Cyber Defense and Disaster Recovery Conference 2013: Mobile Security

Presentations & Speakers

Opening Remarks

Dr. Lynn Pardie – Vice Chancellor For Academic Affairs and Provost, University of Illinois Springfield
David A. Ford – Special Agent in Charge, Federal Bureau of Investigation

Keynote Presentation - Computational Analysis of Cognitive Signatures for Mobile Security

Apple's renowned Siri system is just the beginning of artificial intelligence for smart phones and tablets. What if your smartphone could predict what you are going to do next, and worked behind the scene to ensure that you have safe network and that your data is encrypted automatically? What if your proliferation of devices (phone, tablet, etc.) and multiple users (spouse, kids, employees etc.) could 'instinctively' communicate with each other to ensure personalized security? This is where the future of mobile security is headed. Dr. Howard, Director of the Synthetic Intelligence Lab at MIT, will be discussing his work at the intersection of artificial intelligence, neuroscience, and mobile computing. Dr. Howard will discuss a novel Cognitive Signature technology modeled after human brain function that will influence the next generation of technology security. Cognitive Signatures can identify individuals' behavioral patterns across multiple devices and computationally analyze multiple data streams to develop personalized security platforms for individuals, families, businesses, and the military. Data management, identity theft protection, and secure networks are just the beginning of mobile security. The way we interact with our phones is changing rapidly, especially considering that we use these devices for work and personal use, meaning we put more and more sensitive information on our phone, making these devices more appealing for cybercriminals and malware. The Cognitive Signature technology will not only allow smartphones to act as a digital wallet, but will ensure that your banking information, location tracking, and purchase history is in sync and will be able to communicate with your bank account, and other devices directly. Your phone needs to automatically differentiate business software from personal software and know what data needs to remain confidential. This talk will address the future of mobile security where a cognitive-centric framework will allow for better security for all users in all applications.

Newton Howard, PhD, Director of the Synthetic Intelligence Lab, Resident Scientist, Massachusetts Institute of Technology

SANS Track

Note: Due to the hands-on nature of the lab session, participants must be registered for the SANS track by February 25th. Lab materials will be sent to registered participants at least one week prior to the start of the conference and will not be available during the conference. These files are essential for participation in the SANS lab session.

Morning Plenary Session – Mobile Device Threats, Policies, and Security Models
In order to have a secure mobile phone deployment, policies need to be established that define the acceptable use of the technology and recognize the limitations and threats of mobile phones, tablets and the associated infrastructure systems. This session will look at the significant threats affecting mobile phone deployments and how organizations are being attacked through these systems. Most importantly, this session will address how you can help your organization reduce the risks that these devices and 'attack surfaces' provide. Finally, this presentation will address steps that you can take to positively leverage mobile technology rather than bemoan its existence.

Lab Session – SEC 464: Bad as You Can Be in 15 minutes
Although the term 'APT' is used frequently today, the fact of the matter is that there is nothing advanced about most malware out there. In fact, Hackers today spend no time at all building malware that can slip under current Anti-Virus and intrusion detection software. Join us as we teach you how anyone can build a piece of malware that is undetectable by Anti-Virus or intrusion detection software.

Peter Szczepankiewicz, Senior Security Engineer, IBM

Afternoon Plenary Session – Hiding from the Internet

This presentation will share methods for removing personal information from the internet and will expose how some resources broadcast personal details to public view. Watch demonstration of some of the best methods to remove private details from databases that store profiles on all of us. If you want to disappear from public view on the Internet or want to know how to most effectively guard your privacy don't miss this session.

Mike Bazzell, Computer Crime Detective, 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 2013: Mobile Security

Presentations & Speakers — Presentation Sessions

Mobile Device Security

Whether it’s an iPad, Android phone or iPhone, users are bringing their personal devices to work and expecting IT to support them. Except in heavily regulated shops, trying to turn back this tide may well be counterproductive and cost the company money. In this presentation, learn the threats affecting mobile devices, how to audit mobile policies and processes, and most importantly how to handle the privacy and security issues that accompany a Bring Your own Device program.

Michael A. Davis, CEO, Savid Technologies

DIY Command & Control, For Fun And *No* Profit

Many security professionals have heard about Command & Control botnets, even more have been infected by them. Very few have had the opportunity to actually look inside the server control panel of a C&C. This mainly hands-on presentation will walk you through a very dark corner of the Internet and provide a glimpse of the daily life of a cybercriminal. Live malware will be used during this presentation so make sure you turn off your Wi-Fi.

David Schwartzberg, CISSP, Senior Security Engineer for Strategic Accounts, Enterprise Accounts SE Team Lead, Sophos

Internet Data Security Analysis and the Botnet Threat

This presentation will analyze botnets along with the security challenges and practices used to combat them. Specific areas of discussion will include:

- What is a Botnet and Types of Botnet Threats
- Proactive Security for Success
- Illustrative Power of Botnets
- Remediation Challenges

Michael Paradise, Assistant Vice President of IP Connectivity Network Operations, AT&T

The Mobile Hacker’s Toolkit

The use of mobile devices has exploded over the last few years. Unfortunately, so have the methods and tools to exploit them. This presentation will unveil various tools and attack methods malicious attackers are using against smartphones, tablets, and even public access points. In addition this session will also discuss how malicious attackers are using mobile devices as their attack platform.

Dave Chronister, C|EH, CISSP, MCSE, C|HFI, Founder and Managing Technology Partner, Parameter Security

Mobile Platforms and Cyberwarfare: Diversity is Good; Fragility is Bad; Misplacement is Ugly

This presentation argues that ‘survivability based on diversity’ is the best strategy for an open society that depends on a dynamic use of information technology. The good news for mobile IT is that there is a healthy ecosystem of various vendors, operating systems, and carriers. Mobile platform heterogeneity appeared to exceed the authors guidance for a minimum of 70-20-10 partitioning throughout the hardware and software layers.

The bad news with respect to mobile computing trends and cyberwarfare can be observed in Iraq and Afghanistan today. Our troops are not allowed to use them. They are too easy to corrupt, too easy to packet sniff, too easy to disinform. That's bad when mobile platforms are carrying a lot of the apps that people are used to relying on.

There is a silver lining to the ugliness of mobile computing fragility and our over-reliance on it. Cyberwar is about offense too. If we are prudent in the way that we mix our mobile and hard-wired systems, if we cloud and tether judiciously, so that the allocation of function to device matches national interest, not just market potential, then the onus will be on our future adversaries to be as clever and thoughtful as we can be today.

Ronald P. Loui, PhD, Assistant Professor of Computer Science, University of Illinois Springfield

Mini Session 1 — Mobile Phone (in)Security

Have you ever considered jailbreaking your phone to enhance its value across various platforms or to install third-party applications? Join this session to learn about mobile phone (in)security and the risks that result from jailbroken or otherwise altered phones.

Mini Session 2 — FBI Cyber Jobs

Ever thought about joining the FBI? Want to know what it takes and how to get started? Come ask the FBI Applicant Coordinator himself, who will answer your many questions about an exciting career with the FBI.

Darren Holtz, Special Agent, Cybercrime Investigator, Federal Bureau of Investigation
Jason Shull, Administrative Specialist, Federal Bureau of Investigation
Kirk Staats, Special Agent, Applicant Coordinator, Federal Bureau of Investigation

UIS
UNIVERSITY 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 2013: Mobile Security

Presentations & Speakers — Speakers

Michael Bazzell, Computer Crime Detective, Federal Bureau of Investigation

Michael Bazzell has been a Computer Crime Detective for the past 16 years. He has handled numerous cases involving various types of Computer Crime and Computer Forensic Analysis, including several State and Federal cases throughout the Metro-East St. Louis area. In 2005, Michael was assigned full time to the FBI's Cyber Crime Task Force, where he continues to investigate Federal cases prosecuted by the United State's Attorney's Office. He is also a part time instructor for Lewis & Clark College teaching Ethical Hacking, Computer Forensics, and Computer Investigation. Since 2002 he has been an active member of the elite Technical Operations Group of the Major Case Squad of Greater St. Louis, and served five years as the Director of the Metro-East Regional Computer Crime Enforcement Group under the authority of the Illinois Attorney General. As an active member of these organizations, he has been involved in numerous high-tech crime investigations including online child solicitation, manufacture of child pornography, child abduction, kidnapping, cold-case homicide, terrorist threats, and high level criminal intrusions.

Dave Chronister

Dave Chronister, C|EH, CISSP, MCSE, C|HFI, is the founder and Managing Technology Partner of ethical hacking firm Parameter Security, located in St. Peters, Missouri. Growing up in the wild world of 1980's BBSs and early Internet, Dave obtained a unique, firsthand look at the mind, motives, and methodology of the hacker. Dave has provided auditing, forensics, and training to clients world-wide. Dave's expertise has been featured in many media outlets including Computer World, Popular Science, Information Security Magazine, St. Louis Post Dispatch, and KTVI Fox News, to name a few. Dave can be contacted by phone at 314.44.20472 x501 or via email at dave.chronister@parametersecurity.com.

Michael A. Davis, CEO, Savid Technologies

Michael A. Davis is CEO of Savid Technologies. Based in Chicago, Michael Davis has led his business to be the 23rd fastest growing company in Chicago and #611 on the 2010 Inc. 5000 list of fastest growing companies in America. As an entrepreneur he was voted as one of the Top 25 under 25 by BusinessWeek magazine, semi-finalist of the Ernst and Young Entrepreneur of the Year award, and a Web 2.0 Wonderkid for his online marketing capabilities.

He is an author of the number one computer security book in the world, Hacking Exposed, the recently released book Hacking Exposed: Malware and Rootkits, and a frequent contributor to magazines such as InformationWeek and the Wall Street Journal. Michael spends most of his time on the road touring the world and educating the public on the preventing cyber security data breaches and how to succeed in the digital age.

Specialties include Managed IT Services, Whatever Compliance, Application Security, Penetration Testing/Ethical Hacking, Risk Assessment, Policy Development, and Software Security Development Life Cycle.

Darren Holtz, Special Agent, Cybercrime Investigator, Federal Bureau of Investigation

Special Agent Darren Holtz has worked computer intrusions since he joined the FBI in 2008. Prior to joining the Bureau he earned a Master of Computer Science Degree from Florida State and worked as a Computer Engineer writing medical software.

Newton Howard, PhD, Director of the Synthetic Intelligence Lab, Resident Scientist, Massachusetts Institute of Technology

Newton Howard (nhmit@mit.edu) is the Director of the Synthetic Intelligence Lab and a resident scientist at the Massachusetts Institute of Technology (MIT). He received his Doctoral degree in Cognitive Informatics and Mathematics from La Sorbonne, France where he was also awarded the Habilitation a Diriger des Recherches for his leading work on the Physics of Cognition (PoC) and its applications to complex medical, economical and security equilibriums. While a graduate member of the Faculty of Mathematical Sciences at the University of Oxford, England, he proposed the Theory of Intention Awareness (IA), which made a significant impact on the design of command and control systems and information exchange systems at tactical operational and strategic levels. He founded and served as the Chairman of the Center for Advanced Defense Studies (CADS), the leading Washington, D.C, National Security Group and is currently its board director. He is a national security advisor to several U.S. Government organizations. Dr. Howard works with multidisciplinary teams around the world to reach a deeper understanding of the brain and how we can utilize human brain function as a framework for improving modern day technologies in both medical and commercial applications. Advancing the field of brain sciences opens new opportunities for solving brain disorders and finding new means for developing artificial intelligence. In 2009 Dr. Howard founded the Mind Machine Project at MIT, an interdisciplinary initiative to reconcile natural intelligence with machine intelligence. In 2011 Dr. Howard established the Brain Sciences Foundation (BSF), a not-for profit, multidisciplinary research foundation dedicated to developing novel paradigms that enable the study of both mind and brain and ultimately the treatment of neurological disorders.

Cyber Defense and Disaster Recovery Conference 2013: Mobile Security

Presentations & Speakers — Speakers

Ronald P. Loui, PhD, Assistant Professor of Computer Science, University of Illinois Springfield

Ronald Loui has been a hacker, a sysadmin, a tenured professor, and a technology consultant. He is well published on artificial intelligence, scripting languages, optimal paths, and deep packet inspection.

After 9/11, he worked with SAIC subcontractors on high speed triage and filtering of network traffic.

As an undergraduate at Harvard, he helped found a technology publication for the Institute of Politics at the JFK School of Government and wrote about the potential of market disinformation during the Falklands War. He is building a cyberwarfare test range at the University of Illinois Springfield and leads a graduate readings seminar on cyberwar.

Michael Paradise, Assistant Vice President of IP Connectivity Network Operations, AT&T

Michael Paradise is the Assistant Vice President of IP Connectivity Network Operations, located in Hoffman Estates, Illinois. He is a technical leader with 20 years' experience in designing, integrating, implementing, and operating large scale enterprise and service provider networks. He has held numerous positions in network engineering/architecture, network operations, and multi-protocol network integration.

In his current role (2004-2013), Mr. Paradise oversees the service and network performance for all of AT&T's data network technologies within and outside the United States and supports a globally deployed workforce of approximately 630 management and non-management staff. Technologies supported by Mr. Paradise's team include Global IP/MPLS backbone, IPVPN, Ethernet, Mobility IP Data Core, ATM and Frame Relay, Remote Access Services, and AT&T's U-verse Core IP Infrastructure. His team manages the 24x7 surveillance, maintenance, implementation, and execution responsibilities for the one of the worlds' largest, most converged and geographically reaching MPLS network.

David Schwartzberg, CISSP, Senior Security Engineer for Strategic Accounts, Enterprise Accounts SE Team Lead, Sophos

David Schwartzberg is a Senior Security Engineer at Sophos, where he specializes in latest trends in malware, web threats, endpoint and data protection, mobile security, cloud and network security. David is a regular speaker at SC Congress Toronto, NYC and Chicago, he also presented at GrrCON and BSidesChicago. As a writer, David currently blogs at Dark Reading, he wrote the original CramSession study guide for the Network+ certification in 1999, published "Computers for Kids: Something In, Something Out" in 2011 and has been a guest blogger for the award winning Naked Security blog. After David graduated from Queens College with a B.S. in Accounting and Information Systems, he has earned several certifications in the field of Information Technology including CNA, CNE, MCP, Network+, Sophos Certified Engineer, Security+ and CISSP. David talks regularly with technology executives and professionals to help protect their organizations against the latest security threats. Follow him on Twitter @DSchwartzberg

Kirk Staats, Special Agent, Applicant Coordinator, Federal Bureau of Investigation

Jason Shull, Administrative Specialist, Federal Bureau of Investigation

Peter Szczepankiewicz, Senior Security Engineer, IBM

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. He is also a Community Instructor for the SANS Institute and demonstrates how to bypass security controls so that students can immediately better secure their work place. Peter holds certifications in ITIL Foundations, CISSP, GCFA, GSEC, GPEN, GCIH, and Linux+. He earned a Master of Science in IT Management from the Naval Postgraduate School.

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.