Over 300 representatives from Government, Industry and Education

assemble to share current and emerging trends in information assurance

19TH COLLOQUIUM

LAS VEGAS, NEVADA JUNE 15 - 17, 2015

GOVERNMENT
Monday, June 15

EDUCATION
Tuesday, June 16

INDUSTRY
Wednesday, June 17

Abstracts of Papers and Conference Materials for

19th Annual Colloquium for Information System Security Education

JUNE 15 - 17, 2015

JW MARRIOTT RESORT & SPA,
LAS VEGAS, NV, USA

REVISED JUNE 12, 2015

Table of Contents

Our Colloquium

The Colloquium recognizes that the protection of information and infrastructures that are used to create, store, process, and communicate information, is vital to the continuity and security of business. The Colloquium's goal is to work to define current and emerging requirements for information assurance education and to influence and encourage the development and expansion of information assurance curricula.

Conference Chair
Daniel Likarish

Paper Co-Chairs
Dan Shoemaker, Susanne Wetzel and Tanya Zlateva

Poster Co-Chairs
Erik Fretheim

Women & Minorities WG
Rosemary Shumba

K-12 Working Group Chair
Davina Pruitt-Mentle

Community College Working Group Chair
Casey O'Brien

CISSE Operations Manager
Tamara Shoemaker

Weekend Tours
Mark Hufe and Warren Hoiki

Committee Members

Davina Pruitt-Mentle, John Sands, Steven Brown, Bob DuCharme, Stephen Miller, Yin Pin, Dan Manson, Bruce Waugh, The Tamurbellis, Themis Papageorge, Chris Simpson, Steve Shih, Jeff Tjiputra, Alberto LaCava, Shamsi Moussavi, Aurelia Smith, Ken Sigler, Deanne Crawford Wesley, Z Chen, Brian Woemer, Lonnie Decker, Jeanann Boyce, Brenda Oldfield, Carol Taylor , Virgina Werner and our Operations Manager Tamara Shoemaker.

Special thanks to Jeff Wilson of JW Meeting Services, Lewis Lighter and Jesse Wesley!

The Board of Directors

President

Dr. William “Vic” Maconachy

Vice President

Dr. Susanne Wetzel

Secretary

William H Murray, CISSP

Treasurer

Dr. Daniel Shoemaker

Board Members	
Jay Bavisi	Robert DuCharme
Dr. J.A. “Drew” Hamilton Jr.	Mark Hufe
Karen Leuschner	Daniel Likarish
Dr. Daniel Manson	Brenda Oldfield
Dr. Corey Schou	Patricia Tamburelli
Dr. Tanya Zlateva	

Dr. William Maconachy

The Colloquium Chairman

William “Vic” Maconachy, Ph.D., is vice president for academic affairs at Capitol College. Maconachy comes to Capitol after a distinguished career at the National Security Agency (NSA) as the Deputy Senior Computer Science Authority and as the program manager of the National Information Assurance Education and Training Program. Maconachy has served as chairman of the Education Training and Awareness group of the presidential chartered Committee for National Security Systems, and as the program manager for the Department of Defense’s Information Assurance Scholarship Program. He is also a founder, and current chair of the National Colloquium for Information Systems Security Education.

Maconachy holds a doctorate from the University of Maryland, has published extensively throughout his career in government and has received numerous awards and recognition including the Department of Navy Distinguished Civilian Service medal and the prestigious Department of Defense Meritorious Service Medal. He has the distinction of being a Fellow with the International Information Systems Security Certification Consortium $(ISC)^2$, a designation that honors information security professionals who have made outstanding contributions to the field.

Bill Boni

Vice President Information Security at
T-Mobile USA

Mr. William C. Boni has spent his entire professional career as an information protection specialist and has assisted major organization's in both the public and private sectors. For 30+ years, beginning as a Special Agent in U.S. Army Counter-intelligence, Bill has helped a variety of organizations design and implement cost-effective programs to protect both tangible and intangible assets. In a wide range of assignments Bill has assisted clients in safeguarding their digital assets, especially their key intellectual property, against the many threats arising from the global Internet. In addition, he has pioneered the innovative application of technologies including computer forensics, intrusion detection and others, to deal with incidents directed against electronic business systems.

Bill has served as a consultant in several professional service organizations and now works as the Vice President and Corporate Information Security Officer of T-Mobile. He is responsible for the company's overall program to protect T-Mobile's brand by protecting sensitive customer and company information. He also directs the people, processes and technology programs that safeguard the company's network, computer systems and electronic business initiatives.

Bill has been quoted by leading print publications such as the Wall Street Journal, US News & World Report the Financial Times, LA Times, and CIO Magazine. He has also appeared on many network broadcasts including Prime Time Live, CNN and CNN/fn discussing espionage and cyber crimes directed against American high technology corporations. Other assignments in his distinguished career include work as a U.S. Army Counter-Intelligence Officer; Federal Agent and Private Investigator; investigator and security consult-

ant; Vice President of Information Security for First Interstate Bank; and project security officer for “Star Wars” programs and other defense work with Hughes Aircraft Company and Rockwell.

Keynote: Wednesday, June 17th at 10:30am

Ian Bryant

Programme Manager and Technical Director, Trustworthy Software Initiative (TSI)

The Trustworthy Software Initiative (TSI) has been established under UK Government seedcorn funding to pursue the Public Good aim of improving the overall software culture, not only within the UK, but also working with partners internationally in recognition of the fundamentally globalized nature of the supply base.
Ian Bryant is Professional Engineer, currently assigned as the Technical Director of the UK’s Trustworthy Software Initiative (TSI), on academic secondment as a Principal Fellow at the University of Warwick.

He has spent much of his career as a public servant as a peripatetic Principal technical specialist, assigned to a variety of organizations (including Cabinet Office, Defense, National Archives, National Policing, and the former National Infrastructure Security Coordination Centre (now CPNI)) and roles (including Incident Response, Research, Satellite Engineering, and Software/System Verification).

He was intimately involved with various TSI predecessor activities, including leading the original Cabinet Office (CSIA) study on Secure Software Development, being Technical Manager for the Pilot Operation of the then CSIA Claims Tested Mark (CCT Mark) Scheme, and leading the Secure Software Development Partnership (SSDP) Special Interest Group (SIG) on Standardization.

In the wider Standards context, he is a member of several British Standards Institution (BSI) Committees, in particular the panel on Information Security (IST/033 – UK shadow for ISO/IEC JTC1 SC27) for which he is a Deputy Chair, and Lead UK Expert on Architecture; Cybersecurity; Incidents / Investigations / Evidence; and Software. He is also a Rapporteur in the European Telecommunications Standards Institute (ETSI) Management of Test and Specification (MTS) SIG on Security.

He is a Visiting Lecturer at a number of other Universities, and is a frequently requested at governmental, national and international conferences.

Keynote: Monday, June 15th at 1:45pm

Shaun Cavanaugh

Chief of Cyber for the U.S Nuclear Command and Control System (NCCS) Support Staff (NSS)

The U.S. Nuclear Command and Control System (NCCS) Support Staff (NSS) is an interagency office tasked by the President to monitor, assess, and provide oversight to the NCCS. Prior to this assignment Shaun was assigned to the U.S European Command where he served as a Cyber Engagement Officer for 3.5 years working with over 30 countries through exercises, training events, and information exchanges. Prior to this Shaun worked in Michigan for the US Army in G2 (Intelligence and Security) and G6 (Chief Information Officer) offices. Shaun has a Bachelor and Master of Science in Computer and Information Systems from the University of Detroit Mercy and the Chief Information Security Officer certificate from the National Defense University.

Keynote: Monday, June 15th at 2:45pm

Abe Chen

Director, Information and Product Security at Tesla Motors

Abe T. Chen MSIA, SSCP, CISA, CISSP, CIPP/US is a security leader with expertise in digital and physical investigations, advanced layered security architectures, product security, and compliance/risk mitigation methodologies. He has spent his career deploying bleeding-edge security techniques and leading offensive and defensive teams around the globe across multiple verticals including manufacturing, technology, retail, telecommunication, finance, automotive, and education. Abe currently extends his passion leading the Information and Product Security team at Tesla Motors.

Keynote: Wednesday, June 17th at 11:00am

Lynne Clark

Chief of the National Information Assurance Education and Training Program (NIETP)

The NIETP program includes management of the NSA/DHS Centers of Academic Excellence in Information Assurance Education (CAE IAE) Program, DoD's Information Assurance Scholarship Program (IASP) and the IAD Security Education and Academic Liaison (SEAL) Program.

Ms. Clark was previously Chief of the IAD Communications and Marketing Division, which is responsible for communications support to the IAD Front Office, interface with the NSA Communications, Graphics and Public Affairs offices, and Marketing support to the Information Assurance Directorate.

From 1993 to 2012, Ms. Clark was assigned to the Interagency OPSEC Support Staff, where she had responsibility for Operations Security (OPSEC) con-

sultation to all Federal Departments and Agencies with a national security mission. She has an extensive background in OPSEC surveys and assessments, primarily in direct support of the Department of Defense.

Prior to her tenure at the IOSS, Lynne was on active duty with the U.S. Air Force as a Weapons Controller with tours in Florida, Germany, Texas and the Pentagon. After the Air Staff, she was the OPSEC Officer at U.S. Air Forces Europe where she had management of the command's computer security, communications security, personnel security, TEMPEST, and industrial security programs in addition to OPSEC. She retired in 1999.

Ms. Clark holds National Security Agency Professionalization in Operations Security, is a Lifetime OPSEC Certified Professional, and is a Lifetime member of the OPSEC Professionals Society.

Panel: NSA/DHS National Centers of Academic Excellence
Breakout: CAE-CD KU Review; KU to NICE Framework Mapping

Lisa Foreman-Jiggetts

Founder & CEO, Women's Society of Cyberjutsu (WSC)

Lisa Foreman-Jiggetts is the founder and CEO of the Women's Society of Cyberjutsu (WSC), one of the fastest growing nonprofits dedicated to women in cybersecurity. WSC provides women with the resources and support required to enter and advance as a cybersecurity professional. Her organization uses a holistic approach to develop programs that train women in both the hard technical skills and soft skills, leaving them feeling empowered to succeed. She is most proud to be known as a straight-up but down-to-earth motivator with the women whom she mentors.

Keynote: Tuesday, June 16th at 4:30pm

Catherine Harkness

Government Communications Headquarters (GCHQ)

Catherine joined GCHQ on graduation and has worked in the Information Assurance area of GCHQ since 2009. During this time she has led a cross-government working group briefing UK government Senior Information Risk Owners on the risks of data loss, supported the UK Cyber Security Challenge, written training courses and worked on cyber security for procurement professionals. She has led on the delivery of GCHQ's Academic programme for Cyber Security since its inception in early 2013 choreographing engagement with 13 Academic Centres of Excellence in Cyber Security Research, 3 Research Institutes, 33 sponsored Doctoral Students and 9 universities providing GCHQ-certified Master's degrees in Cyber Security.

Keynote: Monday, June 15th at 3:30pm

Catherine Hogendobler

Board Director, Women's Society of Cyberjutsu (WSC)

Catherine Hogendobler, MS, MBA, CISSP, PMP, CIPP/IT, ITIL has over 20 years' experience in information technology security management. In addition to security management her experience spans business operations , telecommunications, server operations, and database administration. She has worked in the Aerospace, Telecommunications, Logistics and Data Center business sectors.

Keynote: Tuesday, June 16th at 4:30pm

Dr. Corby Hovis

Program Director, The National Science Foundation (NSF)

Dr. Hovis oversees the NSF-wide Research Experiences for Undergraduates (REU) program and co-manages several grant programs in NSF's Directorate for Education and Human Resources. In particular, in the area of cybersecurity education, for many years he has worked in the *CyberCorps: Scholarship for Service (SFS) Program*, which provides scholarships and supports other activities to build strong educational programs in cybersecurity at colleges and universities; and the *Advanced Technological Education (ATE) Program*, which funds efforts to improve and expand technician education, including IT and cybersecurity education, at community colleges.

Before joining NSF, Dr. Hovis served on the faculty of Valparaiso University and, at the same time, as science editor at Encyclopædia Britannica in Chicago. He earned his graduate degrees (Ph.D., M.S., M.A.) from Cornell University and his undergraduate degree from Wake Forest University.

Panel: Funding

Workshop: NSF Proposal Writing and Reviews

Michael Kirton, Ph. D.

Government Communications Headquarters (GCHQ)

Michael has a BSc and PhD in physics and is a member of the ACM and IEEE. His technical background includes solid-state physics, distributed and parallel computing, and cyber security. He has spent much of his career collaborating on research programmes with universities. Since joining GCHQ 4.5 years ago, he has provided technical leadership in the setting up of a number

of GCHQ's academic programmes including Centres of Excellence in Cyber Security Research, Research Institutes, Doctoral Studentships and the certification of Master's degrees in Cyber Security.

Keynote: Monday, June 15th at 3:30pm

Steve LaFountain

Dean of the College of Cyber at the National Security Agency

Mr. LaFountain is the Chief E7, College of Cyber and the Distinguished Academic Chair for Information Assurance and Cyber in the Associate Directorate for Education and Training (ADET) at the National Security Agency. ADET is responsible for providing relevant and superior learning opportunities in the cryptologic disciplines, analysis, cyber, language, and business management necessary to develop a highly analytic, technologically astute workforce for the global NSA/CSS mission.

Mr. LaFountain began work at NSA in 1982 as one of the founding members of the National Computer Security Center's Trusted Product Evaluation Program. Since that time, he has held a variety of technical, supervisory and leadership positions within NSA. In these positions, Mr. LaFountain has had extensive interaction with commercial industry as well as international partners on the subjects of security requirements, security evaluation techniques, and security designs for government and commercial information assurance products and solutions. Mr. LaFountain is a graduate of NSA's Senior Technical Development Program (STDP), focusing on secure virtual private network technologies. In 1999-2000, Mr. LaFountain served as the Deputy Director and Technical Director for Cyber Programs for the Department of Energy's newly formed Office of Counterintelligence, developing advanced intrusion detection and email monitoring capabilities. Prior to his assignment to ADET, Mr. LaFountain was the Technical Director for the Security and Evaluation in

the Information Assurance Architecture and Systems Security Engineering Group (I1) and the Custom Solutions Group (I8) within the Information Assurance Directorate (IAD).

Mr. LaFountain is professionalized as a computer systems analyst and was awarded a Master rating in the Computer Science Tech Track. He has been awarded the Exceptional Service Award from the Department of Energy and the Exceptional Civilian Service Award from NSA.

Mr. LaFountain graduated from Merrimack College in Massachusetts in 1982 with a Bachelor of Science degree in Computer Science and has taken additional technical courses at Johns Hopkins University. He continually enhances and maintains his technical expertise via technical conferences, workshops, seminars and tutorials.

Panels: DHS National Centers of Academic Excellence; Funding
Breakout: CAE-CO KU Review

Casey W. O'Brien

Executive Director of the National CyberWatch Center

National Cyberwatch Center is a national cybersecurity education and research consortium headquartered in Maryland.

Casey has more than 20 years of industry experience in information security and large scale IT implementation and project management in challenging and cutting edge computing environments that include both the public and private sectors.

As a scholarly practitioner, Casey continues to develop curriculum and teach numerous cybersecurity related courses. Casey's research interests include cybersecurity competition design and practice analysis; scalable and cost ef-

fective information security laboratories; and agile and accelerated information security curriculum development. Casey also teaches internationally and is a frequent invited speaker at various conferences.

As well as provide the leadership for the National Cyberwatch's 2nd Annual 3CS conference, Casey has put together our Community College Panel.

Panel: Community College Panel; Articulation Agreements

Joel Palmtag

Information Security Engineering and Operations at SpaceX

Joel Palmtag is a pragmatist, focused on simple and effective methods to manage Information Security risk. His experience is built on a history of digital forensics, network engineering, and working as an active part of the space borne systems and ground support teams. Joel is now responsible for Information Security Engineering and Operations at SpaceX. He is a perpetual student and practitioner of IS. Joel believes in offense and defense working closely to define strategic goals and find tactical opportunities together.

Keynote: Wednesday, June 17th at 11:00am

Rodney J. Petersen

Lead, National Initiative for Cybersecurity Education (NICE)

Rodney Petersen is the lead for the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST). He previously served as the Managing Director of the EDUCAUSE Washington Office and was the Director of IT Policy and Planning in the Office of the Vice President and CIO at the University of Maryland. He is the co-editor of the book *Computer and Network Secu-*

rity in Higher Education. He received his law degree from Wake Forest University and a certificate as an Advanced Graduate Specialist in Education Policy, Planning, and Administration from the University of Maryland.

Keynote: Monday, June 15th at 1:15pm;
Panel: Funding

Dr. Victor Piotrowski

Lead Program Director, The National Science Foundation (NSF)

Victor is responsible for several programs related to Cybersecurity Education and Workforce Development. In particular, he oversees the CyberCorps(R): Scholarship for Service (SFS) program with FY2014 budget of $45 million. This program seeks to increase the number of qualified students entering the field of cybersecurity and to increase the capacity of the United States higher education enterprise to continue to produce professionals in this field to meet the needs of our increasingly technological society.

He is also a Program Officer in a NSF-wide program Secure and Trustworthy Cyberspace (SaTC) supporting projects that address cybersecurity from one or more perspectives: Trustworthy Computing Systems; Social, Behavioral and Economics; and Cybersecurity Education.

Before coming to NSF, Dr. Piotrowski served as a Professor and Chair of the Computer Science Department at the University of Wisconsin and as a faculty at the Institute of Informatics in Poland. He has a 20-year experience in research, teaching and consulting in Information Assurance and holds several cybersecurity certifications.

Dr. Piotrowski is the recipient of the Marcinkiewicz Prize by the Polish Mathematical Society and a finalist of the UW Board of Regents Teaching Excel-

lence Award. He is a graduate of the Federal Executive Institute residency program Leadership for a Democratic Society and the Harvard Kennedy School Executive Education Cybersecurity Policy and Technology program.

Keynote: Monday, June 15th at 11:15am; Panel: Funding
Workshop: NSF Proposal Writing and Reviews

Kathryn Roberson

Human Resources Consultant, The United States Office of Personnel Management

Kathy Roberson is a Human Resources Consultant with the United States Office of Personnel Management (OPM), Human Resources Solutions, Federal Staffing Group. She began her Federal career with OPM in Oklahoma City, OK in 1987. Currently she works in the Staff Acquisition Management Section where she manages the CyberCorps®: Scholarship For Service (SFS) program and is the Contracting Officers Representative for the Recruitment and Branding solution.

Panel: Funding

Dr. Corey Schou

Director, Informatics Research Institute

Corey Schou is The University Professor of Informatics and Associate Dean at Idaho State University, director of the National Information Assurance Training and Education Center (NIATEC) and the Simplot Decision Support Center (SDSC). His program was recognized by the United States Government as a Center of Academic Excellence in Information Assurance and is a leading institution in the CyberCorps/Scholarship for Service program.

In 2003 he was selected as the first University Professor at Idaho State University. He was one of the three founders of the Colloquium for Information Systems Security Education (CISSE); he served as the chair for ten years.

Professor Schou is frequent public speaker and an active researcher with over 300 books, papers, articles, and, other presentations. His interests include information assurance, software engineering, secure applications development, security and privacy, collaborative decision-making, and the impact of technology on organization structure.

In the early 1980s, organizations began to recognize that connected PCs in various locations were much more vulnerable than a mainframe locked away in a single building. These organizations began seeking qualified individuals responsible for selecting, recommending and implementing security policy and procedures. However, few schools were offering information security curricula, much less academic degrees, and organizations would have to take an IT professional at his or her word that they knew how to manage information security for the entire enterprise.

By 1989 Schou and others had established a unified common Body of knowledge for computer security. Schou, with Idaho State University hosted the finalization meetings in Salt Lake City. Schou's work is recognized several

organizations such as (ISC)² as foundational to the Information Assurance discipline in academia. His work for three decades has resulted in standards used internationally by government, industry and academia.

He was nominated and selected as an honorary Certified Information Systems Professional (CISSP) based on his lifetime achievement and has served as a, CISSP®-ISSAP®: Information Systems Security Architecture Professional, and CISSP-ISSMP: Information Systems Security Management Professional.

In 2001 the International Information Systems Security Certifying Consortium selected him as the second recipient of the Tipton award for contribution to the Information Security Profession. In 2007, he was recognized a Fellow of (ISC)².

Keynote: Tuesday, June 16th at 12:00pm

David Shearer

Executive Director (ISC)²

David Shearer, CISSP, PMP has more than 27 years of business experience including the chief operating officer for (ISC)², associate chief information officer for International Technology Services at the U.S. Department of Agriculture, the deputy chief information officer at the U.S. Department of the Interior, and the executive for architecture, engineering and technical services at the U.S. Patent and Trademark Office. Mr. Shearer has been responsible for managing and providing services via international IT infrastructures, and he has implemented large-scale SAP Enterprise Resource Planning (ERP) projects. Mr. Shearer has led large geographically separated staffs that support global solutions. Mr. Shearer holds a B.S. from Park College, a M.S. from Syracuse University, management and technical certificates from the U.S. National Defense University, and he is a U.S. federal executive presidential rank award recipient. As

(ISC)² Executive Director, Mr. Shearer is responsible for the overall direction and management of the organization.

Keynote: Monday, June 15th at 12:00pm

Jacqueline Sullivan

Program Manager, FedVTE/FedCTE

Jacqueline Sullivan is the Acting Program Lead for the Department of Homeland Security's National Cybersecurity Training & Education Program and Program Manager for the Federal Virtual Training Environment (FedVTE) and Federal Cybersecurity Training Events (FedCTE) programs. She has worked in and around the Federal Government for nearly 10 years in various roles including standing up the Joint Program Office for the National Security and Emergency Preparedness Communications Executive Committee in support of Executive Order 13618. As a mom, Jacqueline is extremely passionate about raising awareness among children on online safety and has a personal mission to bring more underrepresented groups into the field of cybersecurity.

Panel: NSA/DHS National Centers of Academic Excellence
Breakout: CAE-CD KU Review

Colin Williams

Director of SBL

As both a businessman and as an academic, Professor Williams is a leading figure in the international cyber security community with twenty years of experience in enterprise IT, Information Assurance and cyber security. As a director of SBL, he develops and leads the business development strategy of a wholly UK owned and controlled market leading provider of vendor independent cyber security solutions to central government, blue light services and the wider public sector.

Professor Williams was a member of the founding cohort of CLAS consultants. He has been involved in initiating and delivering some of the largest software volume license public sector procurement projects in the world.

As an academic, he is developing a body of work around the human, intellectual, cultural, societal and historical context of computing which he is delivering across a series of lectures, seminars and papers.

Professor Williams consults and speaks on cyber, cyber security and strategic enterprise IT procurement in the UK and internationally. He is editor in chief of “CyberTalk” and new journal for the promotion and development of fresh and interdisciplinary thinking about cyber and the human relationships with computers.

Keynote: Wednesday, June 17th at 9:30am

Panel: Cyber Range

Academic Papers

Paper Chairs

Dan Shoemaker, Susanne Wetzel and Tanya Zlateva

Reviewers

Dr. Sherly Abraham, Dr. Subrata Acharya, Dr. Matt Bishop, Dr. Douglas Blakemore, Dr. David Bouvin, Xinwen Fu, Ida Ngambeki, Dr. WIlliam Oblitey, Imani Palmer, Dr. Denise Pheils, Dr. Jason Pittman, Robert Sherman, Patricia Tamburelli, Souheir Trabelsi, Dr. Prem Uppuluri, James Walden, Dr. Ping Wang, Richard Weiss, Virginia Werner

With an initial submission of 40 papers, after a double blind, peer review process there are 11 Academic Papers, and 28 Roundtable presentations. The acceptance rate for this conference was 24%.

The Academic Papers will be published in our journal, Proceeding of the 19th Colloquium for Information System Security Education which may be purchased in the fall via amazon.com

E-Book ISBN and Book Version ISBN will be provided on our website when it becomes available. Last years papers can be found in the Proceeding of the 18th Colloquium for Information System Security Education, Soft Cover ISBN 10: 150062120X Digital Version also available via Amazon.com

Special Edition: Educational Approaches to Transition former Military Personnel into the Cybersecurity Field, Spring 2015 CISSE Edition 2, Issue 2, Soft Cover ISBN 10: 1508808678 Digital Version also available via Amazon.com

Best Paper Award for 2014

Impact of Net Neutrality and the Open Internet Order on Security and Privacy in Education

Lorie M. Liebrock, Judy Holcomb, Jesse B. Crawford, Kaley Goatcher, Tyler Cecil

The Open Internet Order is the result of a multi-year Federal Communications Commission (FCC) effort to address the challenge of net neutrality. This paper analyzes the impact of the Open Internet Order on universities in terms of standard operating procedures, costs, quality of education, privacy, and security. This paper only considers the US regulations that affect Internet access and their implications on universities. These regulations may also have wide-ranging international implications, but those are not considered here.

The Erich Spengler Student Paper Award Winner

A Survey of Student-Discovered Bugs and Vulnerability Disclosure

James Sullivan, Michael E. Locasto

Abstract - There is a high demand for software developers and security professionals with strong software analysis skills. Currently, many students learn software analysis as an auxiliary exercise to their programming projects, and their experience is limited to white-box testing of applications that they or their peers have written. This type of experience does not give students a realistic or practical set of skills which they can immediately apply to more complex tasks. We describe our experiences with an information security course project in which students were tasked with discovering and analyzing software flaws in real software projects, giving students practical experience in flaw analysis and bug reporting. We discuss the focuses and goals of this project, including its emphasis on responsible disclosure, and the trends in student's comfort with analysis techniques and tools.

Organization Security Controls for Effective Cyber Defense

Anne Kohnke , Ph. D.

Even the most technically savvy organizations cannot stop hackers and the risk of poorly implemented IT security controls can be devastating. Technical solutions need to work in harmony with formal security controls, informal organizational culture, and the overriding mission and goals of the organization. With the exponential growth of security breaches and the increasing dependency on external business partners to achieve organizational success, the effective use of enterprise-wide frameworks and implementation of integrated security controls are critical in order to mitigate data theft. Surprisingly, many organizations do not have formal processes or policies to protect their assets from internal or external threats. This paper gives an overview of why an organization should consider using, or tightening up their organizational security controls, an overview of the most widely used frameworks, and a comparative discussion of the various IT security frameworks to assist managers in assessing their own IT security efforts.

Index terms - cybersecurity, enterprise security framework, security controls, risk management

HSPO - A Novel Threat Assessment and Risk Mitigation Approach to Prevent Cyber Intrusions

Paul S. Wang

In this paper, we study recent data breaches from both technical and business operation perspectives and propose an algorithm that calculates threat factors of information systems based on various features in hardware, software, poli-

cies and business operations. The assessment process takes more than 200 features into account. The data are then imported into the algorithm that calculates the threat factor and normalizes the value to [0-1]. A higher threat factor means the information systems would be hacked at higher risk. Mitigation strategies are provided to reduce risks of information systems from being hacked into and to protect data from being misused, stolen or identifiable. Study shows that the threat factor reduced from 0.71 to 0.38 in one month for the company we worked with. It was further reduced to 0.18 after finishing a four-month assessment and mitigation period.

This comprehensive approach can reduce cyber intrusions to corporations such as Anthem, Sony, JP Morgan, Home Depot and Target. It can also deal with privacy concerns in this big data arena. Government agencies and private sectors can reduce risks of cyber intrusions by adopting this innovate threat analysis and risk mitigation strategy.

Cybersecurity in the 21st Century: Applying Cyber Threat Intelligence

Charles E. Wilson

In the twenty-first century, the prevention of cyber attacks on critical infrastructure, key assets, and public/private sector enterprises will become a more important element of national and international security. This paper examines the extant literature published on the increasing need for a more robust, comprehensive and proactive approach to cybersecurity. Specifically, the paper explores the contemporary cyberspace environment and the current cyber threat landscape. The paper recommends the application of cyber threat intelligence (CTI), complemented by predictive analytics as an effective method for countering cyber attacks. The purpose of the paper is to advance the knowledge in this critical area, to increase the understanding of available

methods for proactive detection of network security intrusions, and to highlight two emerging approaches to cyber threat mitigation. The paper proposes that the effective use of cyber threat intelligence complemented by predictive analysis can enhance defensive postures, improve situational awareness, and increase preparedness for and prevention of future cyber attacks.

Keywords: Cybersecurity, cyber threat intelligence, network defense, and predictive analysis

Security Education for Smart Grid: Materials, Experiments, and Evaluation

Weichao Wang, Chuang Wang, Le Xie, Wenzhan Song, Yi Pan

With the fast development of Cyber-Physical systems (CPS), security in these special application environments starts to attract more and more efforts. In this project, we form a team of researchers in information security, power systems, simulation, and education evaluation to jointly develop educational materials and experiments for security education in smart grid. Multiple course modules for infrastructure and data security in smart gird have been designed. We design a simulation/emulation based experiment platform and develop several student projects upon it. These materials have been adopted by both graduate and undergraduate level security courses. Formal evaluations are conducted by third party evaluators.

Hardware Hacking: An Approach to Trustable Computing Systems Security Education

John Chandy, Zhijie Shi, Mark Tehranipoor, Megan Welsh, Chujiao Ma, Ujjwal Guin, Qihang Shi

Traditional approaches to teaching computer security have focused on understanding software and network security. However, computer systems comprise not only software and networks, but also include hardware components. The security of computer systems hardware has been typically ignored in most computer security curricula. In this paper, we describe a set of courses that can form a core of a hardware security curriculum. We pay particular emphasis to a “hardware hacking” class where students are exposed to a variety of hands-on exercises with hardware assurance. The class has shown that it not only introduce students to the topics of hardware assurance but also improve their hardware and digital design skills as well.

Exploring the Vocational Interests of Cybersecurity Competition Participants

Masooda N Bashir, April Lambert, Jian Ming Colin Wee, James Rounds, Nasir Memon

The demand for cybersecurity professionals grows each year, and so do efforts to attract students to cybersecurity. One way educators, industry, and government have come together in a joint effort to train and attract talent is through cybersecurity competitions. However, it is unclear whether cybersecurity competition participants share similar interest profiles with those already employed in the field. This paper begins to explore that issue by assessing the vocational interest of cybersecurity competition participants using Holland's RIASEC model. Our research demonstrate that cybersecurity competition par-

ticipants have vocational interests that can be characterized as investigative, social, and creative.

Practice, Practice, Practice... Secure Programmer!

Ida Ngambeki, Matt Bishop, Melissa Dark, Stephen Belcher

One of the major weaknesses in software today is the failure to practice defensive or secure programming. Most training programs include only a shallow introduction to secure programming, and fail to integrate and emphasize its importance throughout the curriculum. The addition of an ongoing, practical, mentored "clinic" or Secure Programming Clinic (SPC) is one way of addressing this lack without adding significantly to an already stretched curriculum. In order to properly design this clinic, it is important to identify the knowledge, skills and abilities (KSAs) needed to develop effective programmers. This paper describes the results of a Delphi Study undertaken to determine the primary knowledge areas in secure programming.

Teach the Hands, Train the Mind … A Secure Programming Clinic!

Melissa Dark, Matt Bishop, Ida Ngambeki, Stephen Belcher

Computer Science programs often fail to provide students with a complete and comprehensive education in secure programming. The reasons for this failure include: not emphasizing the importance of secure programming beyond basic principles, overloaded curricula in which secure programming courses are elective, and the failure to integrate advanced secure programming along with advanced programming. This paper proposes the use of a Secure Programming Clinic to help address this failure and describes principles for the design, structure, and evaluation of such a clinic.

Teaching Undergraduates Certified Security by Design

Shiu-Kai Chin

Design for assurance of security, from the hardware level on up, is essential for securing the integrity of the smart cyber-physical infrastructure that is the Internet of Things. If the smart cyber-physical infrastructure fails to do the right things - that is, if it loses integrity because it is insecure and vulnerable - then untold social consequences will occur. For the security and integrity of cyber-physical systems to improve, not only must engineers and computer scientists possess the capability to design-in security from the very beginning, but they must do so in ways that enable people other than the designers to reproduce and check verification results easily and quickly. Designers and certifiers must formally describe and verify operations at high levels, such as the command-and-control (C2) protocols used by commanders and operators, down to the operations of applications and hardware. We call this design and verification capability for security and integrity *certified security by design* (CSBD). Hallmarks of CSBD are (1) *complete mediation*—authentication and authorization of all access requests at all levels of abstraction from C2 protocols down to hardware, and (2) *formal verification of assurance of security and integrity* using methods and tools that are readily checked by third parties. Our experience leads us to conclude that CSBD is feasible and practical for undergraduates.

The CISSE Board would like to thank all the submitting authors and the reviewers for the time and effort it takes to write and review these papers.

Papers that did not make full academic paper status were considered for the Roundtable session, so that the authors with the help of their peers can incorporate suggestions and comments into their work for resubmission.

In fact the Editors would like to run a “Special Edition” RFP this fall, around the theme of “Cybersecurity Curriculum and Courseware from across the Country.”

See our website for updates: www.cisse.info

Redefining Digital Dashboard Training and Utilization to Improve Organizational Cyber Defenses

David Bouvin

Training initiatives should be established to define the role of digital dashboard access and technologies for specific cyber defense functionalities based on planned organizational activities. Digital dashboard access can be adjusted for specific stakeholders as firms are structured to enable business operations, reach within evolving industries, adopting growth-based initiatives, and during the realignment of organizational structures. The challenge with each organizational activity in response to market forces is the need for effective and timely decision making, information management, and data access. Utilizing digital dashboards for cyber defenses, all organizational decisions and operational steps can be directly linked to the ability to protect and disseminate pertinent information for the appropriate decision maker, at the right time, and at the correct locale.

Roundtable (WT): Digital Forensics Examiners

Masooda Bashir, Roy H. Campbell

The demand for digital forensics examiners is increasing as digital evidence plays an increasingly important role in our society. As that need goes unfulfilled, a related demand has appeared: the demand for a standardized digital forensics curriculum. Standards have been proposed by various organizations, but there has been resistance against widespread adoption.

This round table's goal is to provide a forum for discussing that challenge, in the context of critiquing the University of Illinois' current effort to take a national lead in defining a standard digital forensics curriculum.

Project-based Curricular Service Learning for Cybersecurity Career Preparation

Ping Wang

Cybersecurity is a fast-growing career field with increasing challenges for educators. Service learning can be an effective educational method to improve career knowledge, skills, and professionalism. This paper proposes a project-based curricular service learning model to enhance education and preparation for cybersecurity careers. The model views student experience, discovery, and learning from course-related service projects as key elements to improving readiness for the cybersecurity profession. The view is supported by data and findings from a service learning project and team collaboration used in an undergraduate information security class.

Framing the ICT Risk: People

Daniel J Bleaken

Who can you trust in today's information society? How can one totally assure information? The best way, I argue, is by enforcing laws and compliance over companies. Doing so in a non-invasive way that establishes cooperation between business and government is critical to individual liability. In particular, counterfeit goods pose a large threat and can be regulated through normal means and prevented by legal executions. This is to assure the general public and government.

Best Practices for Engaging Adolescent Girls in Cybersecurity Education

Monique Jethwani, Nasir Memon

The underrepresentation of women in computer science has been attributed to stereotype threat, or a fear of fulfilling negative stereotypes about women in computing and perceptions of computer science fields as being masculine and isolating. The purpose of this study was to identify best practices for effectively engaging girls in cybersecurity education. This study utilized qualitative data gleaned from focus groups with 38 adolescent girls that attended a two-week single sex cybersecurity summer program at a leading urban university. Results revealed that exposing girls to the practical application and collaborative nature of cybersecurity in a single sex setting with patient teachers and female mentors challenged gender stereotypes about the field, removed stereotype threat, raised girls' confidence and led many to consider computer science as a career. These results contribute to a greater understanding of evidence based practices with girls in cybersecurity.

Impact of Community College Cybersecurity Education on Small Businesses

Debasis Bhattacharya

Small businesses often display a lack of concern towards cybercrime and information security problems. A lack of concern usually results in delayed or incorrectly implemented security measures, which increases vulnerability to cybercrime. This paper initially present an empirical study, conducted in 2008, of 122 small business owners from the state of Hawaii with regards to their information security concerns. These results are compared with earlier studies conducted in 2000 and 2003. A major purpose of this paper is to demonstrate

the impact of a community college on the local small business community with programs in cybersecurity education, workforce development and high school teacher and student engagement.

Integrating Cybersecurity into K-12 Summer Camps through Experiential Learning

Claude Turner, Carlene Turner

Outreach educational programs are an important component in training the next generation of cybersecurity professionals. This paper discusses our experience in integrating cybersecurity into computer science summer camp programs at Bowie State University (BSU) for middle and high school students. BSU has ran an outreach program for middle and high school students that offers training in programming, robotics and basic computer science skills for several years. It also has emergent cybersecurity programs at both the undergraduate and graduate levels. However its outreach program has lacked a cybersecurity component. In the summer of 2013, we added a cybersecurity component to this program by introducing students to the following four key cybersecurity areas through experiential learning: (1) Cybersecurity Awareness, (2) Mobile Forensics, (3) Security in the Cloud, and (4) Security in Satellite Operations. Our approach to integrating security draws from a variety of techniques discussed in the literature, recommendations from the public and private sectors, and our own experience. Results from pre and post-test analyses indicate that students became more cybersecurity aware after completing our modules. Further, reaction from a parents and teachers-targeted workshop on how to use the modules indicated keen interest and excitement among this community.

An Implementation of Peer Learning for High School Students at a Cybersecurity Camp

Jason Pittman, Ron Pike

This paper reports on the design and implementation of a cybersecurity camp offered as a cybersecurity learning experience to a group of female and male high school students. Students ranged in grade level from freshmen to senior. Student demographics, including any existing pre-requisite knowledge, were unknown to camp designers prior to the start of the camp. Such unknowns presented five design constraints that required lateral solutions to address. Chiefly, a peer learning design was deployed that allowed participants to self-organize and autonomously explore learning within secure systems administration, network security, and cryptography. Furthermore, camp participants were provided with three objects to guide the peer learning objective: a booklet containing fundamental commands within the camp knowledge areas, a Xubuntu virtual machine as a digital playground, and a digital scavenger hunt game to reinforce acquired knowledge. Observational data indicate that peer learning was a successful pedagogy. Further, the results demonstrate compelling knowledge and behavioral flows amongst participants. Accordingly, this paper goes on to suggest a Community of Practice (CofP) as an organizational umbrella to support ongoing peer learning in the cybersecurity field. The paper also calls for future research to support the development of peer learning and CofP structures to support cybersecurity education.

Integrative and Experiential Learning Techniques in Cybersecurity Education

Sherly Abraham, Lifang Shih, Jane LeClair

Cybersecurity education requires a holistic approach that focuses on curriculum, experiential learning and building communities of practice. In this paper, we present a multifaceted model to cybersecurity education that draws on integrative learning theory, experiential learning theory and community of practice. We emphasize the need to build conceptual, tactical and practical skills among cybersecurity professionals. The paper will include examples of how integrative and experiential learning can be implemented in cybersecurity education through a number of methods such as curriculum, virtual labs, cyber student clubs and participation in cyber security competitions. The recommendations shared will be beneficial to cybersecurity educators and practitioners in implementing strategies to build an effective cybersecurity workforce.

The FIDO INSuRE (Information Security Research Education) Project: An Agile Research Experience

Rylan C. Chong

Real-world cybersecurity events are unpredictable and fast moving, and can have serious consequences that impact national security and economic well-being. Effective responses can benefit from research conducted by the best minds and organizations carried out by multi-disciplinary, multi-organizational, and self-organizing teams. However, research can be ineffective if it takes too long and is overtaken by events. The Agile Research process is a new approach to provide this type of rapid, authoritative, applied research. The INSuRE (Information Security Research and Education) project has as one of its goals introducing graduate students to real-world cybersecurity research

needs. INSuRE incorporates the Agile Research methodology as the organizing framework for team operations. Students who are part of Agile Research carry out their research fast, authoritatively, and incrementally, with the goal of producing actionable results at each step. INSuRE establishes a tight coupling between research teams and sponsors characterized by open communication and opportunistic management decision-making based on incremental findings. This paper discusses the student experience in applying the Agile Research process within the INSuRE framework, utilizing the FIDO (Fast Identity Online) project as a case study.

Scare, Prepare and Dare: High Impact, Low Cost Incorporation of Cyber Security into High School Curriculum

Prem Uppuluri, Joseph Chase, Jeffrey Pittges, Michael D. Ramos

Over the past two years, with funding from the NSA and other sources we have been working to incorporate cyber security into high school curriculum. The main goal is develop curriculum to serve as a scaffolding between cyber security programs that are aimed at increasing basic awareness in K-12 and those that provide a rigorous multi-semester cyber security course sequence with in-depth networking coverage thus primarily serving the motivated students. The targets of this project are students (a) who have never considered an IT-related field of study or (b) who are considering IT but study in high schools that do not support such a curriculum due to limited personnel and technology resources. In this paper we present our approach and the salient results.

Designing a 2+2 Program in Computer Security

David Charles Bover

This document outlines the design of a joint academic program between a community college and a university, culminating in a baccalaureate degree in computer and information systems security. Students complete the first two years of the program at the community college, earning an Associate in Applied Science. The final two years of the program at the four-year institution enable them to complete the requirements for a BS degree in a total of four years.

This program was developed in response to an urgent need for trained personnel in this field far exceeding the capacity of existing programs. In considering the types of professionals needed for the computer security industry we identify four distinct but related roles. Working back from the knowledge and experience needed for such personnel, we identify the body of knowledge that they, collectively, should attain.

The boundaries of the final two years are then defined by outcomes of the existing two-year program at the community college as the starting point and the body of knowledge as the end point. The final two years at the four-year institution are further constrained by general education requirements and the requirements for residency, upper-division credits and writing proficiency.

Integrate Mobile Devices into CS Security Education

Hongmei Chi

Mobile computing, popularized for social media, has emerged as a delivery vehicle of choice for commercial, medical and military applications. The ubiquity of wireless and satellite communication and the rapid evolution of powerful devices that exploit this infrastructure have pushed mobile application de-

velopment, in many instances, ahead of the capabilities to ensure the secure and safe utilization of these applications. The gap between capabilities and the ability to safeguard information assets must not be ignored, given the documented rise in the number and sophistication of threats and the broadening vulnerabilities of mobile applications and systems worldwide. We are focusing on how to integrate mobile apps/devices into our cyber security courses. In addition, case studies and hands-on labs are discussed in our practice.

Pentest Competitions - a CISSE Roundtable Proposal

Bill Stackpole

In an effort to add a fourth alternative to the competition space, a penetration testing competition is planned. A penetration test is neither a hacking event nor an attack-motivated competition. It is a goal-oriented exercise bound by a contract and subject to a standard (e.g. the Penetration Testing Execution Standard - PTES). The goal is to evaluate and identify vulnerabilities that can be exploited, and to prove the existence of those vulnerabilities in an intelligent and ethical manner. It does not reward for successful discovery of exploitable content unless carefully considered mitigation plans are also offered.

Vulnerable Web Server: A Virtual, Integrated Education Environment with Companion Curriculum

Cort Thompson, Jake Kravitz, Justin Myszka, and Clint Hepworth

Cyber-security awareness has moved to the forefront of national discussion in the past decade. It is widely acknowledged by experts and laymen alike that American infrastructure is increasingly vulnerable to both external and internal

cyber threats. American leadership has identified a gap in our cyber capabilities in respect to the threats we face, and has begun to implement committees, programs, and initiatives in order to increase understanding and awareness in the general public. In order to remain at the forefront of technological capability, the American education system needs to implement programs and initiatives that connect the future work force to required cyber-domain skills. Team Vulnerable Web Server (VWS), an undergraduate capstone design team, is developing a comprehensive, open-source education solution that addresses shortfalls in current secondary school curricula / environment offerings in order to cultivate the future cyber workforce. In this paper we describe the current education initiatives from the federal and state governments, examine several widely distributed education platforms, and finally detail how the VWS package addresses the identified gaps in current offerings.

Creating awareness of the field of cyber forensics with a simulated digital crime scene investigation

Tong Zhang, Krishani Abeysekera, Sharon Perkins Hall, Sadegh Davari

The increased need for professionals in the exploding field of cyber forensics calls for students with an understanding of how information is stored in a computer. The challenge we are faced with is one that requires students to first be aware of the opportunities available in cyber forensics, and then to prepare them with education and experience to enter the workforce. This project describes an engaging activity that gives students an introduction to the many places in which data is stored in a computer, as well as experience using forensics tools.

Tips & Tricks for Running Large-Scale Summer Camps for High School Students

Joshua Pauli

Dakota State University was one of the universities that conducted a pilot camp for the GenCyber project in 2013 as funded by NSF and NSA. The goal of the project is to educate and excite students about cyber security while they are still in high school. Likewise, there are also camp opportunities for high school teachers to gain cyber security content for their classroom.

We hosted 172 high school students (grades 10-12) for a week in an on-campus immersive camp and are coming back in 2014 supporting 200 students on campus for a week! The demand for such camps is extremely high as we have students coming from 26 states and our waiting list is nearly 300. GenCyber is expanding quickly so there is a tremendous opportunity for others to hold camps in 2015 and beyond.

This session will share our experience and provide best practices others can use when hosting large numbers of high school students on their campuses. Topics include, but are not limited to: recruitment strategies, registration processes, camp content, evening activities, overnight safety and management, and other lessons learned.

Modeling Cybercrimes and Investigation Strategies for Digital Forensics Education

Xinwen Fu, Lawrence Wilson, Li Yang, Benyuan Liu, Chao Gao

The Internet has become the primary battlefield of the cyber war and the prevalent environment of cybercrimes. Digital forensics education meets the urgent need of cyberspace operations professionals. Network forensics is one

branch of digital forensics and focuses on evidence collection, analysis and suspect identification in a networked environment. However, the current network forensics education lacks a systematic view of how real-world cybercrimes are committed and how real-world cases are investigated. Individual techniques are taught in class without much real-world case support. In this project, we fill these gaps by modeling real-world crimes reported by FBI and real-world investigations performed by law enforcement, and build a real-world case repository for digital forensics, particularly network forensics, education.

Developing a Multidisciplinary Digital Forensics Curriculum: Utilizing a Workshop Format to Foster Discussion

Gabriela L. Garcia, Imani Palmer, Lizanne DeStefano, Roy H. Campbell, Masooda N. Bashir

The demand for education in the area of digital forensics is high as there is a noticeable shortage of qualified and skilled digital forensics practitioners. While education and training in digital forensics is growing, the need for a standardized curriculum is apparent. In response, a team of researchers are developing and implementing a multidisciplinary digital forensics curriculum with the intent of broadly distributing the curriculum and working for its acceptance as a standard by the greater digital forensics community. To meet this goal, the team hosts annual one-day workshops with the aim of fostering and encouraging discussions with the digital forensics community about the process and development of this curriculum. This paper describes the workshops and includes lessons learned from the community thus far.

Cyber Security Awareness and Education Through a MOOC

Humayun Zafar

MOOCs have been around since 2011, and this model for delivering learning content online to anyone who wants to take a course has been steadily gaining popularity. Among its benefits are no application or tuition, and a single course can educate thousands of students at one time.

We are pleased to present a cyber security MOOC that is designed for students to gain knowledge and understanding of cybersecurity and its domains by engaging in community discussions, and have online interaction with both professors and industry experts.

EVF - An Extensible Vulnerability Framework

Daryl Johnson

The goal of this work-in-progress is to develop an Extensible Vulnerability Framework (EVF). The framework will capture for each vulnerability the requirements to implement, install, attack and monitor or detect an attack, and also provide a collection of escalating tips, advice, and tutorials to assist students to better understand the process of defending or exploiting a vulnerability. In this context vulnerabilities include weaknesses and mis-configurations. One possible application would be to support the deployment of targets in a cyber-gymnasium platform.

Towards the Design and Implementation of a BYOD Security Platform for the K-12 School Environment

Subrata Acharya, William Forrester

Today's world continues to grow more reliant on devices (e.g., mobile devices connected to a global data network). These devices hold our professional and personal information. A shift has occurred as digital devices become ubiquitous, enabling them to become an extension of the self. Connected devices appear earlier in our lives and stay connected to our lives, and are designed with accessibility and usability in mind. It is with this seamless blending into our self that we see a security framework for our youngest learners to our oldest learners (pre-K - 12) setting as necessary. Additionally, it also develops the dialogue to discuss security in design from the beginning of the curriculum in-order to educate and protect our self and generations of learners growing up as digital natives. Hardware is paired with software design in order to create a secure communication that is user friendly and accessible to a mass instead of a few elite experts. Thus, the proposed research provides a seamless collaboration of education and technological leadership to influence decision makers regarding the feasibility and the applicability of implementing a "*Bring Your Own Device (BYOD)*" policy within a public school system.

Impact of Live Acquisitions on Encryption and Forensics

Cynthia M. Shaw

Abstract— In the field of digital forensics, the topic of encryption has become a hot issue, especially in mobile forensics. However, computer forensic analysts are also faced with the encryption issue when performing an acquisition of data on desktop and laptop systems. Encryption was formally a nemesis to

an investigator. The introduction of advanced forensic software and a more extensive knowledge of operating systems has helped investigators to overcome encryption challenges, if a system is handled quickly and efficiently. Live acquisitions of a system's random access memory (RAM) data can crack an encrypted hard drive, allowing a forensic examiner to extract the data needed for a criminal case. RAM holds a plethora of valuable data such as the passwords of the hard drive, as well as system files that are or were recently running. This paper discusses live acquisitions, why it is important, what data can be extracted and how that is beneficial, as well as the impact of live acquisitions in the computer forensic field especially with increasing complex encryption methods.

Case Studies on Browser Security

Lindsay Simpkins, Xiaohong Yuan, Justin Zhan

Case-based teaching methods allow students to better apply learned skills to real world industrial settings. It can bridge the gap that exists in current computer science education between theoretical concepts and industry-related skills and best practices. There is a need to develop case studies due to the lack of case studies used in current computer science curriculum. Three case studies were developed to help students learn browser security related topics, covering the topics of web tracking and privacy, and application logic flaws. Each case study has an accompanying set of discussion questions where students apply what they learned from the cases.

Toward a Practical Information Systems Security Curriculum in Small Universities

Wei Wei, Krishani Abeysekera, Arti Mann

Pervasive usage of information systems generates an urgent need to protect our information assets and systems against breaches and attacks. In order to win this battle, we need professionals versed in information systems security. However, the demand is yet to be fulfilled because the supply of trained cyber-security professionals is not keeping up with the need. In an age where most people use some form of digital devices in their daily life, prevention of computer attacks require not only trained security professionals who can prevent, detect and respond to attacks, but also a general population that is aware of how to secure their information. This paper proposes a unified solution to educating students in cyber security that is flexible and sustainable, while using existing resources.

A New Voice Recognition Based Mobile Security System on Cloud Servers

Zhongli Ding, Yanqing Zhang, Michael Weeks, Yi Pan

Mobile devices bring convenience to the daily lives of people, and make many tasks more efficient. However, there are still many potential issues to be solved urgently, especially in the area of mobile security. In this paper, we discuss and analyze the background of mobile security in order to build an architecture to solve security problems like the unsafe practice of storing passwords on the device itself. As a result, the proposed application, Mobile Security System, would be available to install on Android devices to enhance the protection of owners' data. I can also allow the owner of a stolen device to get the device back. Furthermore, mobile security is a relatively weak area in most

schools' computing curriculum [5]. For the purpose of promoting the interests and knowledge of students about mobile security, we include the manuals of the application, both for developers and users, which would certainly be helpful when students try to use and develop new features on the application. Finally, we list future improvements of the application, to further protect the data and more easily get a stolen device back.

The Challenge of Cyber Science Terminology Management

Joseph Ekstrom, Jessica Richards

The Cyber Education Project (CEP) is an initiative to develop undergraduate curriculum guidelines and a case for accreditation for a baccalaureate in “Cyber Sciences” (The Cyber Education Project, 2015). The Learning Outcomes Working Group (LOWG) is in the process of creating a “Taxonomy” and a set of “learning outcomes” for this baccalaureate program.

In this document we examine concepts from the disciplines of linguistics, terminology management, knowledge management and ontology development that help illuminate the challenges involved with creating and managing the vocabulary we use to communicate about technical topics. We discuss how the concepts of ambiguity and terminology apply to the CEP and the issues of creating and managing a controlled vocabulary to support a field of study.

We discuss the magnitude of the work by providing general characteristics of 31 glossaries and 5 different taxonomies or Bodies of Knowledge proposed by “Cyber security” related organizations.

Finally we conclude with some suggestions of how to approach the creating and managing a vocabulary for Cyber Sciences without losing the connections to the source disciplines.

Finding the Balance Between Guidance and Independence in Cybersecurity Exercises

Richard Weiss, Franklyn Turbak, Michael Locasto, Jens Mache, Erik Nilsen

In order to accomplish security tasks, one needs to know how to analyze complex data and when and how to use the tools. Many hands-on exercises for cybersecurity courses have been developed to teach these skills. There is a spectrum of ways that these exercises can be taught. On one end of the spectrum are prescriptive exercises, in which students follow step-by-step instructions to run scripted exploits, perform penetration testing, do security audits, etc. On the other end of the spectrum are open-ended exercises and capture-the-flag activities, where little guidance is given on how to proceed.

This paper reports on our experience with trying to find a balance between these extremes in the context of a suite of cybersecurity exercises that we have developed. We have found that our students are most successful in these exercises when they are given the right amount of prerequisite knowledge and guidance as well as some opportunity to find creative solutions. Our scenarios are specifically designed to develop analysis skills and the security mindset in students and to complement the theoretical aspects of the discipline and develop practical skills.

Become What They See and Connect to in Cyber Security

The CISSE Women and Minorities in Cybersecurity Working Group, hosts a half-day workshop on Sunday, June 14th. The goal of the workshop is to contribute towards building the pipeline from community colleges by targeting women and minorities in cybersecurity. This will, in turn, contribute towards strengthening and improving the state and participation of women and minorities in cybersecurity.

About 50 participants will attend the half-day. The participants include women and minorities; students currently enrolled in cybersecurity programs, undecided majors from community colleges, 4-year institutions and graduate IT programs, and role models currently working/practicing in the Cybersecurity fields. WG members will facilitate the workshop.

Undecided majors will be exposed to a wide range of practical aspects of cyber security through some hands-on activities. Students will get an opportunity to interact with cybersecurity role models and learn about cybersecurity professions, career paths and jobs, skills needed to be competent and the kind of problems the professionals solve on a daily basis.

This workshop will provide a great social networking/sharing opportunity for students from different institutions and this will help towards building a community.

Our thanks to everyone involved in this amazing event and to NSF for their generous financial support.

Become What They See and Connect to in Cyber Security

Sunday, June 14, 2015 in the Marquis Ballroom

Facilitators

Rebecca Gurley Bace
Karlyn Barilovits
Devon Bryan
Deanne Cranford-Wesley
Delali Dzirasa
Linda McCarthy
Jean Pawluk
Corrinne Sande
Rose Shumba
Veda Woods

Student Facilitators

Aishwarya Ganesan
Eleashia Jackyee' Hodges
Sarah Isaacs
Trang Nguyen

Faculty and Students Participated from

Indiana University of PA
Whatcom Community College
University of Maryland
University College
Forsyth Technical Community College
Montgomery Community College
Walden University
South Alabama University
University of Illinois at Urbana–Champaign
Towson University
Columbus State University
The Metropolitan University
Mississippi State University
California State University San Bernardino
Norfolk State University

NSF Proposal Writing & Review

Monday, June 15th at 1:15pm - Marquis #8

This workshop will explore the characteristics of successful NSF grant proposals, with a focus on proposals for cybersecurity education projects. Before the session, all participants will read, take notes on, and assign a tentative rating to two abbreviated proposals. At the session, the presenters, who are NSF program officers, will discuss proposal-writing guidelines and NSF's review criteria. Then the participants will break into small groups, like an NSF review panel, and discuss the two sample proposals. Each group will then report back its assessment of the strengths and weaknesses of the proposals in terms of NSF's review criteria. Through this exercise, participants will gain an understanding of how proposal-review panels are conducted and what the reviewers and NSF look for in proposals.

Dr. Corby Hovis

Dr. Victor Piotrowski

The National Science Foundation

Security Injections@Towson: Introducing Secure Coding in CS0, CS1, and CS2

Tuesday, June 16th at 1:15pm - Murica

Dr. Blair Taylor

Dr. Blair Taylor is a Clinical Assistant Professor in the Computer and Information Sciences department at Towson University with over 20 years of teaching experience. She developed and assessed many of the injection modules. She has published and organized numerous workshops on introducing secure coding in the introductory courses. She has been funded by the National Science Foundation and Department of Defense and was awarded the University System of Maryland Regents Teaching award.

Dr. Siddharth Kaza

Dr. Siddharth Kaza is an Assistant Professor in the Computer and Information Sciences department at Towson University. Dr. Kaza's research interests lie in secure coding, data mining, social network analysis, and security informatics. He has published and organized workshops on teaching secure coding and has been funded by the National Science Foundation, Department of Defense, and the Maryland Higher Education Commission.

Dr. Joe Adams

Cyber Range

Dr. Joe Adams is the Vice President of Research and Cybersecurity at Merit Network, Inc. Recently retired from the U.S. Army as a colonel, he taught at the U.S. Military Academy (USMA) as an associate professor and was responsible for USMA's cyberdefense course. As the chief information officer of the National Defense University, Joe build an information assurance program that was recognized by the commanding general of the Defense Information Systems Agency in 2010. In his current position, Joe is focused on leading and expanding Merit's network research and cybersecurity programs. He is the director of the Michigan Cyber Range, an internationally recognized platform for education, exercises and testing in cybersecurity.

Joe earned a B.Sc. in computer engineering from Syracuse University and a M.Sc. in computer systems engineering from the University of Arkansas. He earned his Ph.D. in computer engineering from Virginia Tech, where his research focused on network security and access control in mobile ad-hoc networks. He also holds a master's of strategic studies from the U.S. Army War College.

Dr. Helen Barker

Articulation Agreements: Lessons Learned

Dr. Helen Barker serves as Dean of the School of Business and Information Sciences with Capitol Technology University. Before joining Capitol in 2000, Dr. Barker worked in the private sector as a management analyst and resource training specialist in the Washington, DC area and a research analyst in child welfare and economic development in Northern Virginia. Research interests include cyber curriculum, women in STEM, and data security.

Dr. Barker received a B.S.B.A. from Thomas Edison State College, M.S.B.A. from Strayer University, M.S. in Information Telecommunications Management from Capitol Technology University, and doctorate from University of Phoenix in Organizational Leadership. Current research interests include pedagogy relating to online learning and integration of cyber security into business curriculum.

Robin A. Barraco

Incorporating Cyber Security in General Education Classes

Robin A. Barraco earned an M.S. in Information Systems Management and an M.S. in Career and Technical Education from Ferris State University, Big Rapids, Michigan. She also earned a Bachelor of Science Degree in Business Administration and Management/ Computer Information Systems from Park College, Kansas City, Missouri.

Professor Barraco has been teaching for 20 years. She has been teaching in the Ferris State University Information Security and Intelligence program since the fall of 2013. Prior to this she taught at St. Clair County Community College, Baker College, and the St. Clair County Technical Education Center.

During her 23-year career in private industry, she has served as a corporate trainer for software applications and security awareness, Electronic Medical Records (EMR) Project Manager, Information Systems Coordinator, and Application Developer. As a consultant, she has designed and implemented security programs, acted as a Physician Liaison during EMR implementations, developed desktop and web-based applications, designed ecommerce web sites, and developed a web-based system for the call center of a major utility company.

Robin Barraco's passion for sharing information security awareness is evident in her classes and in her writing: "Information Security Awareness and Training for Small Business" and the "Keep it Simple Information Security & Aware-

ness Training: Small Business Workbook." Through her research, she identified over 300 free resources for information security awareness and training.

Jay Bavisi

Industry Certifications

ay Bavisi is the Co--Founder and President of EC-Council, a global leader in information security education, training, and certification. Formed following the 9/11 incident, EC-Council addresses issues of cyber terrorism raised at the forefront of security of nations at large. It is the owner and developer of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Secure Analyst (ECSA), and Licensed Penetration Tester (LPT) programs.

Jay led the efforts in establishing the partnership with the International Telecommunications Union (ITU), an arm of the United Nations, via the International Multilateral Partnership Against Cyber Threats (IMPACT) to develop sustainable knowledge and capabilities in information security awareness amongst government agencies in 194 member countries.

Jay is a Board member of the Department of Homeland Security/National Security Agency's Colloquium for Information Systems Security Education (CISSE), reputed as one of the largest information security gathering of academics, government, and industry professionals in the United States.

Jay is the Chairman of the EC-Council Foundation, a not for profit charity dedicated to raise awareness of information security, build capacity and promote world peace. He has contributed in projects to help the unfortunate gain technical knowledge, help wounded warriors become cyber experts and help kids become aware of cyber risks.

Jay Bavisi is a law graduate from the University of Wales, College of Cardiff, with an LLB (Hons), Barrister - at - Law from Middle Temple, London.

Dr. Douglas Blakemore

Incorporating Cyber Security in General Education Classes

Doug received his Ph.D., Capella University, 2003 and majored Organization and Management. He continues to network at ACFE and Infragard. He has published to journal publications, Blakemore, D. L. (2006). Adam Smith Review and Blakemore, D. L. (2006). Academy of Management Review. And contributed a chapter in the Book: Mobil Devices in Education (2011) by Barbara Ciaramitaro, Editor. Doug continues to hone his skills by keeping up his training in visual analysis using both Threads and I2 Analysts Notebook and is a Certified Intermediate level Encase examiner.

Dr. Deanne Cranford-Wesley

Become What They See and What They Connect to in Cyber Security Workshop; K-12 Working Group

Dr. Deanne Cranford-Wesley is Department Coordinator in the Information System Security Program at Forsyth Technical Community College. Dr. Cranford-Wesley is a cybersecurity professional and has appeared as a subject matter expert on Fox8 and Time Warner News discussing recent advances in cyber security vulnerability. She also teaches Information System Security, Computer Forensics and Networking courses in the Business Information Technology Department. Additionally, Dr. Cranford-Wesley has presented at various conferences including several presentations at The Colloquium Information System Security Education Conference, CompTIA Educators Conference and North Carolina Computer Instructor Conference (NCCIA).

Prior to this role Dr. Cranford-Wesley, held the title of Associate Professor of Networking and Security. During her 12 year tenure she taught undergraduate, and graduate students. Later, she moved on to teach solely in the Gradu-

ate Master of Science in Information Security Program. In this position she led the School of Technology to the designation of "Center of Academic Excellence in Information System Security" acknowledged by the National Security Administration in collaboration with the Department of Homeland Security. Dr. Cranford-Wesley was awarded the title and benefits of "Distinguished Adjunct Faculty" in the College of Technology at Davenport University.

Robert J. Du Charme

Cyber Range

Bob Du Charme is a Principal Professional Services Engineer with Ixia. He was hired by BreakingPoint Systems in May 2012 and Ixia soon acquired BreakingPoint. In this position, Bob has responsibilities for training and professional services for all Security related activities for customers of Ixia.

Prior to working at Ixia, Bob was employed by Cisco Systems from June 1998-July 2011. Bob had multiple positions while at Cisco, including training, security services, and working with higher education. Bob trained all of Cisco's security products for thousands of customers and partners. He also was a speaker at many industry conferences, including Cisco's customer conference Cisco Live on 5 different occasions. While at Cisco, Bob trained hundreds of higher education professors and instructors on practical implementations of security technology. Bob also managed a program that donated millions of dollars of Cisco equipment to colleges and universities to enhance their students learning experiences.

Bob also worked for the United States Federal Courts at their technical support center in San Antonio TX. Bob retired from the United States Air Force after serving for 17 years in various roles.

Dr. Marc J. Dupuis

Transitioning Veterans into Cybersecurity

Dr. Marc J. Dupuis is a researcher and lecturer with the University of Washington as well as the Director of Human Factors for the Center for Information Assurance and Cybersecurity (CIAC). His main focus is on understanding the cybersecurity behavior of individuals, including issues related to decision making and the user experience. This has included research on the role of trait affect, personality, self-efficacy, and risk evaluation on information security decisions made by individuals, as well as an examination of the various security and privacy concerns related to social computing.

Dupuis earned a Ph.D. and M.S. in Information Science in addition to an M.P.A. from the University of Washington. He has also earned an M.A. and B.A. from Western Washington University. He has taught courses on cybersecurity, organizational information assurance, risk management, information assurance strategies, human computer interaction, web design & programming, and research methods.

Dr. Barbara Endicott-Popovsky

Transitioning Veterans into Cybersecurity

Professor Barbara Endicott-Popovsky, Ph.D., is Executive Director of the Center for Information Assurance and Cybersecurity at the University of Washington, designated by NSA/DHS as a Center of Academic Excellence in Information Assurance Education and Research, Director of the Master of Cybersecurity and Leadership program, Academic Director for the Masters in Infrastructure Planning and Management in the Urban Planning Department of the School of Built Environments, holds a faculty appointment with the Institute of Technology in Tacoma, and was named Department Fellow at Aberyswyth University Wales (2012). Fellow with the American Academy of Forensic Science. Her academ-

ic career follows a 20-year career in industry marked by executive and consulting positions in IT architecture and project management.

Her research interests include enterprise-wide information systems security and compliance management, forensic-readiness, the science of security, cybersecurity education and secure coding practices. For her work in the relevance of archival sciences to digital forensics, she is a member of the American Academy of Forensic Scientists. Barbara earned her Ph.D. in Computer Science/Computer Security from the University of Idaho Center for Secure and Dependable Systems (2007), and holds a Master of Science in Information Systems Engineering from Seattle Pacific University (1987), a Master in Business Administration from the University of Washington (1985) and a Bachelor of Arts from the University of Pittsburgh.

Mark Estep

Developing Cybersecurity Talent Before College Through Competitions

Mark has been teaching at Poolesville High School (PHS) in the Science Math Computer Science Magnet program since its inception in 2006. He has degrees from Houghton College, Teachers College Columbia University, and Hood College.

Jay Gehringer

Developing Cybersecurity Talent Before College Through Competitions

Jay has a Bachelor of Music degree from California State University, Long Beach and a Master of Arts in Educational Technology from Pepperdine University. He has worked at N. Hollywood High School for 32 years.

Colonel David S. Gibson, Ph.D.

Toward Curricular Guidance in the "Cyber Sciences"

Colonel David S. "Hoot" Gibson is the Permanent Professor and Head of the Department of Computer Science at the United States Air Force Academy in Colorado Springs, Colorado and the Academy's senior Cyber Operations officer. He leads the 28-member department that administers the Computer Science program and the new Computer and Network Security program. His department also supports the Operations Research, Computer Engineering, and Systems Engineering programs. In addition to teaching over 1400 cadets each year, his department is home to the Academy Center for Cyberspace Research which conducts research in cyber operations, information assurance, and cyber education. In his 31-year Air Force career, Col Gibson has held leadership positions in electronic warfare, computer security, space systems testing, information operations, information technology, intelligence, cyber operations and education.

Col Gibson serves as co-chair of the Learning Outcomes Committee of the Cyber Education Project. He has served as a Commissioner and Program Evaluation Team Chair for ABET's Computing Accreditation Commission since 2007 and has been a member of the Association for Computing Machinery since 1984. Col Gibson has degrees in computer science and physics with a Ph.D. in Computer and Information Science from The Ohio State University.

Robert A. Green

Transitioning Veterans into Cybersecurity

Robert A. Green. PE, F.NSPE, is the Undergraduate Coordinator for the Bagley College of Engineering at Mississippi State University. In this position, Mr. Green works with faculty and students on undergraduate academic issues and represents the Dean on many related issues. In addition to his administrative duties, he

teaches several undergraduate and graduate courses including, most recently, Introduction to Engineering and Public Policy, Engineering Law and Ethics, and Engineering Administration. He is also a frequent lecturer to classes and professional seminars on professional registration and engineering ethics. Mr. Green is a Captain (O-6) in the US Navy Reserve and has completed seven tours as commanding officer. His personal awards include the Meritorious Service Medal, Navy and Marine Corps Commendation Medal (4 awards), Navy and Marine Corps Achievement Medal (4 awards) and others.

Mr. Green's research interests are in the areas of organizational change, leadership development of technical professionals, and issues affecting veterans entering STEM fields. He holds a BS in Chemical Engineering and an MS in Mechanical Engineering from Mississippi State University, and an MA in National Security and Strategic Studies from the US Naval War College. He is working on his dissertation in Public Policy and Administration which is focused on organizational change in risk-averse professions. Mr. Green is also the Immediate Past President of the National Society of Professional Engineers.

Robert Hamilton

Community College: Effective 2/4-Year Information Security Curricula

Robert Hamilton is an Information Security Specialist with the Oklahoma Department of Career and Technology Education. Robert holds a graduate degree from the University of Tulsa's Center for Information Security and also holds the CISSP certification (Certified Information Systems Security Professional). Robert is currently working with Information Assurance and Digital Forensics training initiatives involving the Cyber Security Education Consortium (CSEC), which includes academic institutions in Oklahoma, Texas, Kansas, Louisiana, Arkansas, Colorado, Missouri, and Tennessee. Robert's current focus is in the area of Control Systems Security used in the nation's critical infrastructure in which he is currently holds the

Certified SCADA Security Architect (CSSA) and Global Industrial Cyber Security Professional (GICSP) certifications.

Dr. Elizabeth K. Hawthorne

Community College: Effective 2/4-Year Information Security Curricula; Toward Curricular Guidance in the "Cyber Sciences"

Dr. Elizabeth K. Hawthorne, CISSP, CCFE is a Senior Professor of Computer Science at Union County College in Cranford, NJ with a passion for creating academic pathways in cybersecurity education along with a special interest in attracting and retaining young women to this exciting STEM field. Dr. Hawthorne serves on the advisory board for the National Women in Cybersecurity annual conference, WiCyS. Additionally, she serves as co-chair of the Learning Outcomes Committee for the Cyber Education Project

Dr. Hawthorne is a member of both professional computing societies, the ACM and the IEEE Computer Society. She enjoys serving on the ACM-W Council and chairing its Community College Connections committee. In addition to ACM-W, she is actively engaged in many ACM activities, serving as Chair of the ACM Committee for Computing Education in Community Colleges (acmccecc.org) since 2007, and as a member of both the ACM Education Board and the ACM Education Policy Committee since 2014. Also, Dr. Hawthorne is a featured columnist for ACM Inroads, authoring each quarter the "Community College Corner." In 2012, the ACM Special Interest Group on Computers and Society (SIGCAS) presented Dr. Hawthorne with their annual Outstanding Service Award for her contributions to the Social Issues and Professional Practice Knowledge Area of the ACM/IEEE-CS Computer Science curricular guidelines. She also has served as either the Principal Investigator (PI) or co-PI on National Science Foundation grants, including Security Injections@Towson - Introducing Secure Coding in CS0, CS1, and CS2.

Dr. Hawthorne received her Ph.D. in Computer Information Systems from Nova Southeastern University and in 2014 completed a post-doctoral fellowship program in Digital Forensics and Cyber Investigations from the University of Maryland University College. During the summer of 2013, she was selected as one of ten faculty nationwide to participate in a cybersecurity faculty research and training program at NYU-Polytechnic in Brooklyn, NY. Additionally, she holds the professional certifications of Certified Information Systems Security Professional (CISSP) and Certified Computer Forensics Examiner (CCFE).

Dr. Rae Hayward

Industry Certifications

Dr. Hayward is a highly regarded, experienced educator with a background in the application of sound pedagogical and andragogical theory for the holistic design and development of curriculum and learning content for both academia and corporate knowledge acquisition. She has spent 15+ years developing curriculum structures for corporate organizations, including succession planning education and core job skills acquisition. Her expertise in technology has enabled her to develop and implement Learning Management System platforms and initiate learning object structures to minimize development costs and maximize learning effectiveness. With a doctorate in instructional technology, distance education and curriculum development, Rae has helped academic institutions and corporate organizations develop innovative educational platforms and content that maximizes current advancements for effective and efficient transfer of knowledge. She is responsible for the strategic development of all (ISC)2 educational content, which includes developing courses for the entire career lifecycle of an IT security professional.

Dr. Daniel Manson

Developing Cybersecurity Talent Before College Through Competitions

Dr. Dan Manson, CISSP, is a Professor at California State Polytechnic University, Pomona (Cal Poly Pomona). Dr. Manson teaches Information Systems Auditing, Internet Security and Computer Forensics in the College of Business Administration Computer Information Systems undergraduate and Master of Science in Information Systems Auditing programs.

Kevin Rogers

Cyber Range

Mr. Kevin Rogers is the Founder of Cypherpath Inc, a group of cybersecurity thought leaders who promote disruptive technologies and offer innovative products to advance the cybersecurity workforce. Kevin's career has focused on virtualization, cybersecurity and technology training for the last 25 years. Kevin has held multiple executive positions at technology-based companies to improve human performance using technology. His emphasis has been on using gamification and operationally realistic scenarios to capture the interest of the learners and maximize enjoyment and engagement in order to inspire them to continue learning.

In 2013, Kevin founded Cypherpath Inc. to focus on helping the cybersecurity workforce gain the needed knowledge, skills, and abilities to protect critical data and infrastructure. Cypherpath's software creates cyber ranges that are agile, secure, and fast to deploy. Kevin and his team developed a patented platform based on an open systems architecture which produces massively scalable IT environments with feature rich scenario activities. Cypherpath's platform uses SDx technology to reduce the infrastructure costs, manpower, and configuration time by 80% of traditional cost. The technology uses a con-

tainer approach to isolate and make the network secure which allows cyber practitioners to investigate and defend against live attacks that cannot be deployed on production networks. The Virtual Platform is currently used by; Liberty University, SNHU, Radford University, University of Maryland, US Dept. of State, DHS, DoD Cyber Range, Marine Corps Cyber Range, and the Navy SAGA program.

Corrinne Sande

Community College: Effective 2/4-Year Information Security Curricula

Whatcom Community College's Computer Information Systems Program Coordinator, Corrinne Sande, has extensive experience in the field of information security and holds several industry certifications including the SANS certified incident handler (GCIH) and Cisco Certified Network Professional (CCNP) certifications. Ms. Sande is the Principal Investigator for Cyberwatch West, an NSF funded ATE center designed to develop security awareness, career pathways, professional development, and dissemination of best practices related to cybersecurity. For over seven years Ms. Sande has co-organized the Pacific Rim Regional Cyber Defense Competition with the University of Washington and Highline Community College. Through Ms. Sande's efforts, WCC is a Center of Academic Excellence in Information Assurance Education (CAE2Y). Ms. Sande has also successfully co-administered a $2 million computer forensic/border grant.

Ken Sigler

Articulation Agreements: Lessons Learned

Ken Sigler is co-author of the book Cybersecurity: Engineering a Secure Information Technology Organization. He is also co-author of the books Securing an IT Organization through Governance, Risk Management, and Audit and CyberSecurity: A Guide to the National Initiative for Cybersecurity Education (NICE) Framework

(2.0) both due to publish by the end of 2015. A faculty member, since 2001, of the Computer Information Systems program at the Auburn Hills Michigan campus of Oakland Community College, his primary research is in the area of software management, software assurance, and cybersecurity. He developed the colleges CIS program option “Information Technologies for Homeland Security.” Mr. Sigler serves as the Liaison for the college as one of three founding members of the International Cybersecurity Education Coalition (ICSEC) which is now the Midwest Chapter for CISSE. Throughout his entire tenure at the college he has also served as Post-Secondary Liaison to the articulations program with Oakland County Michigan secondary school districts. Through that role he developed a 2+2+2 Information Security Education process leading students through information security coursework at the secondary level, into a four-year articulated program, leading to a career in information security at a Federal agency. Mr. Sigler is a member of IEEE, Distributed Management Task Force (DMTF), and Association for Information Systems (AIS).

Dr. Tracy Thompson

Transitioning Veterans into Cybersecurity

Tracy Thompson earned her doctorate in Organization Behavior from Northwestern University in 1994. She is a founding faculty of the Milgard School of Business at the University of Washington, Tacoma. Her areas of specialization include strategic management and organizational change, with her research focusing on organizational and institutional change processes. Her current research examines how social entrepreneurs are working to re-invent capitalism, specifically to use market logics and profit-oriented activity to generate social good and collective value. She has published in Administrative Science Quarterly, Corporate Governance, Organization Development Journal, Academy of Management Learning and Education, Journal of Managerial Education, and in several edited volumes. Prior to entering academe, Dr. Thompson's worked in a boutique economic consulting firm where she prepared expert testimony for

complex business and anti-trust litigation. She regularly teaches in executive education programs for the Milgard School and offers workshops and consulting services for organizations in the area.

Dr. Prem Uppuluri

K-12 Working Group

Dr. Dr. Uppuluri works is the coordinator of the Cyber Security Program at Radford University. His research interests include application security (operating systems and embedded devices) and cyber security education. His research is supported by grants from NSF and NSA.

Dr. Kevin Wainwright

Transitioning Veterans into Cybersecurity

Dr. Kevin Wainwright, Ph.D., is a faculty member of the British Columbia Institute of Technology and Simon Fraser University. At BCIT, Kevin is the Program Head for the BCIT Bachelor of Business Administration program and the SITE Centre of Excellence, the research branch of the BCIT School of Business. From 2000 to 2005 he served as president of the BCIT Faculty and Staff Association. Kevin established the Legion Military Skills Conversion Program in 2009 to assist transitioning veterans from the Canadian Forces enter post-secondary programs and the labor market.

Kevin's professional and academic focus has been as an economist and business strategist, with extensive teaching experience. At BCIT, Kevin has taught within the Institute's business, broadcast and engineering programs. As a member of SFU's department of economics, Kevin has supervised both Master's and PhD thesis students, and taught economic theory and policy in the Masters of Public Policy program. His fields of specialization are mathematical economics, industrial organization, law and economics, and environmental

economics. He is the co-author of “Fundamental Methods in Mathematical Economics” (with Alpha Chiang), the most widely adopted text in North American universities in the field of mathematical economics.

Montana Williams

Industry Certification

Robin “Montana” Williams is currently the Senior Manager, Cybersecurity Practices for ISACA. His team is responsible for executing ISACA’s cybersecurity and risk management strategy to include research, communications planning, product development, cross-organizational activity coordination ensuring ISACA education, training, professional development, standards, and assessment requirements enhance the value its members bring to their enterprises. In addition, he manages ISACA’s Cybersecurity Nexus program. The industry’s first end-to-end performance-based cybersecurity knowledge and professional development program for a globally agile cybersecurity workforce promoting organizational cyber resiliency. In addition, he is an adjunct instructor at California State University-San Bernardino teaching cybersecurity risk management. Prior, Mr. Williams served as the Chief, Cybersecurity Education & Awareness Branch at the Department of Homeland Security and the senior strategic advisor to the White House on the National Initiative for Cybersecurity Education (NICE). Mr. Williams spent 25 years in government service including 21 years in the United States Air Force retiring as a Lt. Colonel. During his military career, he held numerous flying, intelligence, training, and cyberspace assignments, including commanding the USAF Cyber Red Team. He is a combat veteran with flying & information operations duties in Afghanistan and Iraq, including serving as the lead air-campaign planner for OPERATION ANACONDA & Chief, Electronic Warfare in the Iraqi Theater of Operations. He earned a Bachelor’s degree from Minnesota State University-Moorhead in 1989, a Master’s degree from Louisiana Tech in 1998, and currently a doctoral candidate at NorthCentral University. Finally, Mr. Williams is a Certified Workforce Development Pro-

fessional (specializing in cybersecurity workforce) by the National Association of Workforce Development Professionals.

Breakout: June 16th at 3:00pm - Murica

Yenny Yi

Developing Cybersecurity Talent Before College Through Competitions

The Site Director of the UCLA After School Program at Franklin High School in Los Angeles. She has been designing and implementing programs at Franklin for the past 7 years.

Morgan Zantua

Transitioning Veterans into Cybersecurity

Morgan Zantua collaboratively constructed transition models placing members of the military community into STEM careers. She is the Architect of Cybersecurity Rapid Education Apprenticeship Training Employment System (CREATES) a collaborative grant with the WA State Department of Commerce and the Washington State Office of the CIO funded by NIST building a pipeline to support military transition into cybersecurity. Morgan Zantua holds Master's Degree from Antioch University Seattle in Whole Systems Design, Organizational Systems Renewal and is a Certified Systems Renewal Consultant. She earned her CNSS Certificate in Information Security in 2013.

She has a twenty year career in workforce development and has focused on military transition for the past seven years. Before joining the Institute of Technology at UWT as Recruiter/Advisor for the Master Degree in Cybersecurity & Leadership she worked in Joint Service Support at the Washington National Guard to build effective employment transition models for National Guard, Reservists and Veterans re-entering the civilian workforce.

NSA/DHS National Centers of Academic Excellence Panel

Mon, June 15th at 9:30am - Ballroom

This panel will discuss recent developments in the NSA/DHS CAE and the NSA CAE Cyber Operations Programs, including the closer relationship between the two programs, an update on Knowledge Unit review, new CAE Community working group and feedback opportunities, the new CAE Tech Talks, and GenCyber.

- Steve LaFountain - Dean, School of Cyber, NSA Associate Directorate for Education and Training
- Lynne Clark - Chief, National Information Assurance Education and Training Program
- Jacqueline Sullivan - DHS, Program Manager, FedVTE/FedCTE

Developing Cybersecurity Talent Before College through Competitions Panel

Tues, June 16th at 9:30am - Ballroom

- Dan Manson - Cal Poly Pomona
- Jay Gehringer - North Hollywood High School
- Yenny Yi - UCLA AfterSchool Program at Franklin High School
- Mark Estep - Poolesville High School

Cyber Range Panel

Tues, June 16th at 10:00am - Ballroom

Today's security environment continues to evolve and it seems like it may never end! The only thing consistent is change. How can we keep people prepared for the next volley of threats? How can we train and educate the next generation? Sometime it takes thinking outside of the box. How about deploying a Cyber Range? In this panel, we will discuss what a Cyber Range is (and is not), how Cyber Ranges can be used, and the best practices for different ways to build a practical Cyber Range.

- Robert J. Du Charme - IXIA
- Colin Williams - U. of Warwick
- Joe Adams - Merit
- Kevin Rogers - Cypherpath

Funding Opportunities with the Fed. Gov. Panel

Tues, June 16th at 10:45am - Ballroom

- Rodney Petersen - NICE
- Corby Hovis - NSF
- Steven M. LaFountain - ADET
- Kathryn Roberson - OPM

Community College Panel, Design Considerations: Effective 2/4 - Year Information Security Curricula

Tues, June 16th at 11:15am - Ballroom

What are the characteristics of effective Information Security curricula? In this panel presentation, answers to this questions will be explored, along with ex-

ample content to include: Cyber Defense, Network Security Administration, Systems Security Administration, Network Forensics, Secure Software Development, Critical Infrastructure Security and Resilience, Supervisory Control and Data Acquisition, and Instrumentation & Process Control Security.

- Casey O'Brien - National Cyberwatch
- Corrinne Sande - Whatcom Community College
- Robert Hamilton - OK Dept. of Career and Technology Education
- Dr. Elizabeth K. Hawthorne - Union County College

Incorporating Cyber Security in General Education Classes Panel

Tues, June 16th at 1:15pm - Ballroom

- Douglas Blakemore, Ph.D. - Ferris State University
- Robin A. Barraco - Ferris State University

Toward Curricular Guidance in the “Cyber Sciences” Panel

Tues, June 16th at 1:45pm - Ballroom

The Cyber Education Project (CEP) is an initiative to develop curricular guidelines and a case for accreditation of undergraduate cyber education programs. Organized in July 2014, the CEP is a diverse group of computing professionals from academia, industry and government. The CEP’s Learning Outcomes Working Group (LOWG) is building upon established bodies of knowledge, sets of learning outcomes, and competency lists in fields such as computer security, information assurance, and cyber operations to develop and organize set learning outcomes for undergraduate programs that the CEP is calling "Cyber Sciences." The intent is for these learning outcomes to help provide

curricular guidance to a growing number of 2- and 4-year “Cyber Sciences” degree programs and to inform the development of accreditation criteria for “Cyber Sciences” programs seeking accreditation. In this session we will present the history, organization, and goals of the CEP followed by a presentation of the initial work of the CEP's LOWG in developing a "Cyber Sciences" body of knowledge with learning outcomes. There will be time allotted for attendees to ask questions and provide feedback to the CEP.

- Colonel David S. Gibson, Ph.D. - United States Air Force Academy
- Dr. Elizabeth K. Hawthorne - Union County College

Transitioning Veterans into Cybersecurity Panel

Tues, June 16th at 3:00pm - Ballroom

Inspired by the 2009 NSF report, *Veteran’s Education for Engineering and Science*, and motivated by a STEM planning grant, NSF funded several universities to study barriers service members face in transitioning to academia in pursuit of civilian careers. A subset specifically explored veterans transition into the cybersecurity where the field has suffered from underemployment. This panel will discuss different aspects of veterans transitioning through academia. A Special Publication of the CISSE journal focuses on this challenge and offers methods and approaches that others might use.

- Dr. Barbara Endicott-Popovsky - University of Washington
- Dr. Tracy Thompson - University of Washington
- Dr. Kevin Wainwright - British Columbia Institute of Technology
- Dr. Marc J. Dupuis - University of Washington
- Robert A. Green - Mississippi State University
- Morgan Zanuta - Cybersecurity Rapid Education Apprenticeship Training Employment System (CREATES)

Articulation Agreements: Lessons Learned Panel

Tues, June 16th at 3:45pm - Ballroom

Articulation agreements are designed to build strong partnerships between schools in order to facilitate a smooth transition for students and build career pathways for success. This panel offers a community discussion on the opportunities, problems and potential solutions surrounding these agreements. Topics include: why we should be building articulation relationships between secondary and post-secondary institutions, articulation based on established workforce frameworks, interesting articulation models, and research findings.

- Casey O'Brien - Director National Cyberwatch
- Ken Sigler - MCISSE and Oakland Community College
- Helen Barker - Capitol Technology University

Industry Certifications Panel

Wed, June 17th at 1:15pm - Ballroom

Representatives from the following organizations:

- Dr. Rae Hayward, $(ISC)^2$
- Jay Bavisi - EC-Council
- Montanna Williams - ISACA

CAE-CO KU Review

Mon, June 15th at 1:45pm - Marbella

- Steve LaFountain - Dean, School of Cyber, NSA Associate Directorate for Education and Training
- Heather Eikenberry - CAE CyberOps Program Manager

NSA Sponsored: The Information Security Research and Education (INSuRE) Program

Mon, June 15th at 1:45pm - Marbella

CAE-CD KU Review

Mon, June 15th at 2:45pm - Marbella

- Lynne Clark - Chief, National Information Assurance Education and Training Program
- Jacqueline Sullivan - DHS, Program Manager, FedVTE/FedCTE

CAE-CD Application Lessons Learned and Q&A

Mon, June 15th at 2:45pm - Murica

- Karen Leuschner - NSA/DHS CAE-CDE Program Manager
- Denisha Jackson - NSA/DHS CAE-2Y Program Manager

KU to NICE Framework Mapping

Mon, June 15th at 3:45pm - Marbella

- Lynne Clark - Chief, National Information Assurance Education and Training Program

CAE Community Website Orientation / Q&A

Mon, June 15th at 3:45pm - Murica

- Dr. Tony Coulson - California State University, San Bernardino/CAE Community Chair

Incident Response Working Group

Sunday, June 14th at 11:00am - Marbella

In the era of massive security breaches and cyberattacks on our computer infrastructures, it won't take long for a state's resources to quickly be overwhelmed. That's when your local National Guard's security experts will join the fight to protect and defend our systems. CAE schools and experts are gathering at the 19th Colloquium to form a working group with the intent to develop a CISSE based strategic initiative; assist you in understanding our current results and develop your own incident response model.

Regis University, the Colorado National Guard and the State of Colorado have conducted a year-long study to develop an extensible incident response training model. The model includes connecting CAE resources, facilities and personnel with state partners to accelerate the skills, knowledge, communications and effectiveness to promote cyber security and implement rapid defense.

Join the conversation and participate in a physical exercise with your National Guard to respond to the call to action – CAEs in Action.

K-12 Working Group

Tuesday, June 16th at 1:15pm - Marquis #8

Lead by Davina Pruitt-Mentle (NCC), Debasis Bhattacharya (UH Maui College), Prem Uppuluri (Radford U) and Deanne Cranford-Wesley

The objectives of the 2015 CISSE K12 Working Group are to share progress, strategies, and challenges to date; engage in discussions and small group work designed to assist with member program outcomes; network and exchange ideas; and inform the working group about other resources and national K12 efforts.

Cybersecurity Women and Minorities

Tuesday June 16th at 3:00pm - Marquis #8

Rose Shumba, University of Maryland University College

Despite the growing demand for security professionals worldwide, women and minority representation in this field is alarmingly low. This raises concerns for the nation's ability to be innovative and compete in a global economy and address the escalating demand for Cybersecurity professionals in the United States. The Women in Minorities Working group propose a break-out session to share best practices and experiences on women and minorities and their advancement in a Cybersecurity career. Through an open discussion, the role models will address a number of questions on the various problems they solve in their profession, skills that have helped them to this point.

Career Fair

June 15th and 16th at 1:15pm - Aragon

To further our commitment to career development in Information Assurance, we are proud to announce a “one-stop shop” career fair for academics and students, to be held at the 2015 Colloquium Conference in Las Vegas. National recruiters will be invited from academia, government and industry to take part in this event. Over 200 Cybersecurity University and Community College professors and their top undergrad, graduate and doctoral students will be available for interviews. No fees will be required from recruiters or students.

Thank you to our Generous Sponsors

T-Mobile and Bill Boni	
Boston University	California Polytechnic State University at Pomona
Capitol Technology University	CENGAGE Learning
CompTIA	Cyberwatch West
EC-Council	Excelsior University
ISACA	$(ISC)^2$
Jones & Bartlett Learning	National Cyberwatch Center
National Science Foundation	SBL
Women's Society of Cyberjutsu (WSC)	

And thank you to our membership for all your support over the last 19 years. See you at the Birthplace of our nation for the 20th Anniversary of CISSE, Philadelphia, PA!

T-Mobile

http://tmobile.jobs/ExploreTmobile/Technology

BOSTON UNIVERSITY

www.bu.edu/riscs/

The Center For Information Assurance
CAL POLY POMONA

www.thecenteratcpp.com

CAPITOL TECHNOLOGY UNIVERSITY

www.captechu.edu

CENGAGE Learning

www.cengage.com

CompTIA

www.comptia.org

CWW cyberwatch west

www.cyberwatchwest.org

EC-Council
Hackers are here. Where are you?

www.eccouncil.org

ISACA
Trust in, and value from, information systems

www.isaca.org/cyber/

(ISC)² GLOBAL ACADEMIC PROGRAM
Education. Research. Outreach.

www.isc2.org/academic/

NATIONAL CYBERSECURITY INSTITUTE AT EXCELSIOR COLLEGE

nationalcybersecurityinstitute.org

JONES & BARTLETT LEARNING

www.issaseries.com

NATIONAL CYBERWATCH CENTER

www.nationalcyberwatch.org

NSF

www.nsf.gov

SBL

www.softbox.co.uk

WOMEN'S SOCIETY OF CYBERJUTSU
A CYBERSECURITY COMMUNITY FOR WOMEN

www.womenscyberjutsu.org

SEE YOU NEXT YEAR

20TH COLLOQUIUM

PHILADELPHIA PA

JUNE 2016

www.CISSE.INFO

THE COLLOQUIUM FOR INFORMATION
SYSTEMS SECURITY EDUCATION
49004 PACKARD CT., BELLEVILLE, MI 48111

 **askCISSE@cisse.info**  **www.cisse.info**