Cyber Defense and Disaster Recovery Conference 2015: The Private Sector and Local Government's Role in Protecting the Homeland

Presentations & Speakers — Featured Sessions

Opening Remarks

Dr. James W. Ermatinger – Dean, College of Liberal Arts & Sciences, University of Illinois Springfield

Tracie Smith – Assistant Special Agent in Charge, Federal Bureau of Investigation

Keynote Presentation - Sniping the Airwaves: A Threatscape and Demo of RFID Hacking (from way over there)

Bump! You're about to give up access to your office or hand over your passport information, your credit card numbers, even your car, without knowing it. It's based on RFID and these implanted chips are everywhere. They track clothing, start cars, open bank vaults, and even manage medical patients. They can be tampered with, lockedup, or cloned. With the market for RFID chips exploding, so have the opportunities for hacking. What's even worse - now it doesn't even take a bump! This presentation includes a demonstration of RFID hacking from over there ... a longer distance than has been seen in the past

Sean Satterlee, Information Security, Findly; Research and Development, Hailey Ordnance Company

Morning Plenary Presentation—When Conventional Wisdom Isn't: Security Tradeoffs Edition

As security assessment professionals working in the low-level, rubber-meets-the-road side of the industry, we frequently see environmental design decisions that end up having the opposite effect of what the designer intended. In this talk, we will cover three technical case studies where decisions resulted in less overall security around vital information assets. Along the way, we'll cover mobile application sandboxing, operating system defenses, vulnerability assessment side effects, and the many ways we shoot ourselves in the feet.

Josh Thomas, Founding Partner, Atredis Partners

Nathan Keltner, Founding Partner, Atredis Partners

UIS University of Illinois Springfield

CSSIA Center for Systems Security and Information Assurance — Cyber Defense Training Center

InfraGard Springfield Members Alliance — Partnership for Protection

Cyber Defense and Disaster Recovery Conference 2015: The Private Sector and Local Government's Role in Protecting the Homeland

Presentations & Speakers — Presentation Sessions

Operation Tovar, A Criminal Takedown Case Study In Private-Public Partnerships

Gameover Zeus and Cryptolocker were some of the most virulent malware campaigns on the internet until recently. Sophisticated banking fraud and cryptographic ransomware were prevalent and causing massive damages to consumers and businesses. A coordinated effort involving dozens of private sector partners and 11 law enforcement agencies around the world go together to investigate and eliminate this threat with Operation Tovar launched in June 2014. Neither malware family has been seen since. This talk will discuss Operation Tovar and the successes and challenges in such an operation from the perspective of one of the private sector participants.

John Bambenek, President, Bambenek Consulting

Methodology for Evaluating Statistical Equivalence in Face Recognition Using Live Subjects with Dissimilar Skin Tones

The general purpose of this study is to propose a methodology that can be employed in the application of facial recognition systems (FRS) to determine if a statistically significant difference exists in a facial recognition system's ability to match two dissimilar skin tone populations to their enrolled images. In particular, to test the face recognition system's ability to recognize dark or light skin tone subjects

Dr. Rigoberto Chinchilla, Integrated Engineering, Eastern Illinois University, School of Technology

Digital Forensics: Open Hands-on Lab

Open lab session with hands-on exposure to digital forensics tools. Join us in exploring the deepest recesses of today's systems using forensics tools, such as memory forensic tools. No previous experience required. All levels welcome to attend.

Frank Fuchs, Certified Forensics Investigator, Instructor, University of Illinois Springfield

Advanced Persistent Marketing: Demystifying APTs and Cyber Attacks

Since the phrase "advanced persistent threat" (APT) was coined nearly ten years ago, it has been the subject of extensive discussion and debate in the IT security community, and terabytes-worth of media buzz. The spotlight on APTs has been critical in bringing the reality of today's threats to light, but the surrounding hype has sometimes generated more fear than it has practical approaches to solving the actual problems. There is a broad tendency for security programs and regulations to be shaped by the most recent cyber incidents, focused mainly on the tactics and procedures of the attackers. While understanding attacker methodology is critical, it doesn't necessarily enable pre-emptive response.

This presentation will begin with a detailed look at threat actor motivations as the basis for pre-emptive capabilities. It will present a taxonomy of the underground ecosystem, provide an overview of tactics and procedures behind today's APTs, and highlight current "advanced" threat trends. Against this groundwork, severalthe following important practical issues will be discussed:

- What aspects of APTs and other advanced attacks are really new?
- How are advanced cybercrime groups and other actors leveraging this evolving ecosystem?
- What are the limits of security monitoring? Do we need new tools and technologies, or better blocking-and-tackling using what we currently have
- What benefits can we expect from intelligence automation versus human intelligence?

Attendees will take from the session a refreshing view of the landscape, and be reminded that effective response to advanced threats does not necessarily require an ever-expanding security budget, and the adversaries are not always as advanced as we fear.

Lance James, Head of Cyber Intelligence, Deloitte

UIS University of Illinois Springfield

CSSIA Center for Systems Security and Information Assurance — Cyber Defense Training Center

InfraGard Springfield Members Alliance — Partnership for Protection

Cyber Defense and Disaster Recovery Conference 2015: The Private Sector and Local Government's Role in Protecting the Homeland

Presentations & Speakers — Presentation Sessions

Homeland Security Perspectives: Building Cyber Security Capacity and Capability

In this presentation, Tony Enriquez, Cyber Security Advisor for the Great Lakes Region, will provide an overview of cyber security within critical infrastructure operations. The audience will walk away with an understanding of how well IT services delivering critical service are managed for cyber threats, vulnerabilities, and risks; and how essential capabilities and capacities implement a managed approach to cyber security. Practical examples will be shared as to how to improve cyber preparedness, risk mitigation, and incident response, based lessons-learned from DHS cyber security evaluations, operational coordination, and critical infrastructure policy development.

Tony Enriquez, Cyber Security Advisor – Great Lakes Region (V), U.S. Department of Homeland Security

The Cyber Covenant & You

Raising the bar on security - compliance is no longer enough. Comparing Cyber Security with a Home Owners Association's Covenant and how our responsibilities must go beyond meeting the letter of the law. As good net-izens, we must focus our security programs towards meeting the intent of the Cyber-Covenant, not just compliance.

Rich Perkins, Senior Security Strategist, TechGuard Security LLC

Lessons from Wide-Spread Retail Data Breaches: Securing the Enterprise from the Inside Out

Traveling around the country working with retail chains has given me a ringside view of the challenges of implementing data security solutions. There is a critical need for more effective security given the increased onslaught and severity of data breaches. As statistics from 2014 show, hackers target businesses of all sizes, across all industries. While no company is immune, breaches typically result from a failure to implement and follow effective data security practices. Retail chains need to secure the Enterprise not only from the perimeter, but from the inside out. Consistent and continuous data security is a necessity.

Shekar Swamy, President & Senior Security Strategist, Omega ATC

Ask a Hacker: How I'm Gonna Pwn U

Jeff Thompson (Certified Ethical Hacker) will share his expertise as a member of the Cyber Security team. This team is responsible for vulnerability assessments for more than 20 state agencies. You will learn to view your servers, network and data from a hacker's perspective which will enable you to better secure your environment. You will see several demonstrations of weakness such as buffer overflows, SQL injection and weak passwords with an emphasis on remediation techniques. You will see the return on investment in proactive security practices. He will also cover physical security, since you can't protect data if he can physically touch your server.

Jeff Thompson, CEH, Central Management Services, State of Illinois

Active Shooter Awareness Briefing

Historical information and security planning suggestions regarding Active Shooter incidents based on research and information provided by the FBI Critical Incident Response Group (CIRG.) You and those who work with or for you deserve to take a some time to consider what you would do if such a rare but exceedingly dangerous event occurred at your workplace.

Chris Trifiletti, Special Agent, Federal Bureau of Investigation

UIS University of Illinois Springfield

CSSIA Center for Systems Security and Information Assurance — Cyber Defense Training Center

InfraGard Springfield Members Alliance — Partnership for Protection

Cyber Defense and Disaster Recovery Conference 2015: The Private Sector and Local Government's Role in Protecting the Homeland

Presentations & Speakers — Speakers (in session order)

Josh Thomas, Founding Partner, Atredis Partners

Josh Thomas began his career 15 years ago in network administration and software development. Prior to moving his focus primarily to security, Josh wrote Artificial Intelligence and cryptographic solutions for the Department of Defense and other governmental agencies. Josh has extensive hands on knowledge of mobile devices, cellular infrastructure and embedded SCADA platforms. He is also dedicated to hardware reverse engineering and embedded device exploitation. Josh has spoken at numerous security conferences around the globe about embedded device exploitation, mobile security and trusted computational platforms.

Nathan Keltner, Founding Partner, Atredis Partners

With over 10 years as a security expert, Nathan Keltner is best known for his research related to reversing proprietary Smart Grid radio frequency systems and other embedded vulnerability research. Nathan has spoken globally at numerous security conferences on topics ranging from exploiting various industrial radio frequency systems to advanced analysis of purpose-built system-on-chip architectures. Nathan's research has included reviews of complex custom RF and ZigBee smart grid infrastructures, 802.15.4 and serial retail networks, multi-function ATM hardware and software, PIN entry devices, IPTV, medical devices, VoIP hardware and software stacks, and modern networking access controls and identity management systems.

John Bambenek, President, Bambenek Consulting

John Bambenek is the President and Chief Forensic Examiner of Bambenek Consulting and an Incident Handler with the SANS Internet Storm Center. He began his career at Ernst & Young as a Project Manager and Senior Consultant providing IT architecture services to top Fortune 500 Firms. He has worked in both the public and private sector providing consulting to financial services firms. He has over 15 years experience in the field, is a published author of several articles, book chapters and one book, and has contributed to IT security courses and certification exams covering subjects such as: penetration testing, reverse engineering malware, forensics, and network security. He has participated in many incident investigations spanning the globe.

Dr. Rigoberto Chinchilla, Integrated Engineering, Eastern Illinois University, School of Technology

Currently an Associate Professor at the Applied Engineering and Technology School at Eastern Illinois University (EIU). His teaching and research interest include Biometrics and Computer Security, Automation and Telecommunications. Dr. Chinchilla has been a Fulbright Scholar and a United Nations Scholar, serves at numerous departmental and university committees at EIU and has been awarded several research grants in his career. Dr. Chinchilla is a book author and has published several peer reviewed technical papers during his tenure at EIU.

Frank Fuchs, Instructor, University of Illinois Springfield

Frank Fuchs is a certified computer forensics investigator with over 28 years of experience with the Illinois State Police. In 1998, he assisted in the development of an Internet Crimes Against Children Task Force where he worked as a liaison for federal, state, and local law enforcement agencies. He has over fifteen years of experience working as a crime scene and evidence recovery specialist for the Divisions of Internal Investigations and Operations. He has performed hundreds casework examinations and analysis involving digital equipment such as computers, networks, cell phones and video surveillance equipment. Frank was also responsible for overseeing the Criminal Justice Information Systems Triennial Federal Audit before retiring from Agency in 2012.

During his time with the Illinois State Police, Frank has earned several forensic software and investigative certifications which include the EnCase Certified Examiner (EnCE); Computer Forensics Certified Examiner (CFCE); Certified NetWare Engineer (CNE); and Microsoft A+ Certifications

Most recently, in 2013, Frank has joined the faculty of the University of Illinois Springfield where he develops and teaches digital forensic courses at the undergraduate level for the computer science department. He applies his information technology, investigative and network security experience to help students learn the profession of digital forensics and crime scene techniques.

Presentations & Speakers — Speakers (in session order)

Lance James, Head of Cyber Intelligence, Deloitte

Lance James is an internationally renowned information security specialist. He has more than fifteen years of experience in programming, network security, digital forensics, malware research, cryptography design, cryptanalysis, and attacking protocols. He has provided advisory services to a wide range of government agencies and Fortune 500 organizations, including America's top financial services institutions. Credited with the identification of Zeus and other malware, James is an active contributor to the betterment of security practices and counter-threat methods through active membership in a wide range of organizations.

Most recently, as a founding force behind the CryptoLocker Working Group, he and his team of researchers were acknowledged for their critical role in disrupting CryptoLocker as part of an FBI-led takedown operation. He has contributed to a number of industry books and publications, including Phishing Exposed (Syngress, 2005), Emerging Threat Analysis (Syngress, 2006), and Reverse Deception (McGraw Hill Professional, 2012). Publications currently in the works include The Threat Intelligence Handbook (No Starch Press) and Hacking Back: Offensive Cyber Counterintelligence (McGraw Hill). Keynote speaking engagements include the SC Congress eSymposium on Cyber Espionage, the First Asia HTCIA Conference (Hong Kong), Digital PhishNet (Germany/San Diego, CA), and SANS Conference (San Diego, CA).

He holds advisory memberships with the NCFTA, the Centre for Strategic Cyberspace + Security Science (CSCSS.org), The Secure Domain Foundation (SDF), and the European Union Agency for Network and Information Security (ENISA). Other contributions include founding the InvisibleNet Project (IIP/I2P) and Secure Science Corp, as well as active participation with 2600 and InfraGard chapter. He is also a founding member of the newly formed Cyber Threat Intelligence Alliance (CTIA).

Tony Enriquez, Cyber Security Advisor – Great Lakes Region (V), U.S. Department of Homeland Security

Mr. Enriquez serves as the U.S. DHS Cyber Security Advisor for the Great Lakes Region, within the U.S. Department of Homeland Security's Office of Cybersecurity & Communications (CS&C). His program works to foster collaboration and coordination on cyber preparedness, risk mitigation and incident response, and to provide cyber security resources, including training, exercises, and assessments, to all 16 critical infrastructure sectors and to state and local government.

Prior to joining DHS, Antonio "Tony" Enriquez served 22 years with the U.S. Secret Service (USSS), Technical Security Division (TSD). As a Physical Security Specialist, Mr. Enriquez was responsible for conducting security assessments supporting Presidential and Vice-Presidential trips world-wide. He also contributed to significant engagements, supporting National Special Security Events such as the 2012 NATO Summit, assisting the Chicago Police Department with the Chicago Marathon, and serving as the USSS representative to the Interagency Training Center.

His final assignment brought him to the Chicago Field Office where he served as the Branch Chief of the Technical Operations Squad. Mr. Enriquez is a Certified Information Security Systems Professional and has a Masters Degree in Management from the John's Hopkins University.

Sean Satterlee, Information Security, Findly; Research and Development, Hailey Ordnance Company

Sean Satterlee is currently the Senior Red Team member for Findly, a San Francisco based member of the Symphony Technology Group. He was previously the Sr. Security Engineer for NetSource Secure where he led the NetSource Secure LABS team in Littleton, Colorado. A proud Oklahoman, during both positions he has remained with his roots living in Oklahoma. In earlier years, Sean was employed by the US government, large ISPs and the Chickasaw Sovereign Nation. He has been a favorite speaker at BerlinSides, RMISC, the IWS, Root66, Defcon Skytalks, Denver Bsides, and Las Vegas Bsides. Sean also trains Law Enforcement agencies for urban surveillance, escape and evasion, close quarters combat and open source intelligence (OSI). He is a competitive marksman.

Cyber Defense and Disaster Recovery Conference 2015: The Private Sector and Local Government's Role in Protecting the Homeland

Presentations & Speakers — Speakers (in session order)

Rich Perkins, Senior Security Strategist, TechGuard Security LLC

- Executive Level IT Security Professional with 20+ years of experience in Information Technology, 10+ years focused on Information Security and Risk Management
- Co-Creator of the Wireless Aerial Surveillance Platform, an autonomous aircraft with onboard WiFi, Bluetooth and Global System for Mobile Communications (GSM) penetration testing capabilities as featured on CNN's "The Situation Room" and the November 2011 issue of *Popular Science*. Currently on exhibit at the International Spy Museum in Washington DC (starting October 2014)
- Serve as the Data Loss Prevention subject matter expert, setting governance and policy as well providing technical expertise allowing full integration between Express Scripts and Medco networks by Day 120. Awarded Employee of the Quarter for Q1 2013
- Served as the Air Force voting member and subject matter expert on the Cross Domain Technical Advisory Board assessing risk of cross domain solutions for the entire Department of Defense (DoD)
- Served as the Air Force voting member on the Technical Risk Rating panel certifying the technical risk of mission critical cross-domain technologies
- Served as instructor and mentor leading the EADS NA DS3 companywide CISSP mentoring program from 2006-2010, resulting in a 96% pass rate
- Created the patented Advanced Risk Management Of Enterprise Security (ARMOES®) to enable automatic tracking/reporting of vulnerabilities within DODI 8500.2 compliant systems. EADS NA DS3 valued the effort and chose to pursue it as a full time project
- Served as the lead technical security engineer performing Certification and Accreditation Security Tests and Evaluations, ensuring secure systems were created and deployed on the Air Force and DoD Global Information Grid (GiG)

Shekar Swamy, President & Senior Security Strategist , Omega ATC

Shekar Swamy is the President and Senior Security Strategist at Omega ATC, a recognized provider of industry-leading Data Security solutions (www.omegasecure.com). He brings over 24 years of experience in this area and Shekar's company was one of the first providers of centralized retail systems management and data security. Today, Omega ATC's solutions are used by quick service restaurants, retail chains, convenience store chains, and petroleum marketers across the country. As Senior Security Strategist for Omega, Shekar is committed to helping merchants secure information and recover from data breaches .

Prior to co-founding Omega ATC in 1991, Shekar served as the Vice President of Client Services at Dun & Bradstreet, where he oversaw large-scale technology projects for a range of corporate clients. Shekar is a frequent conference speaker on retail data security and adherence to standards that pass security audits.

Jeff Thompson, CEH, Central Management Services, State of Illinois

Jeff Thompson (Certified Ethical Hacker) has over 14 years of experience in performing vulnerability assessments, incident response and computer forensics. He is on the Cyber Security Team, responsible for assessing the cyber security of more than 20 state agencies. He has worn many hats including security admin, server admin, white hat, and even a jester hat.

Chris Trifiletti, Special Agent, Federal Bureau of Investigation

Chris 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. Chris 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.

UIS University of Illinois Springfield

CSSIA Center for Systems Security and Information Assurance — Cyber Defense Training Center

InfraGard Springfield Members Alliance — Partnership for Protection