OWASP AppSec USA 2011 | September 20-23 | Minneapolis | www.appsecusa.org

OWASP is a 501(c)(3) not-for-profit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. Find us on the web at **https://www.owasp.org**

Bzz.

You've heard about application security.
Now make it visible.

www.owasp.org

Welcome to **OWASP AppSec USA 2011**, an application security conference for information security and development enthusiasts building software - which plays such a vital role in our lives - to be more secure.

The Open Web Application Security Project (www.owasp.org) is now ten years old. In the last ten years application security threats have multiplied, but fortunately, so have the ranks of people willing to protect applications. As we look ahead, it will be our responsibility to understand the people, processes, and technology in the vast information ecosystem, maintaining our focus on collaboration, predictable frameworks, and more understandable security design patterns.

If this is your first OWASP conference, strike up a conversation with a speaker, talk to someone at a booth, and give the Capture the Flag contest your best shot. OWASP is an open and charitable community, and we're all together in the struggle for more secure software.

We want to thank you - the contributors and attendees - for making this conference possible.

Keep making application security visible.

Lorna Alamri, Sarah Baso, Adam Baso, and
the rest of the OWASP AppSec USA 2011 crew
www.appsecusa.org   @appsecusa   #appsecusa

Table of Contents

Wireless Passwords

[SSID OWASP]	cloudy11
[SSID CTF2011]	packets2go

More Information

Conference Venue: Minneapolis Convention Center **Airport Code:** MSP **Transit:** metrotransit.org
Taxi: Green & White 612-522-2222, Rainbow 612-332-1615, Blue & White 612-333-3333
Emergencies: Dial 911

TALKS: Thursday, September 22, 2011

Abstracts available in this conference program. See http://www.appsecusa.org/speakers.html for bios.

Time	Attacks & Defenses	Cloud	Mobile	Thought Leadership
0730-0830	CONTINENTAL BREAKFAST			
0830-0920	**KEYNOTE: Mark Curphey**, Community - The Killer App			
0920-0930	BREAK			
0930-1020	**Andrés Riancho** Web Application Security Payloads	**Andy Murren** SwA and the Cloud - Counting the Risks	**Blanchou, Osborne, Solnik** Blackbox Android: Breaking “Enterprise Class” Applications and Secure Containers	**Arian Evans** Six Key Metrics: A look at the future of appsec
1020-1040	COFFEE BREAK			
1040-1130	**Jim Manico** Ghosts of XSS Past, Present and Future	**Shankar Babu Chebrolu, PhD, CISSP** Top Ten Risks with Cloud that will keep you Awake at Night	**Ryan W Smith** STAAF: An Efficient Distributed Framework for Performing Large-Scale Android Application Analysis	**Charles Henderson** Global Security Report
1130-1140	BREAK			
1140-1230	**Shreeraj Shah** Next Generation Web Attacks – HTML 5, DOM(L3) and XHR(L2)	**Scott Matsumoto** Threat Modeling in the Cloud: What You Don’t Know Will Hurt You!	**Tom Fischer** Lessons Learned Building Secure ASP. NET Applications ** Moved for schedule*	**John Benninghoff** Behavioral Security Modeling: Eliminating Vulnerabilities by Building Predictable Systems
1230-1330	**LUNCH & OWASP FOUNDATION BOARD DISCUSSION:** Jeff Williams (Chair), Tom Brennan, Eoin Keary, Matt Tesauro, Dave Wichers, and incoming board member Michael Coates ** Sebastien Deleersnyder unavailable due to scheduling conflict*			
1330-1420	**de Prado, Lara** Pwning intranets with HTML5	**Dan Cornell** The Self Healing Cloud: Protecting Applications and Infrastructure with Automated Virtual Patching	**Mike Park** Android Security, or This is not the Kind of “Open” I Meant...	**Veltsos (moderator), Los, McCormick, Williams** Making it in Information Security and Application Security
1420-1430	BREAK			
1430-1520	**Devarajan, Redfoot** Keeping up with the Web-Application Security	**Matt Tesauro** Testing from the Cloud: Is the Sky Falling?	**Stadmeyer, Held** Hacking (and Defending) iPhone Applications	**John B. Dickson, CISSP** Software Security: Is OK Good Enough?
1520-1540	COFFEE BREAK			
1540-1630	**Jon McCoy** Hacking .NET (C#) Applications: The Black Arts	**Adrian Lane** CloudSec 12-Step	**Soltani, Padgham** When Zombies Attack - a Tracking Love Story	**Jeff Williams** AppSec Inception - Exploiting Software Culture
1630-1700	**UNIVERSITY CHALLENGE WINNERS TALK!**			
1700-1800	HAPPY HOUR			

TALKS: Friday, September 23, 2011

Abstracts available in this program. See http://www.appsecusa.org/speakers.html for bios.

Time	Software Assurance	OWASP	Patterns	Secure SDLC
0730-0830	CONTINENTAL BREAKFAST			
0830-0920	**KEYNOTE: Ira Winkler**			
0920-0930	BREAK			
0930-1020	**Richard Struse** Software Assurance Automation throughout the Lifecycle	**Coates** Pure AppSec, No Fillers or Preservatives - OWASP Cheat Sheet Series **Watson** OWASP Codes of Conduct	**Dr. Chu, Xie** Secure Programming Support in IDE	**Brian Chess** Gray, the New Black: Gray-Box Web Penetration Testing
1020-1040	COFFEE BREAK			
1040-1130	**Ryan Stinson** Improve your SDLC with CAPEC and CWE	**Mannino, Lanier, Zusman** OWASP Mobile Top 10 Risks	**Sood, Enbody** The Good Hacker - Dismantling Web Malware	**Chris Wysopal** Application Security Debt and Application Interest Rates
1130-1140	BREAK			
1140-1230	**Willis, Britton** Sticking to the Facts: Scientific Study of Static Analysis Tools	**Simon Bennetts** Introducing the OWASP Zed Attack Proxy	**Collins, Zaw** Brakeman and Jenkins: The Duo Detect Defects in Ruby on Rails Code	**Mike Ware** Simplifying Threat Modeling
1230-1330	**LUNCH & KEYNOTE: Moxie Marlinspike**			
1330-1420	**Adam Meyers** Mobile Applications Software Assurance	**Anthony J. Stieber** How NOT to Implement Cryptography for the OWASP Top 10	**Michael Coates** Security Evolution - Bug Bounty Programs for Web Applications	**Nather (moderator), Cruz, Eng, Hoff, Meyer, Steven, Fay** Speeding Up Security Testing Panel
1420-1430	BREAK			
1430-1520	**Charles Schmidt** You're Not Done (Yet) - Turning Securable Apps into Secure Installations using SCAP	**Beef (Schmidt), Wall** ESAPI 2.0 - Defense Against the Dark Arts **Li** OWASP Projects Portal Launch! (5-10 Minutes)	**Srini Penchikala** Messaging Security using GlassFish 3.1 and Open Message Queue	**Leifheit (moderator), Fuchsberger, Kumar, Tychansky, Moretti** Application Security Advisory Board SDLC Panel
1520-1540	COFFEE BREAK			
1540-1630	**Moss, Bartol** Why do developers make these dangerous software errors?	**Ryan Barnett** OWASP CRS and AppSensor Project	**Alex Smolen** Application Security and User Experience	**Gunnar Peterson** Mobile Web Services * *Moved for schedule*
1630-1640	BREAK			
1700-1800	RECAP AND LOOKING AHEAD TO THE NEXT TEN YEARS AND APPSEC USA 2012			

OPEN SOURCE SHOWCASE: Thursday, September 22, 2011

Time	Booth A	Booth B	Booth C	Booth D	Booth E
0920-1300	**Global Projects Committee**	**ModSecurity - Open Source Web Application Firewall** Ryan Barnett	**Armitage: Fast and Easy Hacking for Metasploit** Raphael Mudge	**MozSecWorld** Michael Coates	**w3af demos, Q&A and code walk-through** Andrés Riancho
1300-1640	**Global Projects Committee**	**Vega: Cross-Platform, Open Source Web Application Assessment Platform** David Mirza	**Armitage: Fast and Easy Hacking for Metasploit** Raphael Mudge	**OWASP Broken Web Application Project Demo** Chuck Willis	**OWASP O2 Platform** Dins Cruz

OPEN SOURCE SHOWCASE: Friday, September 23, 2011

Time	Booth A	Booth B	Booth C	Booth D	Booth E
0920-1300	**Global Projects Committee**	**ModSecurity - Open Source Web Application Firewall** Ryan Barnett	**Why not a hack3rs browser?** Gokul C Gopinath	**Visualizing Tracking on the Web** Sid Stamm	**OWASP O2 Platform** Dinis Cruz
1300-1640	**Global Projects Committee**	**Vega: Cross-Platform, Open Source Web Application Assessment Platform** David Mirza	**Why not a hack3rs browser?** Gokul C Gopinath	**Visualizing Tracking on the Web** Sid Stamm	**JavaScript Analysis Platform** Praveen Murthy

DID YOU KNOW?

For the first time, the OWASP Foundation has gathered funding for a program to increase the participation of women in the field of application security. OWASP is using funding to sponsor women from around the United States to attend a one day OWASP AppSec USA 2011 training course and the OWASP AppSec USA 2011 conference talks. The value of this package, which includes travel and lodging, is estimated at $2,500 per grant recipient. We thank **The Wells Fargo Foundation** for generous seed funding of $4,000.

Congratulations to **Tara Wilson** and **Chandni Bhowmik**, the first OWASP Women in AppSec grant recipients for AppSec USA 2011!

MORE EVENTS:

Tuesday, September 20, 2011

Training Check-in and continental breakfast 0730-0830, class 0830-1630
Matt Tesauro Hands on Web Application Testing: Assessing Web Apps the OWASP Way (2-day course)
Erez Metula .NET Secure Coding Practices (2-day course)
Dave Wichers Building Secure Ajax and Web 2.0 Applications (2-day course)
Shreeraj Shah and Amish Shah Analyzing and Securing Enterprise Application Code (2-day course)
Colin Watson Application Attack Detection & Response - A Hands-on Planning Workshop (1-day course)
Dan Cornell Designing, Building, and Testing Secure Applications on Mobile Devices (1-day course)

Wednesday, September 21, 2011

Training Check-in and continental breakfast 0730-0830, class 0830-1630
Matt Tesauro Hands on Web Application Testing: Assessing Web Apps the OWASP Way (2-day course)
Erez Metula .NET Secure Coding Practices (2-day course)
Dave Wichers Building Secure Ajax and Web 2.0 Applications (2-day course)
Shreeraj Shah and Amish Shah Analyzing and Securing Enterprise Application Code (2-day course)
Robert H'obbes' Zakon WebAppSec: Developing Secure Web Applications (1-day course)
Sumit Siddharth The Art of Exploiting SQL Injection (1-day course)

Community Events
University Challenge 1000-1800
ESAPI Summit 0900-1800
Chapters Workshop 1200-1455
AppSensor Summit 0900-1545
5K/10K for Charity badge at 1630-1700, race 1700-1845

Thursday, September 22, 2011

Vendor Showroom 0730-1830
Open Capture the Flag (CTF) room open by 0930, closes no later than 1630
University Challenge Winners Talk 1630-1700
Happy Hour 1700-1800

Friday, September 23, 2011

Vendor Showroom 0730-1630
Open Capture the Flag (CTF) room open by 0930, wrap at 1630

Media coverage from: TECHdotMN, The 451 Group, InfoSecurity

Keynotes

Mark Curphey

It's a homecoming: OWASP AppSec USA 2011's September 22 morning keynote (8:30-9:20) will be OWASP founder Mark Curphey, who will reflect on community.

OWASP Foundation Board Discussion

The OWASP Foundation Board discussion will be held during lunch (12:30-13:30) September 22, 2011. We welcome Jeff Williams (Chair), Tom Brennan, Eoin Keary, Matt Tesauro, Dave Wichers, and incoming board member Michael Coates. ** Sebastien Deleersnyder will not be able to attend due to a scheduling conflict.*

Ira Winkler

The famous real world spy author Ira Winkler will be the September 23 morning keynote (8:30-9:30).

Moxie Marlinspike

Moxie Marlinspike of SSL cracking fame will be keynoting over lunch September 23 (12:30-13:30).

The Talks

Android Security, or This is not the Kind of "Open" I Meant...
Mike Park

Android phones and applications are rapidly gaining market share and becoming more popular. While the availability of multiple Android Markets provides users with greater choice, it also provides attackers more opportunities.

Not only are Android applications plentiful, but the platform and security model means the apps are easy to abuse. This presentation will expose the security issues associated with Android Apps and how attackers take advantage of them. These include the ease with which Android Apps can be reversed, the ability to store sensitive data locally, and how these apps can be trojaned to access personal information on the device.

The presentation will demonstrate the use of various open source tools for reversing Android Apps, as well as the use of the Android SDK features for pen testing, again including techniques and fast demos. Solutions to app and marketplace security will be covered as well.

Application Security Advisory Board SDLC Panel
Glenn Leifheit (moderator), Andreas Fuchsberger, Ajoy Kumar, Richard Tychansky, Alessandro Moretti

Companies are increasingly concerned about the risks to customer data and the potential damage to their reputation should a breach occur, but many are failing to recognize that software remains a significant weak spot in security defenses. Attackers are increasingly targeting the software and applications, rather than the infrastructure or operating system, as a way in to the organization.

The (ISC)²/Creative Intellect Survey on the State of Secure Application Lifecycle management, conducted late last year to understand the impact of security on the software development and delivery process, found that managers are jeopardizing secure software delivery, but they are not alone. This panel will identify who we need to influence in the SDLC process to ensure security is considered at the beginning of the process and discuss five tips for approaching them.

Application Security and User Experience
Alex Smolen

You might think application security and usability are a zero-sum game. Strong password policies, tight access controls, and cycle-burning cryptography improve system security but hamper the user experience. From a security advocate's perspective, it's important to minimize risk, even if it makes a system hard to use. But what if introducing strict security mechanisms actually increases risk? When do security and usability complement, rather than detract from, each other?

No application is solely technical. Systems operate within a social context. People define, build, and use systems, and their needs and capabilities affect the security of a system. Ignoring the users' perspective when evaluating system security neglects an important attack surface - the human-machine interface.

Security mechanisms should be a barrier to attackers, but not for every user in the system. Draconian security measures can actually have the opposite effect of making systems less secure. Users demand more and more usable software, but security departments shouldn't have to compromise. Instead, security mechanisms should be designed with the user and the attacker in mind, so tradeoffs between security and usability can be minimized or avoided entirely.

Application Security Debt & Application Interest Rates
Chris Wysopal

Architects and developers are well aware of the term technical debt but many in the security community have never heard of this concept. Ward Cunningham, a programmer who developed the first wiki program, describes it like this:

"Shipping first time code is like going into debt. A little debt speeds development so long as it is paid back promptly with a rewrite… The danger occurs when the debt is not repaid. Every minute spent on not-quite-right code counts as interest on that debt. Entire engineering organizations can be brought to a stand-still under the debt load of an unconsolidated implementation, object-oriented or otherwise."

The cost of technical debt is the time and money it will take to rewrite the poor code after you ship and bring it back to the quality required to maintain the software over the long haul. Using debt in the financial world costs more absolute dollars than not using debt but it allows financial flexibility to do things you couldn't do without using debt. It's this flexibility that makes debt a valuable business tool. Technical debt allows development teams to meet a ship deadline or get a particular feature out to customers quickly which ultimately serves the business.

Application Security Debt:
We can think of all the latent vulnerabilities in a piece of software as its application security debt. Security debt accumulates over time as more code is written without performing security processes during the development life cycle. A project takes on a lot of debt during the design phase if there is no threat modeling or architecture risk analysis performed. This will translate into costly redesign work at a later date. If code is written without using static analysis or following secure coding guidelines then security bugs are going to get into the final application that will eventually need to be eliminated at a higher cost. The more code that is written this way the more security debt accumulates.

AppSec Inception - Exploiting Software Culture
Jeff Williams

No matter how fast you are at playing vulnerability whack-a-mole, eventually the moles always win. If you truly want to get in front of application security, you have to start looking at changing your software development *culture*. In this talk, Jeff will share experiences with multiple approaches to changing security culture, going back to the late-80's. Not surprisingly, few of these approaches have made any difference. OWASP represents a new approach, and is an interesting experiment in how we change software culture worldwide. Jeff will extract and clarify the lessons from OWASP that you can use in your own organization to bootstrap a software culture that generates security.

Behavioral Security Modeling: Eliminating Vulnerabilities by Building Predictable Systems
John Benninghoff

In addressing the human behavioral aspects of Information Security, we've largely failed as a profession. Historically, we've tried to force people to adapt to the technology we built, and then blame the user when they fail to use it properly – the talking point is, "people are stupid, and you can't fix stupid," or "People should know better," as discussed in a recent SANS ISC Diary posting on CVE-0. (http://isc.sans.org/diary.html?storyid=10933) Security Awareness training, one of the few tools we have to address people problems, has been and continues to be poorly executed. At best, Awareness explains security rules well enough so that we can fire people when they break them, and at worst is a series of posters asking people to "do good things," or tries to make them security experts, with no evidence that it is even effective. Although we have started to improve, our understanding of human/computer interaction (in the security context) is poor, and we do little, if any, to understand the motivation and behavior of both external attackers as well as internal personnel.

Behavioral Information Security, (BIS) A formal methodology to manage information risk, derived from knowledge of how humans behave and interact with information, is a new philosophy of information security that places people in the center of the model, and can be used to design and implement security architectures and controls based on our understanding of people. Borrowing from other professions, BIS seeks to develop practical tools for security practitioners, with the ultimate goal of reducing the cost and improving the effectiveness of information security. This talk will introduce Behavioral Information Security, and Behavioral Security Modeling; a tool developed using BIS principles.

Blackbox Android: Breaking "Enterprise Class" Applications and Secure Containers
Marc Blanchou, Justine Osborne, Mathew Solnik

The Android platform is growing in popularity and is quickly being adopted in the enterprise environment. In order to facilitate this adoption, security solutions have been developed, such as "secure containers" which claim to provide enterprise grade security for Android devices. There is an increasing need to be able to assess the security claims of such "Enterprise Class" Android software vendors. Yet there are very few publicly released auditing tools and little documentation on penetration techniques, especially in the area of reverse engineering and fuzzing. This talk will cover our research into existing blackbox Android application testing methodologies and the new methods we developed. We will also release our custom Android security tools suite. With the help of these tools and techniques we were able to find major vulnerabilities in some of the industry's top "Enterprise Class" Android Applications. During the talk we will walk the audience through the steps we took, the vulnerabilities we found, and how they can do it themselves.

Brakeman and Jenkins: The Duo Detect Defects in Ruby on Rails Code

Justin Collins, Tin Zaw

Ruby on Rails (RoR) is a popular web application development framework with support for Model-View-Controller architecture, "convention over configuration", "don't repeat yourself" or DRY principle, and test-driven development. The framework is designed to be resistant to web security exploits such as cross-site scripting, SQL injection and cross-site request forgery.

Even with built-in protections, it is possible, and often witnessed, that security flaws get introduced in Ruby on Rails code. Brakeman, a static code analyzer for Ruby on Rails code, is designed and developed at AT&T Interactive by Justin Collins to detect such flaws during early phases of development cycle. To further reduce the burden on the developer, Brakeman is integrated into a continuous build and integration server called Jenkins, formerly known as Hudson.

This talk will focus on basics of security features in Rails framework, advantages of using static analysis for discovering security issues, design and development of Brakeman, and how Brakeman and Jenkins are used together at AT&T Interactive to reduce security defects. The only static code analyzer for detecting security defects in Ruby on Rails code, Brakeman is available on GitHub under open source license.

CloudSec 12-Step

Adrian Lane

Do you think cloud security is mainframe computing all over again? Is Azure security just like Windows security? If so, then join me for CloudSec Anonymous, a 12-step program for those of you who want to understand what's different about cloud security. This presentation if for those of you who talk about "The Cloud" and virtualization in the same breath, but have never actually built your own cloud - much less tried to secure it. For many, 'The Cloud' is just software running on someone else's machine, which you access from your browser. Still others only view the cloud as virtualized resources available to the public. Go ahead, admit it: You don't have a Rackspace account and you have never spun up an AMI. Admitting you don't understand the cloud or cloud security is the first step in figuring out how to secure services or securely deploy your applications. Cloud services are differentiated from traditional IT through elastic, self-service, pay as you go computing models. But these characteristics don't provide clues as to how 'The Cloud' changes data and application security. Rather it depends upon the service model, deployment model and platform provider that you choose. In this presentation I'll discuss 12 areas where cloud security differs from traditional models, focusing on platforms and services commonly used for custom web applications. Topics will include:

- Redeployment of data encryption and key management
- Testing and deployment of cloud applications
- Identity management for cloud applications
- PaaS today, gone tomorrow: reliance on API's
- Infrastructure stack management
- Tradeoffs between Platform as a Service and Infrastructure as a Service
- Fundamental security differences between public and private clouds.

ESAPI 2.0 - Defense Against the Dark Arts
Beef (Chris Schmidt), Kevin Wall

In this presentation Chris, joined by Kevin Wall and other members of the ESAPI team will highlight the latest GA release of OWASP Enterprise Security API 2.0. Key touchpoints of the talk will include:

- What is ESAPI
- Integrating Controls
- Crypto Enhancements (Kevin Wall)
- ESAPI Roadmap & Future (ESAPI Dev Team)
- ESAPI Community Launch

What is ESAPI will feature an updated overview of what an Enterprise Security API is, why it is important, and how it is intended to be used. This will be a high-level overview intended to raise questions from you about specifics that can be addressed in the breakout session or over a cold beer.

Integrating Controls will be a brief view into what it actually takes to build and integrate an ESAPI control into a web application. This demo will focus on solving a XSS issue on a small vulnerable web application.

One of the single largest enhancements to ESAPI 2.0 was a complete overhaul of the Crypto component. Kevin Wall drove this initiative from idea to completed project and will be highlighting the hows, whys, and whats of the enhancements.

CYBER THREATS. MOBILITY.
CLOUD. SOCIAL MEDIA.
INTRODUCING MORE THAN JUST
A LITTLE RISK TO YOUR BUSINESS?
HP Enterprise Security has what you need to secure your applications, information and operations. Backed by our unparalleled security research team, we can help you protect your enterprise and identify risks before you even know they exist.
For more information go to
www.hpenterprisesecurity.com.

Ghosts of XSS Past, Present and Future
Jim Manico

This talk will discuss the past methods used for XSS defense that were only partially effective. Learning from these lessons, will will also discuss present day defensive methodologies that are effective, but place an undue burden on the developer. We will then finish with a discussion of future XSS defense methodologies that shift the burden of XSS defense from the developer to various frameworks. These include auto-escaping template technologies, browser-based defenses such as Content Security Policy, and Javascript sandboxes such as the Google CAJA project and JSReg.

The Good Hacker - Dismantling Web Malware
Aditya K Sood, Richard Enbody

The talk sheds light on the new trends of web based malware. Technology and insecurity go hand in hand. With the advent of new attacks and techniques, the distribution of malware through the web has been increased tremendously. Browser Exploit Packs (BEP) (BlackHole, Phoenix, Bleeding Life, etc.) are increasing infections day by day. Most of these BEPs are used in conjunction with botnets such as Zeus and SpyEye to initiate infections across the web. The attackers spread malware elegantly by exploiting the vulnerabilities and drive by downloads. The infection strategies opted by attackers like malware distribution through IFRAME injections, SEO poisoning, URL trickery, social network manipulations, and web vulnerabilities act as a launchpad for web malware. Third generation banking malware such as SpyEye and Zeus has shown devastating artifacts. The question is, how we have to deal with them? Are our protection mechanisms sound enough? Do we need to hunt them back? All the answers will be provided in this talk covering the following points:

- Tracing the malware entry points in-network and hunting them
- Building up methodologies like a hacker to hit back at malware domains
- Analyzing trade and tactics of third generation banking malware
- Demonstrate the static, dynamic and behavioral analysis of web malware including PCAP analytics
- Understanding the design and relevance of Browser Exploit Packs

- Some hidden truths from the underground community
- Real time case studies will be discussed as part of our professional experience

Global Security Report
Charles Henderson

Featuring analysis of more than 220 data breach investigations and more than 2,300 penetration tests conducted by Trustwave's SpiderLabs, the Global Security Report identifies the top vulnerabilities business encountered in the past year as well as a list of strategic initiatives to help your business improve its overall security.

The data gathered from these engagements is substantial and comprehensive. This presentation will be a summary of the results of the analysis of the data gathered during the past year. The results will be presented to cover both technical and business impact analysis.

Gray, the New Black: Gray-Box Web Penetration Testing
Brian Chess, Ph.D.

Penetration testers who use only black-box tools are destined to lose to attackers who are willing to spend more time or effort looking for vulnerabilities. Defenders need to make use of one of the few natural advantages at their disposal: ready access to the system they're trying to protect.

In this talk I will build on previous research around defending running systems and discuss gray-box vulnerability testing techniques that expose web application internals so that testers understand what an application is doing and can spot vulnerabilities faster. The tool observes the program while it executes. It reveals attack surface, points out vulnerable program behavior, opens up a code-level view of the application, and allows a tester to understand information flow inside the program.

Hacking (and Defending) iPhone Applications
Kevin Stadmeyer, Garrett Held

iPhone security is increasingly becoming a news-worthy event. As companies in all industries embrace mobile technology, mobile applications are the hot new technology. Writing iPhone applications presents unique challenges to application developers – and new opportunities to attackers looking to separate users and companies from their hard earned money. Many of the techniques and concerns discussed will also apply to other mobile platforms. This talk will start with the basics - why do we care about mobile security, what the implications are for us as developers and assessors, and how to get your application into a testable state. We will discuss the benefits and negatives of testing on a device vs. testing on an emulator and how each to go down each path.

Hacking .NET (C#) Applications: The Black Arts
Jon McCoy

This talk will focus on attacking the .NET Runtime, Framework DLLs, Security of .NET applications and Security inside of a running .NET application.

Both white hat and black hat hacking will be shown on common security concerns such as intellectual property protection and licensing systems.

Last year I showed how to bend .NET applications and the Runtime. This year I will show how to break the rules of both the application and the Runtime. I will break rules like executing ASM shells and infecting the IL (byte code) of signed and protected EXE/DLLs. This breaking of the rules will make it easy to take out the most hardcore security systems such as USB dongles and network handshakes. I will show some of the Black Arts like making malware and Key-Gens/Cracks. This will take us to the point of also attacking malware and cracks.

I will show how to lock down a application to ensure it has no ability to attack the system it runs on. This will cover what security systems can be used and how to check if they are. Evaluations of what security systems are good/strong and others that are bad/weak, this will also talk about security systems that open vulnerabilities.

How NOT to Implement Cryptography for the OWASP Top 10 (Reloaded)
Anthony J. Stieber

This talk is an update of a talk in 2008 at the OWASP Minneapolis-St.Paul Chapter which was about encryption as it applies to parts of the OWASP Top Ten. The new talk uses fresh examples of application cryptography successes and failures, and also incorporates the new OWASP ESAPI. Audience questions, participation, and contributions are encouraged.

Improve your SDLC with CAPEC and CWE
Ryan Stinson

IT security needs to move from fighting fires to preventing fires. Unfortunately, developer incentives are all about meeting functional requirements and ship dates for their applications. The requirements and methods for developing rugged software have been challenging to articulate and implement; hence they are largely omitted from the development process. Mr. Stinson will show how to avoid making the "Top 25 Most Dangerous Software Errors" with the lessons he has learned from working with various application development teams throughout the SDLC. He will share how organizations can use the Common Attack Pattern Enumeration and Classification (CAPEC) and Common Weakness Enumeration (CWE) to reduce code vulnerabilities and improve their SDLC approaches. He will also provide real-world examples of how organizations can use these tools to set priorities and make practical risk-based decisions. The audience will see real exploitation scenarios that were made possible by the smallest of errors that were a result of translation issues early in the lifecycle but manifested themselves during in-depth application penetration testing.

Introducing the OWASP Zed Attack Proxy
Simon Bennetts

The OWASP Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing as well as experienced pentesters.

A fork of the well regarded Paros Proxy, it was released in September 2010, has been downloaded over 10,000 times and has now been identified by the OWASP Global Projects Committee as a flagship OWASP project. ZAP's functionality includes:

- Intercepting Proxy
- Active scanner
- Passive scanner
- Spider
- Brute Force scanner (using DirBuster code)
- Fuzzer (using JBroFuzz code)
- Port Scanner
- Dynamic SSL certificates
- REST API
- Beanshell integration

Keeping up with the Web-Application Security
Ganesh Devarajan, Todd Redfoot

You read everyday in the news that so and so company got popped using xyz methodology. Go Daddy is the world's largest hosting provider, with data centers across the world, and more than one third of the Internet goes through our servers. We see over 120 million brute force attempts per day, a few thousand DDoS attempts per day and a couple of million web application attacks per day, which we do our best to block straight out of the gate. Most often people enumerate their top 10 or top 20 based on what they have seen or heard about... In this talk I will show you the true numbers behind the various attack types and show which part of the world favors what attack type. I will show graphs and maps of all the common attack types and from where they are originating. I will follow that up with an overview of what we are currently doing to defend against these attacks. Based on all this we have developed our own Internet threat level gauge. Also, we have developed our own Internet Blacklist, which we use in various parts of our network to better protect our devices and our network.

In the second part of the talk I will cover how these vulnerabilities are exploited and what are the most common obfuscation techniques used by the attacker. I will also go over what the attacker's end objective was and what we are doing in order to detect and clean up those compromises. I will also go over various options and tools that domain owners have at their disposal that can help them better secure their sites.

Lessons Learned Building Secure ASP.NET Applications
Tom Fischer

Building more secure web applications which requires realistic goals and practical tools. In the real world of delivering web sites and services capable of passing security audits that often translates into meeting OWASP defined goals with vendor provided tools. After designing, building and enhancing several Microsoft-based applications over the years as consultant I learned a few lessons about delivering more secure web sites and services with OWASP and .NET. This presentation discusses a few of these lessons that will help most Microsoft developers today.

Out of the Box - The ASP.NET API provides several valuable tools which will immediately enhance security. Whether or not they're employed also involves trade-offs. This section discusses some of the more well known tools and their costs.

FxCop - While intended as a tool for enforcing the .NET Framework Design Guidelines, it can help your organization apply both community and custom secure coding guidelines. For example, the latest set rules for Visual Studio supports ASP.NET and its incantation of MVC.

New Technologies, New Opportunities - The recent explosion of tantalizing technologies from Microsoft comes with some new security unknowns. Successfully dealing with them may determine whether or not some of these new technologies, such as, AJAX, Azure, MVC, and LINQ, become the next hot area in security.

Making it in Information Security and Application Security Panel
Rafal Los, Mike McCormick, Christophe Veltsos, Jeff Williams

Information security, and especially application security, is a growing career field. Learn what works, what to avoid, and where to place your bets for the future - from people working in different capacities: a CEO at a consulting firm, a VP of security architecture at a company in a major industry vertical, a strategist at a major IT and solutions provider, and a professor.

Messaging Security using GlassFish 3.1 and Open Message Queue
Srini Penchikala

Open Message Queue is an open source message oriented middleware (MOM) and business integration system that can be used to design and implement reliable and scalable messaging based Java enterprise applications. OpenMQ container also provides an excellent support for securing the messaging applications. The security can be enabled at various levels of the application tier (like broker, destination, message, etc.) which gives the Architects, Developers, and Operations a complete solution to enforce and monitor security throughout the lifecycle of a message without having to install several different software components or services.

This session will cover the security aspects of Open Message Queue container. We will look at how to enable and configure security for various components in the messaging architecture. The discussion includes application security features (Authentication and Authorization) for controlling access to the message broker components as well as how to implement security at a message level using the encryption techniques.

I will explain how to connect to an LDAP data store (OpenDS Directory Server) to perform the user authentication. I will also cover the Message Queue support for the clients to communicate with the broker using secure protocol (HTTPS).

We will briefly look at how to integrate SOAP and Message Queue to process a JMS message containing a SOAP payload, to take advantage of the reliable messaging service offered by Message Queue. In the presentation, I will also discuss the monitoring aspect and how we can use JMX API to monitor and manage various messaging resources such as the Broker, Services, Connections, Destinations, Producers, Consumers and Messages. Open MQ Administration Console as well as the VisualVM plugin for Open Message Queue will be used to demonstrate the monitoring of messaging components.

Mobile Applications Software Assurance
Adam Meyers

Mobile computing has opened a new arena for consumer and enterprise usage. Originally for consumer use, mobile devices are now moving into the enterprise, making security an issue. Driven by consumer demand for features, these devices have few if any security controls, such as security updates, encryption, and perimeter control. Nor does the life cycle of a mobile device include secure removal of malware and control of applications downloaded. Mr. Meyers outlines the steps organizations and their developers need to take to protect their mobile applications from the bad guys. Some of these steps should be quite familiar but many have new wrinkles thanks to the unique characteristics of these small yet powerful devices.

Mobile Web Services
Gunnar Peterson

They're not mobile applications, they're mobile web applications. This distinction is important because some of the most important vulnerabilities of mobile apps are found in the web service layer. This talk explores the weird but crucial area of server side plumbing and shows how to defend your servers.

Next Generation Web Attacks – HTML 5, DOM(L3) and XHR(L2)
Shreeraj Shah

Browsers are escalating their feature set to accommodate new specifications like HTML 5, XHR Level 2 and DOM Level 3. It is forming the backbone of next generation applications running on mobile, PDA devices or desktops. The blend of DOM (Remote Execution stack) , XHR L2 (Sockets for injections) and HTML5 (Exploit delivery platform) is becoming an easy victim for attackers and worms. We have already witnessed these types of attacks on popular sites like Twitter, Facebook and Yahoo. It is of the essence to understand attack surface and vectors to protect next generation applications. We have an enormous expansion of attack surface after inclusion of features like audio/video tags, drag/drop APIs, CSS-Opacity, localstorage, web workers, DOM selectors, Mouse gesturing, native JSON, Cross Site access controls, offline browsing, etc. This extension of attack surface and exposure of server side APIs allow attacker to perform following lethal attacks and abuses.

- XHR abuse with attacking Cross Site access controls using level 2 calls
- JSON manipulations and poisoning
- DOM API injections and script executions
- Abusing HTML5 tag structure and attributes
- Localstorage manipulation and foreign site access
- Attacking client side sandbox architectures
- DOM scrubbing and logical abuse
- Browser hijacking and exploitation through advanced DOM features
- One-way CSRF and abusing vulnerable sites
- DOM event injections and controlling (Click-jacking)
- Hacking widgets, mashups and social networking sites
- Abusing client side Web 2.0 and RIA libraries

We will be covering the above attacks and their variants in detail along with some real life cases and demonstrations.

OWASP Codes of Conduct
Colin Watson

The new OWASP Codes of Conduct are a collection of documents defining a set of minimal requirements for other types organizations specifying what OWASP believes to be the most effective ways they could support OWASP's mission. The Codes were largely developed at working sessions during the OWASP Summit in Portugal earlier this year and their scope includes government bodies, educational institutions, standards groups, trade organizations and certifying bodies. The Codes have now become a formal OWASP project and this presentation will outline the objectives, requirements and future plans for the Codes.

OWASP Mobile Top 10 Risks
Jack Mannino, Zach Lanier, Mike Zusman

This presentation will feature the first public unveiling of the official OWASP Mobile Top 10 Risks. As many agree that mobile application security is in its infancy, this list is intended to help developers and organizations prioritize their security efforts throughout the development life cycle. Many of the same mistakes made over the past decade in other areas of application security have managed to resurface in the mobile world. There have also been many new security challenges introduced by mobile applications and platforms. Through the OWASP Mobile Security Project, the primary goal is to enhance the visibility of mobile security risks just as OWASP has successfully done for the web.

As the attack surface and threat landscape for mobile applications continues to rapidly evolve, arming developers with the tools they need to succeed is essential. Each environment presents very unique and different risks to consider. Our research and findings will be presented from a platform agnostic perspective.

OWASP Projects Portal Launch! (5-10 Minutes)
Jason Li

The OWASP Global Projects Committee (GPC) is launching the new OWASP Projects Portal to manage and promote OWASP projects. The days of searching for project source code, project pages being clobbering by other project pages, and desperately reading pages of project listings to find the relevant project are coming to an end! The GPC has partnered with SourceForge to create individualized project pages, each with their own supporting infrastructure, all under the OWASP banner!

The project infrastructure perfectly complements the new OWASP Project Lifecycle, developed in conjunction with the community to simplify the project workflow and make project management more community driven. The new centralized infrastructure will help OWASP consumers more easily navigate the OWASP project landscape and help OWASP contributors receive the recognition and promotion they deserve for their projects! Come learn about the new features of the OWASP Projects Portal, see some of the projects already migrated to the new infrastructure, and help drive the future of projects at OWASP!

Pure AppSec, No Fillers or Preservatives - OWASP Cheat Sheet Series
Michael Coates

There is a small window of opportunity when someone is looking for the best advice to tackle a security concern. In those 15 seconds OWASP can provide an answer to the proposed question or be left behind for some other site that provides faulty or incomplete security guidance. Enter the OWASP Cheat Sheet series. These documents provide concise and complete security guidance on the most pressing application security topics. From cross site scripting, to SQL injection, to correct TLS usage and design, the cheat sheet series provides actionable information that can be quickly absorbed by the reader. Join us as we discuss the currently available cheat sheet topics, how you can get this information to your developers, and the future of the OWASP cheat sheet series.

Pwning intranets with HTML5

Javier Marcos de Prado, Juan Galiana Lara

A huge proportion of modern software are deployed as Web Applications. Following from this it has not taken attackers very long to migrate their effort into targeting these applications through their common means of access: the web browser. Taking advantage of modern web browsers features can be an important attack vector to break into a secured intranet.

This research is based on how to perform targeted attacks by enumerating internal resources and services belonging to a company's intranet using a client connected to the secure network, even behind a firewall. The attack is initiated by simply visiting a malicious website or exploiting well known web application vulnerabilities like Phishing or Cross-Site Scripting. It relies on web browser features such as HTML5, Websockets, Cross-Origin Resource Sharing and JavaScript, therefore, it will work in the latest version of a full-patched browser.

The presentation shows how far an attacker can get using a maliciously crafted website. For this purpose, several modules were designed and implemented to run on the open source Browser Exploitation Framework (BeEF). They allow an attacker to gather information about the victim's computer, network, and machines or devices in adjacent networks. Using this tool-set an attacker could discover hosts and draw a topology diagram of the network, perform a port scan of a specific host, internal DNS enumeration, basic OS fingerprinting and the ability to locate and exploit targets inside the victim's domain, including services that are not using the HTTP protocol using a technique called inter-protocol exploitation.

These tasks can be performed automatically with the set of modules we will be presenting and shows a clear example of how the tools can be weaponized and used by real targeted attacks, also known as Advanced Persistent Threats (APT), like Operation Aurora or the Apache.org attack.

Secure Programming Support in IDE

Dr. Bill Chu, Jing Xie

Many of today's application security vulnerabilities are introduced by software developers writing insecure code. The OWASP community has already reached a consensus that developers do not write secure code for all kinds of reasons. We believe a lack of understanding of secure programming practices and developers' lapses of attention on security account for the top ones.

Much work, from both academia and industry including OWASP, on software/application security has focused on detecting software vulnerabilities through automated analysis techniques. While they are effective, we believe they are not sufficient. Tools that embody this approach tend to be used to find vulnerabilities at the end of the development lifecycle; thus, other business priorities may take precedence. Moreover, using such tools often requires some security expertise and can be costly. Additionally, if programmers are removed from this analysis process, these tools will also not help prevent them from continuing to write insecure code.

Expecting the majority of developers to proactively adopt secure coding practices is risky. Developers prioritize security at level six among all other software development focuses according to John Wilander's recent survey on more than 200 developers (). Swamped with all activities involved by the other development focuses and constrained by human inertia characteristics such as bounded rationality, developers rarely have the spare time and energy to attend to the activities required by producing high security quality applications. What is worse, without comprehensive understanding of how, where and when to use the given security technology, developers may introduce unwanted and unintended errors that may eventually turn to be security vulnerabilities when incorporating it to their development.

We use a case study to illustrate the practical benefits of integrating ESAPI with ASIDE to push secure coding knowledge and concrete best practices into developers' minds instead of relying on developers pulling them out from the application security sphere. More specifically, we use the IDE as a medium to direct developers when to use ESAPI, where to use ESAPI, which ESAPI API to use, how to use ESAPI, and how to use ESAPI in a correct way.

Security Evolution - Bug Bounty Programs for Web Applications
Michael Coates

It's all about scale; how can an organization possibly keep up with a growing number of web applications, features, and supported capabilities with a limited security team? One option that has provided successful results for several companies is a bug bounty program. These programs successfully engage the world community and bring many eyes towards the common good.

This talk will discuss the benefits and risks of a bounty program for web applications. What types of organizations consider starting a bounty? How would an organization start such a program and what should they expect? Is the return worth the effort? How does such a program compete with the black market?

In addition to these topics, we will also discuss the progress, metrics and lessons learned from the Mozilla web application bounty that was launched in December 2010.

The Self Healing Cloud: Protecting Applications and Infrastructure with Automated Virtual Patching
Dan Cornell

Organizations often have to deploy arbitrary applications on their infrastructure without thorough security testing. These applications can contain serious security vulnerabilities that can be detected and exploited remotely and in an automated manner. The applications themselves and the infrastructure they are deployed on are then at risk of exploitation. Configuration changes or vendor-provided software updates and patches are typically used to address infrastructure vulnerabilities. However, application-level vulnerabilities often require coding changes to be fully addressed.

Virtual patching is a technique where targeted rules are created for web application firewalls (WAFs) or other IDS/IPS technologies to help mitigate specific known application vulnerabilities. This allows applications to be &virtually& patched prior to actual code-level patches being applied. These virtual patches are most often applicable to vulnerabilities that have a strong detection signature such as SQL injection and cross-site scripting (XSS) because the detection rules can be targeted to detect these signatures, but limited only to specific parts of the application attack surface where the application is known to be vulnerable.

Simplifying Threat Modeling
Mike Ware

Is threat modeling too tough to produce actionable results? Is it too overbearing on resources? Does it demand too much documentation?

Architects and developers often perceive threat modeling as being too difficult, heavy on documentation, and costly to both produce an initial threat model from a clean slate and to maintain it as the system evolves. During this talk, we'll attempt to bust these myths and show how organizations can incrementally obtain better results over time while making threat modeling "seem easy."

How does one simplify threat modeling? By removing the fluff and following 5-10 steps designed to produce 3 simple "security views" which architects, developers, and testers can act on: misuse/abuse view, asset flow view, and attack surface view. We'll explain how organizations just getting started with threat modeling can leverage or enhance SDLC artifacts they already produce to illuminate these security views. We'll also explain where these security views should be produced within a typical SDLC and who should create them. Finally, we'll describe how these security views are used to develop a threat matrix which describes who your threats are, where they might attack, what they will go after, and how they will do it.

Six Key Metrics: A look at the future of AppSec
Arian Evans

This presentation covers real-world key performance indicators (KPIs) necessary to create and sustain a successful, trustworthy, and scalable application security program in the enterprise. This presentation will overview

1. The 2011 threat landscape from public forensic data
2. The 2011 vulnerability landscape and stats
3. The 2011 attacker profiles (from supporting stats)
4. The challenges surrounding existing standards, programs, and metrics
5. Keep it simple approach to quantitative and qualitative metrics
6. Six Appsec KPIs broken down into two categories:
    - Risk Analysis metrics – how to Qualify quantitative vulnerability data
    - Appsec Program metrics – how to Quantify appsec program success

Scaling: Initial results from "How to scale web application security" survey, OWASP Summit Portugal, and feedback from OWASP Europe

- Additional KPIs and program metrics suggested from OWASP summit scaling roundtable

This presentation won't have any sexy zero-days or product demos, but it will include sexy pictures, charts, ideas, and a sexy speaker.

Software Assurance Automation throughout the Lifecycle
Richard Struse

Over the past decade, software developers have been regularly prodded to write more secure code. While lists of common software weaknesses such as the OWASP Top Ten and the CWE/SANS Top Twenty Five are a good start, there is a clear need for tools, languages and repositories to help stem the tide of vulnerable code. Given the extraordinarily diverse landscape of software development languages, methodologies and tool sets, it is critical to have standards-based solutions that everyone can leverage. This presentation will provide an overview of the languages, enumerations and repositories that support and enable the automation of software assurance, with specific emphasis on practical applications that can improve software security today.

Sticking to the Facts: Scientific Study of Static Analysis Tools
Chuck Willis, Kris Britton

The National Security Agency's Center for Assured Software (CAS) researches tools and techniques that can be used throughout the development lifecycle to evaluate and improve the assurance of software and to avoid and eliminate exploitable vulnerabilities. Over the past two years, the CAS has extensively and scientifically studied commercial and open source static analysis tools for C, C++, and Java. The purpose of this research is to determine the strengths and limitations of modern static analysis tools with respect to the flaws they identify, the flaws they miss, and the false positives they report. This presentation will describe the CAS's most recent study of commonly used static analysis tools and include details on the test cases, methodology, and analysis techniques used. It will cover the study's conclusions, aggregate results, and trending information from previous studies, and also provide guidance for those using or considering static analysis tools.

SwA and the Cloud - Counting the Risks
Andy Murren

As organizations move to Cloud Computing the types and management of business risks changes. Measuring and assessing these risks presents a unique set of challenges. This presentation will cover the basic Cloud Computing service models and examine some business risks the resulting measurement and assessment methods organizations need to address.

- What is the impact on the organization's risk exposure and responsibilities?

- Are some of the risks associated with insecure design, code, and system configuration actually decreased or just transferred to other organizations?
- What steps should the organization take to reasonably manage those risks?
- Understand features of different Cloud Computing environments
- Integrate Cloud specific considerations into their SDLC and software management governance model
- How QA and Test professionals should consider extending their roles to better address "reliability, resilience, robustness, and security."

Threat Modeling in the Cloud: What You Don't Know Will Hurt You!
Scott Matsumoto

When you deploy your application in the Cloud, how do you know whether you've introduced vulnerabilities that do not exist in your current deployment model? If you wait until you are about to deploy, that's too late. Threat Modeling is a critical activity for identifying such vulnerabilities early in the development process. Proper threat modeling requires the identification of application's assets, security controls and attackers. For applications based on Amazon Web Services (AWS), there are subtle differences in the security controls provided by AWS when compared to more traditional data center hosted applications. These differences manifest themselves beyond the definitions of the security controls themselves; they also affect the application's overall structure and the design patterns required to create a secure application. This talk first discusses the security controls in the AWS components: EC2, S3, EBS and SQS. It then describes how to build a threat model for an application built using these components. This talk does assume some familiarity with the AWS components, common web application design patterns and web application vulnerabilities; although in depth knowledge of these topics is not required.

Software Security: Is OK Good Enough?
John B. Dickson, CISSP

Widely publicized breaches regularly occur involving insecure software. This is due to the fact that the vast majority of software in use today was not designed to withstand attacks encountered when deployed on hostile networks such as the Internet. What limited vulnerability statistics that exist confirm that most modern software includes coding flaws and design errors that put sensitive customer data at risk. Unfortunately, security officers and software project owners still struggle to justify investment to build secure software. Initial efforts to build justification models have not been embraced beyond the most security conscious organizations. Concepts like the "Rugged Software" are gaining traction, but have yet to make a deep impact. How does an organization – short of a breach – justify expending critical resources to build more secure software? Is it realistic to believe that an industry-driven solution such as the Payment Card Industry's Data Security Standard (PCI-DSS) can drive secure software investment before headlines prompt government to demand top-down regulation to "fix" the security of software?

This presentation will attempt to characterize the current landscape of software security from the perspective of a practitioner who regularly works with Fortune 500 chief security officers to build business cases for software security initiatives. Given the current status of software security efforts, and the struggles for business justification, industry would be well-served to look further afield to other competing models to identify future justification efforts. There is still much that can be learned from models outside the security and information technology fields. For example, the history of food safety provides lessons that the software security industry can draw from when developing justification models. We can also learn from building code adoption by earthquake-prone

communities and draw comparisons to communities that have less rigorous building codes. Finally, we can learn much from certain financial regulations that have or have not improved confidence in our financial system.

Speeding Up Security Testing Panel

Wendy Nather (moderator), Dinis Cruz, Chris Eng, Jerry Hoff, Darren Meyer, John Steven, Sean Fay

Dynamic and static analysis practices are converging quickly. Now how will organizations speed up security testing to make a compelling case for security/quality investment? Wendy Nather, who provides analysis on the current state of security in her position at The 451 Group, will moderate what is sure to be an entertaining panel with some of the sharpest researchers in this area.

STAAF: An Efficient Distributed Framework for Performing Large-Scale Android Application Analysis

Ryan W Smith

There has been no shortage of Android malware analysis reports recently, but thus far that trend has not been accompanied with an equivalent scale of released public Android application tools or frameworks. To address this issue, we are presenting the Scalable Tailored Application Analysis Framework (STAAF), released as a new OWASP project for public use under Apache License 2.0. The goal of this framework is to allow a team of one or more analysts to efficiently analyze a large number of Android applications. In addition to large scale analysis, the framework aims to promote collaborative analysis through shared processing and results.

Our framework is designed using a modular and distributed approach, which allows each processing node to be highly tailored for a particular task. At the heart of the framework is the Resource Manager (RM) module, which is responsible for tracking samples, managing analysis modules, and storing results. The RM also serves to reduce processing time and data management through the deduplication of data and work, and it also aids with the scheduling of tasks so that they can be completed as a pipeline or as a single unit. When processing begins, the RM uses several default “primitive” modules that carry out the fundamental operations, such as extracting the manifest, transforming the Dalvik bytecode, and extracting application resources. The analysis modules then use the raw results to extract specific attributes such as permissions, receivers, invoked methods, external resources accessed, control flow graphs, etc., and these results are then stored in a distributed data store, after which the information can be queried for high level trends or targeted searches.

OWASP CRS and AppSensor Project
Ryan Barnett

This talk will build on the working session of the OWASP AppSensor project working session at AppSecUSA and additional insight from the open-source showcase and provide a hands on view of https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project

Testing from the Cloud: Is the Sky Falling?
Matt Tesauro

More and more IT is being moved to the cloud, why shouldn't your testing move there too? This talk will cover what it takes to take your testing tools from your laptop to the cloud using new features of the OWASP Web Testing Environment (WTE). WTE allows you to create custom installations of application security tools in the cloud on demand. Has your IP been shunned? No problem, kill that cloud instance and startup another. Is your life as mobile as your phone? No problem, a laptop + Internet = access to all your favorite tools from anywhere. Multiple clients? No problem, start an instance for each one. By the end of this talk, you'll know all you need to fire up an cloud instance with all of your favorite tools and start having fun.

Top Ten Risks with Cloud that will keep you Awake at Night
Shankar Babu Chebrolu, PhD, CISSP

Against the backdrop of new economic realities, one of the larger forces that is affecting businesses worldwide is cloud computing, whose benefits include agility, time to market, time to capability and reduced cost. Cloud computing is already transforming the majority of the IT industry into services oriented IT organizations or simply IT as a Service (ITaaS), changing the way how solutions and services are designed and purchased. IT spending related to cloud adoption is projected to reach $42.2 B in 2012. Recently, US Federal CIO, Vivek Kundra, announced a major push towards Cloud to lower the cost of IT operations and drive innovations for US government.

However, there are many challenges that come along with cloud concept, biggest of them being security including trust, privacy, data ownership and control, availability, compliance and legal challenges. As borderless enterprises grow more reliant on cloud based solutions and services, data no longer resides within the physical premises of the enterprise creating ineffective network boundary controls. This shift demonstrates the need for data centric security models and extends trust boundaries with the cloud providers. Security is the top concern for cloud adoption and expectations from the security staff are all time high to apply a defense-in-depth strategy to protect enterprises, thus giving them sleepless nights.

In this presentation, Cisco infosec professional Shankar Babu Chebrolu will share the security challenges faced with cloud adoption at Cisco and other large enterprises. Shankar Babu Chebrolu has evaluated multiple cloud vendors for security and privacy risks and has also worked on the OWASP Cloud Top Ten Security Risks initiative describing risks faced with Cloud computing and XaaS models.

• Application Security • Enterprise Security • Penetration Testing
• Vulnerability Research • Exploit Development • Malware Analysis • Training
ACCUVANT LABS
Security Assessment and Research
......Proud to Sponsor OWASP 2011
www.accuvant.com

Web Application Security Payloads
Andrés Riancho

Web Application Payloads are the evolution of old school system call payloads which are used in memory corruption exploits since the 70's. The basic problem solved by any payload is pretty simple: "I have *access*, what now?". In memory corruption exploits it's pretty easy to perform any specific task because after successful exploitation the attacker is able to control the CPU / memory and execute arbitrary system calls in order to create a new user or run an arbitrary command; but in the Web Application field, the attacker is restricted to the "system calls" that the vulnerable Web Application exposes:

- Local File Read - read()
- OS Commanding - exec()
- SQL Injection - read(), write() and possibly exec()

Web Application Payloads are small pieces of code that are run in the attackers box, and then translated by the Web application exploit to a combination of GET and POST requests to be sent to the remote web-server.

This talk will introduce attendees to the subject and show a working implementation of Web Application Payloads that uses the "system calls" exposed by vulnerable Web Applications to collect information from, and gain access to the remote Web server.

Our greatest achievement regarding web application payloads is the possibility of automatically downloading the remote application's source code, statically analyzing it to identify more vulnerabilities, and exploit those new vulnerabiliies to keep escalating privileges in the remote system.

When Zombies Attack - a Tracking Love Story
Ashkan Soltani, Gerrit Padgham

Online privacy and behavioral profiling are of growing concern among both consumers and government regulators. Consumers use the web for a variety of business and personal activities, including things that they would prefer to keep private. Mobile devices introduce additional concerns as typically, they are carried with us nearly everywhere we go. The "always on" nature of these systems closely mirror the activity of their owners, thereby revealing a historical trail of online and offline activities to multiple unknown third parties.

In this talk, we will present the current state of online tracking and highlight current practices such as "cookie respawning" and non-cookie based tracking that popular websites and mobile applications engage in. We will discuss theories on why the platforms we use do not adequately protect users from these threats and highlight the proposed solutions, such as additional transparency tools and Do-Not-Track that are intended to help mitigate these issues. We will also demonstrate MobileScope, a technical solution we have been developing to give the end user ultimate visibility into the traffic their device is sending. Finally, we will discuss open questions surrounding the ability to adequately assess risk drawing from behavioral economics and risk management theories for cues as to potential outcomes in this space.

Why do developers make these dangerous software errors?
Michelle Moss, Nadya Bartol

According to the US Computer Emergency Readiness Team (US-CERT), most successful cyber-attacks result from targeting and exploiting software vulnerabilities, a significant number of which are introduced during software design, development, and sustainment phases of the lifecycle. Today's software modules and hardware components are created and assembled globally, and delivered physically and/or virtually. Unfortunately, many organizations do not understand the likelihood of a software vulnerability being exploited and the impact it could have on the organization's critical functions or business relationships. As a result, it is more challenging for security professionals to ensure the integrity, confidentiality, and availability of high-value data crucial to mission and business functions. It is understandable that IT security organizations struggle to justify funding, assign responsibly, and measure progress for application security. This presentation will provide insight to engaged appropriate stakeholders to address the technical, management, and operational aspects of incorporating software assurance into the IT lifecycle.

You're Not Done (Yet) – Turning Securable Apps into Secure Installations using SCAP
Charles Schmidt

Secure software engineering practices get a great deal of attention today and deservedly so – they form a foundation without which effective security becomes impossible. However, this is not the end of a developer's part in supporting application security. Even the best software development methodology will only be able to make application security a possibility. To have a truly secure application, the end user or sysadmin must install and configure it and its dependencies correctly. Doing this requires that good security configuration practices be conveyed from the application developer to the end user in a format the user can utilize. While often neglected, this aspect of application security is what turns security theater into practical security that has a real benefit

for enterprises and end users. This presentation gives the developer a roadmap on how to use the Security Content Automation Protocol (SCAP) suite of standards to ensure that their applications are correctly installed and configured.

The OWASP AppSec USA 2011 team was happy to receive assistance from the U.S. Department of Homeland Security on the Software Assurance track.

About the Track:

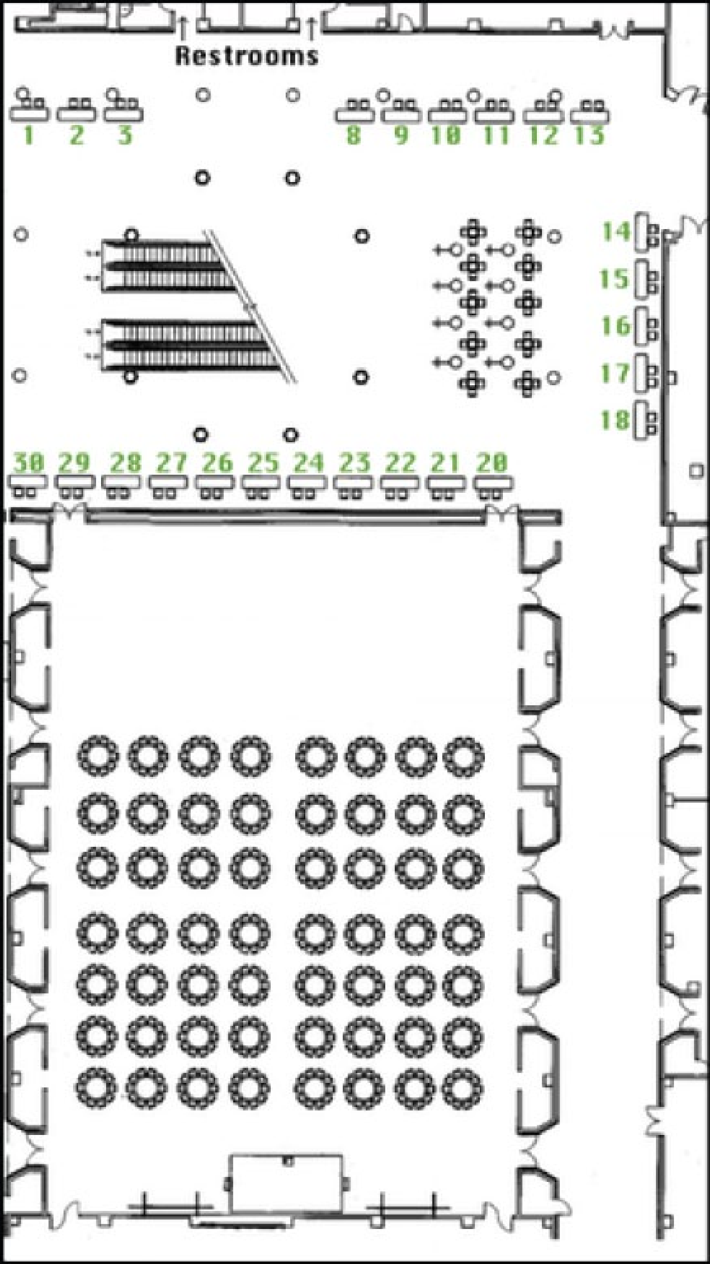
Preventing Zero-Day Attacks with Software Assurance (SwA) and Automation It is estimated that 90 percent of reported security incidents result from exploits against defects in the design or implementation of software. Vulnerabilities in software can jeopardize intellectual property, consumer trust, and business operations and services. Additionally, a broad spectrum of critical applications and infrastructure, from process control systems to commercial application products, depend on secure, reliable software. In order to ensure system reliability, integrity, and safety, it is critical to address security throughout the software lifecycle.

The presentations will look at how leading organizations from both the public and private sectors are leveraging software assurance techniques and tools to quantify and fundamentally improve the security and reliability of systems. Developers will gain insights into practical techniques that they can use today to enhance the security and reliability of the software that they build. In addition, the speakers will demonstrate how organizations can use processes and tools to set priorities and make practical risk-based security decisions.

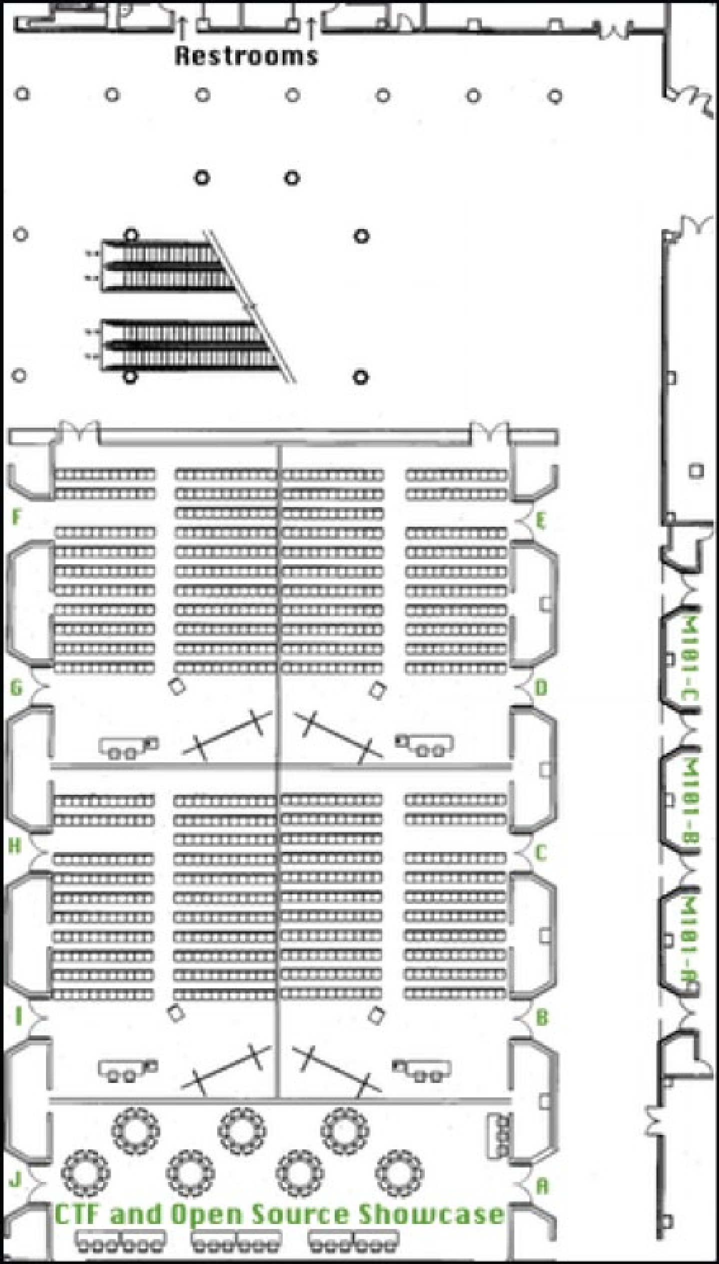
Vendor Booth Numbers:

1	Imperva
2	Fishnet Security
3	ISC(2)
8	Qualys
9	Cigital
10	Veracode
11	Radware
12	Barracuda
13	Accuvant
14	Fortify
15	ISSA
16	WhiteHat
17 & 18	Trustwave
20 & 21	Security Innovation
22	Core Security
23	Rapid 7
24	Aspect Security
25	NTObjectives
26	OWASP Book Store
27	Intrepidus Group
28	F5
29	IBM
30	NetSpi

MCC Lower Level (L100): Sponsor Booths, Keynotes, and Food



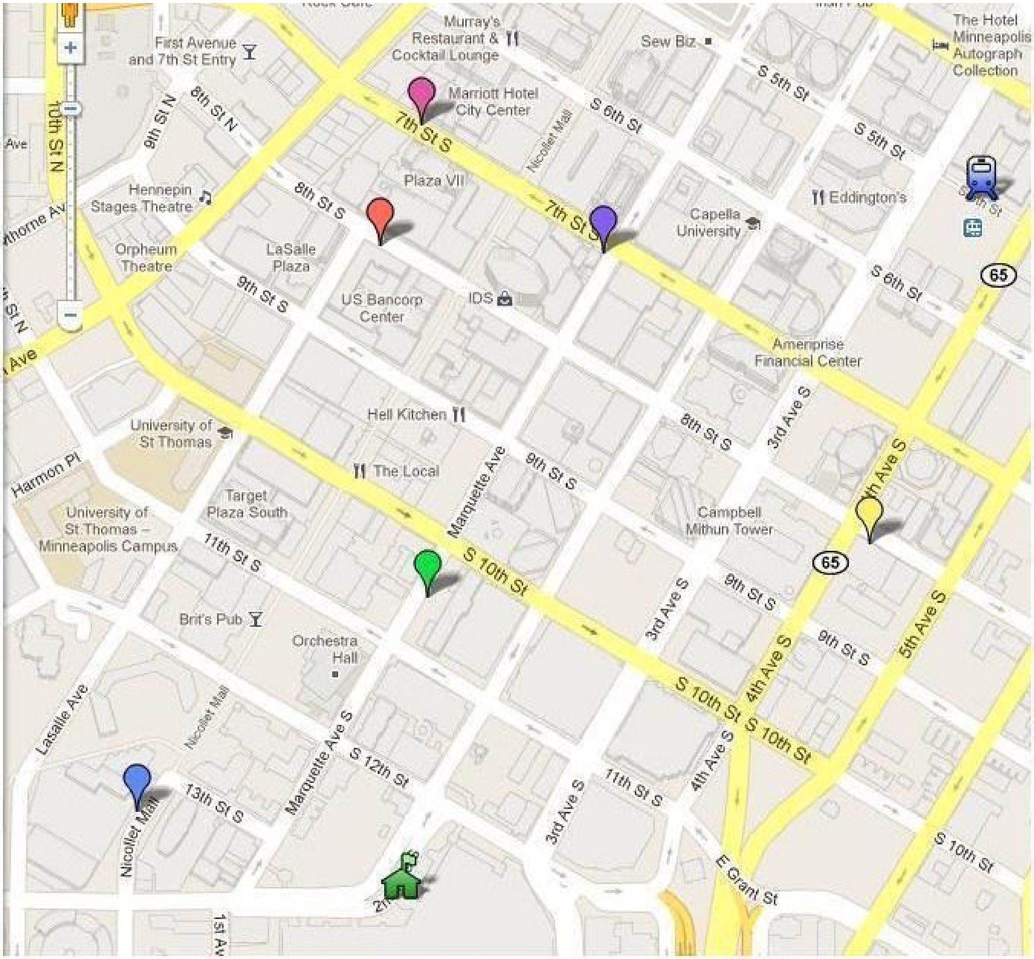
MCC Mezzanine Level (M100 & M101): Track Rooms, CTF, and Open Source Showcase



Downtown Minneapolis

OWASP AppSec USA 2011
Downtown Minneapolis

- Government Plaza Lightrail Station
  350 S 5th St Minneapolis, MN 55415-1371
- Minneapolis Convention Center
  1301 2nd Ave S
  Minneapolis, Minnesota 55403
  (612) 335-6000
- Best Western Plus Normandy Inn
  405 S 8th St
  Minneapolis, MN 55404-1026
  (612) 370-1400
- Hilton Hotel Minneapolis
  1001 Marquette Avenue South
  Minneapolis, MN 55403
  (612) 376-1000
- Hilton: The Marquette Hotel
  710 Marquette Avenue South
  Minneapolis, MN 55402
  (612) 333-4545
- Hyatt Regency (Minneapolis)
  1300 Nicollet Mall
  Minneapolis, MN 55403
  (612) 370-1234
- Mariott City Center
  30 South 7th Street
  Minneapolis, MN 55402
  (612) 349-4000
- Residence Inn
  45 South Eighth Street
  Minneapolis, MN 55402
  (612) 677-1000



From Airport to Downtown Minneapolis

OWASP AppSec USA 2011

Airport, Bloomington Hyatt and Mall of America to Downtown Minneapolis

MSP International Airport
4300 Glumack Dr
St Paul, Minnesota 55111-3010
(612) 726-5141

Minneapolis Convention Center
1301 2nd Ave S
Minneapolis, Minnesota 55403
(612) 335-6000

Hyatt Place Hotel (Bloomington)
7800 International Drive
Bloomington, MN 55425
(952) 854-0700

Light Rail

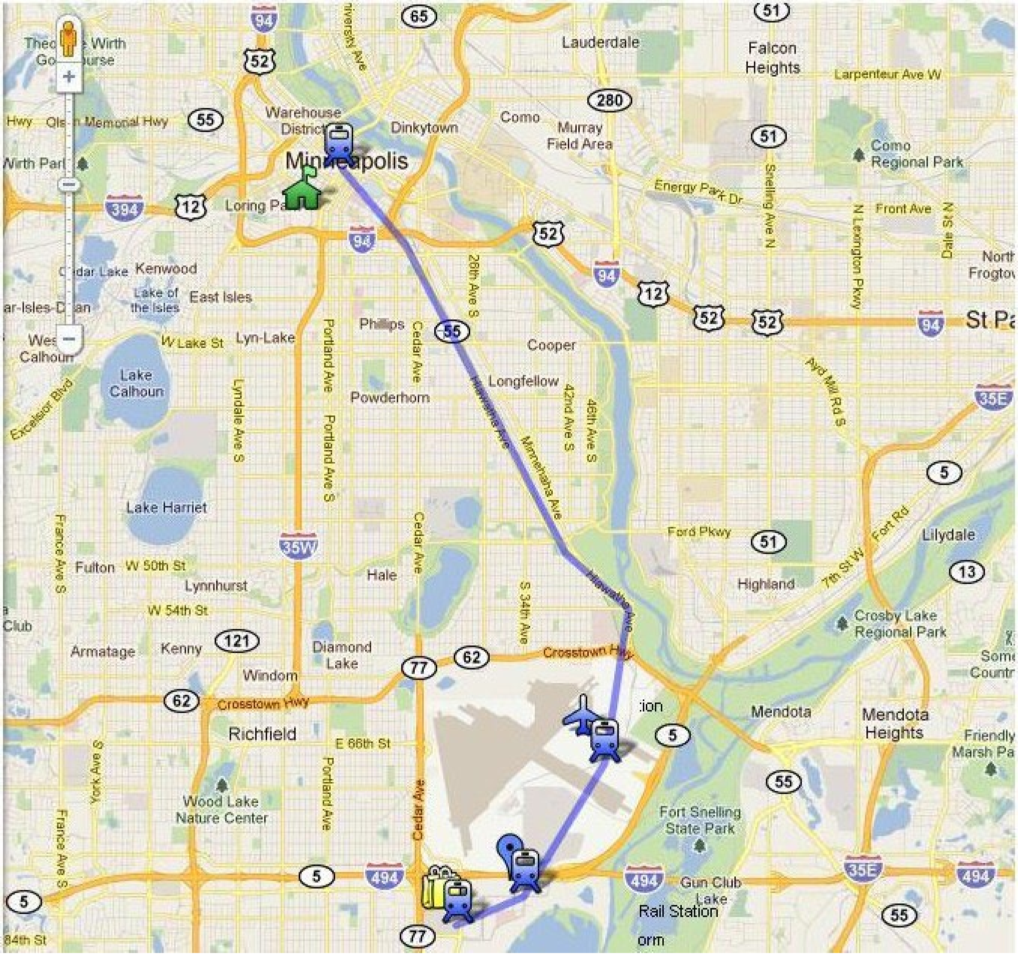
Lindbergh Station & Platform
MSP International Airport and
Lindbergh Station & Platform

Bloomington Light Rail Station
34th Ave & American BLVD
Bloomington, MN 55425

Government Plaza Lightrail Station
350 S 5th St
Minneapolis, MN 55415-1371

MOA Transit Station & Platform
Mall of America Transit Station & Platform

Mall of America (MOA)
60 East Brodway
Bloomington, MN 55425
(952) 883-8800



Platinum Sponsors:

Security Innovation is a leading organization specializing in application security products and services that are designed to build secure systems for Fortune 1000 organizations that focus on building security into every phase of the software development cycle (SDLC), dramatically reducing software vulnerabilities. http://securityinovation.com

Trustwave is a leading provider of information security and compliance management solutions to businesses and government entities throughout the world. Trustwave has helped thousands of organizations manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout the world. For more information, visit https://www.trustwave.com

Gold Sponsors:

IBM Security Solutions include an extensive portfolio of hardware, software solutions, professional and managed services offerings covering the spectrum of IT and business security risks. Through world-class solutions that address risk across the enterprise, IBM helps organizations reduce costs, improve service, and manage risk. Visit us at ibm.com/security

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. http://veracode.com

HP is a leading provider of security and compliance solutions for modern enterprises that want to mitigate risk in their hybrid environments and defend against advanced threats. Based on market leading products from ArcSight, Fortify, and TippingPoint, the HP Security Intelligence and Risk Management (SIRM) Platform uniquely delivers the advanced correlation, application protection, and network defense technology to protect today's applications and IT infrastructures from sophisticated cyber threats.   Visit HP Enterprise Security at: www.hpenterprisesecurity.com.

NetSPI is a privately held information-security consulting company, founded in 2001. The company provides advisory, assessment, and audit services designed to analyze and mitigate risks and ensure compliance with laws and industry standards. Clients include financial firms, retailers, hospitals, educational institutions, and energy companies. More information is available at www.netspi.com.

Qualys is the leading provider performs over 500 million IP audits per year, providing customers an of Software-as-a-Service IT security risk and compliance management solutions. QualysGuard® is used by more than 5,000 organizations, including 45 of the Fortune 100, and immediate, continuous view of their security and compliance postures. www.qualys.com

Silver Sponsors:

As thought leaders in software security consulting since 1992, Cigital helps companies design, build, and maintain secure software. Our recognized experts apply a combination of proven methodologies, tools, and best practices to meet each client's unique requirements. Cigital is headquartered outside Washington, D.C., with regional offices in U.S., Europe, and India. www.cigital.com

Core Security enables organizations to get ahead of threats with security test and measurement solutions that continuously identify and prove real-world exposures to their most critical assets. Our customers gain real visibility into their security standing, real validation of their security controls, and real metrics for more effective information security. www.coresecurity.com

Imperva is a pioneer and leader of data security solutions for high-value business data. Imperva Web Application Security solutions protect Web applications from online attacks-- by continuously adapting to evolving threats and enabling security professionals, network managers, and application developers to mitigate the risk of a data breach and address compliance requirements. www.imperva.com

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes protection against email, web, IM threats, and solutions that improve application delivery and network access, message archiving, backup and data protection. www.baraudanetworks.com

Accuvant is the only research-driven information security partner delivering alignment between IT security and business objectives, clarity to complex security challenges and confidence in complex security decisions. Accuvant delivers these solutions through three practice areas: Risk and Compliance Management, Accuvant LABS and Solution Services. Based on our clients' unique requirements, Accuvant assesses, architects and implements the policies, procedures and technologies that most efficiently and effectively protect valuable data assets. www.accuvant.com

Radware, a global leader in integrated application delivery and application security solutions, assures the full availability, maximum performance, and complete security of business-critical applications for 10,000 enterprises and carriers worldwide. Radware's full suite of attack mitigation technologies include: intrusion prevention, WAF, DoS protection, network behavioral analysis, and reputation preservation capabilities. www.radware.com

WhiteHat Security is the leading provider of website risk management solutions that protect critical data, ensure compliance and narrow the window of risk. WhiteHat Sentinel, the company's flagship product family, is the most accurate and cost-effective website vulnerability management solution available, delivering the visibility, flexibility, and control that organizations need to prevent website attacks. www.whitehatsec.com.

Rapid7® is the leading provider of security risk intelligence solutions. Rapid7's integrated vulnerability management and penetration testing products, NeXpose® and Metasploit®, empower organizations to obtain accurate, actionable and contextual intelligence into their threat and risk posture. Rapid7's solutions are being used by more than 1,600 enterprises and government agencies, while the Company's free products are downloaded more than one million times per year and enhanced further by over 125,000 security community users and contributors. www.rapid7.com

Silver Sponsors:

Aspect Security specializes exclusively in application security services including code review, penetration testing, developer training, elearning, and appsec program consulting to many of the most security conscious commercial and government organizations. Aspect is active at OWASP and is responsible for many influential projects, such as WebGoat, ASVS, ESAPI, and Top Ten. www.aspectsecurity.com

Committed to security excellence, FishNet Security is the #1 provider of information security solutions that combine technology, services, support, and training. FishNet Security solutions have enabled 5,000 clients to better manage risk, meet compliance requirements, and reduce cost while maximizing security effectiveness and operational efficiency. For more information on FishNet Security, Inc., visit www.fishnetsecurity.com

Intrepidus Group is a leading provider of mobile application and device security services. We assess iPhone, Android, and Blackberry applications, train developers to code defensively and evaluate security mechanisms of cutting edge telecommunications products and smart phone devices. We serve start-ups developing mobile applications to the world's largest telecommunications providers. www.intrepidusgroup.com

NT OBJECTives (NTO brings together an innovative collection of top experts in information security to provide a comprehensive suite of technologies and services to solve today's toughest application security challenges. NTO solutions are well-known as the most comprehensive and accurate Web Application security solutions available. For more information visit www.ntobjectives.com.

About OWASP

The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

Notes:

Notes:

Notes: