Cyber Defense and Disaster Recovery Conference 2010: Protecting Yourself and Your Business from International Threats

Speaker Information

James J. Barlow, Head of Security Operations and Incident Response — NCSA
From Sweden With Love: Foreign Power Hacking or Motivated Black Hat?

Mr. Barlow is in the National Center for Supercomputing Applications (NCSA) CyberSecurity Directorate working as a Senior Security Engineer. He currently leads the Security Operations and Incident Response team which focuses on the day to day security of NCSA. He also collaborates with other security engineers working on security for projects such as the Teragrid. Mr. Barlow also has been involved with a couple of the NCASSR security research projects at NCSA. Specifically he has worked a lot with the SIFT group on data mining and visualization for intrusion detection and has published and presented a few papers with that group.

Mike Bernico, Network Analyst — Information Security Professional
Enterprise Public Key Infrastructure Architecture and Design

Mr. Bernico is a Certified Information Systems Security Professional with interests in network security, authentication, and cryptography. Mike has over 13 years of experience working with networking and security in State government as well as in the private sector. Mike is very active in the sport of triathlon and is currently training for the Ironman 70.3 Steelhead triathlon; which includes a 1.2 mile swim in Lake Michigan, a 56 mile bike ride, and lastly a 13.1 mile run.

Steven Borbash, Sr. Researcher in Information Security — National Security Agency
Information Security in the Next Ten Years

Mr. Borbash is a senior researcher at the National Security Agency, where he has worked for 21 years on problems of computer and communications security. For the past seven years he has worked to provide secure wireless solutions for military customers. He received the PhD in 2004 at the University of Maryland in Electrical Engineering, where he worked on interference and other wireless network problems.

Michael A. Davis, CEO — Savid Technologies
Securing the Human: How Determining Intent is the Future of Security

Mr. Davis is CEO of Savid Technologies, Inc. a technology and security consulting firm headquartered in Chicago with offices nationwide. Michael is a deployer of intrusion detection systems, with contributions to the Snort Intrusion Detection System. He is also a member of the Honeynet project. Michael is an active developer in the Open Source community and has ported many popular network security applications to the Windows platform including snort and honeyd. Michael is a contributing author to Hacking Exposed, the number one book on hacker methodology. He is also author of a new book, Hacking Exposed: Malware and Rootkits which was released in October 2009.

Speaker Information

Caroline Hamilton, President — Risk Watch, Inc.
Risk Assessment as a Business Process in an International Threat Environment

Ms. Hamilton is President of Risk Watch International, and a leading security risk assessment expert and was a Charter member of the National Institute of Standards and Technology's Risk Management Model Builders Workshop. She has developed specialized risk assessment programs for Information Security, HIPAA, FFIEC, GLBA, Sarbanes Oxley, and corporate security programs including working with The Clearinghouse, large investment banks, the Federal Reserve and a variety of other Federal agencies on Risk Assessment guidelines. Hamilton works around the world on critical risk issues including a new set of risk assessment guidelines for the Nuclear Regulatory Commission, a risk model for airport security and a risk model for medication error with Philadelphia Children's Hospital.

TBA — Federal Bureau of Investigation
Counterterrorism

Note: speaker to be announced at conference.

William O'Sullivan, Forensics Examiner — Federal Bureau of Investigation
Cyber Incident Response: Preserving the Evidence

Mr. O'Sullivan is a Forensic Examiner on the FBI's Computer Analysis Response Team, and a former US Marine. Bill has his Master's Degree in organizational communication, and a minor is his favorite subject, Philosophy. Bill also possesses a number of industry certifications, and maintains an interest in all things technical, and when he is not working with technology, he is parenting his two boys Connor and Carson, with his wife Becky.

Peter Szczepankiewicz, Senior Security Engineer — IBM
SANS Security Course 564: Catching the Wily Hacker

Formerly working with the military, Mr. Szczepankiewicz responded to network attacks, and worked with both defensive and offensive red teams. Currently, Peter is a Senior Security Engineer with IBM. People lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable.

Cyber Defense and Disaster Recovery Conference 2010:
Protecting Yourself and Your Business from International Threats

Speaker Information
Page 3 of 3

Bryan Tillett, Sr. Principal Security Strategist — Symantec Public Sector
State of the Internet and Security Strategy Overview

Mr. Tillett is one of two Sr. Principal Security Strategists supporting Symantec Public Sector. He regularly meets with Symantec customer and partner C-level executives and other key personnel to focus on understanding and meeting real-world IT security challenges; and drives this feedback directly to Symantec business unit leaders in order to strengthen the connections between Symantec's solutions and customer goals. With more than 17 years in the Voice and IT Security Industries, Brian is a contributor at focused security forums and panels as a frequent speaker on relevant topics; including the overall Symantec Security Perspective and Strategy. Brian has held a variety of technical positions prior to working for Symantec. Brian's career began in the United States Air Force, including assignment to the Air Force Pentagon Communications Agency, serving HQ USAF, Joint Chiefs of Staff, Ballistic Missile Defense Organization, and Office of Secretary of Defense; and continues to maintain a DoD Top Secret Clearance.

Chris Trifiletti, Special Agent — Federal Bureau of Investigation
Joe Zacharias, IT Security Specialist — Information Security Professional
Social Networking? You Could Put an Eye Out With That Thing

Special Agent Trifiletti serves as the InfraGard Coordinator and Counterintelligence Strategic Partnerships Coordinator for the Springfield Division of the FBI. He has worked a variety of cyber and violent crimes cases across the U.S. and around the world. SA Trifiletti has provided training and case assistance in over twenty-eight states and thirteen countries and has served on Interpol and G8 committees on Internet child exploitation and victim identification.

Mr. Zacharias is the Computer Security Incident Response Team (CSIRT) Lead for a large Financial Services company in Central Illinois. He has 8 years of IT experience in the Financial Services industry, with concentrations in security risk management, incident response, security architecture consulting, and vulnerability management. Joe holds MCSE and ACSA industry designations. He has an undergraduate degree from Loyola University Chicago, and a masters degree from Northwestern University.

Cyber Defense and Disaster Recovery Conference 2010: Protecting Yourself and Your Business from International Threats

Presentation Information

Note: Presentations include an estimated "Tech Level" on a 1 to 5 scale where 1 is for a general audience and 5 is for a highly technical audience.

SANS Track Information

Peter Szczepankiewicz, Senior Security Engineer — IBM

SANS Security Course 564: Catching the Wily Hacker

Notes: Pre-registration required for attendance at SANS sessions
Attending the pre-session and both hands on sessions constitutes the entire SANS Security Course 564
Each of the hands on sessions stands on its own merit and does not require the attendee to be in the other hands on Session, although it is strongly encouraged.

SANS Pre-Session Presentation: State of the Hack

Course required to give familiarity with terms and concepts to be used in the hands on sessions.

SANS Hands On Session 1: Windows Command Line Kung Fu

Note: Offered in Speaker Sessions 1 and 3

Many people do not realize the power of the Windows command-line and have confined themselves inside the prison of the Windows GUI. But, sometimes, in the face of extremely nasty malware that disables GUI-based tools, security personnel are forced to the command line to analyze an infestation. This session will teach you how to become a Windows command line Kung Fu Master.

SANS Hands On Session 2: The Not-Normal Lab

Note: Offered in Speaker Sessions 2 and 4

We will analyze the traffic capture of an actual attack. Students will learn the difference between normal network traffic and not normal network traffic, and what steps to take when "not normal" (possibly attack) traffic is detected.

Speaker Session 1

Caroline Hamilton, President — Risk Watch, Inc.

Understanding Risk Assessment as a Business Process in an International Threat Environment

This session focuses on how to get the most bang for the buck. It will show how to develop and manage an effective security risk and compliance assessment program, based on metrics, and by combining elements of both the information and corporate security programs. Through the use of actual studies, you will learn the basic building blocks of risk management including how to evaluate whether the organization has the right controls, whether is has enough protection and how to measure potential new controls by their Return On Investment.

Cyber Defense and Disaster Recovery Conference 2010: Protecting Yourself and Your Business from International Threats

New information from current research on the value of threat assessment and how to do it; how to use the risk assessment to increase organizational security awareness and increase accountability will also be included. It will illustrate how to create a thorough risk assessment report and the working papers that go with it. An actual report from a Fortune 500 company will be used to illustrate these concepts and show how to present results to management. It will also cover how to use the results of the risk assessment to justify the security budget and build the case for mitigative security controls. (Tech Level 3)

TBA — Federal Bureau of Investigation
Counterterrorism

Note: presentation content to be announced at conference. (Tech Level 1)

Speaker Session 2

Bryan Tillett, Sr. Principal Security Strategist — Symantec Public Sector
State of the Internet and Security Strategy Overview

We will start with an overall view of the worldwide Symantec Security footprint. As a direct derivative of that footprint, we will touch on the Symantec Internet Security Threat Report. The presentation will provide insight into how Symantec views security in the enterprise environment. Next we will move through the 4 major solution suites including: Protection, Data Loss Prevention, Compliance, and Management. Lastly, we will visit Symantec Services, Breach Response Team, and the brief competitive market analysis. We will end with a period of Q&A. (Tech Level 3)

Steven Borbash, Sr. Researcher in Information Security — National Security Agency
Information Security in the Next Ten Years

Some current trends, including cloud computing and an explosion of new mobile device technologies, mean there will be changes in the way we defend our information systems. The presenter will offer a personal view of what's to come in the next decade. (Tech Level 3)

Keynote Speaker

Michael A. Davis, CEO — Savid Technologies
Securing the Human: How Determining Intent is the Future of Security

As more malware, spyware, and other tools are developed by attackers, the line between whether an application, website, or email is malicious is being greatly blurred. Attackers are now using the same technologies we use to defend ourselves to convince us that we need to pay them for increased protection. Learn what the latest threats are and how to educate yourself and your employees on determining the intent of an attack in order to reduce risk.

Cyber Defense and Disaster Recovery Conference 2010: Protecting Yourself and Your Business from International Threats

Speaker Session 3

James J. Barlow, Head of Security Operations and Incident Response — NCSA
From Sweden With Love: Foreign Power Hacking or Motivated Black Hat?

This case study describes FBI Major Case 216, which ultimately became a collaborative investigation between the FBI and site security professionals into a series of cyberattacks that took place from August 2003 to March 2005. Incident response specialists at the National Center for Supercomputing Applications (NCSA), located at the University of Illinois at Urbana-Champaign (UIUC), played a significant and crucial role in this investigation. The attacks encompassed over a thousand sites, including high-security military sites and federal research laboratories, university sites, private sector sites, and machines owned by individuals, both in the U.S. and in Europe. (Tech Level 3)

William O'Sullivan, Forensics Examiner — Federal Bureau of Investigation
Cyber Incident Response: Preserving the Evidence

Mr. O'Sullivan will be covering a hypothetical "typical" computer intrusion case. He will describe and illustrate the the computer forensics process, including imaging, processing, and analysis of the intrusion, and what information investigators need from victims of the intrusion. Mr. O'Sullivan will also exhibit malware and memory analysis samples from actual cases and will provide some examples of real intrusions and the results. Lastly, Mr. O'Sullivan will discuss the importance of volatile evidence in intrusion cases, and just what volatile memory can contain and its importance. (Tech Level 4)

Speaker Session 4

Mike Bernico, Network Analyst — Information Security Professional
Enterprise Public Key Infrastructure Architecture and Design

This presentation will discuss PKI's place in the enterprise. Topics discussed will include PKI Concept Refresher; Why Would You Want Your Own PKI infrastructure Anyway?; PKI's role in multifactor authentication; PKI for code signing; PKI Deployment Design; Certificate Distribution Options; and Certificate Revocation Options. (Tech Level 4).

Chris Trifiletti, Special Agent — Federal Bureau of Investigation
Joe Zacharias, IT Security Specialist — Information Security Professional
Social Networking? You Could Put an Eye Out With That Thing

The increasing use of social networking sites and applications online is changing the way society communicates, but also brings with it tremendous short and long-term risks to businesses and individuals. This joint presentation will give the FBI and corporate perspectives on managing this risk to reduce the danger to individuals and the organization. (Tech Level 2)