UNC CHARLOTTE PRESENTS

The 14th Annual

CYBER SECURITY SYMPOSIUM

October 9, 2013
<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGENDA .................. 4</td>
</tr>
<tr>
<td>SPEAKERS ............... 5</td>
</tr>
</tbody>
</table>
Welcome to the 14th Annual Cybersecurity Symposium. Recognized as the premier security event in the region, it will again feature expert guest speakers from around the country who will address the latest issues surrounding cyber crime, cyber war, privacy issues, the piracy of intellectual property, and what is being done to combat these ever-increasing global threats.

President Obama has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America’s economic prosperity in the 21st Century will depend on cybersecurity.” I hope that these thought-provoking presentations and dialogues will result in a better understanding of the prevailing threats, viable solutions, and practices. I also hope that the Symposium will serve as a platform to facilitate the development of a dynamic ecosystem of information sharing, collaboration, and partnerships among the participating organizations.

Please fill out your surveys and let us know we can make this event even more successful and productive.

Yi Deng, Ph.D.
Dean and Professor
College of Computing and Informatics
<table>
<thead>
<tr>
<th>TIME</th>
<th>LOCATION</th>
<th>ACTIVITY</th>
<th>SPEAKER</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL DAY</td>
<td>Lucas</td>
<td>Exhibitors and Refreshments</td>
<td>Capture the Flag Competition presented by 49th Security Division and Rapid 7</td>
</tr>
<tr>
<td>8:30-9:30</td>
<td>McKnight</td>
<td>Introduction</td>
<td>Bob Wilhelm, Vice Chancellor for Research and Economic Development Executive Director, Charlotte Research Institute Professor of Mechanical Engineering &amp; Engineering Science</td>
</tr>
<tr>
<td>9:30-10:00</td>
<td>Lucas</td>
<td>BREAK</td>
<td>Steve Surdu, Mandiant</td>
</tr>
<tr>
<td>10:00-10:45</td>
<td>McKnight</td>
<td>Defining the Necessity for Real Time Endpoint Data</td>
<td>Orion Hindawi, Tanium</td>
</tr>
<tr>
<td>10:00-10:45</td>
<td>210</td>
<td>Managing Vendor Risk in the IT Supply Chain</td>
<td>Jack Freund, TIAA-CREF</td>
</tr>
<tr>
<td>10:00-10:45</td>
<td>112</td>
<td>The Human Element of Cyber Security</td>
<td>Brent Rowe, RTI International</td>
</tr>
<tr>
<td>10:45-11:30</td>
<td>McKnight</td>
<td>Multi-Dimensional Behavioral Analytics</td>
<td>Jon Normand, Logrythm</td>
</tr>
<tr>
<td>11:00-11:30</td>
<td>210</td>
<td>The Malware Economy: Structure and Goals of the Attack</td>
<td>Erik Yunghans, Checkpoint</td>
</tr>
<tr>
<td>11:00-11:30</td>
<td>112</td>
<td>Framework Under Attack · Building Apps on Shifting Sand</td>
<td>Will Stranathan, CyberDNA</td>
</tr>
<tr>
<td>11:30-11:45</td>
<td>Student</td>
<td>travel</td>
<td>Steve Surdu, Mandiant</td>
</tr>
<tr>
<td>Union 340</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:45-12:15</td>
<td>Student</td>
<td>LUNCH</td>
<td>Steve Surdu, Mandiant</td>
</tr>
<tr>
<td>Union 340</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:15-12:40</td>
<td>Student</td>
<td>College of Computing and Informatics</td>
<td>Yi Deng, Dean, CCI</td>
</tr>
<tr>
<td>Union 340</td>
<td></td>
<td>Center for Configuration Analytics and Automation Update</td>
<td>Marjorie Bray, Development Director, CCI</td>
</tr>
<tr>
<td>12:15-12:40</td>
<td></td>
<td></td>
<td>Ehab Al-Shaer, Director of CCAAA</td>
</tr>
<tr>
<td>12:40-1:30</td>
<td>Student</td>
<td>Tradeoffs in Cybersecurity</td>
<td>Dan Geer, Geer Risk Services</td>
</tr>
<tr>
<td>Union 340</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:40-2:00</td>
<td>Lucas</td>
<td>BREAK</td>
<td>Steve Surdu, Mandiant</td>
</tr>
<tr>
<td>2:00-2:45</td>
<td>McKnight</td>
<td>Improving Internet Security via Large-Scale DNS Monitoring</td>
<td>Brian Foster, Damballa</td>
</tr>
<tr>
<td>2:00-2:45</td>
<td>210</td>
<td>Social Engineering: Fight Phishing with Phishing</td>
<td>Joseph Dubin, Rapid 7</td>
</tr>
<tr>
<td>2:00-2:45</td>
<td>112</td>
<td>A Data Repository for Cyber Security Research</td>
<td>Charlotte Schepers, RTI International</td>
</tr>
<tr>
<td>2:45-3:30</td>
<td>McKnight</td>
<td>Understanding Modern Malware</td>
<td>Randy Lee, FireEye</td>
</tr>
<tr>
<td>2:45-3:30</td>
<td>210</td>
<td>Metasploit Pro for Penetration Testing and for IT Security Administration</td>
<td>Joseph Dubin, Rapid 7</td>
</tr>
<tr>
<td>2:45-3:30</td>
<td>112</td>
<td>Red Dawn: Protecting small organizations from attacks</td>
<td>Thom Dosedel, Secure Ideas</td>
</tr>
<tr>
<td>3:30-3:45</td>
<td>Lucas</td>
<td>BREAK</td>
<td>Steve Surdu, Mandiant</td>
</tr>
<tr>
<td>3:45-4:30</td>
<td>McKnight</td>
<td>Insurance for Data Breach</td>
<td>Ted Claypoole, WCSR</td>
</tr>
<tr>
<td>3:45-4:30</td>
<td>210</td>
<td>TBD</td>
<td>Jack Freund, TIAA-CREF</td>
</tr>
<tr>
<td>3:45-4:30</td>
<td></td>
<td></td>
<td>Madhav Manjrekar, EPIC UNCC</td>
</tr>
<tr>
<td>4:30-5:15</td>
<td>McKnight</td>
<td>Conspicuous Insights Panel</td>
<td>Moderator: Roger Callahan, IAAdvisory</td>
</tr>
<tr>
<td>4:30-5:15</td>
<td></td>
<td></td>
<td>Tom Bartolomeo, First Citizens</td>
</tr>
<tr>
<td>4:30-5:15</td>
<td></td>
<td></td>
<td>Colleen Moss, FBI</td>
</tr>
<tr>
<td>4:30-5:15</td>
<td></td>
<td></td>
<td>Pete Murphy, Cardinal Innovations Healthcare Solutions</td>
</tr>
<tr>
<td>4:30-5:15</td>
<td></td>
<td></td>
<td>Sam Phillips, Blackberry</td>
</tr>
<tr>
<td>5:15-6:15</td>
<td>Lucas</td>
<td>RECEPTION and Poster Session</td>
<td>Steve Surdu, Mandiant</td>
</tr>
</tbody>
</table>
Ehab Al-Shaer
Professor and Director of CyberDNA Center and the Center for Configuration Analytics and Automation | UNCC SIS
Presentation Title: Center for Configuration Analytics and Automation Update

Ehab Al-Shaer, Ph.D., recently received the IBM Faculty Award, which is a competitive worldwide program offered by IBM to foster collaboration between researchers at leading universities worldwide and those in IBM research, development, and services organizations, to promote courseware and curriculum innovations that are strategic to IBM. His primary research areas are network security, security management, fault diagnosis, and network assurability. Prof. Al-Shaer edited/co-edited more than 10 books and book chapters, and published about 100 refereed journals and conferences papers in his area.

ABSTRACT:
The University of North Carolina at Charlotte and George Mason University have formed the Center for Configuration Analytics and Automation under the National Science Foundations’ (NSFs) Industry/University Cooperative Research Center (I/UCRC) Program. The mission of the center is to enable collaborative industry and government directed research in configuration analytics and automation capabilities and their integration for the efficient, accurate, and timely operations management and defense of complex networked information technology (IT) systems and environments; and the encouragement and development of top-quality graduates with knowledge and experience in this field.

Thom Dosedel
Senior Security Consultant | Secure Ideas
Presentation Title: Red Dawn: Protecting Small Organizations From Attacks

Thom Dosedel is a Senior Security Consultant with Secure Ideas. He comes with a long history of working in the IT industry fulfilling multiple positions throughout his career, predominantly in the healthcare and technology industries. Thom’s experience includes system administration, development, network and application architecture, and management. Thom has worked with companies and organizations that range from educational institutions to Fortune 100 companies. In addition, Thom brings a wide range of training and educational experience to Secure Ideas. Thom has also provided presentations and trainings around the country. Thom speaks to all levels of IT and business units, including C-Level management. He has spoken at places such as HP Universe and many internal training events. He focuses on web and mobile security, as well as IT operation integrations.

ABSTRACT:
Secure Ideas spends a lot of time working with organizations both large and small. During this work, we deal with and help people trying to figure out what the threats and risks are in the world today. For larger companies, this exercise is something they deal with often, but smaller organizations may not have the resources or the view to help them figure this out.
**Joe Dubin**  
Senior Product Manager for Metasploit  |  Rapid7  
**Social Engineering: Fight Phishing with Phishing**

Joe Dubin is Senior Product Manager for Metasploit at Rapid7. Prior to joining Rapid7, Joe was responsible for product marketing at Pervasive Software’s Big Data startup division. With over 20 years of experience in the software industry, he has held product management and marketing positions at both startups and Fortune 500 companies in the U.S. and in France, and he has presented and spoken at industry conferences in the U.S., Europe, and Israel. Joe holds a B.S. in Electrical Engineering from Washington University in St. Louis.

**ABSTRACT:**
Phishing is on the rise as an attack vector because it is often the fastest and easiest way to penetrate an organization's defenses. Even when organizations conduct security awareness training, an average of 20% of users still fall for a well-crafted phishing e-mail. How can organizations defend themselves? This talk will analyze recent phishing incidents and then make the case for organizations to conduct their own internal phishing campaigns to measure and reduce user risk. The focus will be on best practices, including establishing a program, key metrics to monitor, and potential legal and organizational concerns.

**Brian Foster**  
Chief Technology Officer  |  Damballa  
**Presentation title: Improving Internet Security via Large-Scale DNS Monitoring**

Brian Foster brings over 25 years of successful product management and development experience to Damballa. Recently, Brian was Senior Vice President of product management for consumer security at McAfee, where he directed the strategy and development of consumer and mobile security solutions. Before focusing on consumer solutions, Foster also directed the strategy and development of McAfee’s enterpise security solutions. Foster expanded McAfee’s enterprise product line to over 80 products, and he played key roles in numerous acquisitions, including the Intel acquisition. He was integral in creating McAfee’s differentiated technical strategy around Integrated and Deep Security. Foster spent over 20 years at Symantec, growing from technical support to roles in software engineering, project management, development, and product management on lines such as Norton Utilities and Norton AntiVirus. He spent eight years at Symantec managing the commercial desktop and server security product lines. Foster earned a Bachelor of Arts degree in Economics, and he has attended the Executive Program in Management at the University of California, Los Angeles.

**ABSTRACT:**
In this talk, Foster will describe how Damballa uses research from Georgia Tech and Damballa Labs to monitor large-scale passive DNS data to detect internet abuse. Foster will give examples of how Damballa’s products, based on the before mentioned research, have dedicated new and unknown threats by observing network behavior.
**Jack Freund**
Manager, Information Risk Assessment | TIAA-CREF

**Presentation title: Managing Vendor Risk in the IT Supply Chain**

Dr. Jack Freund is an expert in IT risk management, specializing in analyzing and communicating complex IT risk scenarios in plain language to business executives. He currently leads a team of risk analysts at TIAA-CREF. Jack has over 15 years of experience in IT and technology, working for organizations such as Nationwide Insurance, CVS/Caremark, Lucent Technologies, Sony Ericsson, AEP, Wendy's International, and The State of Ohio. He holds a B.S. in CIS, a Master's in Telecom and Project Management, a Ph.D. in Information Systems, and the CISSP, CISA, CISM, CRISC, CIIP, and PMP certifications. Jack is a Visiting Professor at DeVry University and a Senior Member of the ISSA, IEEE, and ACM. Jack chairs a CRISC subcommittee for ISACA, and he is a member of the Open Group’s risk analyst certification committee. Jack’s writings have appeared in the ISSA Journal, Bell Labs Technical Journal, Columbus CEO Magazine, and he currently writes a risk column for @ISACA. Jack is also authoring a book entitled Measuring and Managing Information Risk: A FAIR Approach, under contract with Elsevier. You can follow all Jack’s work and writings at riskdr.com.

**ABSTRACT:**
Organizations are increasingly relying on their suppliers to conduct critical work in furtherance of their goals. In support of this, information security departments routinely conduct assessments of their suppliers in order to help minimize risk in their supply chains. These assessments usually consist of some combination of questionnaires, onsite observations, testing, and interviews. Such assessment routines tend to reveal superficial (or overly obvious) issues with the suppliers. However, what decision makers really need to know is whether or not the supplier will handle the information entrusted to them with care. Amongst other things, what managers and executives want to know is if they have had problems doing this in the past and what are the odds of them making mistakes in the future? This presentation will provide a technique to help better inform management of supplier risk and to make better information security decisions about vendor and supplier choices.

---

**Daniel Earl Geer, Jr., Sc.D.**
Principal | Geer Risk Services

**Tradeoffs in Cyber Security**

Dan Geer has ten years of experience in clinical and research medical computing followed by five years running MIT’s Project Athena, the first distributed computing emplacement. He then had a small stint in the Research division of the then Digital Equipment Corporation. From then on Dan Geer has worked in a series of entrepreneurial endeavors, in all cases either a founder outright or an officer of the company, and now he is in government service at In-Q-Tel, the investment arm of the U.S. intelligence community. Dan Geer is advisor to or a board member for a number of promising startups and their funding sources, over 100 refereed publications, two books and many book chapters, three patents, over two hundred fifty invited presentations. Twenty percent of which were keynote presentation, including ten abroad, technology selection and standardization work, and five appearances before the U.S. Congress, of which two were as lead witness. He has a commercial teaching history, both extensive in scope and in excess of ten thousand students in the aggregate. Dan Geer participates in government advisory roles for the Federal Trade Commission, the Departments of Justice and Treasury, the National Academy of Sciences, the National Science Foundation, the U.S. Secret Service, the Department of Homeland Security, the Commonwealth of Massachusetts, the White House, and In-Q-Tel’s counterparties.

**ABSTRACT:**
We all know that cyber security is about tradeoffs, tradeoffs between cost and benefit, between practicality and protection, and so forth. Some of these tradeoffs are at the personal level and some are not, but as the word “tradeoff” implies, choice is the core of freedom. The question is whether, and to what degree, we can preserve choice in the face of increasing digital interdependence.
Randy Lee
Director of FireEye Labs | FireEye Inc.
Presentation title: Understanding Modern Malware

Randy Lee, an IT systems and security veteran with 20 years of engineering experience, is currently a Director of FireEye labs and network and malware/security expert at security vendor FireEye, Inc. Prior to FireEye, Randy was the engineering director for Fortinet Inc, leveraging systems and security knowledge to design and build global security solutions. Before Fortinet, Randy was the infrastructure manager at Foundry Networks, leveraging PHP, MySQL, Perl, and Apache to deliver robust web-based applications. Randy also held engineering positions at Covasoft, IBM/Tivoli, and Applied Materials.

ABSTRACT:
Advanced targeted attacks are the new norm as cybercriminals penetrate the vast majority of enterprises. Research shows that over 95% of companies are already compromised and most are unaware of it. Two thirds of U.S. firms have been victims of cyber attacks by various studies. 92% of them discovered the breaches through an external party. Modern malware is stealthy, complex, state funded, and effective.

Orion Hindawi
Chief Technology Officer | Tanium Inc.
Presentation title: Defining the Necessity for Real Time Endpoint Data

Orion co-founded Tanium in 2007, with the mission of creating security products that provide truly instant data collection and action capabilities. This allows enterprises to manage their assets with 15 second latencies, rather than the hours or days of latency they are used to today, with huge benefits to their security and stability. An accomplished entrepreneur and inventor, Orion holds multiple software patents in the fields of communications, endpoint security, and systems management. He has led the development of security management platforms over the past 15 years, first at BigFix and now at Tanium, and remains singularly focused on understanding and simplifying the significant challenges IT departments face securing large enterprise environments globally.

ABSTRACT:
Modern threats are capable of exfiltrating gigabytes of targeted, sensitive information from an enterprise within minutes. Trying to make informed decisions and take timely remediating action against threats of this speed is impossible when visibility is based on data that is hours or days old. By the time the problem is discovered, the damage has been done and the threat may have moved on to new machines within the environment. Strategies that focus on the network alone have proven to have gaps in visibility, and heuristic-based strategies for identifying malware based on its behavior are well known and tested against by malware authors. In order to shift the balance of power from being the hunted to becoming a hunter, what is required is visibility and control at speeds fast enough to find and stop these modern threats as they happen. This requires the ability to answer questions such as, “What processes are executing globally across my environment that match a particular hash?” and “Which machines are connecting to a known bad address at this moment, and what are the egress points of those connections?” Answering these questions at scale and in time to take remediating action requires real time data and control at the endpoint level.

Madhav Manijrekar
**Jon Normand**  
Senior Sales Engineer | LogRhythm Inc.  
**Presentation Title: Multi-Dimensional Behavioral Analytics**

Jon Normand is a Senior Sales engineer with extensive experience in Commercial /Government IT security and works for a hi-tech Security Information and Event Management company. The company is the largest and fastest growing independent Security Information and Event Management (SIEM) provider in the world. The company's patented and award-winning Security Analytics platform and Network Monitor product empower organizations around the globe to detect breaches and the most sophisticated cyber threats of today, faster and with greater accuracy than ever before. His professional interests include information systems security, web and Internet technology, the technical, business, and public policy aspects of Global Social Media and Cloud computing.

**Abstract**

The 2013 Verizon Data Breach Report found that 66% of breaches took months or more to discover and that 69% were discovered by external parties. Increasingly, organizations are struggling to identify new or existing threats within the massive volumes of incoming security data. In order to identify true abnormalities across the enterprise, organizations need to be able to understand what constitutes “normal” behavior. Who are the appropriate departments and roles to have access to your organizations sensitive servers and files? Which web applications are appropriate for users to access? Which countries are considered acceptable for IP traffic into and out of your network?

Answering these type questions and defining “normal” has long been impractical due to the sheer volume of data, as well as the limitations of first generation behavior analysis technologies. During this presentation LogRhythm’s, Jon Normand will outline how new advances in SIEM technology have allowed organizations to automate the discovery of “normal” through Multi-Dimensional Behavioral Analytics. By utilizing contextual data feeds, monitoring techniques and analytic functions such as Geo-Location information, Behavioral Whitelisting, Trending, Privileged User Monitoring along, with Host and Network Forensics, users are able to automate the discovery of “normal” across the enterprise and detect exception to these baselines, that can be indicative of advanced threats and breaches. Mr. Normad will also walk the audience through some specific use cases where Multi-Dimensional Behavioral Analysis technology was able to identify malicious data exfiltration and the attempted introduction of malware.

**Brent Rowe**  
Senior Economist | RTI International  
**Presentation Title: The Human Element of Cyber Security**

Brent Rowe is a senior economist with expertise in the evaluation of innovative technologies, the development of economic impact models, and the analysis of technology and security policies. Mr. Rowe has led numerous studies looking at issues surrounding the adoption of new technologies and standards by such industries as semiconductors, biotechnology, information technology, and nuclear energy. He has particular expertise in assessing the economic factors (e.g., incentives and disincentives) associated with cyber security. Mr. Rowe frequently presents at academic, industry, and government conferences, and he publishes his work in a variety of journals. In 2008, he coauthored a book entitled Cyber Security: Economic Strategies and Public Policy Alternatives.

**ABSTRACT:**

The level of cyber security maintained by an individual is based on the availability of robust cyber security products and services and the cyber security knowledge, perceptions, and behaviors of that individual, as well as how much they are willing to pay for cyber security. For an organization, every individual can affect the level of cyber security of the organization and their roles can be quite diverse. These include managers involved in making cyber security investment decisions, technical staff who implement and maintain cyber security products and services and enforce policies, and other staff who are users of the organization’s network resources. Research that aims to develop a better understanding of what factors affect individuals’ and organizations’ (groups of individuals) cyber security-related decisions is critical to reducing the overall impact of cyber security. The presentation will focus on the economic, psychological, and policy frameworks behind such research, and it will include a discussion of the results of several recent studies in this area.
**Steve Surdu**  
**Vice President of Professional Services | Mandiant**  
**Presentation Title: Advanced Threat Groups and Defending Your Network Against Them**

Steve Surdu is the Vice President of Professional Services at Mandiant. Steve oversees the activities of Mandiant’s consulting organization: service delivery, personnel development, recruitment, process improvement, and business development. Because Mandiant specializes in responding to large scale computer security breaches, Steve spends significant time understanding advanced threats, developing new approaches to respond to enterprise-wide compromises, identifying effective remediation approaches, and collaborating with law enforcement. Steve has more than 30 years of experience in information technology consulting. He has worked with clients in many industries including financial services, high technology, healthcare, regulated industry, manufacturing, hospitality, energy, state and federal government, and retail. Over the course of his career he has performed large scale application development, third-party software system integration, project management, information security consulting, and general business consulting for services organizations. Steve earned a Bachelor’s degree in Business Administration from the University of Michigan in Ann Arbor.

**ABSTRACT:**  
Whether the organizations are public or private, commercial or government – they have information that may be of interest to others. This presentation will provide an overview of several different information security threats facing organizations today. Mandiant deals with insiders, hacktivists, organized crime, and nation-state attack groups. In this presentation the attack groups will be profiled. In addition, their objectives and tactics will be contrasted with one another. Lastly, we will touch on the factors that expose organizations to greater risk and the steps organizations can take to improve their information security defenses against these threats.
**Erik Yunghans**  
Regional Technical Expert, Threat Mitigation | Check Point Software Technologies Ltd.  
Presentation Title: The Malware Economy: Structure and Goals of the Attack

Erik Yunghans is a Subject Matter Expert in Threat Mitigation for Check Point Software Technologies, Ltd. In his tenure, he has consulted with Fortune 500 companies to provide guidance and thought leadership in developing unified and cohesive strategies for combating the modern day threat landscape. Through the use of real-world examples used in the creation of malware, exploits, and DDoS attacks, Erik provides unique insight into the security landscape through the eyes of an attacker.

**ABSTRACT:**
How easy it is to build a zero-day attack? What is the primary purpose? Through the use of malware kits and live demonstration the audience will learn how an attacker plans, assembles, and launches targeted malware attacks. In addition, the audience will learn how enterprises build unified and multi-layered defense systems, providing the ability to fully mitigate the attack.

---

**Conspectus Insights**

**ABSTRACT:**
Don’t miss this one. A plenary panel of cyber security professionals, who are managing cyber risks in different business sectors. Panelists will provide their perspectives on important insights heard during the symposium and engage in a town hall discussion; as they offer their prognostication of emerging threats and risks to pay attention to during the coming year.

---

**Roger M. Callahan**  
Managing Director | Information Assurance Advisory, LLC

Roger Callahan has over 45 years of prior experience spanning executive management and engineering responsibilities within both the National Security community and the Financial Services industry. He served as the Director for Information Assurance in the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (1995-1998). In the Pentagon, he directed the transformation of “information security” efforts to a Department of Defense-wide “information assurance” strategy. At Bank of America (1998-2008) he was a Senior Vice President within the Corporate Information Security Organization, and he was responsible for developing the Bank of America information security policy and program foundations. During both his government and private sector careers, he served as an advisor to DOD’s Defense Science Board on the subject of Defensive Information Warfare and also to a variety of financial industry, congressional, and GAO advisory efforts dealing with cyber security. He currently serves as an advisor to the Office of the Chairman of the Financial Services Sector Coordinating Council (FSSCC). He recently led an effort to establish a new multi-university research center under the National Science Foundation’s (NSF’s) Industry/University Cooperative Research Center (I/UCRC) Program. In May 2013, the NSF approved the Center for Configuration Analytics and Automation (CCAA) and provided five year grants for the new Center to both UNC Charlotte and George Mason University.

---

**Colleen Moss**  
Supervisory Special agent | FBI
Ted Claypoole and Jack Freund group presentation
Title: Insurance for Data Breach

ABSTRACT:
As company obligations toward data grow each year, a maturing data breach insurance industry is finally catching up with the needs of the market. This presentation will illustrate why insurance is necessary in this field and how the offerings have changed over time, culminating with a look at the current industry standards.
Dr. Jack Freund is an expert in IT risk management, specializing in analyzing and communicating complex IT risk scenarios in plain language to business executives. He currently leads a team of risk analysts at TIAA-CREF. Jack has over 15 years of experience in IT and technology, working for organizations such as Nationwide Insurance, CVS/Caremark, Lucent Technologies, Sony Ericsson, AEP, Wendy's International, and The State of Ohio. He holds a B.S. in CIS, a Master's in Telecom and Project Management, a Ph.D. in Information Systems, and the CISSP, CISA, CISM, CRISC, CIPP, and PMP certifications. Jack is a Visiting Professor at DeVry University and a Senior Member of the ISSA, IEEE, and ACM. Jack chairs a CRISC subcommittee for ISACA, and he is a member of the Open Group’s risk analyst certification committee. Jack’s writings have appeared in the ISSA Journal, Bell Labs Technical Journal, Columbus CEO Magazine, and he currently writes a risk column for @ISACA. Jack is also authoring a book entitled Measuring and Managing Information Risk: A FAIR Approach, under contract with Elsevier. You can follow all Jack’s work and writings at riskdr.com.

John Melton and Will Stranathan group Presentation
Title: Framework Under Attack - Building Apps on Shifting Sand

ABSTRACT: Over the past two years, attackers have moved from attacking the application to attacking the application framework. Existing DAST and SAST tools rarely look for framework vulnerabilities, as this is a very new ground. We will look at recent attacks against the .NET Framework, Ruby on Rails, Struts 2, and others, and we will discuss how organizations, which host applications based on framework code, are supposed to defend themselves against these very serious attacks.

John Melton
Senior Security Researcher | White Hat Security

John is a senior security researcher for WhiteHat Security. His current focus is on using static analysis technology to improve application security. His background is in software development and security engineering.

William Stranathan
Cyber DNA

Will Stranathan currently engineers systems to manage, analyze, and triage static analysis results from hundreds of different applications. He has been involved in application security in all facets, including application pen testing, architecture risk analysis, code review, and defensive programming training. He has written rotten code since the age of seven, when he began writing rotten code in Turtle Logo. He lives in Charlotte with his wife and two daughters.
**TuToRiAL**

**SPEAKERS**

---

**Joe Dubin**  
Senior Product Manager for Metasploit | Rapid7

**Metasploit Pro for Penetration Testing and for IT Security Administration**

**ABSTRACT:**
This session for IT security administrators and security professionals covers how to reduce risk using Metasploit Pro. Use cases covered will include:

- Vulnerability Validation, or how to provide a closed-loop Security Risk program by exploiting vulnerabilities found by Vulnerability Management software
- Measure and reduce User Risk by conducting automated social engineering campaigns
- Security Controls Testing: measure the efficiency of network perimeter controls
- Simplify penetration tests through the use of automated workflows
DEPARTMENT OF
SOFTWARE +
INFORMATION SYSTEMS
WWW.SIS.UNCC.EDU

The Department of Software and Information Systems (SIS) is a pioneer in Information Technology research and education. SIS was one of the first institutions in the United States to be recognized by the National Security Agency as a National Center for Academic Excellence in Information Assurance Education and Information Assurance Research. The Department offers a wide selection of courses in information technology and software engineering, emphasizing designing and deploying IT infrastructures that deliver integrated, secure, reliable, and easy-to-use services. We have partnerships with the Departments of Business Information Systems and Operations Management, Computer Science, Geography and Earth Sciences, and the College of Health and Human Services delivering specific concentrations for our students.

Academic programs:
- BA Software and Information Systems
- Web Development, Software Engineering, Information Technology, and Financial Services Informatics tracks within the B.A. program
- M.S. Information Technology
- Graduate Certificate in Information Technology Management
- Graduate Certificate in Information Security and Privacy
- Graduate Certificate in Healthcare Information Technology
- Ph.D. Information Technology

Graduate students can choose a variety of concentrations including:
- Information Security and Privacy
- Software Design and Engineering
- Human Computer Interaction
- Information Technology Management
- Health Informatics
- Geographical Information Systems
- Intelligent Information Systems
- Advanced Database and Knowledge Discovery
FACT:

“SIS IS ONE OF THE FEW DEPARTMENTS IN THE UNITED STATES TO BE RECOGNIZED AS A NATIONAL CENTER FOR ACADEMIC EXCELLENCE IN INFORMATION ASSURANCE EDUCATION AND INFORMATION ASSURANCE RESEARCH.”

Bill Chu, Ph.D.
Professor, Department of Software and Information Systems
College of Computing and Informatics

CONTINUED FROM PAGE 15

The curriculum emphasizes hands-on experiences with specialized labs including:

- Computer Forensics
- Vulnerability Assessment and System Assurance (Penetration Testing)
- Useable Security and Privacy
- IT Infrastructure Design and Implementation
- Secure Software Development

Cyber Corps Program

- One of 34 highly-competitive national programs
- Offers full scholarships for students to study information security
- Students are required to work for a federal, state, or local government agency after graduation for a maximum of two years
- The second largest program in the U.S.
- The only program in North and South Carolina

Student Success Stories:

- First Place, U.S. South Region, iCTF 2006. “Miner’s Threat,” a team of UNC Charlotte cyber-defenders ranked #1 in the South in the 2005 International (cyber) Capture The Flag (iCTF) competition – overcoming NC State, Georgia Tech, and the University of South Florida. iCTF, hosted by UCSB, is the most prestigious, international, intercollegiate cyber game and includes both defensive and offensive aspects. A total of 22 teams from universities in six countries took part in the competition. UNC Charlotte placed 4th among 15 U.S. teams.
- First Place, National, Collegiate Cyber Defense Competition 2006. A team of eight College of Computing and Informatics’ students won first place in the inaugural National Collegiate Cyber Defense Competition (CCDC) hosted by the University of Texas at San Antonio. The UNC Charlotte team overcame three other regional champions and a team comprised of members representing all U.S. military academies. The competition is an important part of the Department of Homeland Security’s (DHS) effort to promote better protection of the nation’s information infrastructure, in that it focuses on cyber defense. Teams are assessed based on their ability to deploy secure IT infrastructure and services.
- Second place, Southeast Collegiate Cyber Defense Competition 2007
- Second place, Southeast Collegiate Cyber Defense Competition 2008
- First place, Southeast Collegiate Cyber Defense Competition 2009
- Second place, Southeast Collegiate Cyber Defense Competition 2010
- First place, Southeast Collegiate Cyber Defense Competition 2011
- Enrolled students taking the CISSP exam have a 100% passage rate.
The College of Computing and Informatics’ Department of Software and Information Systems offers the following short courses on-demand. Most of these can be offered on-site at company locations as well. If you are interested, please contact billchu@uncc.edu with the subject line: SIS short courses.

**Web-Application Penetration Testing I (6 CPE)**
Web applications are primary targets for on-line criminals stealing personal information, as well as committing financial fraud. Through detailed hands-on instruction, this one-day course is intended to introduce to Web application developers basics of Web application penetration testing/ethical hacking by learning the techniques your enemies use to compromise interactive Web sites.

Participants will learn how to use basic penetration testing techniques such as tampering data and encoding/decoding data. Basic hacking techniques for data injection (e.g. SQL injection, cross site scripting) and session management will be covered. Students will have an opportunity to perform penetration testing on a micro-blog Web application. A laptop is required; please review laptop requirements in the box to the right. Each participant will be provided with a take-home DVD with all tools, as well as exercises covered in class. **Prerequisite: Working knowledge of building interactive Web applications in any language (e.g. PHP, Java, Python, Ruby) and familiarity with basic http protocol and session management.**

**Web-Application Penetration Testing II (6 CPE)**
This one-day course is designed to develop the necessary skills for participants to conduct basic Web application penetration testing with confidence. Specific techniques covered include: injection attacks (e.g. SQL injection, cross site scripting), session management attacks, cross request forgery, and direct manipulation. Major focus will be placed on hands-on exercises involving realistic Web sites. A laptop is required; please review laptop requirements in the box to the right. Each participant will be provided with a take-home DVD with all tools, as well as exercises covered in class. **Prerequisite: Web-Application Penetration Testing I or equivalent.**

**Web-Application Penetration Testing III (6 CPE)**
This one-day course is designed to develop advanced skills for participants to conduct Web-application penetration testing by combining multiple techniques. Major focus will be placed on a capture-the-flag exercise which requires multi-staged attacks to be successful. Case studies will be analyzed. A laptop is required; please review laptop requirements in the box to the right. Each participant will be provided with a take-home DVD with all tools, as well as exercises covered in class. **Prerequisite: Web-Application Penetration Testing II or equivalent.**

**Secure Software Development I (6 CPE)**
Vulnerable software is a root cause of many of the security problems we have today. Software vulnerabilities are especially more visible in Web applications as they are most exposed to attacks. This one-day course is designed to provide basic secure software development training to Web developers. Topics covered include: input validation, black box vs. white box validation, regular expressions, proper use of SQL Prepared Statement, and session management. This course is focused on hands-on training. Participants will be able to examine source code of working Web applications and identify security flaws as well as fixing vulnerabilities found. A laptop is required; please review laptop requirements in the box to the right. Each participant will be provided with a take-home DVD with all tools, as well as exercises covered in class. **Prerequisite: Web-Application Penetration Testing I, or equivalent; familiarity with Java/EE development.**

**Secure Software Development II (6 CPE)**
This one-day course is a follow-up to Secure Software Development I. Topics covered include arithmetic operations, common data structures, managing secret information, authentication, authorization, cross domain protection, race conditions, code signing and sealing applications, static analysis, and software considerations for hardware security. A laptop is required; please review laptop requirements in the box to the right. Each participant will be provided with a take-home DVD with all tools, as well as exercises covered in class. **Prerequisite: Secure Software Development I, or equivalent.**
CENTERS, INSTITUTES, AND LABS

Complex Systems Institute (CSI)
The Complex Systems Institute (CSI) brings academia, industry, and federal agencies together to advance computing simulation, analysis, and modeling. Tools developed by CSI members help analysts model infrastructure and social networks, visualize and understand how individual networks behave, and understand multiple-network interdependency behavior, including second- and third-order effects, and unintended consequences.

There are two centers within the Institute. The Complexity Laboratory focuses on dynamic non-linear systems and the development of tools and techniques for studying complexity in natural, physical, and social domains. The Defense Computing Center is responsible for defense- and intelligence-related research, emphasizing system-of-systems modeling and simulation for analysis of complex problems and phenomena.

Director: Dr. Mirsad Hadzikadic
For more information: complexity.uncc.edu

The Cyber Defense and Network Assurability (CyberDNA) Center
The Cyber Defense and Network Assurability (CyberDNA) Center offers high-impact quality research and education in the area of network security, defense, assurability, and privacy. Specific domains of interest include: assurable and usable network security configuration, security automation, security evaluation and optimization, security policy synthesis, and problem/threat diagnosis. In addition, CyberDNA seeks novel, scalable authentication, accountability, and privacy techniques for emerging technologies as well as critical infrastructure networks. The CyberDNA offers an excellent educational environment through conferences, seminars, mentoring, security labs, and test beds, which attracts many graduate and undergraduate students to pursue rigorous research.

Director: Dr. Ehab Al-Shaer
For more information: cyberDNA.uncc.edu

The Defense Computing Center
The Defense Computing Center conducts basic and applied research in computing-related disciplines to address society's defense, intelligence, and security challenges. Research within the Center emphasizes integrated modeling, simulation for analysis of complex problems, and phenomena with application areas including critical infrastructure protection, multi-network interdependency and consequence analysis, and information infrastructure behavior analysis.

Director: Dr. William J. Tolone
For more information: complexity.uncc.edu/complexity-laboratory
The CCI Center for Education Innovation (CEI)
The CCI Center for Education Innovation (CEI) is established in the College of Computing and Informatics for the development and coordination of externally funded projects that incorporate strategies and new technologies for innovation in computing and informatics education. This Center builds on and extends the efforts of DITI and STARS, where DITI has a focus on increasing diversity in the students that choose computing as a career path and STARS establishes educational practices and programs that broaden the skills of computing students.

**Director:** Mary Lou Maer

For more information: cci.uncc.edu/research/Center-for-Education-Innovation

The Human-Computer Interaction Lab
The Human-Computer Interaction Lab investigates novel ways for people to interact with computers, and through computers, in their environments. This lab's research covers a broad range of areas related to human-computer interaction, such as novel interaction and multimedia, computer supported cooperative work, and privacy. We collaborate with researchers in a number of areas related to HCI, such as visualization, virtual reality, gaming, and technical communications.

**Co-Directors:** Dr. Celine Latulipe and Dr. Heather Lipford

For more information: hci.uncc.edu

Laboratory of Information Integration, Security, and Privacy (LIISP)
The mission of the Laboratory of Information Integration, Security, and Privacy (LIISP) is to add value to the university, community, and society through innovative educational programs, research and development in the areas of information integration, security, and privacy. We aim to be one of the leading academic institution for research in information integration, security, and privacy and provide innovative education and training programs in information integration, security, and privacy.

**Director:** Dr. Mohamed Shehab

For more information: liisp.uncc.edu

Interaction Design (InDe) Lab
The InDe Lab investigates how novel interface technologies can be applied to change the way we think, work and behave. We combine methodologies from interaction design, human-centred computing and design cognition to explore new approaches to learning, participating and creating. Our current research focuses include tangible and gestural interaction, crowdsourcing, citizen science, and computational and cognitive studies of creativity.

**Director:** Dr. Mary Lou Maer
For more information about CCI event sponsorship opportunities, please contact Marjorie Bray at Marjorie.Bray@uncc.edu.

For any questions regarding the College of Computing and Informatics, please contact Clark Curtis, Director of Communications, at clarkcurtis@uncc.edu.

**WIRELESS LOGIN**

**Before You Arrive**
1. Set up a new wireless network on your computer.
   SSID (network name): uncc49er
   Security: none
2. Set your computer to connect to this network even if it is not broadcasting.

**When You Arrive**
3. Make sure your computer and wireless access are turned on.
4. Open a web browser window and navigate to any website (you will be re-directed).
5. Accept/allow the security exception pop-up.
6. On the next screen, login as a guest account (use email address of your choice).

For additional information: http://www.helpcenter.uncc.edu/network/wireless_FAQs.html

---

**INFORMATION + QUESTIONS**

1. For more information about CCI event sponsorship opportunities, please contact Marjorie Bray at Marjorie.Bray@uncc.edu.

2. For any questions regarding the College of Computing and Informatics, please contact Clark Curtis, Director of Communications, at clarkcurtis@uncc.edu.
THANK YOU
TO OUR SPONSORS

CYBER SECURITY SPONSORS
GOLD Sponsors
Charlotte Research Institute
UNC CHARLOTTE

BRONZE Sponsors
RTI
Microsoft
RAPID7

TABLE Sponsors
LogRhythm
ORACLE
Bank of America
Womble Carlyle Innovators at Law
PMMC
Cardinal Innovations Healthcare Solutions
FireEye
TIAA-CREF
Wells Fargo
AT&T

EXHIBITORS
Infoblox
Check Point Software Technologies Ltd
paloalto Networks
Qualys
PREMIER
peak 10

BREAK Sponsors
hp
e+

BREAKFAST Sponsor
splunk
The College of Computing and Informatics has already begun planning for the 15th Annual Cyber Security Symposium in 2014. We welcome your suggestions about possible topics, speakers, or enquiries about volunteer opportunities. Please contact Dr. Bill Chu at billchu@uncc.edu. Submissions are due by January 31, 2014.

Stay tuned to cci.uncc.edu.