AGENDA

March 1st

ISSA DV

3/1/2013

Verizon
8 Neshaminy Interplex
Suite 300 (3rd Floor)
Trevose, Pa

9:00 – 9:45	**Mark Wireman** ***OpenSky Corporation***	**“Mobile Application Security.”**
9:45 – 10:00	**BREAK**	
10:00 – 11:00	**Tom McKnight ,** ***Solutions Architect*** ***Veracode***	**"Tips for Building a Successful Application Security Program".**
11:00 – 12:00	**Jack Walsh,** ***Mobility Program Manager*** ***ICSA Labs.***	**“Testing Your Mobile Apps”**
12:00 – 1:00	**Lunch**	
1:00 – 1:30	**Dr. Xiao-Jiang Du(James) Associate Professor Dept. of Computer and Information Sciences Temple University**	**Temple University**
1:30 – 2:30	**Andrew Gavin,** ***Executive Consultant*** ***Verizon Enterprise Services*** ***Global Consulting & Integration Services***	**“Application Security in the mobile and cloud computing environments”**

2:30 – 3:30	**Michael Piscopo,** ***Director of Technical Consulting Services with Allied InfoSecurity, Inc.***	**"Defending the Web! A Hacking Perspective"**
3:30 – 3:45	**Break**	
3:15 - 4:15	**Steven C. Markey** ***nControl, LLC***	**TBA**

Profiles

Mark Wireman

Practice Lead, Application Security
OpenSky Corporation

* Software Assurance Assessment - reviews current state of software development, security awareness, security training, frameworks, gates, etc. Provides a score based on CMMI using the open SAMM, BSIMM-2, and other rating methodologies
* Secure Software Development - Software Assurance plus implementation of controls identified as missing as part of the SwA assessment: also includes tools and technologies recommendation, installation, and training as needed.
* 3rd Party Risk Assessment (Software) - reviews current processes related to acquisition, implementation, and remediation of 3rd party components. Also reviews current contracts to identify gaps both in language to protect organization and organization's processes, i.e., if organization has the right to scan make sure organization is scanning the 3rd party.
* Static Code and Dynamic Scanning - Within either the Development or QA cycle, scan identified applications and assist organization with understanding the results and remediation efforts. If organization has a GRC product, feed the results and track remediation through the GRC appliance.

Jack Walsh

Mobility Program Manager
ICSA Labs, an independent division of Verizon

BIO

Jack has worked fourteen years at ICSA Labs. Currently managing new initiatives including all things mobile, Jack's prior roles included network IPS program manager, anti-spam program manager, and firewall lab technical lead. Prior to joining ICSA Labs, Jack tested products at the National Security Agency. While there he co-authored the first Firewall Protection Profile. Jack earned his B.S. in Electrical Engineering from Penn State and later earned an M.S. in Computer Science from Johns Hopkins.

Tom McKnight
BIO

Software Security Professional
Greater New York City Area
| Computer & Network Security

Current	Veracode
Previous	HP, Fortify Software, Inc., Secure Software, Inc.

ABSTRACT

Find out what works to reduce risk in applications. It's not just about your internal developers writing secure code or pen testers hacking away at your apps. I will share some statistics and trends around the state of software security and the best ways to address the threat. What are the most mature organizations doing in application security? The tips, techniques, and strategies presented here are gleaned from the experience of Veracode scanning over 130 billion lines of code and working with some of the world's largest companies.

Andrew Gavin

BIO

Andrew Gavin is an information security executive consultant at Verizon, and he has more than 13 years of experience in security assessments of networks and applications. He has consulted for numerous customers across various industries on six continents. He is the creator of the free and open source tool OpenDLP, which finds sensitive data on Windows and UNIX systems and in databases. He is also the inventor of a US patent that describes a method for converting real-time intrusion detection events into help desk tickets.

Abstract

Even though SQL injection has been around for more than ten years and cross-site scripting has been around even longer, these vulnerabilities are still widespread and extremely dangerous today. Cross-user data access, which is one of the most manually intensive vulnerabilities to find, is also prevalent in applications. Other vulnerabilities, such as command execution and directory traversal attacks, still pop up from time to time. Throw into the mix mobile and HTML5 applications and even more vulnerabilities surface, such as not validating certificates and trusting the security of the client's local storage. How can we protect ourselves?

This talk will explain all of these weaknesses, as well as how to proactively mitigate them by infusing security throughout the software development lifecycle.

Michael Piscopo,

BIO

CISSP, INFOSEC, CCNP, MCSE, is the Director of Technical Consulting Services with Allied InfoSecurity, Inc. Throughout his career, Mike held roles in network and server engineering, software development, and information security. These skills, combined with years of ethical hacking experience, result in a unique understanding of technical risks, as well as a world class capability to help organizations understand (and just as importantly to avoid) many of the common pitfalls in building a web application defense strategy. Mike holds a BS in Aerospace Engineering from Virginia Tech.

Abstract

The safety and security of an organization's most sensitive business and customer data could rest on how securely the web applications have been developed. Without security training, developers may not fully understand the adversary trying to break their code.

This presentation reveals how common vulnerabilities allow hackers to gain illicit access to web applications and sensitive client information, and some of the basic approaches hackers may take to uncover and exploit the most common vulnerabilities. Pulling real-world examples and experience from Allied InfoSecurity's penetration testing team, some of the most common OWASP Top-10 categories are discussed. Demonstrations are provided.