

## MS Blue Hat Hackers Headline Chicago Security Con

Microsoft pen testers AKA ethical hackers, Billy Rios and John Walton, headline an impressive list of presentations by security researchers, practitioners and executives on Oct 31 and Nov 1, 2008 for the Ethical Hacking Conference portion of ChicagoCon. And for only \$100 including food and swag, it's a steal.

Presented by The Ethical Hacker Network, a free online magazine for the security professional, ChicagoCon is a bi-annual security event held in the Windy City. In addition to numerous security boot camp courses taught by world-class instructors, ChicagoCon also features an Ethical Hacking Conference for two days of cutting-edge talks, peer networking and career advancement in the exciting and growing field of computer security.

[del.icio.us](#)

Discuss in Forums {[mos\\_smf\\_discuss:News Items and General Discussion About EH-Net](#)}

Podcast Interviews with Speakers by [PaulDotCom](#)

Opening Keynote: Friday Oct 31 - 2:00 PM  
Billy Rios & John Walton

Microsoft Pen Testers (Blue Hat)  
Mischievous Eyes and Malicious Mindsets

The browser is our window to your secrets&hellip; and we&rsquo;ve got mischievous eyes. As organizations push to increase the &ldquo;richness&rdquo; of online user experiences, they are also unwittingly increasing attack surface for organizations and their users. Join two of the best looking security researchers in the world as we dissect the current state of client side and web application security. We&rsquo;ll dive into the gory details and demonstrate the impact of client side vulnerabilities, blended threats, and targeted attacks. We&rsquo;ll cover everything from benign application vulnerabilities that gave college hopefuls a sneak peak on their admissions status, all the way to vulnerabilities used to steal your data and compromise your machine.

Billy Rios is a Security Engineer with Microsoft where he is helping to secure software used by millions of people across the world. Before joining Microsoft, Billy was a penetration tester for both VeriSign and Ernst and Young. As a penetration tester, Billy was hired by numerous organizations within the Fortune 500 to assess the effectiveness of their organization's security posture. Billy made his living by outsmarting security teams, bypassing security measures, and demonstrating the business risk of security exposures to executives and organizational decision makers. Before his life as a penetration tester, Billy worked as an Information Assurance Analyst for the Defense Information Systems Agency (DISA). While at DISA, Billy helped protect Department of Defense (DoD) information systems by performing network intrusion detection, vulnerability analysis, incident handling, and formal incident reporting on security related events involving DoD information systems. Before attacking and defending information systems, Billy was an active duty Officer in the United States Marine Corps. Billy has spoken at numerous security conferences including: Blackhat briefings, Bluehat, RSA and Hack in the Box. Billy holds a Bachelors degree in Business Administration, Master of Science degree in Information Systems, and is currently pursuing his Master of Business Administration. Check out his blog at <http://xs-sniper.com/blog/>.

John Walton is a Lead Security Engineer with Microsoft, where he spends his time code auditing, penetration testing and managing the Microsoft Online security team. Prior to joining Microsoft, John started a security consulting company, Penetration Technologies, specializing in application and infrastructure security and worked as Lead Security Engineer at Avaya. While at Avaya John built the Avaya Product Security Support Team, hacked every piece of Voice over IP (VoIP) equipment imaginable and helped develop VoIP encryption and security technology. Admittedly John is a self proclaimed computer security nut who rarely ponders anything else. He hold a Bachelors degree in Computer Science and is a Certified Information Systems Security Professional. While not working on security at Microsoft John spends his time security consulting for major financial and government institutions and occasionally finds time to sleep.

Friday Oct 31 - 3:00 PM

Nailing the Insider

Karsten Abata, Halock Security Labs

Information security controls, whether technical or process-driven, are often resisted by management over concerns about barriers to creativity, which sometimes breed contempt amongst otherwise productive employees. Frequently, the balance between protection and availability is tipped so as to not impede overall communication and collaboration within high value teams, such as those charged with product development or corporate strategy. So should you trust your "Insiders" with access to assets to which they have no justifiable need simply to preserve their loyalty? Do the chances of an internal breach outweigh the costs associated with the administration of stringent logical access controls? Could there be another way to accomplish the same objective in a less invasive, more economical and highly reliable manner?

Before addressing these questions, we will define the scope of the problem using examples from recent history. After delving into potential solutions, we will revisit cases to determine whether our solutions could have helped to detect or prevent specific incidents.

Karsten Abata currently runs the Network and Security Systems practice at local Halock Security Labs. Throughout the past several years, while functioning in both consultative and management roles within various organizations, he has helped companies recover from large data breaches. This experience has led to driven a more recent focus on technical

solutions that enable data-driven security control. Karsten enjoys educating audiences on technologies such as DLP, DAM, and IRM, which, he believes, represent a rapidly maturing niche of automated solutions that protect assets in a manner that is extremely efficient and incredibly non-invasive.

Friday Oct 31 - 4:00 PM  
Modernization of Malware Factories

Michael A. Davis, CEO of Savid Technologies, Inc.

Malware is getting more aggressive, violent, and profitable. Current malware authors have started to utilize standard development techniques utilized by professional software development organizations in order to build better malware. During an intensive source code audit, it has been discovered that the techniques and methodologies employed by the malware authors are the cause of such rampant distribution, profit making, and difficulty of removal. Gone are the days of the solo kid in a basement building a virus for fun. The new generation of malware authors are smart, agile, and use the same development patterns and methods as those developers that write the software that protects us. I will discuss the tools, methodologies, and techniques this new generation of malware writers use and provide documented examples of these techniques within the source code of the malware.

Michael A. Davis is CEO of Savid Tech, a technology and security consulting firm in Chicago and has spoken at numerous events including Black Hat and Defcon. Michael is also a member of the HoneyNet Project where he is working to develop data and network control mechanisms for Windows-based honeynets. Michael has worked with McAfee as Senior Manager of Global Threats where he lead a team of researchers investigating confidential and cutting-edge security research. He also worked for 3com and managed two ISPs. Lastly, Michael is an active developer in the Open Source community and has ported many popular network security apps to the Windows platform including snort and honeyd. Currently, Michael is finalizing Hacking Exposed: Malware and Rootkits due in 2009.

Friday Oct 31 - 5:00 PM  
DIY Career in Ethical Hacking

Donald C. Donzal, CISSP, MCSE, CEH, Security+ SME

The sub-title of this presentation is "Remodeling Your Career for Little to No Money Down," and never has this been more vital now than in these tough economic times. Inside you'll find practical exercises in finding out who you are and what gets your blood flowing. Although the talk contains plenty of practical advice on pushing your career in this growing field of ethical hacking with some inexpensive (and sometimes free) actions one can take, we will also talk very candidly about personal choices, balancing work and family, finding your superpower, taking risks and, most importantly, using free will to ensure happiness not just in your next job but for your career and ultimately your life.

"Since the first time I gave this talk at the SANS WhatWorks in Pen Testing Summit, I have been overwhelmed by the positive response from those who either heard the speech live or listened to the freely available audio recording on EH-Net. From career changes to accepted marriage proposals, the stories of inspiration have truly touched me. I have since been encouraged by friends and colleagues to continue this personal quest to not only give back to the community that gave me so much but also push the dialogue for all to benefit."

Don is the Founder of The Digital Construction Company and Editor-In-Chief of The Ethical Hacker Network (EH-Net). He is also the creative force behind ChicagoCon.

Friday Oct 31 - 6:00 PM  
Pizza Party

Keynote: Saturday Nov 1 - 9:00 AM  
Daniel V. Hoffman CTO SMobile Systems, EH-Net Columnist  
Smartphones Aren't Currently Being Exploited - And the Titanic is Unsinkable

Many people think that threats to BlackBerry's, Symbian, Windows Mobile and iPhone devices don't exist. With 2 of the top 3 BlackBerry infectors and 3 of the top 4 Windows Mobile infectors being spyware, that's exactly what the hackers want you to think. The goal of malware and attacks in general have changed from simply being disruptive, to being financially motivated, non-disruptive and stealthy. By showing specific, current exploits, see how users and enterprises who are waiting to experience an infection or data loss before implementing security software for their smartphones are placing themselves into the unsavory position of unknowingly becoming exploited and having absolutely no security software to address that exploitation.

Mr. Hoffman is a world renown mobile security expert. He joins SMobile Systems with more than 10 years of experience in mobile security. He has built his expertise as a Telecommunications Specialist with the U.S. Coast Guard, IT Director and as Senior Engineer at Fiberlink, architecting security solutions for the largest companies in the world. He has been the keynote speaker at numerous security events including Hacker Halted, InfoSec World and ChicagoCon and is known for his live hacking demonstrations and videos, which have been featured in the Department of Homeland Security's open source infrastructure report. Mr. Hoffman is the author of Blackjacking: Security Threats to Blackberry Devices, PDAs and Cell Phones in the Enterprise and Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control.

Saturday Nov 1 - 10:00 AM  
SSL: Tips, Tricks, Facts and Myths

Jay Graver, nCircle

We use SSL everyday, it makes us feel safe. That little lock icon keeps the Russian Business Network out of my chequing account and the guy in the back corner of Starbucks from reading my email. SSL waters my lawn, dries my dishes and prevents cavities. Can you spot SSL on the wire? Why aren't all websites using SSL? Why have all the recently released web browsers completely screwed up the SSL experience? Where did SSL come from and where is it going? Who invited ASN.1 anyway? Will EV SSL Certificates do anything more than make CAs money? By the way, what is TLS? This talk will answer questions about SSL you didn't even know you had.

Jay Graver is a Lead Engineer at nCircle Network Security. For the past several years he has worked with the Vulnerability and Exposure Research Team specializing in interrogating Applications and Services over the network. He has years of experience creating non invasive detection of vulnerabilities. Current Areas of research include; Regulatory Compliance, SSL library fingerprinting, security automation and unobfuscation techniques. Based in Toronto Ontario, he holds a Computer Engineering degree from the University of Guelph.

Saturday Nov 1 - 11:00 AM  
Malware - The Continuing Evolving Threat

Michael Gregg, Author, Founder & CEO of Superior Solutions, Inc.

Not long ago hackers concentrated their efforts on malicious software that was designed for recognition, fame, and glory. Today's information age attack vectors have changed; many incidents are financial in nature. Current FBI estimates are that malicious software and attacks targeting identity theft costs American businesses and consumers more than \$50 billion a year. Yesterday's virus is today's custom malware; while denial of service attacks have been replaced with botnets. It's not about bragging rights any more. Learn how these evolving threats have forced organizations to view risk assessments differently and develop new techniques to counter these emerging threats. Get the essential solutions every IS and IT professional needs to counter current and future threats.

Mr. Gregg brings more than 20 years of experience building real security solutions and driving strategic development. He is an expert on security, networking, and Internet technologies. Even though leading the firm consumes a large amount of Mr. Gregg's time, he enjoys teaching. Mr. Gregg has a proven reputation as both a dynamic and influential speaker. His written works in the field of IT security include the publication of eleven security books he has either authored or co-authored. Some of these titles include: Syngress's Hack the Stack, Sybex's Security Street Smarts, Que's CISSP Cram 2, CISSP Exam Cram 2 Questions Edition, and The Certified Ethical Hacker Exam Prep 2. He also authored Inside Network Security Assessment by Sam's publishing and The Certified Information Security Auditor (CISA) Exam Prep by Que. Mr. Gregg holds two associate's degrees, a bachelor's degree, and a master's degree. His latest work is Build Your Own Security Lab: A Field Guide for Network Testing.

Saturday Nov 1 - 12:00 Noon

What Are We \*Really\* Supposed to be Worrying About?

Arlene Yetnikoff, CISA, CISSP

There's a lot going on out there that's out to get us. And it's a lot easier today to break into systems than it is to protect them. Can we defend ourselves from all of it? Most of it? Okay, how about just the really harmful stuff? Problem is, it can be pretty difficult to determine what the most damaging vector of attack will be. Most companies can't afford to put unlimited funding into their information security program, either in technology or personnel. And most information security officers these days have projects they'd love to get to, but time and budget factors force these projects into the future. This talk will delve into determining, in your environment, what priorities to address and how protection of corporate data should be at the core of deciding where the scarce control dollars will be spent first.

Arlene Yetnikoff is the Director of Information Security for DePaul University, one of the ten largest private universities in the United States, offering numerous degrees in Computer Science and other fields, including a Masters in Computer, Information and Network Security and a Bachelor's in Information Assurance and Security Engineering. Arlene has worked in Information Security for twenty-five years as a consultant, educator and hands-on practitioner. Arlene's many years of consulting experience in the Technology Risk group of a major accounting firm allowed her to help clients of varied sizes in numerous industries assess and design their information protection architecture, policies and processes. Today, Arlene leads DePaul's Information Security and Business Continuity initiatives. Arlene also teaches Information Security at DePaul and the University of Chicago for the Masters of Computer Science program. Arlene holds a Bachelor's degree in Mathematics from the University of Chicago and a Masters in Computer Science, Telecommunications from DePaul University.

Saturday Nov 1 - 1:00  
Lunch  
Saturday Nov 1 - 2:00 PM  
Layer 2 Tai Sigung

Brian Wilson, CISSP, CCSE, EH-Net Columnist

Brian will extend his series of ChicagoCon talks with continued mastery of Layer 2 fundamentals. This time he adds Wireshark (formerly Ethereal) together with his favorite tool, Cain & Abel, to prove once again, he is the Layer 2 Great Grandmaster. Follow along with his natural, free-flowing style of presenting practical tutorials with real-world implications.

Brian Wilson, now of Cisco Systems, has over 14 years experience in IT starting with a tour in the United States Army. This Ethical Hacker Network Columnist has worked in and out of the US Government in many different organizations and technical roles including a stint as a Cisco Certified Instructor. Currently he works for an industry leading vendor supporting millions of customers of broadband & VoIP services (ISPs). He has attained a number of industry credentials covering many aspects of IT including CISSP, CCNA, CCSE, CCAI, MCP, JNCIA, Network+, Security+, and many DoD Certifications. He also uses his knowledge of IT to benefit a number of charitable organizations.

Saturday Nov 1 - 3:00 PM  
The Renaissance of Human Exploitation

Mike Murray

Information security has seen some major changes in the paradigms of attackers through the past 15 years. From the early days of social engineering, through the golden age of server hacking, and to the present times where the human is

once again the target, we have seen significant changes in the way that attackers exploit targets. Mike Murray, Director of Neohapsis Labs and social engineering expert will detail those changes and provide a detailed understanding of the types of skills that are being used to exploit human targets today, as well as examples of strategies that you can take to defend against skilled social engineers.

Mike Murray has spent his entire career in information security, from his work in the late 90's as a penetration tester and vulnerability researcher to leadership positions at nCircle, Neohapsis and Liberty Mutual Insurance Group. He currently leads Michael Murray and Associates, LLC where his team and their business partners consult with organizations on their security postures and human systems. His years of experience as a vulnerability researcher and leader of research teams have convinced him that the most important system to focus on in information security is the human one, and he works to assist security companies with those systems and their interactions with technology. Mike's talks about how to build a great career in security have been seen at major conferences like RSA and Defcon, and his work on advanced social engineering has been widely recognized. Mike's thoughts on security can be found on his blog at Episteme.ca, and his work on helping build careers can be found at TheConnectedCareer.com. He has written technical articles in publications including BusinessWeek Online and Sys Admin, as well as a regular column on EthicalHacker.net.

Saturday Nov 1 - 4:00 PM  
Pen Testing ROI

Ryan Linn, CISSP, MCSE, GPEN

Are you having a pen test done, are you planning a pen test, or are you a pen tester ? Great! This talk will focus on maximizing the value of your pen test from the planning stages through remediation. You will discover what things you can do even before the planning stages occur to make sure that you are fully prepared to get the most bang for your buck. We will discuss important considerations while your testing is occurring to help maximize results and minimize impact as well as ways to help garner support from co-workers to remedy the problems found.

Ryan Linn is currently an Information Security Engineer at SAS Institute. Employed in the computer industry since 1997, he has held positions ranging from web developer to Unix Systems Programmer at a large university to his current position in Information Security. Ryan has been responsible for working with large scale deployments of various flavors of \*nix, high availability web and database clusters, as well as for application programming in high availability environments. In the past few years, Ryan has incorporated Windows security into his responsibilities, and is now part of the team responsible for information security globally in one of the largest privately held software companies in the world.

Saturday Breakout Sessions

Your Security Career in Interesting Times

Mike Murray

The focus of the sessions are around creating and keeping job opportunities during tumultuous times.

Additional sessions and more details to come.