windows security controls to cause problems for the university, he quickly realized he had a passion for security.

This early encounter prompted some unique course work for Tom. He partnered with Cisco Systems on a class project that involved developing a secure distance learning application that included evaluating the efficiency of using IPSec versus

A Security PS Team Member Profile



Tom Stripling, CISSP

SSL for application traffic security and reporting these findings back to Cisco.

Tom joined Security PS in October, 2004 as a member of the web application security assessment team. Since then, he has proven himself to be a valuable team player and has recently been promoted to Security Consultant.

"With his driving work ethic and application assessment experience, Tom is a strong consultant who delivers value to our clients and our team" said Security PS CTO Kris Drent.

(Continued on page 3)

Inside this issue:

The Roots of Application Security	1
Title of Tom Stripling	1
Speaking of Web Services	2
Upcoming Training Sessions	5
How to Register for Training	5



Tom Stripling, CISSP

“Web services are so easy to implement that they often are implemented without the careful process that was used for the rest of the application.”

Speaking of Web Services

By Tom Stripling, CISSP

By now, we are all pretty familiar with web applications. The dot com era saw to that. Businesses everywhere are incorporating web applications as an integral part of their public presence. Web applications themselves have evolved as well. These once-basic systems have now grown into multi-tier, highly scalable applications used to manage complex business processes with a significant amount of our trust.

Today, applications are going even further. A new breed of web application is emerging that allows businesses to interact with applications from other organizations across the Internet. They utilize components called “web services”. For example, imagine an online store that sells monogrammed socks. The store must be able to authenticate users, but doesn’t want to go through the time and expense of implementing that process itself. The application could connect to a web service provided by Microsoft Passport and use it to authenticate users. The web service doesn’t even have to reside on a server within the organization. It can be anywhere on the Internet.

Sounds easy, right? In some regards, it really is. Web services are so easy to implement that they often are implemented without the careful process that was used for the rest of the application. Which leads to unwanted security risks. In the example above, what would happen if an attacker could forge a response from the Microsoft Passport authentication service to the store application? He could impersonate a user and change their monogrammed sock orders, and the store would never know the difference. We certainly don’t want that, so here are a few guidelines on how to implement or make use of web services securely.

1. Design for security

Whether you are planning on using someone else’s web service or creating one yourself, it is important to incorporate security practices and principles into the design from the beginning. By taking the time to address security before it becomes a problem, you can avoid the costs of retrofitting the application with security or frantically responding to an incident.

2. Learn how to spot the common web service security flaws

It isn’t possible to design or implement web services securely if you don’t know what the problems are. Even developers well versed in web application security may need support when it comes to designing a secure web service. Many of the potential risks are unique to web service architectures. Plus less security-related functionality is currently supported by web services frameworks than in a typical web application. These challenges can lead to security threats that the average web application developer may not consider. For instance, because web services communicate using XML instead of HTML, they are often vulnerable to different types of injection attacks than other web applications. Whereas HTML injection and cross site scripting are common problems elsewhere, web services are prone to injection attacks within the XML data structure. These attacks may even target the application’s XML parser itself.

3. Be aware of your exposure

Web services are designed to be easily used, and there are a lot of supporting



technologies and standards to support this. This includes a URL advertising the functionality available in a Web service. This information, expressed in the Web Services Description Language (or WSDL) response, is generally published alongside the web service for use by connecting clients. Depending on your implementation, you may not want this information to be available to everyone. It may be created and published without any specific action on the part of the developer. Microsoft's Visual Studio, for example, creates a WSDL by default with every web service. Understand what application functionality is exposed by the web service and how this information is published.

4. *Check your work*

Even when security is incorporated into the design process, incorrect security assumptions or flaws in the implementation can lead to exploitable vulnerabilities. Prior to the deployment of any web service or application, have an internal or external security team perform a security assessment. This check helps to not only reduce the likelihood of a costly security incident, but demonstrates your security commitment to customers and develops trust in your application.

“This check helps to not only reduce the likelihood of a costly security incident, but demonstrates your security commitment to customers and develops trust in your application.”

Consultant on the Rise: Tom Stripling, cont.

The new role excites Tom. “It's a good opportunity to continue to build client and professional relationships.” And Tom continues to hone another valuable skill – the ability to understand and describe the ultimate outcome of possible attacks from a client's perspective. Tom explained a key component to his role is educating his clients. “Rather than just describing the technical risk of a vulnerability, I consult on the risk to the business if a particular issue is exploited. This process is constantly evolving as new security issues develop” This straightforward approach has been praised by many clients.

After evaluating security in a variety of different industries and environments, Tom believes the biggest security challenge is convincing organizations to incorporate security into their development processes. He sees education as an important step in that process. “I don't think the average developer really cares any less about security in their products than security people do. They're just less informed about the results of poor security, so they're less

alarmed,” Tom said.

Tom keeps busy developing his skills and staying on top of key issues in his role of vice president and program director for the Kansas City ISSA chapter. He has attracted national speakers to address the group this year on topics such as VoIP security and SQL database protection.

Tom's upcoming plans include speaking on the topic of Web Services security at a national conference for credit unions. His article on Web Services security appears in this edition of our newsletter and includes some of the material covered in the presentation. Tom will add a CISA certification this year which will compliment his expertise in security demonstrated by his CISSP.

If you haven't had a chance to meet Tom and pick up some great security tips, give him a call at (913) 888-2111 or email tstripling@securityps.com.

“After evaluating security in a variety of different industries and environments, Tom believes the biggest security challenge is convincing organizations to incorporate security into their development processes.”

The Roots of Application Security, cont.

(Continued from page 1)

the obvious, most organizations would rather build it right the first time rather than use a trial and error approach, especially when security is on the line.

How does an organization apply security early in development to reduce the problems down the road? The answer is to take a hard look at the process that creates the application: the SDLC. I make the analogy in our training events that you can't expect an apple tree to grow bananas. In the same way, you can't expect a development process that has no security practices and principles built into it to produce secure applications. The goal then, is to design a development process that creates secure applications.

Software Development Life Cycles differ widely from organization to organization, but the first step is to commit to having a defined process that takes applications from concept all the way to deployment and ongoing maintenance. While this sounds obvious, some organizations have such a loose development process that it would be difficult to apply security practices and checkpoints to it.

Having a defined SDLC, key components must be added to provide security throughout the various phases. Organizations starting from ground zero will want to prioritize the implementation of these new security practices and implement them incrementally. This allows adoption of the new practices to take root and provides time for development teams to work out the details of the new activities without causing too much chaos.

Based on our experience, the top three SDLC security activities that provide the highest security value for the effort are:

1. Education: application security training for architects and developers
2. Threat Modeling: conducted in the design phase
3. Developer Security Tools: security tools geared for developers, used during development

Adding tasks such as these to the SDLC will make a quantum leap in security by putting risk-reducing efforts into proactive mode. While assessments are a critical part of managing risk, activities such as these three dramatically reduce the number of security weaknesses and vulnerabilities that are built into an application from the start.

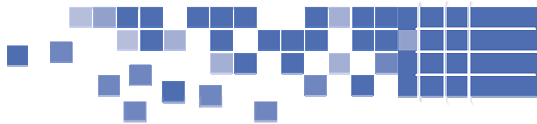
Education enables developers to be an active part of the daily development security process first by making them aware of threats and pitfalls, and further, by providing best practices to apply to design and development. Threat modeling is an exercise conducted by developers and security personnel that identifies a range of threats against the application during the design phase. This enables the development team to design and code against these threats as part of the normal development process.

Finally, there are a number of valuable tools that can provide immediate feedback to developers as they're coding. Like unit testing tools, security tools such as static code review utilities and milestone vulnerability scanners can identify coding flaws early in the SDLC. The cost savings of fixing coding flaws in the development phase instead of later phases (such as testing or deployment) is significant.

In summary, embedding security practices in the SDLC allows a proactive approach to application security that saves organizations time and money. It also avoids a reactive approach that can cause design and coding flaws to eat up maintenance development costs for managing risk. If your goal is to develop and deploy applications with a solid security posture and low risk, look at the root of the application: the SDLC.



“...you can't expect an apple tree to grow bananas. In the same way, you can't expect a development process that has no security practices and principles built into it to produce secure applications.”



Security PS

7300 College Blvd, Suite 175
Overland Park, Kansas 66210
USA

Phone: +1 (913) 888-2111
Toll Free +1 (877) 9 SPS INC
Fax: +1 (913) 888-2120

Prefer a hardcopy of the InfoSec Advisor?

If you would like to receive this newsletter in hardcopy, please email us a quick note along with your mailing address to: info@securityps.com

Visit our Web site at www.securityps.com

Coming Next...

In an upcoming issue of *InfoSec Advisor*, the Security PS newsletter, we'll share our insight on security compliance and regulations.



Training from Security PS



Upcoming Training:

Information Security Foundations	May 9 & 10
In-Depth Web Application Security	June 20
Hands-on WebInspect™ Training & Certification	June 21 & 22

For further information on classes and locations, please visit our Web site: <http://www.securityps.com/training>

Over 1000 people have attended our Web Application Security class alone — have you attended a Security PS training session yet? If not, sign up to one of our upcoming events to find out what you've been missing.

In-Depth Web Applications Security provides the attacks, demonstrations, principles and best practices of web application security by the experts in the industry. Up-to-date and designed to impact the security of your on-line applications for the long term, managers, developers and security staff will benefit from this course.

Hands-on WebInspect™ Training & Certification teaches manual and automated assessment techniques using SPI Dynamics' WebInspect™ product.

Information Security Foundations is a survey course aimed at system administrators and others charged with supporting IT security. The course addresses both hardware and software

issues and potential threats both physical and electronic in nature.

Securing Windows & Active Directory. Attendees will discover how hackers can profile, extract information from, and attack computers running Windows. They will learn how to close security gaps using techniques and Windows security features demonstrated during the training.

For more information on all Security PS Training offerings, visit our Web site at www.securityps.com.

Three Easy Ways to Register for Training:

- Complete and fax registration form available at: <http://www.securityps.com/training>
- E-mail us at training@securityps.com
- Call toll free +1 (877) 977-7467 and ask for the Training Coordinator

Remember, early registration discount ends 4 weeks prior to event date. Register now!