Cyber Defense and Disaster Recovery Conference 2016:
The Internet of Things: Risks and Opportunities when Everything is Online

Presentations & Speakers — Featured Sessions

Opening Remarks

Dr. Ted Mims, Chair, Computer Science Department, University of Illinois Springfield

ASAC Tracie Smith, Assistant Special Agent in Charge, FBI Springfield Division

Keynote Presentation - Forensics and the Internet of Things

Digital Forensics encompasses the recovery, investigation, and preservation of digital evidence found in computers and digital devices. It is a new discipline and has many challenges including the rapid evolution, scale, and application of computing. In this talk, I will discuss how the Internet of Things may have a potentially disruptive influence on Digital Forensics and what measures should be taken to ameliorate its impact.

Dr. Roy Campbell, Associate Dean for Information Technology, College of Engineering, University of Illinois

Morning Plenary Presentation— A Smarter and Secure Illinois

The international focus on Smart Cities is well justified, as cities are the economic, social and political hubs of the world. U.S. cities, however, operate with the support and influence of U.S. states, which have an important role in the Smart Cities movement. State of Illinois Chief Information Officer Hardik Bhatt will introduce the concept of the Smart State, and share the roadmap toward a Smarter Illinois. State of Illinois Chief Information Officer Kirk Lonbom will provide some insight to the security posture of the State of Illinois and a strategy for ensuring that the State of Illinois is not only Smarter, but Secure.

Hardik Bhatt, Chief Information Officer, State of Illinois

Kirk Lonbom, Chief Information Security Officer, State of Illinois

UIS University of Illinois Springfield

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

InfraGard Springfield Members Alliance — Partnership for Protection

Presentations & Speakers — Presentation Sessions

Using the SANS Top 20 Critical Controls to Manage the IoT

This session introduces attendees to both the SANS Top 20 Critical Controls and a set of tools and techniques to implement the controls. With the uncertainty and risks associated with IoT it is essential to understand how to assess a system or a business network and implement controls to eliminate, minimize, mitigate or manage risk. The SANS Top 20 is an industry accepted framework for cybersecurity managers to address all elements within and threats to a network. A list of resources will be made available to help attendees implement the controls at their company or home.

Dr. Denise Pheils, National Cybersecurity Institute

The Smart(er) Grid

The advent of the Internet of Things (IOT) has found manufacturers affixing the adjective "smart" to the front of practically every item people have in their homes. At the University of Illinois we like to think about the emerging generation of improvements to the electric grid as the Smart(er) grid. Modernized electronic systems have transformed the delivery of electricity in the last 25 years. This Internet of Everything that we are rapidly approaching could learn a lesson or two from some of the fundamental security practices developed in the first iteration of "smart," the US electric grid. This presentation will provide an overview of the complexities of the electric grid's cyber systems, highlight techniques that can be used in deployment of IOT, and showcase some of the research that is being performed at the university to keep the lights on.

Edmond J Rogers, Smart Grid Security Engineer, Information Trust Institute

Privacy of User Data in Internet of Things

The rise of the Internet of Things and high adoption of mobile devices brings to light important ethical questions regarding privacy of user data. Passive beaconing and device fingerprinting allows organizations to build unique profiles for users enabling a variety of existing use cases, but also exposes a new class of risks. As IoT devices become more prominent, they will be used not just for targeted advertising as done in malls today, but will see usage in everything from home management to medical applications. I will highlight examples of data correlation revealing potentially sensitive information about user from IoT data samples and discuss ways to allows users to control data anonymity.

Read Sprabery, Graduate Research Fellow, National Science Foundation

Presentations & Speakers — Presentation Sessions

Network Forensics: What's in Your Wire?

Explore the evidence roaming throughout of your network, and get to know your enemy.

This hands-on open lab session offers exposure to various open-source network tools. Join us in discovering the deepest recesses of today's systems by using network and memory forensics tools. No previous experience required. All levels welcome to attend.

Frank Fuchs, Certified Forensics Investigator, Instructor, University of Illinois Springfield
Vishnu Panati, Graduate Student, University of Illinois Springfield

Mitigating the Cyber Threat Landscape and the Rise of the Sensemaking Machines

The cyber security universe remains an increasingly 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 and then the new technologies and the Sensemaking architectures required to mitigate these Advanced Persistent Threats will be discussed.

John McLaughlin, Chief Security Architect, IBM Security
Wesley Rhodes, Executive Security Architect, IBM Security

The Lure of the Game: Hacking for Sport (and how it beat me)

Austin Alcala (Former blackhat hacker) will share his experience about becoming a teenage hacker and how the thrill will take your mind away from reality. He will talk about how hacking at a young age, becomes such an addiction that you lose sight of what matters most. He will also address how we enter the age of IOT, the ability to become addicted to "the game", can and will take away from what morals you were taught and how the protection of IOT is important as those devices can be used to gain access to connected systems.

Austin Alcala, Former Blackhat Hacker

Presentations & Speakers — Presentation Sessions

Quantification of Digital Forensics Analysis

The forensic process relies on the scientific method to scrutinize recovered evidence that either supports or negates an investigative hypothesis. Currently, analysis of digital evidence remains highly subjective to the forensic practitioner. Digital forensics is in need of a deterministic approach to obtain the most judicious conclusions from evidence. The objective of this talk is to examine potential methods for digital evidence analysis. Lastly, I describe a framework to properly evaluate these methods and suggestions for further improvement.

Imani Palmer, Ph.D. Student of Computer Science, University of Illinois

Moving to Ubiquitous Computing and The Internet of Things

Pervasive computing (also called ubiquitous computing) is the growing trend towards embedding microprocessors in everyday objects so they can communicate information. The words pervasive and ubiquitous mean "existing everywhere." Pervasive computing devices are completely connected and constantly available. According to the MIT Media Lab the future of computing is where the computer is imbedded in everything we do. This is causing a shift in how communications takes place as me move from mobile devices as the primary channel to one where computing truly become ubiquitous and communications becomes a part of devices we use daily. What does this mean and how will it impact our lives and how we secure critical data. During this presentation we will look at current research and methods including how the IoT are, and can, be used then we will discuss how you can secure, or not, data transferring between IoT devices and other computing devices.

Steven Hurst, CISSP, ISO 27001 Auditor, Director of Security Services and Technology, AT&T

How I Met Your Data—The Threat Landscape and a Hacker's Play Book to Compromise an Organization (Use Case)

The cyber security universe remains an increasingly 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 and then a use case on how an attacker would compromise an organization will be presented.

John McLaughlin, Chief Security Architect, IBM Security
Wesley Rhodes, Executive Security Architect, IBM Security

Presentations & Speakers — Presentation Sessions

SDN for Resilient and Fault-Tolerant Infrastructure

SDN is a new architecture that offers fine grained control and fast failover mechanisms for network administrators. During the last few years there has been a lot of interest among academics as well as corporations to leverage the potential of SDN to meet various needs. However, critical network infrastructures like the ones deployed for the power grid have yet to embrace SDN. This talk highlights the potential of SDN to improve the resilience and fault tolerance of critical infrastructures like the power grid.

Syed Hasan, Visiting Research Scholar, Information Trust Institute

Round Table Discussion: iPhone Controversy, Apple –vs– FBI

Join us for a round table discussion on the issue of encrypted mobile devises and the ability or lack there of for law enforcement and others to access the information stored on them. We will use engaging technologies to allow session attendees to evaluate the questions surrounding the current iPhone access controversy.

Clayton Bellot, CISSP, Information Security Analyst, University of Illinois Springfield
Thomas Sidener, Instructor, University of Illinois Springfield

PITM (Pineapple in the Middle)

This session explores the current state of hardware hacking devices and will demonstrate how easy it is to deploy a Man-in-the-Middle attack using the HAK5 Pineapple.

Lucinda Caughey, Instructor, University of Illinois Springfield
Brian-Thomas Rodgers , Instructor, University of Illinois Springfield

Containing Vulnerabilities in Containers

The explosive growth in the use of digital technology has created the need for secure computing infrastructure. As existing hypervisor-based virtualization technologies have left this need unfulfilled, GNU/Linux based Docker has presented a promising alternative in the form of an efficient, lightweight container system. While Docker has gained much popularity for its portability, it is plagued by a number of critical security vulnerabilities. This paper discusses several of these vulnerabilities that can be leveraged to compromise both systems and sibling containers within a given container hierarchy

Shane Rogers, Research Engineer, Cybersecurity and Network Technologies, Boeing Research & Technology
Rachel Wheelock, Student, University of Illinois

Cyber Defense and Disaster Recovery Conference 2016:
The Internet of Things: Risks and Opportunities when Everything is Online

Presentations & Speakers — Speakers (in session order)

Hardik Bhatt, Chief Information Officer, State of Illinois

Hardik rejoined public sector when he was appointed the State of Illinois CIO in March 2015. As the State CIO, he works with all state agencies to align, utilize and streamline technology to drive business priorities to transform services provided by State agencies to their constituents. Hardik also leads the Bureau of Computer and Communication Services and is responsible for IT infrastructure, service delivery and governance across the state.

Prior to joining the State of Illinois, Hardik returned to the private sector as a Senior Director with Cisco to lead the market development of the Internet of Everything for the Global Public Sector. He worked with Mayors, Governors, CIOs and Prime Ministers around the globe to extract value by connecting the public assets like parking spots, fleets of vehicles and streetlights. Hardik led Internet of Everything strategy and execution planning with cities such as Hamburg, Rio, Barcelona, Jakarta and many others. Prior to that, Hardik lead Cisco's Business Development for the Americas for Cisco's Smart and Connected Communities business.

Hardik joined Cisco in October 2010, after being the Chief Information Officer for the City of Chicago and Commissioner for Chicago Department of Innovation and Technology for 5 years. Hardik also built and lead the Smart Chicago program, which is considered a national model for improving access to affordable broadband in the community, while increasing technology awareness, talent and usage.

Prior to joining the public sector the first time, Hardik worked as a consultant with Oracle Corporation in the US and Tata Consultancy Services (TCS) in India.

Hardik has an MBA from Northwestern University's Kellogg Graduate School of Management, a Bachelor's degree in Computer Science from M. S. University, Baroda, India and lives in Chicago with his wife and two children.

Kirk Lonbom, Chief Information Security Officer, State of Illinois

Kirk Lonbom is the Chief Information Security Officer for the State of Illinois, leading a statewide transformative cyber security strategy in support of Governor Bruce Rauner's Turnaround Agenda. As the state CISO, Kirk is providing leadership and oversight in the strategic planning, execution, and assessment of all statewide information and cyber security strategies, policies, procedures and guiding practices to be implemented by all Executive Branch State agencies.

Kirk began his career as a police officer, ultimately specializing in criminal intelligence focusing on organized criminal groups and terrorism. Kirk's entry to information technology as a subject matter expert over twenty years ago led to a growing expertise in information technology and security. Over the past fifteen years, Kirk has served as Assistant Deputy Director and Deputy Chief Information Officer for the Illinois State Police and Chief Information Officer for the Illinois Emergency Management Agency.

Kirk is bringing over 35 years of progressively responsible and diverse public service experience to the mission of ensuring a cyber-secure and cyber-resilient Illinois. Kirk lives in Springfield, Illinois and in his spare time is a blues guitar player and songwriter.

Dr. Denise Pheils, National Cybersecurity Institute

Dr. Denise Pheils is a Fellow of the National Cybersecurity Institute. Formerly a security analyst, she currently consults on a wide variety of cybersecurity topics. Dr. Pheils holds teaching positions with several schools, working with students from the associate to post doctorate levels in cybersecurity. She has been the president of Toledo InfraGard Members Alliance for four years and holds many certifications including CISSP and PMP.

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 2016:
The Internet of Things: Risks and Opportunities when Everything is Online

Presentations & Speakers — Speakers (in session order)

Edmond J Rogers, Smart Grid Security Engineer, Information Trust Institute

Before joining ITI, Edmond Rogers (CISSP) was actively involved as an industry participant in many research activities in ITI's TCIPG Center, including work on NetAPT (the Network Access Policy Tool) and LZFuzz (Proprietary Protocol Fuzzing). Prior to joining ITI, Rogers was a security analyst for Ameren Services, a Fortune 500 investor-owned utility, where his responsibilities included cyber security and compliance aspects of Ameren's SCADA network. Before joining Ameren, he was a security manager and network architect for Boston Financial Data Systems (BFDS), a transfer agent for 43% of all mutual funds. He began his career by founding Bluegrass.Net, one of the first Internet service providers in Kentucky. Rogers leverages his wealth of experience to assist ITI researchers in creating laboratory conditions that closely reflect real-world configurations.

Read Sprabery, Graduate Research Fellow, National Science Foundation

Read received a B.S. in Computer Engineering from Mississippi State University in 2013 where his researched focused on security of cyber-physical systems. He then joined UIUC as a PhD Student in Computer Science and now focuses on various security topics including mobile device protocols and side channel attack resilience. Read is an NSF Graduate Research Fellow.

Frank Fuchs, Instructor, University of Illinois Springfield

Frank Fuchs is a certified computer forensics investigator and an instructor for the University of Illinois Springfield. He currently develops and teaches digital forensic courses at the undergraduate level for the computer science department.

Frank has 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 teaches digital forensic courses. He applies his information technology, investigative and network security experience to help students learn the profession of digital forensics and crime scene techniques.

Vishnu Panati, Graduate Student, University of Illinois Springfield

Vishnu Panati is a graduate student at UIS. He has earned the Certified Ethical Hacker (CEH) and Redhat Certified Engineer (RHCE) during his undergraduate work. Vishnu plans to pursue a career in Cyber Security Research.

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 2016:
The Internet of Things: Risks and Opportunities when Everything is Online

Presentations & Speakers — Speakers (in session order)

John McLaughlin, Chief Security Architect, IBM Security

John McLaughlin is the Chief Security Architect, IBM Security. In this role, John specializes in the development of holistic Information Security solutions across Fortune 500 companies and the US Government concentrating on the hardest of engineering problems. . His technical expertise includes 25 years of experience across the cyber-security spectrum. John specializes information assurance, system and network engineering, and engineering project management. In addition to his professional expertise, Mr. McLaughlin is an adjunct professor at George Mason University in northern Virginia. John 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.

Wesley Rhodes, Executive Security Architect, IBM Security

Wesley Rhodes is an Executive Security Architect, Director of the Network Science Research Center and the Sensemaking Chief Technology Officer for IBM. Wesley has 40 years of information technology experience, 15 years of which with IBM, in Energy and Utilities, Oil and Gas, National Defense & Security, Retail, Manufacturing, Transportation, and other industries. Wesley specializes in cyber security and critical infrastructure protection, Disaster Recovery and Business Continuity, high-risk program management, cognitive and context computing technologies. Wesley focuses on hard information technology engineering problems for Fortune 100 companies and National Defense & Security issues for the US Government.

Austin Alcala, Former Blackhat Hacker

Austin Alcala was born and raised in Indiana. He started using computers at the age of 3 years old; and at 8, he built his first computer application. Austin now attends Ball State University and is double Majoring in Computer Technology and Criminal Justice. He is also double minoring in Business Administration and Computer Security. He started his career by freelancing in software development and network administration. He has around 8 years of experience in Penetration Testing, programming, network security, mobile device exploitation, and video game console exploitation. He is currently being mentored by Andrew Garrett from Garrett Discovery Inc.

Imani Palmer, Ph.D. Student of Computer Science, University of Illinois

Imani received her B.Sc. Degree in Computer Science, from the University of Pittsburgh in 2013. In 2013, she joined UIUC, where she is currently a Ph.D. Student of Computer Science. She is a member of the Systems Research Group (SRG) and is advised by Professor Roy Campbell. Currently, her research involves Digital Forensics, Cyber Security, and Intrusion Detection. Her latest project is focused on the quantification of digital forensic analysis.

UIS UNIVERSITY of ILLINOIS SPRINGFIELD

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

INFRAGARD SPRINGFIELD MEMBERS ALLIANCE

Cyber Defense and Disaster Recovery Conference 2016:
The Internet of Things: Risks and Opportunities when Everything is Online

Presentations & Speakers — Speakers (in session order)

Dr. Roy Campbell, Associate Dean for Information Technology, College of Engineering, University of Illinois

Notable Appointments/Activities:
- Director of the Air Force Assured Cloud Computing Center of Academic Excellence (funded by AFRL and AFSOL.)
- Member of IFIP WG 10.3 "Concurrent Systems"
- Member, Architecture and Operations Advisory Council, Internet 2.

Awards:
- IEEE Fellow
- Ten Year Best Paper Award, Middleware 2010 for the paper: Kon, Roman, Liu, Mao, Yamane, Magalha, Campbell, Monitoring, security, and dynamic configuration with the dynamic TAO reflective ORB, Middleware 2000.
- Ten year Best Paper Award, Pervasive 2012 for the paper Hess, Roman, Campbell, Building Applications for Ubiquitous Computing Environments, Pervasive 2002.

Research Interests:
Problems and techniques of complex computer system organization and software engineering including: cloud computing, software development environments, operating systems, distributed and parallel systems, object-oriented design, networks, real-time systems, programming language design, verification, reliability, abstract data types, synchronization, data bases, security, fault tolerant systems, compilers, machine architecture, digital video and audio networking.

Steven Hurst, CISSP, ISO 27001 Auditor, Director of Security Services and Technology, AT&T

Steve Hurst leads a Cross Functional Security team within the AT&T Global Customer Security Services organization. His team provides security architecture and staffing support for outsourcing and complex customers in addition to being responsible for security compliance across AT&T commercial and government services.

Steve has been with AT&T for over sixteen years serving in a number of roles ranging from technical pre-sales support to security product management and service assurance. He holds degrees in Criminal Science, Communications, and Educational Media from Temple University in Philadelphia and is active in the Boy Scouts.

Syed Hasan, Visiting Research Scholar, Information Trust Institute

Syed Hasan is currently working as a Visiting Research Scholar at the Information Trust Institute (ITI), University of Illinois at Urbana-Champaign. Currently, he is doing research as a member of the 'SDN Project' which is a joint project with industry partners (SEL, PNNL and Ameren). He is also advising the Illinois Cyber Security Scholars (ICSSP) and hosting the ICSSP seminar session every week. Previously, he worked with the Network Access Policy Tool (NetAPT) developers' team in addition to teaching ECE422/CS461 Computer Security 1 (Spring 2013, Fall 2015) and continuing teaching the network forensics part of CS 498 AL: Digital Forensics 1 (Fall 2013, 2014, Fall 2015) and Digital Forensics 2 (Spring 2015, 2016). His research Interest is in Software Defined Networks, Network Security, Congestion Control on the Internet, Information Centric Networks, Distributed Computing, Systems and Networking in general.

Clayton Bellot, CISSP, Information Security Analyst, University of Illinois Springfield

Mr. Clayton Bellot is the most senior information security expert reporting directly to the CIO at the University of Illinois Springfield campus. He holds a Certified Information Systems Security Professional (CISSP) certification and is responsible for communicating risks to IT senior administration, developing and updating campus IT privacy and security policies to ensure compliance with Federal, State and University information security regulations, and acts as a security representative on several cross-campus committees to further develop the university's security posture.

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 2016:
The Internet of Things: Risks and Opportunities when Everything is Online

Presentations & Speakers — Speakers (in session order)

Thomas Sidener, Instructor, University of Illinois Springfield

Mr. Thomas Sidener is a faculty member at the University of Illinois Springfield in the Department of Computer Science. He holds a M.S. in Computer Science from The University of Illinois Springfield. He currently teaches courses in mobile development, database administration, and software engineering. His current research interests include robotics, video game development, and steganography.

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 MS 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 Data Analytics, Robot Vision, and the Semantic Web.

Brian-Thomas Rodgers, Instructor, University of Illinois Springfield

Brian-Thomas Rogers holds a Master's degree from the University of Illinois Springfield. Now a member of its faculty, Brian has taught a variety of courses, including Android App Development, Data Structures and Algorithms, Java, Discrete Structures, Programming Languages, and Security Testing Essentials. Additionally, he has developed a Python course which focuses on professional application development in Python, including topics such as web, network, and multiprocessing.

A Ph.D. applicant, Brian's research interests include compromises of security systems and the growing field of artificial intelligence. He recently coauthored a publication on integrating security into undergraduate courses.

Shane Rogers, Research Engineer, Cybersecurity and Network Technologies, Boeing Research & Technology

Shane is working toward his Masters Degree in Computer Science as an Illinois Cyber Security Scholars Program member at the University of Illinois at Urbana Champaign. He has worked as a research assistant for Information Trust Institute at UIUC, focusing on OpenFlow enabled software defined networks and as an EO&T Systems Engineering Intern at Boeing Defense, Space, and Security. As an undergraduate, he served as the ACM chair of the Open Network Security Monitoring (open-nsm.net) and Gnu/Linux Users Group (gnulug.org) at UIUC and as a member of the security group SIGPony. He enjoys participating in and writing network challeges for netsec Capture the Flag events.

Rachel Wheelock, Student, University of Illinois

Rachel will be completing her Bachelors Degree in Computer Science within the James Scholar Honors College at the University of Illinois at Urbana-Champaign at the end of this spring. Rachel has worked as a research assistant for the Information Trust Institute of UIUC studying secure caching in container systems, and currently is working under Dr. David Nicol analyzing vulnerabilities in Docker images. Rachel is a member of ACM special interest groups Open Network Security Monitoring and SIGPony.

UIS University of Illinois Springfield

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

InfraGard Springfield Members Alliance — Partnership for Protection