College of Computing and Informatics
UNC CHARLOTTE

CHAT ABOUT THE EVENT:
#CSSUNCC

UNC CHARLOTTE
PRESENTS

The 13th Annual CYBER SECURITY SYMPOSIUM

October 10, 2012

UNC CHARLOTTE

Charlotte
Research
Institute

College of Computing and Informatics
UNC CHARLOTTE

9201 University City Boulevard
Charlotte, North Carolina 28223
704-687-7983
www.cci.uncc.edu

SHARE YOUR THOUGHTS:
#CSSUNCC

TABLE OF CONTENTS

FRIENDS + COLLEAGUES

Welcome to the Annual Cyber Security Symposium. This is the 13th 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

TIME	LOCATION	ACTIVITY	SPEAKER
7:30-8:15	McKnight	Registration	
	Lucas	Continental Breakfast	
8:15-8:30	McKnight	Introduction	Bob Wilhelm, Vice Chancellor Research and Economic Development and Executive Director, CRI
8:30-9:20	McKnight	Security Intelligence, Analytics, and the Changing Threat Landscape	Steve Robinson, IBM
9:20-9:40	Lucas	**BREAK**	
9:40-10:30	McKnight	Top Ten Defenses for Web Application Security	Jim Manico, WhiteHat Security
10:30-10:50	Lucas	**BREAK**	
10:50-11:40	McKnight	**PANEL DISCUSSION:** Big Data for Security	Vince Crisler, Zeichner Risk Analytics Lisa Donnan, The Analytic Sciences Corp. Theresa Payton, Fortalice®, LLC
	210	Bring Your Own Risk	Frank Witter, Symantec
	208	TUTORIAL I: Advanced Phishing Tactics – Beyond user awareness	Martin Bos and Eric Milam, Sr. Security Analysts for Accuvant Labs
	112	Improving Manual Code Review with SAST	William Stranathan, Cyber DNA
11:40-12:30	McKnight	When Time is of the Essence…	Steve Salinas, Guidance Software, Inc
	210	The “New” Organized Crime Paradigm	Chris Swecker, Chris Swecker Enterprises
	112	DHS Cyber Test Bed Overview and Lessons Learned	Theresa Payton, Fortalice®, LLC Kemal Piskin, Applied Research Associates, Inc.
12:30-1:10	SAC	**LUNCH**	
1:10-1:20	SAC	A Word from CCI Staff	Yi Deng, Dean, College of Computing and Informatics (CCI); Marjorie Bray, Director of Development, CCI
1:20-1:30	SAC	Center for Configuration, Analytics, and Automation	Ehab Al-Shaer, Director CyberDNA Center, CCI
1:30-2:30	SAC	**PANEL DISCUSSION:** Future of Enterprise Security and Privacy	Rich Baich, Wells Fargo Ron Ritchey, Bank of America Dick Langford, BB&T Tom Bartolomeo, First Citizens Bank
2:30-3:10	Lucas	**BREAK**	
	Lucas	Hack Fortress	49th Security Division
3:10-4:00	McKnight	Is that a Laptop in Your Pocket?	David Merrill, IBM
	210	Governance, Risk and Compliance Program	Sanjeev Sah, UNC Charlotte
	Lucas	Hack Fortress	49th Security Division
4:00-4:50	McKnight	Principles for Achieving Success in Information Security	William Thornhill, TIAA-CREF
	Lucas	Hack Fortress	49th Security Division
5:00-6:15	Lucas	**RECEPTION**	
	Lucas	Hack Fortress	49th Security Division

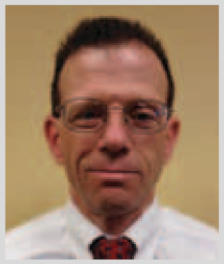
SPEAKER PROFILES

Rich Baich

Chief Information Security Officer For Enterprise Technology Services | Wells Fargo

Panel Discussion: Future of Enterprise Security and Privacy

Rich currently is the Chief Information Security Officer for Enterprise Technology Services for Wells Fargo. Prior to his current position at Wells Fargo, Rich led 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 the 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.

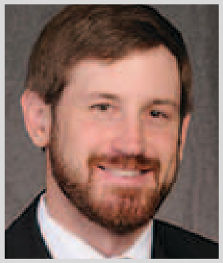


Tom Bartolomeo

CISO and Group Vice President | First Citizens Bank

Panel Discussion: Future of Enterprise Security and Privacy

Tom Bartolomeo joined First Citizens Bank in March of 2011 as the Chief Information Security Officer. Prior to that he spent the past 17 years at Wells Fargo (First Union & Wachovia). Tom has over 17 years in running all aspects of information security including, ecommerce security and online fraud protection. In addition, Tom developed and implemented the initial Internet and online strategy for First Union in 1994.



Vince Crisler

Senior Vice President | Zeichner Risk Analytics (ZRA)

Panel Discussion: Big Data for Security

Vince Crisler is a Senior Vice President at Zeichner Risk Analytics (ZRA), a company that focuses on cybersecurity risk management, program management, and consulting for both the public and private sectors. Vince oversees the company's efforts in supporting federal departments and agencies, national labs, and private sector cybersecurity consulting.

Prior to joining ZRA, Vince served in two different leadership roles at the White House's Office of Administration to include the Director of Customer Advocacy and Director of Information Assurance. In the latter role, he led a significant modernization program overhauling IT Security to include the creation of the first-ever 24x7x365 Security Operations Center for the EOP. His efforts included significant work with the Department of Homeland Security, the National Security Counsel, the Homeland Security Counsel, the National Security Agency, and the Defense Information Systems Agency.
Prior to working with the White House, Vince served in the United States Air Force as a communications officer and completed assignments to include the White House Communications Agency, the National Military Command Center in the Pentagon, and Ramstein Air Base in Germany. Vince graduated from The Ohio State University with a degree in Computer and Information Science and lives in Alexandria, Virginia with his wife, Marcy, and two children

Lisa Donnan

Vice President, Strategy & Technology | The Analytic Sciences Corporation (TASC)

Panel Discussion: Big Data for Security

Lisa Donnan is an accomplished senior executive with twenty years of global technology experience. Lisa has built a reputation around successfully commercializing technology and launching new markets and products in the government and commercial markets. She has a proven leadership ability to set growth agendas by redefining market strategies, overhauling operations, recruiting top talent, and delivering profitable results. Lisa most recently led Salient Federal Solutions' cyber security business unit bringing advanced cyber security solutions, information assurance, engineering services and technology to public and private sector organizations. Lisa created and built the Cyber Security unit, while at Command Information, a venture of The Carlyle Group, Novak Biddle Venture Partners, and Paladin Capital Group. She maximized its ability to scale, launched an early venture software business to meet the full needs of the market, and to exceed projected revenue goals. This resulted in the purchase of Command Information to Salient Federal Solutions in March 2011.

Dick Langford

VP, Information Security Officer | BB&T

Panel Discussion: Future of Enterprise Security and Privacy

Dick Langford has over twenty years of experience in information security within the financial services industry, first with the Federal Reserve Bank of Kansas City and now with BB&T for the past 14 years. Dick reports to the CISO and manages Information Security Governance, which includes responsibility for policy/standards, education and awareness, and compliance monitoring and reporting. His expertise focuses on the people/process part of information protection - creating a security-conscious culture that is aware of and compliant with corporate information security policies and standards. He has also led incident response efforts, and is very knowledgeable in client notification requirements of privacy/information security laws and regulations. Dick has presented to diverse groups such as the Computer Security Institute, Western Carolina University, Kentucky Society of CPAs, and the Northern Virginia Technology Council.

Jim Manico

VP, Security Architecture | WhiteHat Security

Presentation Title: Top Ten Defenses for Web Application Security

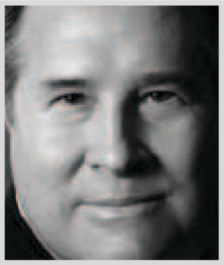
Jim Manico is the VP of Security Architecture for WhiteHat Security. Jim is also the host of the OWASP Podcast Series, is the committee chair of the OWASP Connections Committee, is the project manager of the OWASP Cheatsheet series, and is a significant contributor to several additional OWASP projects. Jim provides secure coding and developer awareness training for WhiteHat Security, using his 8+ years of experience delivering developer-training courses for SANS, Aspect Security, and others. He brings 16 years of database-driven Web software development and analysis experience to WhiteHat and OWASP as well. Jim works on the beautiful island of Kauai, Hawaii where he lives with his wife Tracey.

ABSTRACT: We cannot hack or firewall our way secure. Application programmers need to learn to code in a secure fashion if we have any chance of providing organizations with proper defenses in the current threatscape. This talk will discuss the 10 most important security-centric computer programming techniques necessary to build low-risk web-based applications. This talk is best suited for technical web application development professionals at any stage of the software development lifecycle.

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



David Merrill

Senior Technical Staff Member | IBM, Security Systems Division

Presentation Title: Is that a Laptop in Your Pocket? Security and Privacy in the Age of Mobility

David Merrill is a Security Consultant in IBM's newly formed Security Division. Prior to that, he was the strategist for endpoint security and malware protection in IBM's Chief Information Security Office, while also advising dozens of IBM's Fortune 500 clients. Previously, David also served as IBM's Global Security Operations Manager, where he directed the daily operation of IBM's worldwide internal IT security. David is a popular speaker and industry-recognized expert in the areas of endpoint, mobile, and cyber security.

Bloomberg News, eWeek, Network World, Baseline, CIO Insight, SiliconAngle, Forbes, and Institute of Advanced Security have all recently interviewed David. He was a keynote speaker at the Juniper Networks Mobile Security press launch and is a frequent presenter at Tivoli Pulse and SANS. The 2011 and 2012 X-Force Annual Trend and Risk Report features his mobile security insights, along with sharing his thoughts and insights as a regular contributor to the Institute of Advanced Security.

A multiple patent holder, David is also the inventor and architect of the IBM Threat Mitigation Service (ITMS), the automated malware response system in use within IBM today.

ABSTRACT: In the past decade, mobile platforms and applications have become a critical part of an organization's infrastructure. And this trend is expected to continue. While the productivity benefits are obvious, IT security professionals and business leaders are struggling with the security, privacy, and compliance consequences of this trend. Smart phones are more like laptops than phones, and as a result, need to have all of the same security controls and configuration requirements that laptops have. The challenge is how to implement and verify those controls – across platforms, across networks, and across the world. The IBM CIO office has met this challenge head-on, for its more than 400,000 globally-distributed employees and contractors. In this session, we'll provide an overview of the data-focused approach that was used, mobile threat landscape, key considerations for mobile device security and management, and share lessons learned from the IBM CIO office.

Theresa Payton

CEO and Chief Advisor | Fortalice®, LLC

Presentation Title: DHS Cyber Test Bed Overview and Lessons Learned
Panel Discussion: Big Data for Security

Theresa Payton is a well-known and highly respected national authority on cybersecurity, e-crime and fraud mitigation, and technology implementation. She has over twenty years of advanced business and security technology expertise and leadership at the highest levels of government and in the financial services industry, including being the first woman to serve as Chief Information Officer at the White House.

From May 2006 until September 2008, Payton served as Chief Information Officer at the White House. In this role, she provided oversight of the information technology enterprise for the President and 3,000 staff members. She oversaw dramatic upgrades to the IT security posture for the Executive Office of the President and worked closely with security assets of the U.S. Government in the civilian, military, and intelligence community. Payton was the first woman to hold this position.

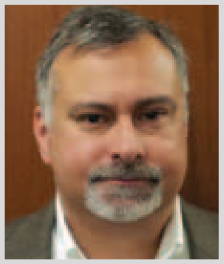
Prior to government service, Payton had a long career in the financial services industry, leading teams focused on improving banking technology and security. Ms. Payton has held senior leadership positions at both Bank of America and Wells Fargo. She led strategic planning teams, managed mergers and acquisitions, ran technology operations, internet and call centers, and oversaw fraud and risk management technology operations. Payton currently runs Fortalice®, LLC, which provides security, risk, and fraud consulting services. Payton is also a co-author of a new book "Protecting Your Internet Identity: Are You Naked Online?," published by Rowman & Littlefield. She serves on several college and university boards, is involved in a national cybersecurity curriculum initiative, and is a member of FBI's North Carolina Infragard.

ABSTRACT: The Cyber Test Bed is a project of the Institute of Homeland Security Solutions (Research Triangle Institute, Duke University, the University of North Carolina and the NC Military Foundation), and Applied Research Associates (ARA). ARA is the principle subcontractor and architect of the Test Bed methodology and conceptual framework.

The Cyber Test Bed tested ways to identify, deploy, and evaluate best practices for cyber security in small and mid-size companies in the corporate sectors by:

- Identifying key incentives, create incentive models, and test proactive motivators
- Benchmarking changes in core security behaviors and decision-making
- Providing a security model associated with asset awareness
- Defining a simple, scalable methodology for small to mid-size companies to reduce cyber security risks
- Developing a prototype of the elements of a corporate culture that views cyber security from a holistic asset protection environment

The Test Bed is using the results of the project to produce a best practice methodology for small and mid-size companies. The Test Bed approach will lead to a better understanding of threats, the development of models to predict potential impacts, and the deployment of tactical deterrents. By identifying and testing best practices using existing technologies in cyber security for the private sector, the Test Bed will contribute to the DHS mission to improve cyber security, while also mitigating intellectual property loss critical to economic and national security.



Kemal Piskin

Senior Cyber Security Engineer | Applied Research Associates, Inc.

Presentation Title: DHS Cyber Test Bed Overview and Lessons Learned

Mr. Piskin is a decorated, retired Naval Officer with an MS in Information Systems, specializing in Cyber Security, Signals Intelligence (SIGINT), and Command and Control (C2) systems. He currently serves as a program manager of Cyber Security and Information Operations for Applied Research Associates, Inc. Most recently, he has led a Department of Homeland Security-sponsored Cyber Test Bed Project to devise a multi-disciplinary security program for small to medium businesses. In previous positions, he oversaw U.S. Navy cyber security technology development and managed Navy enterprise network security. Mr. Piskin has also earned a post graduate CIO certificate through the National Defense University and is Security+ certified.

ABSTRACT: The Cyber Test Bed is a project of the Institute of Homeland Security Solutions (Research Triangle Institute, Duke University, the University of North Carolina and the NC Military Foundation), and Applied Research Associates (ARA). ARA is the principle subcontractor and architect of the Test Bed methodology and conceptual framework.

The Cyber Test Bed tested ways to identify, deploy, and evaluate best practices for cyber security in small and mid-size companies in the corporate sectors by:

- Identifying key incentives, create incentive models, and test proactive motivators
- Benchmarking changes in core security behaviors and decision-making
- Providing a security model associated with asset awareness
- Defining a simple, scalable methodology for small to mid-size companies to reduce cyber security risks
- Developing a prototype of the elements of a corporate culture that views cyber security from a holistic asset protection environment

The Test Bed is using the results of the project to produce a best practice methodology for small and mid-size companies. The Test Bed approach will lead to a better understanding of threats, the development of models to predict potential impacts, and the deployment of tactical deterrents. By identifying and testing best practices using existing technologies in cyber security for the private sector, the Test Bed will contribute to the DHS mission to improve cyber security, while also mitigating intellectual property loss critical to economic and national security.

Ron Ritchey

Chief Scientist Information Security | Bank of America

Panel Discussion: Future of Enterprise Security and Privacy

Steve Robinson

VP of Development, Product Management and Strategy | IBM, Security Systems Division

Presentation Title: Security Intelligence, Analytics, and the Changing Threat Landscape

Steve Robinson is the Vice President of Development, Strategy, and Product Management for the IBM Security Systems Division. He is responsible for a broad portfolio of commercial security solutions that help IBM clients with identity and access management, database activity monitoring, secure application development, network and endpoint security, and analytics that provide integration and intelligence to the security platform. Steve manages over 1000 technical professionals, 14 world wide Security software development labs, and IBM's X-Force security research team. He is a member of the Integration and Values Team (I&VT), a group of 300 senior leaders helping to steer the entire IBM business, as well as IBM's Cybersecurity Advisory Council, which helps guide IBM's internal security policies and practices.

Steve has held many executive positions in sales, technical services, product management, and acquisition integration in IBM's Software Group. Steve joined IBM in 1984 as a programmer, was involved in many of the company's early projects around object-oriented programming, and was instrumental in bringing both Smalltalk and Java to IBM. He was an early driver of IBM's distributed application development strategy as the Product Manager of IBM's VisualAge family, and introduced and launched technical services into IBM's Software Group. Most recently he was the GM of IBM Security Solutions, the precursor to the new division, and was responsible for formulating IBM's overall security product strategy. Steve earned his undergraduate degree from Wake Forest University and his MBA from Duke University.

ABSTRACT: The IT threat landscape is changing, with attacks coming from new sources with new motives - including insiders and business partners - using sophisticated tools and techniques. Perimeter protection and traditional security defenses, while necessary, are no longer sufficient. In order to identify and fend off attacks, security teams must think differently. They must move from defense-in-depth mode to counter-intelligence mode - they have to think like an attacker. Security Intelligence and advanced analytics provide the tools to collect and correlate massive amounts of security data, perform anomaly detection, and predict risk in the IT environment.

Sanjeev Sah

Chief Information Security Officer | The University of North Carolina at Charlotte

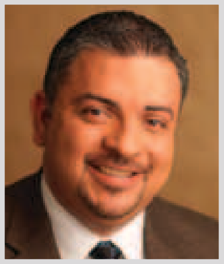
Presentation Title: Governance, Risk and Compliance Program

Sanjeev Sah is Chief Information Security Officer at the University of North Carolina at Charlotte. Sah is responsible for executing the University's information security strategy and program, designed to protect information assets, while complying with applicable legal, regulatory, and industry standards. He leads the University's Information Security, IS Compliance, and IT Governance functions.

Sah is a visionary and thought leader, with more than 15 years of experience in Information Technology and Information Security. Prior to joining UNC Charlotte, Mr. Sah served as Information Security Officer at Amedisys, the nation's leading home health and hospice company, where he successfully developed, implemented and managed the organization's information security program.

Prior to Amedisys, Sah served as Information Security Manager at School Specialty, an education company helping the organization successfully comply with the PCI Data Security Standards. As Information Security Manager at Federal-Mogul Corporation, a global supplier of automotive products, he managed the global information security function.
Sah is a member of Educause, where he serves on the Higher Education Information Security Council (HEISC) Governance, Risk & Compliance working group. Sah earned his B.S. in Information Technology and Information Systems Security from the University of Phoenix, and holds the CISM and CRISC certifications from ISACA.

ABSTRACT: In an environment where Bring Your Own Device (BYOD) is the new strategy for end point services and the Consumer Cloud Services are ever more powerful, there is potential for significant information security, data protection, and privacy challenges. Sanjeev will discuss and share his experiences on how governance, risk and compliance strategy, and programs can be leveraged to help address related challenges.



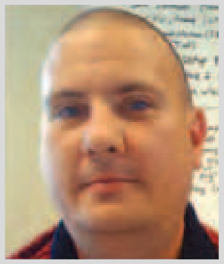
Steve Salinas

Senior Solutions Consultant | Guidance Software, Inc.

Presentation Title: When Time is of the Essence…
Integrating Real Time Forensic Analysis into an Incident Response Plan

Steve Salinas is a Senior Solutions Consultant for Guidance Software, Inc. Steve works with educational institutions, government agencies, law enforcement, and businesses to help them understand and overcome their challenges in the areas of forensics, eDiscovery, and Cybersecurity. Prior to this position, Steve spent over three years as Product Marketing Manager for the forensic business unit of Guidance Software, where he spent significant time working with the forensic community conducting user group meetings, delivering presentations at conferences, and managing the EnCase Forensic blog. Steve holds an MBA from Pepperdine University and an undergraduate degree from Texas A&M University.

ABSTRACT: During this session we will discuss the current challenges organizations face in managing incidents, reviewing relevant statistics from recent studies that reveal the areas where organizations are focusing their security investments. We will then discuss how incorporating real-time forensic analysis into an incident response plan can reduce the risk, time, and cost associated with incident response.



William Stranathan

Affiliated Scientist | Cyber DNA

Presentation Title: Improving Manual Code Review with SAST

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.

ABSTRACT: Manual source code review is one of the most effective ways to identify patterns of weakness in an application. However, manual code review is an extremely time-consuming process. This presentation will look at methods whereby Static Analysis Security Tools (SAST) can be used to reduce the time involved in a manual code review, while still providing a great deal of benefit. Furthermore, we'll look at ways that manual code review can be used to improve the SAST findings.

Chris Swecker

Founder and CEO | Chris Swecker Enterprises

Presentation Title: The "New" Organized Crime Paradigm

Swecker served 24 years as a Special Agent with the Federal Bureau of Investigation (FBI), retiring in 2006 as Assistant Director, CID, with oversight over all FBI Criminal Investigations. Swecker also served as the FBI's On Scene Commander in Iraq in 2003 where he led a team of FBI Agents conducting counter-intelligence, terror financing, and international terrorism investigations, including investigating suicide bombing attacks on the UN headquarters and other civilian-occupied facilities. As CSO for Bank of America from July 2006 to January 2009, Swecker led investigations, physical security, international security, employment screening, and executive protection. He provided strategic direction and overall management for over 600 proprietary associates and over 3800 contract security guards with an annual budget of over $250 million. Swecker created a world class advanced Security Operations Analysis and Command Center (SOAC) to support security operations worldwide. The SOAC consolidated, monitored, and managed the largest alarm access control and digital video surveillance system in the financial sector, with responsibility for 6100 bank branches,18,000 ATMs, and 450 administrative facilities. He led the bank's crisis and business continuity response for security or terrorism events. Swecker has testified before US Congressional Committees on topics such as identity theft, crimes against children, mortgage fraud, human trafficking, financial crimes, information privacy, terrorism, data compromise, crimes on the Internet, drug trafficking on the southwest border, and gangs. He has also appeared as a guest on such media programs as 60 Minutes, CBS This Morning, Oprah Winfrey, Good Morning America, CSPAN Washington Journal, and North Carolina People. He is a frequent public speaker and author of articles on Financial Crimes, Money Laundering, Security, and Cyber Crimes. Swecker is a graduate of Appalachian State University where he was a 4 year varsity football letterman, graduating in 1978. He attended Wake Forest School of Law receiving his Juris Doctor in 1981. He is a member of both the North Carolina and Virginia State Bars. Swecker received the prestigious Presidential Rank Award in 2003 for his service in Iraq and as Special Agent in Charge of the NC Office. Swecker currently manages his own law practice and founded a successful security and financial crimes consulting firm, Chris Swecker Enterprises.

ABSTRACT: How virtual criminal networks focused on financial crimes, have replaced traditional "bricks and mortar" organized crime as the dominant crime problem of the millennium.

William Thornhill

Director, Threat and Vulnerability Management | TIAA-CREF

Presentation Title: Principles for Achieving Success in Information Security

William Thornhill is currently responsible for Threat and Vulnerability Management operations as a central part of TIAA-CREF's information security control portfolio. In partnership with Access and Entitlement Management and Information Technology Risk Management, the TVM team serves as the front line for threat detection and mitigation with operations spanning forensics, incident response and management, and vulnerability assessments. Will came to TIAA-CREF from Bank of America, having led early development of their Insider Threat Behavioral Analysis, Red Team, and Threat Intelligence programs. Before coming to the Financial Services industry, Will worked in the defense community for large firms such as Anteon (General Dynamics) and Lockheed Martin Information Technology. He is a graduate of the Georgia Institute of Technology and has contributed multiple entries to The Encyclopedia of American Espionage.

ABSTRACT: Information Security is one of the fastest growing and arguably most exciting career paths in Information Technology. On any given day, an Info Sec analyst or engineer will impact the lives and operations of customers, citizens, business partners, and technology strategies. This presentation covers eight operating principles to guide individual success as part of a modern, cross-functional information security team: Acting with Speed, Being Agile, Total Visibility, Owning your Space, Fusion and Collaboration, Innovate-Innovate-Innovate, and Competing on the Quality of your Analytics.

Franklin Witter, CISSP

Senior Principal Security Strategist | Symantec Corporation

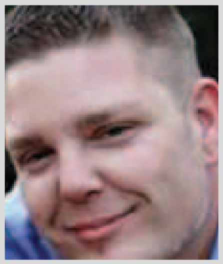
Presentation Title: Bring Your Own Risk

Franklin Witter is an accomplished information security practitioner working in IT across multiple industries for 15 years and over a decade with his primary focus on security for large enterprise and service provider infrastructure. At Symantec, Franklin is responsible for security strategy and direction, industry trends, threat landscape, best practices, as well as trusted advisor to security executives, senior management, and executives of our customers across the Southeast. He is an extension of Symantec's CTO Office, and works closely with the Business Unit Executives to focus on the real-world IT security challenges our customer face, to drive Symantec's overall security direction. Professional experience includes management of IT/IS, consulting and business development teams, information security strategy and architecture, information systems integration, information risk assessment and management, teaching, and project management from concept through implementation.

Franklin holds an MBA from Auburn University and a BS in Liberal Arts from Southwest Baptist University. He also holds CISSP Certification from ISC2 and CISM certification from ISACA. In 2009, Franklin won the ISACA Geographic Excellence Award for North America.

ABSTRACT: BYOD creates a unique set of challenges that must be carefully addressed in order to manage risk. In this presentation, we will look at the mobile threat landscape, the challenges presented by BYOD, and approaches to ensuring risks associated with BYOD are properly managed.

TUTORIAL I:



Martin Bos and Eric Milam

Sr. Security Analysts, Accuvant Labs

Presentation Title: Advanced Phishing Tactics – Beyond user awareness

Martin Bos is a senior security assessor with the Accuvant LABS enterprise assessment team and has five (5) years of experience in the information technology industry. Martin specializes in black-box penetration testing, social engineering, physical security testing, and enterprise network security assessments. Martin also has extensive knowledge in performing wireless assessments. Martin Bos is a core developer of the Backtrack-Linux project and one of the founders of Derbycon.

Eric Milam is a senior security assessor on the Accuvant LABS enterprise assessment team, with over fourteen (14) years of experience in information technology. Eric has performed innumerable consultative engagements including enterprise security and risk assessments, perimeter penetration testing, vulnerability assessments, social engineering, physical security testing, wireless assessments, and extensive experience in PCI compliance controls and assessments. Eric is a project steward for the Ettercap project as well as creator and developer of the easy-creds and smbexec projects.

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.*

Laptop Requirement:

- Windows XP or Vista
- Can run latest version of VMware Player
- 1GHz processor with 1GB RAM or higher
- 2GB free disk space or higher.

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

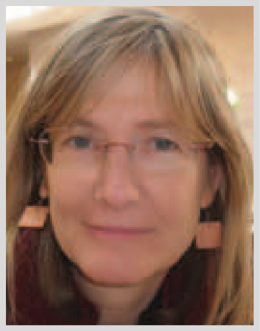
The Diversity in Information Technology Institute (DITI)

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: diti.uncc.edu

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

NEW DEPARTMENT CHAIR



"IN MY NEW ROLE AS CHAIR OF SOFTWARE AND INFORMATION SYSTEMS, I LOOK FORWARD TO BRINGING A DESIGN FOCUS TO RESEARCH AND EDUCATION. IN RESEARCH, THE DEPARTMENT'S STRENGTHS IN AREAS SUCH AS PRIVACY AND SECURITY, COMPLEX ADAPTIVE AND INTELLIGENT SYSTEMS, HUMAN-COMPUTER INTERACTION, AND CREATIVE COMPUTING, PROVIDE A STRONG FOUNDATION FOR SYNTHESIZING AND EXTENDING HUMANCENTERED COMPUTING WITH A FOCUS ON DESIGN."

Mary Lou Maher, Ph.D.
Chair, The Department of Software and Information Systems

BIO: Mary Lou Maher, Ph.D., most recently a Senior Research Scientist in the iSchool at the University of Maryland and Honorary Professor of Design Computing in the Design Lab at the University of Sydney, is joining the College of Computing and Informatics as the Chair of the Department of Software and Information Systems. Mary Lou completed a BSc at Columbia University in 1979, and a MS and Ph.D. at Carnegie Mellon University, completing the Ph.D. in 1984. As the Professor of Design Computing at the University of Sydney she was co-Director of the Key Centre of Design Computing and she established a new degree program: the Bachelor of Design Computing. While at the National Science Foundation (NSF) from 2006-2010, she was Deputy Director of the Information and Intelligent Systems Division and a Program Director. At NSF, she established the CreativeIT program and helped manage the Human Centered Computing, Cyber-Enabled Discovery and Innovation, Design Science, and Social-Computational Systems Programs. While at the University of Maryland, she developed collaborative projects on crowdsourcing design for citizen science and introduced design thinking to graduate projects in information management.

Mary Lou's research interests span a broad area of design and computing, specifically the study and development of novel interaction and communications technology, and models of design and creativity. Her research draws on and contributes to human-computer interaction, intelligent systems, computer-supported collaborative work, design science, and computational creativity. Her current research has a focus on developing social-computational models and new technology as we scale up from creativity enhancing human-computer interaction, through effective collaborative systems, to large-scale and highly motivating collective intelligence and crowdsourcing. Some highlights of her recent research are: developing models of motivation, innovation, and diversity in collective intelligence, designing tangible and immersive interaction environments and evaluating their impact on creative cognition; the design and study of virtual worlds for collaboration and education; and developing computational models of curiosity for extending the functionality of search and motivated reinforcement learning algorithms.

NOTES

NOTES

NOTES

SAVE THE DATE Wednesday, April 24, 2013

UNC CHARLOTTE PRESENTS

The 5th Annual

SaaS CLOUD COMPUTING CONFERENCE

College of Computing and Informatics
UNC CHARLOTTE

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 OSX).
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).

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

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.

UNC CHARLOTTE
College of Computing and Informatics

THANK YOU

TO OUR SPONSORS

UNC Charlotte Partner Sponsor

UNC CHARLOTTE

CHARLOTTE RESEARCH INSTITUTE

GOLD Sponsors

Duke Energy®

BRONZE Sponsors

ACCUVANT
Alignment • Clarity • Confidence

Deloitte.

Microsoft®

TREND MICRO™

TABLE Sponsors

AT™

Bank of America

TIAA CREF
FINANCIAL SERVICES
FOR THE GREATER GOOD®

Tekelec

RAPID7

RTI
INTERNATIONAL

WOMBLE CARLYLE®
INNOVATORS AT LAW®

EXHIBITORS

ESM Technology
Managing People & Technology

Guidance®
SOFTWARE

hp

paloalto
NETWORKS

peak 10™
DATA CENTER SOLUTIONS

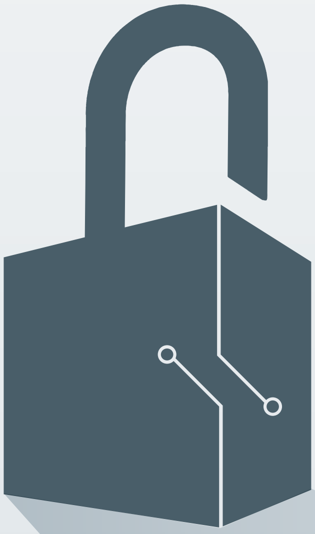
QUALYS®
ON DEMAND SECURITY

RAPID7

STALWART
Secure IT Architectures...Right the First Time

College of Computing and Informatics
UNC CHARLOTTE

The 14th Annual
CYBER SECURITY SYMPOSIUM
Coming Fall 2013



The College of Computing and Informatics has already begun planning for the 14th Annual Cyber Security Symposium in 2013. 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, 2013.

Stay tuned to **cci.uncc.edu**.