23rd Colloquium for Information Systems Security Education

JW Marriott Resort and Spa
Las Vegas, Nevada
10-12 June 2019

Connecting Academia, Industry and Government

Colloquium for Information Systems Security Education

Cybersecurity Education Innovation

The National Colloquium for Information Systems Security Education (NCISSE) was created in 1996 to provide a forum for dialogue among leading figures in government, industry, and academia. In June 2002, NCISSE expanded its mission to include greater international participation. To reflect this the organization formally changed its name to The Colloquium for Information Systems Security Education or more simply -- The Colloquium.

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

What We Can Grow to Be

An organization with comprehensive Reach:

Reaching **all** cybersecurity educators, at all levels, to provide a platform for them to share their ideas, their research, their successes, and their needs.

Reaching business and industry leaders and cybersecurity practitioners to provide a platform for them to sare their cybersecurity educational needs, and how they can help.

Reaching government leaders an cybersecurity practitioners to provide a platform for them to share their cybersecurity educational needs, and how they can help.

Reaching organizations that produce textbooks, reference materials, and other resources that enhance instruction in cybersecurity, providing a venue for obtaining feedback to improve their products.

Reaching citizens across America via regional chapters, focusing on regional cybersecurity issues, challenges and successes.

Reaching citizens across the global community who wish to promote cybersecurity education for a safer and more secure cyber ecosystem through membership in an organization dedicated to promoting cybersecurity education at all levels.

An organization that provides services to the cybersecurity education community:

- Annual colloquy for sharing and networking, simulcast to the world.
- Periodic electronic magazine with articles for and from the community.
- Membership in a professional organization devoted to cybersecurity education.
- Opportunity for academics to publish in an internationally recognized journal—devoted to cybersecurity education.
- Referral services for institutions in need of cybersecurity educators as well as workers.
- Updates in research and grant opportunities in cybersecurity education.
- Support to institutions of higher education accrediting institutions seeking cybersecurity accreditations, certifications, and designations.
- Working groups with focused areas of need for members to participate and share knowledge.
- Serves as an advisory boy for industry, Government and Educational Institutions seeking solutions in cybersecurity education.

The Professional Association for Cybersecurity Education (PACE):
Cybersecurity leaders and practitioners dedicated to advancing cybersecurityeducation!

Connecting Academia, Industry and Government

Speaker Profiles

Kevin Cardwell is an expert Cybersecurity Penetration tester with over 30 years of experience in the public and private sector. He spent 22 years in the U.S. Navy where he worked as both a software and systems engineer on a variety of Department of Defense projects. Kevin currently teaches at the University of Maryland University College (UMUC) and University of California Los Angeles Extension (UCLA) and has instructed hundreds of students through bachelor's and master's level programs. He currently works as a free-lance consultant and provides consulting services for companies throughout the world, and as an advisor to numerous government entities within the US, Middle East, Africa, Asia and the UK . He is an Instructor, Technical Editor and Author for Computer Forensics, and Hacking courses. He is the author of the Center for Advanced Security and Training (CAST) Advanced Network Defense and Advanced Penetration Testing courses. He holds a BS in Computer Science from National University in California and a MS in Software Engineering from the Southern Methodist University (SMU) in Texas.

Lynne Clark is Chief of the NSA/DHS National Centers of Academic Excellence in Cyber Defense (CAE-CD) Program Office. She has 40 years of combined military and civilian service. Ms Clark served in the U.S. Air Force with worldwide assignments in airspace management, radar operations, information operations and risk management. She spent eight years serving in NATO during the Cold War and during the Germany reunification. She was involved in development of secure range operations for military RDT&E facilities, advised on risk management issues involved in the START and Open Skies treaties, and managed the Air Force OPSEC Program at the Pentagon. She retired at the rank of Lieutenant Colonel in 1999.

For CAE-CDE designated schools with designation expiration in 2020 and CAE Application Reviewer volunteers.

From 9:00-2:00 on Thursday, June 13, the CAE-CD Program Office team will conduct a special KU mapping workshop for designated CAE-CDEs preparing to re-designate in the next application cycle, Oct 2019 - 1 May 2020, and CAE Application Reviewer training.

The College of Southern Nevada will host at 3200 E. Cheyenne Ave, North Las Vegas, NV, Building C, Room C2658.

Register at the CISSE info desk.

Tony Coulson is a professor and the Executive Director of the Cyber Security Center at California State University San Bernardino. Having a well-earned reputation for not being a "typical" professor he has won numerous awards, grants and accolades for his innovative approaches in education and leadership in the Cybersecurity and technology fields. In 2008 he was awarded a national Innovation in Teaching and Learning award. Dr. Coulson firmly believes in an interdisciplinary approach to technology education and has used that passion to make Cal State San Bernardino a recognized leader in Cyber Security. As the Executive Director of the Cal State San Bernardino Cyber Security Center, he has worked with industry and government to map opportunities for students and Cyber Security strategies for the nation. Tony runs multiple grant programs in excess of $18 million that provide specialized skills to the Federal government and private companies. He is a founder of Cyberwatch West, a national Advanced Technology Education Center focusing on Cyber Security in the western United States. Cal State San Bernardino is also designated a Center of Academic Excellence in Cyber Defense by DHS & NSA and is a National Resource Center for the CAE-CD program.

Laura Lee is the Executive Vice President at Circadence Corporation. In this role, she applies her extensive knowledge and experience in cybersecurity workforce development to help organizations understand how to identify, screen, assess, train and retain cybersecurity professionals. She previously led the product development for the Circadence Project Ares® next generation cybersecurity training and assessment platform and the Orion Mission Builder. She uses Project Ares to teach a graduate level course on Immersive Cyber Defense at the University of Colorado-Boulder. Laura holds a Bachelor of Science in Aerospace Engineering and Mechanics from the University of Minnesota and a Master of Science in Aerospace Engineering from the University of Notre Dame. She also has a Juris Doctorate from George Mason University School of Law. Laura is a Certified Information Systems Security Professional (CISSP) and holds certifications in gamification and game development.

Speaker Profiles

Mark S. Loepker is a master practitioner in Information Assurance (IA) and International Partnerships with over 39 years of government experience. He is the Senior Advisor and Education Lead to the National Cryptologic Museum Foundation, focused on developing educational programs to be delivered from the new Cyber Center for Education & Innovation (CCEI). He focuses on K-12/STEM initiatives that are tightly aligned with national cyber curriculum standards and that the CCEI becomes a national resource addressing workforce development. Mr. Loepker's educational degrees include a Master in Business Administration – Quantitative Analysis, University of Missouri; Bachelor of Science in Electrical Engineering Technology, Purdue University; Associate in Aviation Electronic Technology, Purdue University and numerous NSA technical, executive and legislative development programs.

Stephen Miller has been in the Information Systems Profession since 1966 working in business, government, and education sectors. He is currently a tenured Professor, Subject Matter Expert and Director for Information Systems/Cyber Security Center of Excellence, where he is responsible for developing Information Systems curriculum, SCADA, cybersecurity program development, research, and teaching. He has developed an online Computer and Network Security Certification and Associates Degree program offered since spring 2011 and created a Center of Excellence for Cyber and SCADA Forensics Security. Mr. Miller is retired from Exxon Mobil Global Information Systems where he served in management, supervisory and technical roles over his 27 year career. He has been employed at Ford TechRep Division (programmer), U.S. Army 1st Calvary Div. in Vietnam computer specialist), and Univac Corp. - NASA Mission Control on the APOLLO—including APOLLO 13, and Skylab Missions. Mr. Miller is currently a mentor for Cyber Watch West and the National Science Foundation to other community colleges in the United States, helping them achieve CAE -2Y status. Mr. Miller is participating in SCADA Cyber Forensics coalition with New Mexico Tech, Idaho National Labs, Department of Homeland Security, and Ruidoso Independent School District, the NIST workshops for the Cybersecurity Critical Infrastructure Framework standards, and recently coauthored an e-textbook "Framework for SCADA Cybersecurity" ISBN: 9781310309960.

Lucas Moody is the Vice President and Chief Information Security Officer at Palo Alto Networks. He has a true passion for protecting the Internet community. He is a global-minded technology executive noted for driving information security thought leadership and business innovation. With strong technical and operations roots, Lucas brings extensive experience in information security operations, e-crime investigations, threat management, security engineering, cyber fraud, forensics and threat intelligence. Prior to joining Palo Alto Networks in 2015, Lucas developed security operations and engineering capabilities at Fortune 1000 companies like Intuit, eBay, and Oracle and within the Big 4 at KPMG LLP.

Tom Muehleisen is a proven leader and executive with over 3 decades of experience in and out of uniform. He wrote Washington State's cyber response plan and created the cyber operations element within the state's Military Department. He is a proven executive and sought-after public speaker for his ability to relate complex topics to diverse audiences. He is currently with Norwich University's Applied Research Institute (NUARI) as its Scenario Author and Market Outreach.

Gordon W. Romney, Ph.D., is the Director of the Center for Cyber Security Engineering and Technology, and oversees the MS in Cyber Security Engineering program at USD. Current research includes developing an Artificial Neural Network for HIPAA-compliant eVisit telemedicine medical diagnosis and hardening of IoT Electronic Control Units in Cisco's Connected Vehicle initiative Coordinator.

Speaker Profile

Dan Stein is the Branch Chief for Cybersecurity Education and Awareness (CE&A), Cybersecurity and Infrastructure Security Agency (CISA). CE&A oversees the nationally-focused Federal Virtual Training Environment, DHS's partnerships with the National Security Agency on the National Centers of Academic Excellence programs and with the National Science Foundation for the CyberCorps®: Scholarship for Service (SFS) program, the National Initiative for Cybersecurity Careers and Studies (NICCS) and the National Cybersecurity Awareness Campaign. Mr. Stein has supported DHS cybersecurity education, training, and workforce development programs for over ten years and has supported federal information security efforts for over fifteen years. Mr. Stein graduated from the U.S. National War College with a Master of Science in National Security Strategy. He also holds two master's degrees from the University of Texas at Austin and a bachelor's degree from the University of Rochester.

Session Abstract

ABET/CAE-CD Collaboration

The NSA/DHS Centers of Academic Excellence in Cybersecurity programs and ABET are working together to identify commonalities and synergies that can be leveraged to help academic institutions pursue multiple designations and accreditations while minimizing duplication of effort. Learn how ABET and CAE program managers are working together to help you create and maintain a strong cybersecurity curriculum.

ABET accreditation provides assurance a college or university program meets quality standards of a profession. While the Curricular Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC 2017) from the Joint Task Force of the Association of Computing Machinery (ACM), IEEE-Computer Society, AIS and International Federation for Information Processing describe different aspects of cybersecurity education, they do not define what constitutes an undergraduate cybersecurity program. Guided by CSEC 2017 and input from the computing community, ABET created accreditation criteria that provide flexibility for programs to meet the criteria while supporting outcomes, quality and continuous improvement.

For 20 years, the NSA/DHS Centers of Academic Excellence in Cybersecurity program has worked with academia to establish guidelines for cybersecurity education. Requirements for CAE-CD designation go beyond academics, including faculty qualifications, contribution to development of the cybersecurity profession, involvement and outreach to the community, among other program requirements.

These two organizations are working together to share information, collaborate on requirements, and establish reciprocity in designation and accreditation.

Session Abstracts

Community College Cyber Pilot (C3P)

A new National Science Foundation (NSF) program, the Community College Cyber Pilot (C3P) program issued three awards to build research collaborations among partners in six states: California, Illinois, New Jersey, Ohio, Texas and Washington. "We know that community colleges play an important role in providing essential academic and training opportunities to a wide range of individuals," said Karen Marrongelle, NSF's assistant director for Education and Human Resources. "The awards made through the pilot C3P Program will provide scholarships and create professional pathways for both veterans of the Armed Forces and for bachelor's degree holders who want to pursue careers in cybersecurity."

The partnerships will allow collaboration on activities, including student skills competitions, certification preparation workshops, faculty-student mentorship and visits to local federal agencies.
The awards aim to help protect American economic prosperity and security through the development of an innovative and efficient cybersecurity education system that will produce a 21st century cybersecurity workforce as well as a cyber-informed citizenry.

DECIDE: Using a Proven Platform to Enable Academic Engagement with Government and Industry to Solve Sector-Wide Cybersecurity Issues

In March of this year, the University of Washington's Center for Information Assurance and Cybersecurity (UW-CIAC) partnered with Norwich University's Applied Research Institute (NUARI) to conduct a tabletop exercise, focused at the executive level, exploring the state level of cyber response in a telecommunications context. The speaker was the primary architect of this exercise and was able to leverage a proven distributed platform (DECIDE) in a new vertical. The use of this mature tool allowed the stakeholders to envision, plan, prepare, deliver and assess the effort in just over 3 months. This training will review use of mature tools to enable rapid engagement of stakeholders and delivery of effective exercises, training, and education.

Session Abstracts

Distance Learning Challenge: Maintaining Quality of Instruction and High Student Satisfaction

Distance learning is heavily utilized to deliver high quality cybersecurity content. For some schools it is the primary mode of delivery, for others it is one of several modes available (on ground, online—synchronous or asynchronous– hybrid). In some cases, Distance Learning is used as a backup when ground delivery is not feasible, for example, due to weather-related events. The delivery of distance education is almost exclusively adjunct professors for many of our schools. This panel will discuss how they maintain teaching excellence while heavily reliant on adjunct professors. Also discussed will be the supporting infrastructure tools required to maintain quality content and high student satisfaction.

Essential Defensive Cybersecurity Strategies and Deception As A Defense

Too many programs in higher education are focusing on offense. In this presentation, the concepts of defense will be explored as a follow on to all of the offensive education. The presentation will also showcase the methods of deception that can be added to curriculum and incorporated in the classroom. These methods are powerful ways to confuse and frustrate the attackers, and allow for "war gaming" implementation in the classroom.

How to Use the NIST Cybersecurity Framework for Education

We spend a lot of time talking about the FUTURE of the cybersecurity workforce. By 2021, more than 3.5 million job openings will impact the security posture of enterprise, government, and academic institutions across the globe. But we don't spend a lot of time talking about the PAST. History can tell us a lot about where we've been and inform where we're going—and the case is no exception when it comes to teaching the next generation of cyber professionals.

Laura will discuss why examining the hiring methods leading up to World War II can help the cybersecurity workforce challenges of today and how we can use modern techniques, such as gamification to IDENTIFY – SCREEN - ASSESS – PLACE – TRAIN – RETAIN staff. She will describe methods that rely on Artificial Intelligence to help instruct and score cybersecurity professionals. Laura will describe how she uses the NIST Cybersecurity Framework and NICE Cybersecurity Workforce Framework to prepare students for careers in cyber. This talk is designed to stimulate ideas in the audience on "How to Grow Cybersecurity Professionals" in the modern world. As part of the workshop, Laura will engage the audience with example cyber games that illustrate the attacker's kill chain, show the relationship between common ports and protocols, reinforce binary and hexadecimal conversion and play good old-fashioned cyber trivia! Audience participation is a must.

Leveraging Artificial Intelligence for Cybersecurity

In February 2011 an historic event took place. IBM's Watson computer competed against the two biggest winners of the TV quiz show Jeopardy! — and the Watson won. Since that time artificial intelligence (AI) has found its way into increasingly more and different types of applications ranging from cybersecurity to cancer treatment . This session will cover some of the various AI - Cybersecurity technologies and how they are being used to give the good guys an advantage in the cyberwar.

NSA's Vision for Cybersecurity Education: the National Cyber Curriculum Program (NCCP) and GenCyber

The goal of NCCP is to provide free cyber curriculum to help schools build and expand cyber programs. The program has funded development of SCADA, secure coding, reverse engineering, and more subjects. Over 85 curriculum objects are currently available in the CLARK digital library. The GenCyber program provides summer cybersecurity camps free of charge for K-12 students and teachers nationwide. This presentation will discuss different types of camps and opportunities to host a camp.

NICE Challenge Project

The NICE Challenge Project develops real-world cybersecurity challenges within virtualized business environments that bring students the workforce experience before the workforce. Our goal is to provide the most realistic experiences to students, at-scale year-round, while also generating useful assessment data about their knowledge, skills, and abilities for educators.

NICE Collegiate Working Group

The NICE Collegiate Working Group is working to identify and share Tools, Technologies and Skill Sets in the academic environment. This presentation will discuss the group's progress and objectives in the value of Higher Education and establishing Career Pathways.

NSA/DHS National Centers of Academic Excellence in Cyber Defense — Future Vision

The Centers of Academic Excellence in Cyber Defense (CAE-CD) program is in a period of rapid growth and influence in the community, with evolution of the program and new opportunities on the horizon. This presentation will cover strategic plans and vision for the program coming in the next few years.

Cybersecurity In Quantum Time—NIST PQC Standardization

The presentation provides an overview on quantum impact to cybersecurity. It introduces NIST Post-Quantum Cryptography (PQC) Standardization process. The presentation highlights challenges in the PQC standardization and explores possible path to migrate to quantum resistant cybersecurity tools.

Session Abstracts

So You Want to Build a SOC on Your Campus?

Today, many educational institutions are considering building Security Operations Centers (SOC) to provide increased security and rapid response to outside threats, and as a way to train students in a real environment. Building a SOC can be a monumental task . Although the finer points of SOC deployment are very much network-specific, there are several major components that every organization must include: people, process, and technology. The three exist in all elements of security and should be considered equally critical components. This panel consists of educational institutions that have implemented or considering implementing a SOC. The panelists will discuss their experiences and share the lessons learned with the audience considering such as endeavor.

Stimulating a National Cybersecurity Education Dialogue

This presentation updates progress from the Cyber Center for Education and Innovation, home of the National Cryptologic Museum. This unique national value proposition brings together cybersecurity education and invites collaboration. The mission is to broaden cyber threat awareness, cybersecurity best practices and educational outreach, and to enhance operational cybersecurity workforce development in support of our nation's critical infrastructures. CCEI-NCM is creating a cybersecurity center of gravity integrating industry, government and academic stakeholder resources, and advancing cybersecurity education. Planned educational outreach programs will leverage the unsurpassed resources, curriculum and know-how of the NSA in an unclassified, publicly-accessible setting addressing both the K-12 and 13-20 age cohorts. Their cornerstones are the Digital Curriculum Library of assured quality cybersecurity curriculum and sharing experiences through virtual technologies.

Sponsors

EC-COUNCIL

IBM

california cyberhub Powered By synED

women in CYBERSECURITY WiCyS

JONES & BARTLETT LEARNING An Ascend Learning Company

CWW cyberwatch west

paloalto NETWORKS CYBERSECURITY ACADEMY

CAE IN CYBERSECURITY COMMUNITY

NICCS™ NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

NIST

CISA CYBER+INFRASTRUCTURE

CompTIA

MARCRAFT an ETG Brand

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

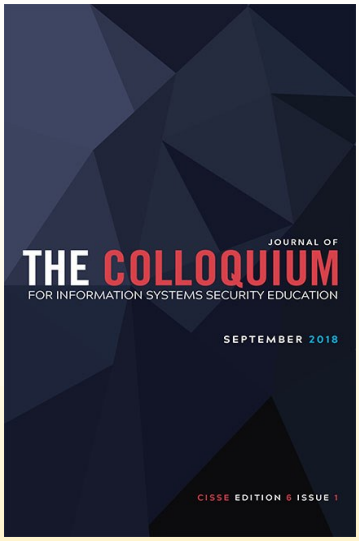
NATIONAL CRYPTOLOGIC MUSEUM FOUNDATION

Colloquium for Information Systems Security Education

CISSE Board of Directors

Journal of The Colloquium for Information System Security Education

Since 1996 the Colloquium for Information System Security Education (CISSE) has been the academic voice of the field of cybersecurity education. CISSE was established to encourage meaningful dialogue between government, industry, and academia involved in protecting our nation's information and its information technology assets.



The Community meets every year at a different part of the United States to discuss the most effective and highest standards of practice in cybersecurity education. To have credibility as a source of new and evolving knowledge it is important that the highest academic standards apply to presentation of new knowledge to the membership.

Thus, the papers submitted to the conference undergo a double blind refereeing process and a percentage are presented in individual sessions at the Conference. After the Conference, an Editorial Board selects a small set of papers that are considered to be important to the community. These are processed as a Journal publication.

These publications reflect the best scholarship in the field of cybersecurity and their selection is highly competitive. It is the aim of this Journal to offer only the most outstanding scholarship available. However, the editors and publishers also work with new authors in order to help them to bring their work to publishable standards.

Given that background, it should be understood that the ideas contained in this Journal represent the best thinking in the methods and practices for integrating cybersecurity education into conventional curricula. Cybersecurity is an emerging discipline. It is critical to publicize the broadest and most comprehensive range of meaningful new ideas about where the discipline will evolve going forward. The ideas presented here are not constrained by any preconceived notions of what the field ought to be like. Instead we are focusing on their merit as a means of solving difficult problems that exist in our modern society.

The articles in this Journal address ways to more effectively leverage the range of sub-disciplines in the defense of information. Spreading the net as wide as possible is a particularly obvious and justifiable way to address threat. And that is our mandate and challenge to the researchers, and cybersecurity professionals of the future.

Contact Us:

712 Northwood Estates Dr.
Severn, MD 21144

202.573.7263 ph

https://cisse.info/

Joseph Tamburelli
jtamburelli@thecolloquium.org
Patricia Tamburelli
ptamburelli@thecolloquium.org