OCTOBER 11, 2011

UNC CHARLOTTE PRESENTS
The 12th Annual
CYBER SECURITY SYMPOSIUM
Welcome to the annual Cyber Security Symposium. This is the 12th year that our College of Computing and Informatics has organized and hosted the Symposium. It has evolved into the premier event in the region, which brings together both industry practitioners and university researchers to discuss cutting-edge solutions, best practices, and pressing challenges facing cyber security, information assurance, and privacy.

This year’s event is no exception. It features a number of outstanding speakers and experts in the critically important and growing fields of information security and privacy, as well as the global threat of cyber crime and terrorism. 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 let us know how we can make this event even more successful and productive for you by filling out your surveys.

Yi Deng, Ph.D.
Dean and Professor
College of Computing and Informatics
# Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Location</th>
<th>McKnight</th>
<th>Room 210</th>
<th>Room 209</th>
<th>Room 112</th>
<th>SAC</th>
<th>LUCAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:15-8:30a</td>
<td>WELCOME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 8:30-9:20a | Jeff Williams  
CEO, Aspect Security and Volunteer Chair of IASWP  
Securing Code and Culture |          |          |          |          |       |       |
| 9:20-10:10a | Patrick German  
Chief Information Security Officer, Bank of America  
The Next Generation of Cybersecurity |          |          |          |          |       |       |
| 10:10-10:40a | Todd Inskip  
Senior Associate, Booz Allen Hamilton  
Social Networking Security |          |          |          |          |       |       |
| 10:40-11:30a | Elizabeth Johnson  
Partner, Payner Spruill, LLP  
Data Security Legislative Update - What’s Good, What’s Bad, and What’s Really, Really Ugly in Current Bills and New Government Initiatives |          |          |          |          |       |       |
| 11:30-12:20p | Shawn Raborn  
Consultant, InforSec ACE Infrastructure Services, Microsoft Corporation  
Cyber Security  
Organized Crime: The Advanced Persistent Threat |          |          |          |          |       |       |
| 11:30-12:20p | Rich Baich  
Principal, Security & Privacy, Deloitte & Touche, LLP  
Cyber Espionage: Harsh Reality of Advanced Security Threats |          |          |          |          |       |       |
| 11:30-12:20p | Jay Barbour  
Security Advisor, Research in Motion  
Smartphone Security: From a Perspective of the Ten Immutable Laws of Security |          |          |          |          |       |       |
| 11:30-12:20p | Booz Allen Hamilton Tutorial  
Speaker: Eric Cole  
Cyber Security 2011 and Beyond |          |          |          |          |       |       |
| 12:20-1:00p | LUNCH/WELCOME  
Yi Zheng, Dean, CCI |          |          |          |          |       |       |
| 1:00-1:20p | ISSA Presentation |          |          |          |          |       |       |
| 1:20-2:10p | Jessica Staddon  
Privacy Research Manager, SS&G  
Privacy and Social Networks |          |          |          |          |       |       |
| 2:20-3:10p | John Bumpartner  
Chief Technology Officer, U.S. Cyber Consequences Unit (US-CCU)  
Deciphering Cyberwar |          |          |          |          |       |       |
| 2:20-3:10p | John Linkous  
Vice President, Chief Security and Compliance Officer, eBay.com  
FrankenLaws: The Sad State of the Information Security Regulatory Landscape |          |          |          |          |       |       |
| 2:20-3:10p | John Melton  
CCIO, Department of Software and Information Systems  
Securing the SDLC for ten Win |          |          |          |          |       |       |
| 3:10-3:30p | BREAK |          |          |          |          |       |       |
| 3:30-4:20p | Theresa Payton  
CEO and President, Fortigate, LLC  
What Eve from Walk-E Can Teach You About Evolving Threat Vectors |          |          |          |          |       |       |
| 3:30-4:20p | Pete Murphy  
Chief Information Officer, PBH  
Healthcare IT: Under Control or on Life Support? |          |          |          |          |       |       |
| 3:30-4:20p | Will Stranahan  
Affiliated Scientist, CyberDNA  
Epic Foresight: Spectacular Espionage Failures of 2011 |          |          |          |          |       |       |
| 4:20-5:10p | David Brown  
Solutions Engineer, Acquiant, Inc.  
Malware Mitigation Trends |          |          |          |          |       |       |
| 5:15-6:15p | RECEPTION |          |          |          |          |       |       |
SPEAKER PROFILES

Rich Baich
Principal, Security & Privacy | Deloitte and Touche, LLP

Presentation Title: Cyber Espionage: Harsh Reality of Advanced Security Threats

Rich leads Deloitte’s Global Cyber Threat and Vulnerability Management practice and has led multi-national teams designing, implementing, measuring and advising organizations to effectively and efficiently balance risk, technology, and data management decisions with data protection risks, regulatory compliance issues, privacy and security controls. Rich is former Chief Information Security Officer (CISO) at ChoicePoint, Inc. where he held enterprise-wide responsibility for information and technology security. Previously, he held leadership positions within NSA, McAfee, and the FBI. In 2005, Rich authored Winning as a CISO, a security executive leadership guidebook, and was an advisor to the President’s Commission for Cyber Security.

ABSTRACT: Cyber criminals are increasingly attempting to embed covert activities within organizations and government institutions by using stealth techniques and exploits. It’s time for organizations to create a more appropriate preemptive and proactive security posture with business-enabling capabilities. First-generation security practices are no longer sufficient to protect rich targets:

- research and development
- business strategy
- intellectual property
- other business-sensitive information

Advanced Persistent Threats (APT) are modern, automated versions of traditional espionage. APT rarely employs tactics that hurt the current security infrastructure because they have an ulterior motive that benefits from hiding — that is, to set up undetected occupancy, allowing criminals a right-of-entry for doing surveillance, and gathering data. Ultimately, fighting APT, or even the potential for APT, requires continuous monitoring, enriched with actionable cyber intelligence. Please join us for a discussion designed to provide an updated view of the cyber security threats that we perceive as most serious and to present potentially more effective ways of addressing these threats.
Jay Barbour
Security Advisor | Research in Motion
Presentation Title: Smartphone Security: From a Perspective of the Ten Immutable Laws of Security

Jay brings more than ten years of security experience to Research In Motion (RIM) where he serves as an advisor for the BlackBerry Security Group. He works closely with government agencies, strategic and carrier sales teams, and key customers to champion security policy for BlackBerry smartphones. Prior to joining RIM, Jay was vice president of marketing at Intrusion Inc., a pioneering company in data leak prevention appliances. His previous roles include vice president of product management at ScanSafe (now Cisco), the world’s first managed web security start-up, consultant in the wireless industry, as well as various security product management and marketing roles at 3Com and Hewlett-Packard. He started his career in the energy sector, working for Schlumberger in the Middle East and South America as a senior field engineer, as well as ARCO (now BP) as a senior planning analyst. Jay holds a degree in Engineering Physics from Queen’s University, Canada, an MBA from INSEAD, France, and is a Certified Information Systems Security Professional (CISSP). Jay is based out of Dallas.

ABSTRACT: “The Ten Immutable Laws of Security” were first published by Microsoft about ten years ago and they bluntly capture the hard-learned lessons from PC and server security. This presentation reviews these laws and illustrates how many current smartphone security issues have arisen because of their disregard. Another major smartphone security risk, not covered by the Ten Laws, is enterprise data leakage through the personal use case. An innovative approach to address this security issue will also be discussed. The introduction to this session will review why smartphone security is becoming more critical as enterprises mobilize their sensitive back-end IT systems, and hence why the “Ten Laws” are important, now more than ever.

Sean Bodmer
Senior Threat Intelligence Analyst | Damballa, Inc.
Presentation Title: SpyJackers - Countering Persistent Threats

Sean is an active senior threat intelligence analyst at Damballa. He specializes in the analysis of signatures and behaviors used by the cyber criminal community. Sean focuses his time learning tools, techniques, and procedures behind attacks and intrusions related to various persistent threats. Sean has worked in several information system security roles for various firms and customers over the past fifteen years across the United States. Most notably he has spent several years performing black box penetration testing, exploit development, incident response, and intrusion and intruder analysis for Fortune 100 companies, the Defense Department, and other federal agencies. Sean has shared numerous accounts of his findings at various industry conferences relating to the inner-workings of advanced cyber threats. Sean has lectured at industry conferences such as Hacker Halted, Blushtag, Defcon, Decon Skytalks, TakeDownCon, PhreakNIC, DC3, NWSIC, NSA, DHS Annual Security Symposium, Pentagon Security Forum, CERTCC, InfowarCon, and before US Congress discussing his interest in analyzing and manipulating the minds and morale of persistent threats without their knowledge. Sean co-authored Hacking Exposed: Malware & Rootkits: Malware & Rootkits & Secrets & Solutions (the definitive Computer Security book series) with McGraw-Hill in 2009. Sean is currently working on his second book covering “Countering Advanced Cyber Threats,” a comprehensive manual that illustrates how to employ various methods of counter-intelligence, disinformation, and deception against active threats in order to learn the ‘who’ and ‘why’ behind the breach of your enterprise.

ABSTRACT: This lecture builds on a series of threats and countermeasures used to attribute specific occurring events to the individual or group. In this lecture, intelligence analysis, cyber-counterintelligence, and operational implantations will be covered specifically, how to objectively analyze the details of an intrusion in order to generate highly-accurate assessments (profiles) of your adversary which can help IT security professionals and/or authorities with attribution and/or apprehension of a cyber criminal. The ability to maintain access and collect information on a target with advanced or persistent access to your enterprise is the bread-and-butter of premier intelligence agencies around the world. After attending this lecture, attendees will have a better understanding of concepts that utilize counter-intelligence, deception, and disinformation in the realm of cyber while amplifying attribution and will be equipped with techniques they can implement to better protect their networks and hackers who are hacking private and commercial assets for political, economical, and personal leverage.
David Brown, CISSP, CISM
Solutions Engineer | Accuvant, Inc.
Presentation Title: Malware Mitigation Trends

Mr. Brown has over 25 years of experience in IT-related fields, including more than 15 years focused on information security. David has a long history of solving the business and information security needs of a wide range of clients from Fortune 50 accounts to small businesses. Areas of expertise include security program design and review, incident management planning and response, including litigation hold (eDiscovery); policy and process development; vulnerability assessment; secure application development; security technology implementation, and training and project management. David has held the positions of director of management information systems, corporate information security officer, managing consultant, solutions architect, and senior security engineer. In these positions, Mr. Brown has provided information security services for the financial, utilities, telecommunications, retail, health care, pharmaceuticals, and entertainment industries.

ABSTRACT: The nature of the continually-evolving malware threat and the criminal innovations that are taking place at a record pace require enterprises to adopt a multi-faceted approach to malware, if they even hope to have a chance. Attack surface management, active controls at either the host and/or network, combined with an effective investigative capability will provide organizations the tools needed to help mitigate the impact of malware on its business. A countermeasure, or compensating control used in isolation, will likely not provide the breadth needed to cover all the possible attack vectors presented by modern malware threats.

Please join Accuvant for a lively discussion on malware mitigation trends. Topics to be covered include:

- Commercialization of the malware market
- Changes in the malware market that have made current countermeasures less effective (IPS, AV and SWG aren’t cutting it)
- New entrants into the malware defense market and where they best fit into a security infrastructure

John Bumgarner
Chief Technology Officer (CTO), U.S. | Cyber Consequences Unit (US-CCU)
Presentation Title: Deciphering Cyberwar

John is a former U.S. Marine and U.S. Army Special Operations soldier. During his eighteen-year career, he conducted a wide range of military and intelligence missions throughout the world. Bumgarner is the recipient of numerous awards and decorations, including those for participation in several foreign campaigns, meritorious service, and heroism. In his civilian career, he holds several private sector certifications including CISSP, GIAC (Gold), and dual master's degrees in Information Systems Management and Security Management. John is the principal author of the US-CCU's much-acclaimed analysis of the August 2008 cyber campaign against Georgia. In collaboration with Scott Borg, Bumgarner is also the co-author of US-CCU Cyber Security Check List, which is currently used by cyber security professionals in over eighty countries. Bumgarner has regularly served as an expert source and commentator for numerous national and international news organizations, including The Wall Street Journal, Business Week, The Los Angeles Times, Reuters, The Economist, the Indian Times, and The Guardian, as well as numerous specialty and trade publications. He has appeared on NBC, CNN, and the BBC, and has been heard on CBC/Radio-Canada, BBC Radio Northern Ireland, and Federal News Radio in the United States. He is featured in the International Spy Museum's "Weapons of Mass Disruption" cyber warfare exhibit in Washington, D.C.

ABSTRACT: One of the most misunderstood and misused terms in the world today is cyberwar. Militaries around the world are gearing up for battle in cyberspace against digital foes, both foreign and domestic. Some experts have proclaimed that nations are currently locked into a Cyber Cold War with an accompanying cyber arms race fully underway.

The United States has begun working with its allies to add a cyber warfare doctrines to existing military treaties. Russia has stated that a devastating cyber attack will warrant a conventional military strike and hasn't ruled out using nuclear weapons as a response strategy. Unfortunately, the United Nations still hasn't formally reviewed Article 51 for its applicability in cyber attacks against member nations. Hopefully, before the first cyber strike is launched politicians and warriors alike will be able to decipher the 5th domain of warfare, before it's too late.
Patrick Gorman
Chief Information Security Officer | Bank of America
Presentation Title: The Next Generation of Cybersecurity

Patrick Gorman is Chief Information Security Officer at Bank of America. He leads the team responsible for the bank's information security strategy, policy, and programs. Gorman is a senior strategy and technology executive with more than 25 years of experience in government and the private sector, including serving as associate director of national intelligence, and chief information officer for the U.S. Director of National Intelligence. Prior to joining the bank, he was senior executive advisor for cybersecurity and advanced analytics at Booz Allen Hamilton, responsible for strategic planning and capability development for the firm’s cybersecurity portfolio. He rejoined Booz Allen Hamilton from the Office of Director of National Intelligence where he managed the Intelligence Community’s Incident Response Center.


ABSTRACT: Bank of America chief information security officer Patrick Gorman will discuss current cybersecurity threats, risks to the global financial services industry, and Bank of America’s approach to protect its information assets and secure its infrastructure.

Todd K. Inskeep
Senior Associate | Booz Allen Hamilton
Presentation Title: Social Networking Security

Todd recently joined Booz Allen Hamilton as a senior associate working on commercial banking services, security, mobile, and social networking. Todd previously led Bank of America’s consumer team exploring the future of authentication, customer protection and social spaces, where he improved consumer security experiences, fighting fraud across channels including ATM, telephone, mobile, and on-line banking. Inskeep also championed the enterprise strategy for using social spaces to deliver products and services through services like Facebook, Twitter, and YouTube. Inskeep brings over 20 years experience in innovation, information security, and Internet experience. He has filed multiple patent applications, and spent time as an executive-in-residence at the MIT Media Lab’s Center for Future Banking. Inskeep started his career in the Information Security group of the National Security Agency.

ABSTRACT: Social media and networking have been the “hot topics” in business, risk, and security circles. Marketing teams are focusing on social media for brand and relationship management. Security and compliance are focusing on managing risk to protect the enterprise. Often the risk benefits lean towards blocking access to social network sites because of the persistent threats. People have always been social - our conversations connect us to each other, to brands, and to products. For security professionals, the challenge is to enable our business partners to utilize these sites, while minimizing the risk. Mr. Inskeep will talk about how leading companies are saying ‘yes’ to social media and networking, while balancing the risk management.
VISION:

"I 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."

Yi Deng, Ph.D.
Dean and Professor
College of Computing and Informatics

Elizabeth Johnson
Partner | Poyner Spruill LLP

Presentation Title: Data Security Legislative Update - What's Good, What's Bad, and What's Really, Really Ugly in Current Bills and New Government Initiatives

Elizabeth Johnson is based in Poyner Spruill's Raleigh office. She leads the firm's Privacy and Information Security Practice Group. Elizabeth's practice focuses on privacy, information security, and records management. Her comprehensive, practical approach to privacy law is reflected by the diversity of her clients, which hail from a variety of industries including health care, financial services, insurance, retail, telecom, utility, technology, consumer goods, and client services. Elizabeth has also worked with organizations of various sizes and scope, ranging from Fortune 100 companies with international reach, to local charities. In her spare time, Elizabeth enjoys volunteering with the Red Cross. She can be reached at 919-783-2971, or ejohnson@poynerspruill.com.

ABSTRACT: Elizabeth will discuss some of the recent federal legislative proposals aimed at data security and breach notification, describing key features of some pending federal bills and the real-world impact should some of these requirements become law. Select developments in federal regulatory and state-based initiatives, and their potential impact nationwide, will also be discussed. In all cases, real-world examples will be used to illustrate what is good, bad, and ugly about these proposals and initiatives.
John Linkous is a 15-year information security industry veteran, and a trusted technology and governance advisor to CISOs, CIOs, and CTOs across the Fortune 500 and federal agencies. At elQnetworks, John is responsible for helping customers map their real-world challenges in security and compliance with the extensive capabilities of elQnetworks’ unified situational awareness solutions.

Prior to elQnetworks, John was VP of Technology at NSC-Sabera, where he was responsible for the design and architecture of the Common Compliance Framework (CCF), a comprehensive IT-GRC solution. Previously, John was a co-founder of Technology Workflow Solutions, where he was a hands-on security consultant and outsourced CISO for a number of global organizations in the healthcare, financial services, aerospace, and manufacturing industries. Earlier in his career, he was CIO at Widmeyer Group, one of the largest privately-held public relations firms in the United States. John began his career at NASA, where he was the recipient of Goddard’s individual “Contractor of the Year” award. John earned a B.A. in History and English Literature from the University of Maryland, and holds numerous industry technical certifications.

**ABSTRACT:** In Mary Shelley’s “Frankenstein,” the eponymous doctor used a patchwork of parts from cadavers to make a living, breathing creature that he hoped would usher in a new era for mankind. The result, as we all know, was not quite what he had originally envisioned.

In a similar vein, over the past decade information security practitioners have been subject to a similar random patchwork of well-meaning – but only marginally effective – regulatory mandates from every possible source – governments, international bodies, industry authorities, and even business partners. By and large, the end result, for the public and private organizations that are required to implement them, has been a byzantine labyrinth of complex — and sometimes conflicting — requirements that have understandably left security and compliance professionals frustrated as a steady flow of auditors and consultants ingress into their organizations, while valuable budget dollars, that could otherwise be used on real security solutions, flow out. Meanwhile, the industry has seen a relentless onslaught of successful data breaches and other attacks in recent months against a plethora of household names ranging from Sony, the CIA, and the US Senate, to Citibank and the IMF. If these security-related mandates are intended to prevent bad things from happening, they’re clearly failing miserably at that goal.

In this presentation, security and compliance expert John Linkous provides a detailed overview of how we got into this sad state, and what both security and compliance professionals, as well as regulators, can do to get us out of the quagmire. Attendees will walk away with practical knowledge that includes:

- a comprehensive overview of current regulations, best practices and standards related to information security across both commercial and government organizations
- the significant gaps between the mandates in these laws and actual security, and why the disciplines of compliance and security are not the same thing
- what both security practitioners and regulatory bodies can do to close this gap, and why some upcoming regulations should provide a glimmer of hope to information security practitioners
- what the regulatory compliance landscape should look like in another ten years, if we really want compliance to help us stop data breaches and other attacks
John Melton
CCI Department of Software and Information Systems
Presentation Title: Securing the SDLC For teh Win

John's current work is in web application security analysis. Previous work has included systems development and web application development, with a focus on security. John received both his B.S. in Computer Science and M.S. in Information Technology at UNC Charlotte. He has worked at The National Security Agency, U.S. Bank, Wells Fargo, and UNC Charlotte. He is married and has two baby boys.

ABSTRACT: In Epic Failpalm, we uncovered the application weaknesses which threats have been attacking for the past year. In this presentation, we show you practices you can incorporate into your own SDLC to identify, mitigate, and prevent these weaknesses within your own applications. We'll look at the people, processes, and technology which can help to reduce the risk presented by your application. We'll look at existing industry recommendations and draw out some common practices that can help.

Pete Murphy
Chief Information Officer | Piedmont Behavioral Healthcare (PBH)
Presentation Title: Healthcare IT - Under Control or on Life Support?

Pete is the CIO of Piedmont Behavioral Healthcare. Mr. Murphy has more than 25 years' experience in technology management, information security, and risk management roles in the financial services industry. These roles include application systems development and management, technology risk and control, information security, technology resiliency, operational risk management, and infrastructure service delivery.

ABSTRACT: The healthcare industry is under tremendous pressure to change the way care is managed and paid for and Healthcare IT (HIT) is a key lever being used to facilitate these changes. All of the parties involved with giving care and paying for it are struggling to move at light speed to improve health outcomes, reduce fraud, waste and abuse, and control escalating costs. This session will examine what is going on with HIT and what information security and risk management professionals should be focusing on, as this industry struggles with significant government deadlines for interconnection, information exchange, and access.

Theresa Payton
CEO and President | Fortalice®, LLC
Presentation Title: What Eve from Wall-E Can Teach You About An Evolving Threat Vector

Starting her career in banking technology in 1980, Theresa has worked at Barnett (now Bank of America), First Union (now Wells Fargo), and Bank of America. She's led strategic planning teams, managed mergers and acquisitions, run technology and operations for branches, internet and call centers, and has overseen fraud, risk and security management technology operations. From May 2006 until September 2008, Theresa worked for the Bush Administration as the White House Chief Information Officer (CIO) in the Executive Office of the President (EOP). She was the first woman to hold this position, and her team served the President and the 3,000+ members of the EOP. Now the Chief Advisor and CEO of Fortalice, LLC, Theresa and her team deliver security, risk and fraud consulting services to private and public sector organizations. She holds a TS-SCI. She has a Bachelor of Arts double major in Economics and Business Administration. Certification in Computers; Cum Laude, Immaculata University, 1989; a Masters of Science, Management Information Systems (MIS), University of Virginia, 1990, and Certificate of Graduate Banking Studies, The Graduate School of Banking at Louisiana State University, 1997. She recently attended a session with the U.S. Army Special Operations Forces where she was trained to shoot sniper rifles and rescue injured soldiers in the field.

ABSTRACT: Forensic analysis of breaches show that human error contributed to vulnerabilities, creating a weakness that was exploited. There is a group of focused, dedicated employees that love working for you. They are creative, innovative, and hard chargers. And like Eve, put your company mission at risk by the likes of Auto, the supercomputer in Wall-E. This presentation will provide an in-depth overview, based on real cases, of how social media can either be a boon to your business or become the next major threat vector.
Shawn Rabourn  
Senior Security Consultant, InfoSec ACE Infrastructure Services | Microsoft Corporation  
Presentation Title: Cyber Security Organized Crime: The Advanced Persistent Threat

A graduate of Colorado State University, Shawn Rabourn joined Microsoft in 2001 on the Enterprise Active Directory Support team where he became a specialist in a number of Windows Security Technologies. He moved to Premier Field Engineering and helped charter the Scarce Skills team, focusing on low-volume and incubation technologies. Shawn later joined the Microsoft IT Information Security (InfoSec) ACE Team for Infrastructure Services. Shawn currently specializes in a number of infrastructure security technologies, including public key infrastructure and identity management. Shawn holds the Certified Information Systems Security Professional (CISSP), Microsoft Certified Systems Engineer (MCSE), Microsoft Certified Solutions Developer (MCSD), Microsoft Certified Database Administrator (MCDBA), Microsoft Certified Systems Administrator (MCSE), and Microsoft Certified Application Developer (MCAD) certifications.

Jessica Staddon  
Privacy Research Manager | Google  
Presentation Title: Privacy and Social Networks

Jessica is a research scientist at Google working on leveraging large datasets for better security and privacy. Her other interests include usability of security and privacy technology, and cryptographic algorithms. Prior to Google, she was an area manager at Xerox PARC and a research scientist at Bell Labs and RSA Labs. She serves regularly on the program committees of ACM- and IEEE-sponsored security/privacy conferences and is on the editorial boards of the Journal of Computer Security and the International Journal of Information and Computer Security. Jessica holds a Ph.D. in Mathematics from U.C. Berkeley.

ABSTRACT: The tension between on-line social services and privacy is readily apparent. On-line social networks are invaluable for making connections between people and facilitating sharing, but can also include the unintentional over-sharing of content and incidents of unwanted on-line attention from other users. Jessica will talk about gauging privacy concerns, expectations, and feature utility as integral parts of the process of building an engaging and privacy-aware social network. Drawing examples from experience with Google+, she will discuss how each is key to our iterative privacy design process, which includes threat assessment, data analysis, and ample user studies.
Will Stranathan
Affiliated Scientist | CyberDNA
Presentation Title: Epic Facepalm: Spectacular Appsec Failures of 2011

Will Stranathan is an affiliated scientist with CyberDNA. Mr. Stranathan has been a security professional for eight years, and has been writing in secure code for 33 years. He performs ethical hacking engagements against applications, and performs security source code reviews. He also maintains an application security blog geared toward writing secure code, rather than emphasizing insecurity. Mr. Stranathan lives in the Charlotte area.

Jeff Williams
CEO | Aspect Security and the Volunteer Chair | OWASP
Presentation Title: Securing Code and Culture

Jeff Williams is the founder and CEO of Aspect Security, specializing in application security services including code review, penetration testing, training, and eLearning. Jeff also serves as the volunteer Chair of the Open Web Application Security Project (OWASP), where he has made extensive contributions, including the Top Ten, WebGoat, Secure Software Contract Annex, Enterprise Security API, Application Security Verification Standard, OWASP Risk Rating Methodology, creating the worldwide local chapters program, and starting the Rugged Software movement. Jeff holds advanced degrees in psychology, computer science, and human factors, and graduated cum laude from Georgetown Law. You can contact Jeff at jeff.williams@aspectsecurity.com.

ABSTRACT: There’s a math problem with application security. The costs associated with finding and fixing an organization’s software vulnerabilities are dramatically more than anyone has to spend. Attempts to automate our way out of this crisis have left us with inch-deep coverage and huge numbers of minor findings to address. In this talk, Jeff will share his experiences working with organizations to create a culture that naturally produces application security—breaking the cycle of trying to hack ourselves secure. You’ll learn techniques for building bridges between developers and security, how to give developers the foundation they need to build secure code, and why you should stop application penetration testing.
**TUTORIAL:**

**Booz | Allen | Hamilton**

delivering results that endure

---

**Eric Cole**  
Principal, Booz Allen Hamilton  
**Presentation Title:**  
Cyber Security 2011 and Beyond

---

**ABSTRACT:** Over the last few years cyber attacks on a variety of public and private companies have grabbed headlines and attention. Stuxnet laid out a blueprint for future attacks threatening both cyber and physical systems. Advanced Persistent Threats have been the latest to grab headlines in the media. With all this attention, what should companies be worried about and how can they protect themselves? Join Booz Allen Hamilton’s, Dr. Eric Cole, author of several books, including; "Hackers Beware," "Hiding in Plain Site," "Network Security Bible," and "Insider Threat." Eric Cole will discuss his unique perspective on the state-of-security as a former member of the Commission on Cyber Security for the 44th President.

---

**TUTORIAL:**

**RSA**

---

**Jim Guido**  
Stalwart Principal Engineer, RSA  
**Presentation Title:**  
Developing a Governance, Risk and Compliance Framework in Your Enterprise

---

**ABSTRACT:** Enterprise Governance, Risk and Compliance, or eGRC, is an umbrella term that describes how an organization defines the objectives, policies and procedures by which it is managed; pursues opportunities while avoiding or managing negative events; and demonstrates adherence to laws, regulations, policies, contractual obligations, and industry standards. Organizations have been practicing eGRC in a piecemeal fashion for decades, but only in recent history have they approached eGRC as a holistic strategy for managing risk and compliance across functional domains and the lines of business. In the current atmosphere of global economic stress, heightened regulation and increasingly complex risks, an eGRC strategy, supported by the right technology platform, is more important than ever before.
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
- Healthcare IT
- Geographical Information Systems
- Intelligent Information Systems
- Advanced Database and Knowledge Discovery
FACT:

"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."

Bill Chu, Ph.D.
Chair, 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)
- Usable 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
- 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. 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. 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. 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 PreparedStatement, 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. 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. 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: http://www.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 Center 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: http://www.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: http://www.complexity.uncc.edu/?q=Defense-Computing-Center

The Diversity in Information Technology Institute (DITI)
The Diversity in Information Technology Institute (DITI) is an organized effort to increase the size and diversity of the information technology workforce to meet the growing demand for IT professionals across a wide range of disciplines. The Institute brings together IT and education researchers, K-12 educators, and industry and community leaders to deploy DITI initiatives.

Director: Dr. Teresa Dahlberg
For more information: http://www.coit.uncc.edu/diti/

The Human-Computer Interaction Lab (HCI)
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: http://hci.sis.uncc.edu/
NOTES
**SAVE THE DATE**  Wednesday, April 25, 2012

UNC CHARLOTTE PRESENTS
The 4th Annual
SaaS CLOUD COMPUTING CONFERENCE

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

---

**WIRELESS LOGIN**

1. Open the network settings for your wireless device.
2. Enter “uncc49er” as the SSID or Network Name in the wireless settings. (“Add Network” for Windows Xo – “Other Network” in Airport for Mac OS X.)
3. Disable WEP or other encryptions, if enabled.
4. Your wireless devices should find the network if you are in an area where wireless is available.
5. Open your web browser (Internet Explorer, Firefox, Safari, etc.).
6. You will be prompted to enter a campus login. If you are a guest, enter your email address in the guest login area.
7. A guest login on the UNC Charlotte wireless network will only be able to use web sites or web mail using port 80 (standard http port).

---

**INFORMATION + QUESTIONS**

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.
THANK YOU
TO OUR SPONSORS

UNC Charlotte Partner Sponsor

UNC CHARLOTTE

Charlotte Research Institute

GOLD Sponsors

Bank of America

Duke Energy®

TIAA CREF

FINANCIAL SERVICES
FOR THE GREATER GOOD®

BRONZE Sponsors

Booz Allen Hamilton
delivering results that endure

Microsoft

RSA

TABLE Sponsors

Accuvant

Bank of America

Deloitte

EXHIBITORS

ARA

SecureWorks

fishnet SECURITY

hp

peak 10

data center solutions
The College of Computing and Informatics has already begun planning for the 13th Annual Cyber Security Symposium in 2012. 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, 2012.

cci.uncc.edu/security