

What: 2nd Annual **Idea Information Security Summit**

When: Tuesday September 9, 2008

Where: Modis Building

1 Independent Drive

Jacksonville, FL 32202



Agenda of speakers:

Speaker: Billy Austin
Position: Chief Security Officer - Saint Corporation
Title: Automating Attacks for Known Vulnerabilities



Abstract: The vulnerability management and remediation process has become a daunting battle over the years including the record high releases for both the number of vulnerabilities and exploits released in year 2008. In this presentation you will understand how attackers are now automating their new attack techniques. You will see live illustrations on the latest exploits in addition to what systems and information are being compromised. The goal of the presentation would be able to enhance your vulnerability program by validating that your network could not be exploited by such attack techniques.

Speaker: Nathan Hamiel
Position: Sr. Security Researcher / Idea Information Security
Title: Application Security



Nathan Hamiel is a Senior Consultant for Idea Information Security and is also an Associate Professor at the University of Advancing Technology. Nathan is currently focused on projects related to application security and privacy as well as pondering other problems in the Information Security space. He has previously presented at many other conferences including: Black Hat, Defcon, Shmoocon, Toorcon, and HOPE just to name a few.

Speaker: Scott Simpson
Position: Director – Security Consulting Services / Solutionary
Title: PCI Compliance



Scott Simpson is a director in the Solutionary, Inc. Security Consulting Services group. Scott is responsible for staffing and leading engagements, organizing customer requirements, on-site project management and client support while ensuring quality and timeliness of Solutionary's products and services.

Scott Simpson will present information relevant to organizations striving to achieve and sustain PCI compliance. The presentation will focus on requirements 6, 10, and 11 as well as the methods organizations are leveraging to achieve compliance in each of these areas. Scott will make recommendations on moving from compliance to sustainability and provide his thoughts on enhancing your information security processes to create programs that will meet PCI requirements.

Speaker: Ryan Barnett
Position: Director of Application Security / Breach Security
Title: **The Web Hacking Incidents Database (WHID) 2007 Report**



Ryan C. Barnett is a recognized security thought leader and evangelist who frequently speaks with the media and industry groups.

He is the director of application security at Breach Security. He is also a faculty member for the SANS Institute, where his duties include instructor/courseware developer for Apache Security/Building a Web Application Firewall Workshop, Top 20 Vulnerabilities Team Member and Local Mentor for the SANS Track 4, "Hacker Techniques, Exploits and Incident Handling" course. He holds six SANS Global Information Assurance Certifications (GIAC): Intrusion Analyst (GCI), Systems and Network Auditor (GSNA), Forensic Analyst (GCFA), Incident Handler (GCIH), Unix Security Administrator (GCUX) and Security Essentials (GSEC).

Mr. Barnett also serves as the team lead for the Center for Internet Security Apache Benchmark Project and is a member of the Web Application Security Consortium. His web security book, "Preventing Web Attacks with Apache," was published by Addison/Wesley in 2006.

The Web Hacking Incidents Database (WHID) 2007 Report

The [web hacking incident database \(WHID\)](#) is a Web Application Security Consortium project dedicated to maintaining a list of web applications related security incidents. The database classifies each reported attack by, among other criteria, the method used, the outcome of the attack and the industry and the country of the attacked organization. Based on the database [Breach Labs](#) which sponsors WHID issues a periodical report on trends in Web Application Security.

By providing answers to questions such as:

- The drivers behind Web hacking.
- The technology hackers use.
- The types of organizations attacked most often.
- The common outcomes

Speaker: Chad Smith
Position: CISCO Information Security Product Specialist
Title: **Strategic Steps to Avoid Data Leakage & Compliance Requirements for PCI, GLBA and SB1386**



Chad Smith, **CISCO** Information Security Product Specialist, has been a featured speaker over the years at numerous security and business related conferences. Drawing from his background as a Certified International Privacy Professional, a Certified Information Systems Security Professional, and a SANS Specialist on ISO17799, Chad enjoys sharing past experiences and current solutions to encourage others in developing sound business and technical practices to secure their environments. Chad is currently pursuing his Certified Protection Professional designation with ASIS to enhance his understanding of physical security controls to complement his technology and business focused acumen. Chad now works with businesses to co-develop balanced, secure business solutions.

The presentation will focus upon data leakage and how businesses can implement strategies to stop it from happening. Additionally, he will explain the compliance requirements for PCI, GLBA and SB1386 and how to map out your company's path to achieve each.