Cyber Defense and Disaster Recovery Conference 2017:
Big Data, Data Analytics, and Security: Big Savings, Big Risks

Presentations & Speakers — Featured Sessions

Opening Remarks

Thomas Turpin, Office of Advancement, University of Illinois Springfield

SAC Sean Cox, Special Agent in Charge, FBI Springfield Division

Keynote Presentation - Security Data Analytics: Let's Catch Them Earlier!

We are currently overwhelmed with cyber-attacks and compromises. Examples are too numerous to mention, but theft of over 20 million OPM sensitive personnel records must rank among the top attacks. Massive Yahoo account record compromises set new records. U.S. fighter plane plans, money from private bank accounts, and even highly likely influence in the recent U.S. Presidential election all come to mind, among many others. Is not having enough data the problem? Or is the focus of our security analytics missing the mark? The presenter makes a significant distinction between network behavior and human behavior analytics. To be more proactive and even predictive we must learn how to identify underlying malicious intent and precursor behaviors to serious cyber-attacks that lead to damage or theft.

Dr. Gary M. Jackson, President and CEO, ANBECO, LLC

Featured Presentation— Defending a Compromised Network

Designing and securing a network is very complex. With detailed requirements to support all of the latest devices, mobile computing, cloud services and the portability requirements of data, current networks are very porous, very difficult to secure and very compromised. When people hear about networks being compromised, they should not be surprised. Networks directly connected to the Internet are compromised and should be the new baseline for designing and building out security. The question that has to be answered is how to implement security based on the assumption that security is more than just setting up and protecting perimeters. In this talk, Dr. Cole will share real-life examples of security solutions that work to protect current environments that might be already compromised. Attendees will learn how to drive this new thought process into decision makers and solutions covering data protection, network design and network monitoring. The focus of security is not just on preventing a compromise, but also on controlling the amount of damage caused by a compromise, which is done by focusing in on dwell time and lateral movement.

Dr. Eric B. Cole, Founder and Chief Scientist, Secure Anchor Consulting

UIS University of Illinois Springfield

GARRETT DISCOVERY

CSSIA Center for Systems Security and Information Assurance CYBER DEFENSE TRAINING CENTER

INFRAGARD SPRINGFIELD MEMBERS ALLIANCE

The Cyber Security Threat Landscape

The cyber security universe remains an increasing and dynamic threat to the American national infrastructure. This presentation will provide a quantitative analysis of the attacks seen by IBM and the thousands of IBM customers in the preceding year. Specific attention will be paid to the protocols engaged, attack patterns, and trends seen in these attacks. In addition, these attacks will be characterized by targets, time, and degree of success.

Following the quantitative reporting, the remainder of the presentation will focus on an actionable plan for securing the enterprise. Simply describing the problem is no longer sufficient. This plan will consist of a multi-step roadmap, a product independent approach to securing the enterprise against the previously described attack vectors.

John McLaughlin, Chief Security Architect, IBM Security

InfoSec: Before or After Compromise?

During the past decades we have had two general methodologies to detect network attacks: signature detection and anomaly detection. Both have significant problems, which is why our networks are being compromised at record levels. We must improve our technologies and methods to be proactive as well as defensive. We must improve our security to be both more proactive and defensive once compromise has occurred. The presenters provide a roadmap for potential solutions to get ahead of current, significant cyber-attacks and to limit damage or theft after compromise. Is it more important to protect or defend and fix? This question will be explored and answered.

Dr. Gary M. Jackson, President and CEO, ANBECO, LLC
Dr. Eric B. Cole, Founder and Chief Scientist, Secure Anchor Consulting

Managing Complexity in Cybersecurity

For its promising potential to help cybersecurity professionals, big data adds yet another layer of complexity to an already chaotic and complex field. Perhaps the biggest challenge--and certainly the first task--of a cyber leader is to sift through an ever-increasing amount of things to know, do and deliver, in order to focus on the things that matter most. This session will explore ways to manage this complexity, drawing on best practices and the presenter's personal experiences in military operations and cybersecurity. Topics include cybersecurity best practices, excellence in the essentials, leveraging existing platforms, and security at scale to reduce cyber risk in a complex environment.

Maurice Uenuma, Author, Security Blog, Tripwire

Presentations & Speakers — Presentation Sessions

Twitter Graph Analysis and Visualization

In this hands on lab we will create a small twitter social sub-graph of the session participants using Twitter API and Python to stream and filter tweets. We then construct and visualize the user-to-user mention network of the participants and analyze various graph properties such as density, degree distribution, centrality, and community detection.

Dr. Elham Sahebaarkhorasani, Assistant Professor, University of Illinois Springfield
Lucinda Caughey, Instructor, University of Illinois Springfield

Cognitive Security and the rise of the Sensemaking Machines

As in the 1983 movie WARGAMES, each day we man the defensives we construct to shield our companies from devastating loss with our adversaries taunting us with the challenge, "Shall we play a game?". Compared to the attacker, we are outnumbered and woefully underfunded with no hope of keeping pace. What is needed is to change the game to one we can win through the integration of Cognitive Computing, Context Computing, Cloud Computing, and advanced analytics. Attend this presentation to find out how you can win the challenge when the gauntlet is thrown down.

Wesley Rhodes, Executive Security Architect, IBM Security

Detecting the Undetectable

Advanced persistent threats are still one of the most dangerous threats facing organizations today. The 2016 Verizon data breach investigation report indicated that malware was used in 90% of successful security attacks and over a million malware variants are released everyday (Symantec, Verizon 2016). Further, many security breaches go undetected for several months, but what can we do about it? In this discussion I'll explore opportunities to block APT's before you are breached and tools used to detect them if you are.

Johnathan Hunt, VP of Information Security, InVision

Presentations & Speakers — Presentation Sessions

The 'Never Ending Story': OIG vs. Healthcare Bandits!!!

"Healthcare is a tempting target for thieves. Medicaid doles out $415 billion a year. Medicare spends nearly $600 billion. Total healthcare spending in America is $2.7 trillion or 17% of GDP. Fraud (and the rules and inspections to combat it) add as much as $98 billion or roughly 10% to Medicaid and Medicare spending – and up to $272 billion across the entire health system."
The Economist http://www.economist.com/news/united-states/21603078-why-thieves-love-americas-health-care-system-272-billion-swindle

A glimpse of OIG daily life in fighting with healthcare fraud, waste and abuse in Illinois… The presentation will discuss operational protocols and methods, the successes and challenges from the perspective of Bureau of Fraud Science and Technology, Office Inspector General.

Wei-Shin Wang, Chief, Bureau of Fraud Science and Technology, Office of Inspector General, ILHFS

You Cyber Security Team Needs a Data Scientist! I'll tell you why...

I'll be discussing multiple applications of Data Science in the IT Security space including:

- Identifying Day 0 Threats with Unsupervised Machine Learning for Anomaly Detection
- Spotting Key Threats with Graph Theory
- Estimating the cost of a data breach using public data and Monte Carlo Simulation

Data Science is a multidisciplinary field that blends statistics, applied mathematics, and computer science to build data products focused around machine learning and statistical inference to business.

Mike Bernico, Lead Data Scientist, State Farm Insurance

Integrating Human Factors into Holistic Cybersecurity

This session explores the "X" factor in cyber defense: the human. Humans remain the greatest vulnerability--and strongest defense--in any organization. And human factors extend beyond relevant knowledge or technical skills to the intangibles with tangible effects, such as mindset and habits. From behavioral psychology to organizational culture, talent acquisition and workforce management, these factors must be a part of any holistic approach to cybersecurity, and are the focus of a new public-private working group at NIST, which the presenter co-chairs. Topics include human behavior, culture, training and education, workforce planning and crisis decision making.

Maurice Uenuma, Author, Security Blog, Tripwire

Presentations & Speakers — Presentation Sessions

Privacy & Data Security Issues in the World of Big Data

The FTC is the lead federal agency for protecting the privacy rights and data security of American consumers. In the last year, it brought several enforcement actions against companies for violating consumer privacy and data security and launched new initiatives – PrivacyCon, Start with Security, and a new Office of Technology Research and Investigation – to improve its capabilities and responsiveness to new threats to consumer privacy and security. In this session, learn about the FTC's enforcement efforts and other initiatives.

Steve Wernikoff, Enforcement Director, Office of Technology Research and Investigation, Federal Trade Commission

The Largest Network Vulnerability —You!

In the breakout session, Dr. Jackson will expand on the concept of network behavior vs. human behavior. Networks do not attack networks, but people do. Human beings attack and YOU are the target. Techniques such as Phishing, Spear Phishing, Typosquatting, etc. point to you as the target as the largest vulnerability. Methods will be presented to protect your networks from well-designed attacks based on human vulnerabilities and not just network vulnerabilities that require traditional patches. Increased knowledge as to how we humans can protect ourselves and our networks is the best patch to date!

Dr. Gary M. Jackson, President and CEO, ANBECO, LLC

Silent but Deadly—Hacking Trusted Networks

This presentation will demonstrate how an attacker can use passive tools to obtain usernames and hashes, which then can be loaded into a password cracking machine. Upon cracking the hashes, the attacker can then combine the credentials with other passive tools, leading to possible limited system shells, to be leveraged to access memory. Once access to memory is gained, the attacker can then dump the credentials that are still held in memory. Through demonstrations, the presenter will walk the audience through the attacker using these passive tools to obtain domain administration, while flying under the radar. In many cases these tools and methods will not be picked up by many of the security tools currently on the market.

Greg McKoy, Penetration Tester, Red Teamer

The Ransomware Problem

Ransomware attacks are surging to epic levels never before seen – is anyone's data safe? From hospitals and schools to government, attacks have grown over 6000% since 2015. The public and private sector paid out nearly 1 billion dollars in 2016 alone. This presentation will explore the results of recent ransomware takeovers and what organizations can do to protect themselves.

Johnathan Hunt, VP of Information Security, InVision

UIS University of Illinois Springfield

GARRETT DISCOVERY

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

INFRAGARD Springfield Members Alliance

Presentations & Speakers — Speakers (in session order)

Dr. Eric B. Cole, Founder and Chief Scientist, Secure Anchor Consulting

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible 2nd Edition, and Insider Threat. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting where he provides leading-edge cyber security consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole was the lone inductee into the InfoSec European Hall of Fame in 2014. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty Fellow and course author who works with students, teaches, and develops and maintains courseware.

Primary areas of expertise:

- Building and capturing intellectual property to increase net worth
- Cyber security technologies and solutions
- Designing, implementing and deploying effective security products
- Writing, teaching and speaking on technology
- Lead technology teams

John McLaughlin, Chief Security Architect, IBM Security

John McLaughlin is the Chief Security Architect for IBM Security. In this role, Mr. McLaughlin leverages his extensive experience working with a diverse range of stakeholders, leading collaboration, and translating business and technical requirements into actionable strategies and solutions. His technical expertise includes 25 years of experience across the cyber-security spectrum. Mr. McLaughlin is an expert in risk-based approaches to cyber security, critical infrastructure protection, high-risk program management, national security, data exploitation, project decision making, and teambuilding. In addition to his professional expertise, Mr. McLaughlin is an adjunct professor at George Mason University, and maintains academic relationships with Texas Tech University and the University of Illinois, instructing in several classes around network security, security frameworks, cryptography, and attack vectors. Mr. McLaughlin has an MS in Computer Science from University of Southern Mississippi, and a B.S. in Electrical Engineering from George Mason University. He is also a Distinguished Architect with The Open Group and a member of INSA.

Presentations & Speakers — Speakers (in session order)

Dr. Gary M. Jackson, President and CEO, ANBECO, LLC

Dr. Gary M. Jackson is the CEO and President of ANBECO, LLC. Trained as a behavioral psychologist with specialties in artificial intelligence and automated assessment, Dr. Jackson has designed and developed scores of advanced applications across both corporate and U.S. Government settings. Dr. Jackson's career has spanned academia as a professor, director of R&D and treatment development in various clinical settings, research psychologist within the U.S. Secret Service Intelligence Division, Intelligence Officer and Chief of three advanced technology branches within the Central Intelligence Agency, vice president and director of research and development for a major psychological test development company, Director of the Center for the Advancement of Intelligent Systems (CAIS) for the American Institutes for Research and, the founding president and CEO of Psynapse Technologies in Washington DC. Dr. Jackson has extensive R&D and operational field experience in counterterrorism, counterintelligence, counternarcotics, and asymmetric warfare prediction, tracking, and locating. He holds B.A. and Ph.D. degrees from Southern Illinois University-Carbondale and an M.A. degree from University of Illinois-Springfield. He has completed additional postdoctoral training in neurophysiology at the University of South Florida Medical School. Dr. Jackson is the inventor of the patented automated behavior assessment Checkmate network intrusion protection system, Inmate network misuse detection system for insider threat, and Automated Behavior Analysis (AuBA) technology and tools. His latest book: Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security (Wiley & Sons, 2012), describes the developed and patented automated behavior analysis (AuBA) and applications.

Primary Ares of Expertise

- Design of fused behavior and computer science predictive applications
- Behavioral/psychological assessment
- Artificial intelligence/pattern classification
- Cyber threat within global and network domains
- Insider threat

Maurice Uenuma, Author, Security Blog, Tripwire

Maurice Uenuma is a Strategic Account Manager with Tripwire, serving state governments and large enterprises in the central United States.

Maurice held previous roles as Chief Operating Officer at the Council on CyberSecurity and Vice President at the Center for Internet Security (CIS), independent non-profit organizations which produce the CIS Critical Security Controls, CIS Security Benchmarks and guidelines on implementing cybersecurity best practices.

Maurice currently serves as Workforce Management co-chair of the National Initiative for Cybersecurity Education (NICE) Working Group at the National Institute of Standards and Technology (NIST), and brings an appreciation for the complexities of implementing enterprise-wide solutions from previous leadership roles at Perot Systems and Dell.

Following his graduation from the United States Naval Academy, Maurice served for nine years as an infantry and special operations officer in the United States Marine Corps. He holds a Master's degree in National Security Studies from Georgetown University, and is a GIAC-certified Global Industrial Cyber Security Professional (GICSP).

Presentations & Speakers — Speakers (in session order)

Dr. Elham Sahebaarkhorasani, Assistant Professor, University of Illinois Springfield

Dr. Elham Sahebkarkhroasani (Buxton) joined the Computer Science faculty at UIS as an assistant professor in fall 2013. She received her Ph.D. in Computer Science from Southern Illinois University Carbondale in 2012. Dr. Khorasani's research interests are in Computational Intelligence, Soft Computing, and Big Data Analytics. She has published over 18 articles in refereed journals and conference proceedings and developed courses in Intelligent Systems and Big Data Analytics. Dr. Khorasani chaired a committee to initiate a new Master of Data Analytics program. Dr. Khorasani served as a co-PI for a recent grant from the Caryl Towsley Moy, Ph.D., Endowed Fund for Collaborative Research with SIU school of Medicine on pediatric big data analysis.

Lucinda Caughey, Instructor, University of Illinois Springfield

Ms. Lucinda M. Caughey graduated from St. Louis University with a BS in Aerospace Engineering in 1984. She worked in the Aerospace Industry for sixteen years specializing in propulsion test, data acquisition, and data analysis. Lucinda completed a M.S. in Computer Science from the University of Illinois Springfield in 2001. She taught as an Associate Professor in the Department of Computer Science at Texas Wesleyan University in Ft. Worth, Texas from fall 2000 through summer 2006. She joined the faculty of University of Illinois Springfield as an Instructor in the fall semester of 2006. Her research interests include Agent-based Parallel and Distributed Graphics, Robot Vision, and the Semantic Web. Ms. Caughey also serves as Advisor for the Computer Science Club, Mentor for the University Sponsored First Robotics Team, Co-Director of the Girl Tech Summer Camp, Site Director for the Mid-Central ACM-IBM International Computer Programming Contest, and Virtual Machine Administrator for the UIS/InfraGard Digital Forensics Challenge.

Wesley Rhodes, Executive Cybersecurity Architect, IBM Security

Wesley currently serves with IBM as the Chief Technology Officer (CTO) for Sensemaking, Director of the Network Science Research Center and as an Executive Cybersecurity Architect with the Cognitive and Cloud computing group serving many Industries. Wesley specializes in the application of cognitive and context computing technologies with Big Data and Analytics techniques for advanced insight. Wesley earned four graduate degrees in relevant technologies and disciplines, and has academic appointments in cyber security, high-performance computing and health informatics.

Presentations & Speakers — Speakers (in session order)

Johnathan Hunt, VP of Information Security, InVision

Johnathan Hunt is a security advisor, consultant and enthusiast. He is currently a VP of Information Security at InVision and has built and designed information security programs and strategies for companies in the sectors of finance, payment processing, healthcare, insurance, utilities and SaaS. He is an active member of Infragard, ISC2 and ISACA and holds several certifications including CISSP, CCISO, CISA and CISM. He also holds a Master's degree in Information Systems from UIS and is an avid pen tester and security researcher.

Wei-Shin Wang, Chief, Bureau of Fraud Science and Technology, Office of Inspector General, ILHFS

Wei-Shin Wang is currently the Bureau Chief of the Bureau of Information Technology under the Illinois Department of Healthcare and Family Services, Office of Inspector General. Mr. Wang is also the system architect lead person of the OIG data analytic system, the Dynamic Network Analytic (DNA) framework system, which is the information inquiry monitoring center for the Office of Inspector General. This DNA system meets the Federal Service Utilization Review System requirements to oversee the entire Illinois Medicaid services. In addition, Mr. Wang has successfully streamlined the case management information, sampling process, and audit routines under the OIG DNA data framework infrastructure.

Mr. Wang was the Project Manager for a $4.8 million CMS Medicaid Transformation Grant. During the project years from 2007 to 2011, Mr. Wang successfully led the team in establishing a predictive modeling data analytic system, DNA, for the Illinois Medicaid providers and beneficiaries. He was also instrumental in the construction and design of the service utilization Early Warning System protocol.

Cost of Avoidance of the Aforementioned

Medicaid Transformation Grant is very prominent: The OIG has utilized the DNA system to identify $23 million of fraud, waste or abuse of transportation services, leading to corresponding policy changes. Additionally, through OIG's identification of fraudulent billing practices for Group Psychotherapy, there was a 70% payment reduction of Group Psychiatric Services from 2009 to 2011 with an estimated savings of $30 million, also leading to Department policy changes. OIG's Recipient Lock-In program increased productivity 600% due to DNA Predictive Modeling selection protocol. In 2016, OIG saved the state of Illinois $220 million based on fraud, waste and abuse findings.

Mr. Wang has received a Master Degree in Mathematics concentrating in Computer Science and a Bachelor Degree in Computer Science from the University of Illinois. He served 2 terms as chairman of SAS Users Group in Central Illinois. Mr. Wang served as a data symposium instructor on topic of Predictive Modeling Data Analytics at the Department of Justice Medicaid Integrity Institute.

Presentations & Speakers — Speakers (in session order)

Mike Bernico, Lead Data Scientist, State Farm Insurance

Mike Bernico is a Lead Data Scientist for State Farm Insurance. His work at State Farm focuses on the application of machine learning on business problems, establishing and developing best practices for analytics throughout the organization, and raising the organization's 'analytical IQ.' Mike is also an adjunct instructor for UIS teaching Data Science Essentials and Deep Learning an Advanced Neural Networks for UIS's new data analytics degree.

Data Science is a multidisciplinary field that blends statistics, applied mathematics, and computer science to build data products focused around machine learning and statistical inference to business.

Steve Wernikoff, Enforcement Director, Office of Technology Research and Investigation, Federal Trade Commission

Steve Wernikoff is the Enforcement Director with the Federal Trade Commission's Office of Technology Research and Investigation. Steve has managed dozens of investigations and litigated civil law enforcement actions in U.S. federal court concerning a wide variety of e-commerce and emerging technology issues, including Internet and mobile advertising, credit card and other financial fraud, data privacy and security, email and text message spam, and telemarketing. Steve also has served as an adjunct faculty member at two Chicago law schools, where he has taught courses involving Internet fraud, online advertising and privacy issues. Prior to working at the FTC, Steve litigated at a law firm in Chicago and served as a law clerk in the U.S. District Court of the Northern District of Illinois.

Greg McKoy, Penetration Tester, Red Teamer

Greg is a graduate of Limestone College with a BS in Computer Science. He started working in computer networking in 1993 and began to focus specifically on the computer security arena in 2004. Over the years he has worked as a computer security professional in various industries, including the DoD and financial industries.