



CAE in Cybersecurity Symposium

November 21-22, 2019
Sheraton Grand Phoenix
340 N 3rd St
Phoenix, AZ 85004



Welcome to the annual **CAE** *in Cybersecurity Symposium!*



Message from the Community

Cybersecurity educators are facing demands from government and industry to produce more graduates to fill the current and future workforce needs. Each year the Centers of Academic Excellence (CAE) in Cybersecurity Community assembles to discuss the workforce problem as well as to discuss issues unique to our community including faculty shortages, bridging the skills gap, and career pathways.

Six years ago, the CAE in Cybersecurity Community met for the first time in Gaithersburg, MD to discuss our progress as CAE designated institutions. Since then, the CAE in Cybersecurity Symposium has traveled to Columbia, MD, San Diego, CA, Kansas City, KS, Dayton, OH, Miami, FL, and now Phoenix, AZ, to discuss changes in the CAE program, receive updates from the community, network with other members, and discuss pressing issues within the community.

To help drive conversation among the community, today's symposium will include fastpitch talks and presentations meant to highlight important contributions from the CAE in Cybersecurity Community as well as important updates from the CAE-C Program Office.
























Contents

Welcome.....	2
Navigate the Symposium.....	3
Agendas.....	4-7
Welcome.....	8-9
Executive/CNRC Panels.....	10
Committees.....	11
Speaker Biographies.....	12-17
Fastpitch Abstracts.....	17-19
Special Interest Group Abstracts.....	19-20
Presentation Abstracts.....	20-23

Agenda

Thursday, November 21, 2019			
7:30am	Registration (Breakfast on your own)		
8:00am	Welcome and Logistics CAE in Cybersecurity Community Updates (Tony Coulson, CSUSB)		
8:15am	NSA-Academic Partnership (Diane Janosek, NSA)		
8:45am	Evolution of the CAE-C Program: (Lynne Clark, NSA)		
9:30am	Morning Break		
9:45am	Executive Leadership Panel (Maurer, Rose, Carstens, VanWagoner)		
10:15am	CNRC Panel (Coulson, Sande, Leary, Conklin)		
11:00am	Other Program Updates 11:00am NIST (Rodney Petersen, Director, National Initiative for Cybersecurity Education (NICE)) 11:45 NSF (Corby Hovis, Li Yang)		
12:00pm	Working Lunch 12:00 CAE in Cybersecurity Community Website (Anastacia Webster) 12:15pm CAE Virtual Career Fair (Amy Hysell) 12:30pm CAE Spotlight (Paul Wagner and Jason Denno, University of Arizona)		
CAE-CDE Track		CAE-R Track	
1:00pm	2020 Critical Community Actions 	Successful Research Projects 	
2:00pm	CAE-C 2020 Initiatives 	Research Projects of Interest 	
2:45pm	Afternoon Break		
3:00pm	Fastpitch (see page 6 for schedule) 	Overview and Collaboration 	
4:00pm	Discussion		
5:00pm	Dismissal (Dinner on your own)		
Evening Meetings			
5:15pm	DoD Cyber Scholarship Program 	Mentor/Reviewer Meeting 	













Agenda

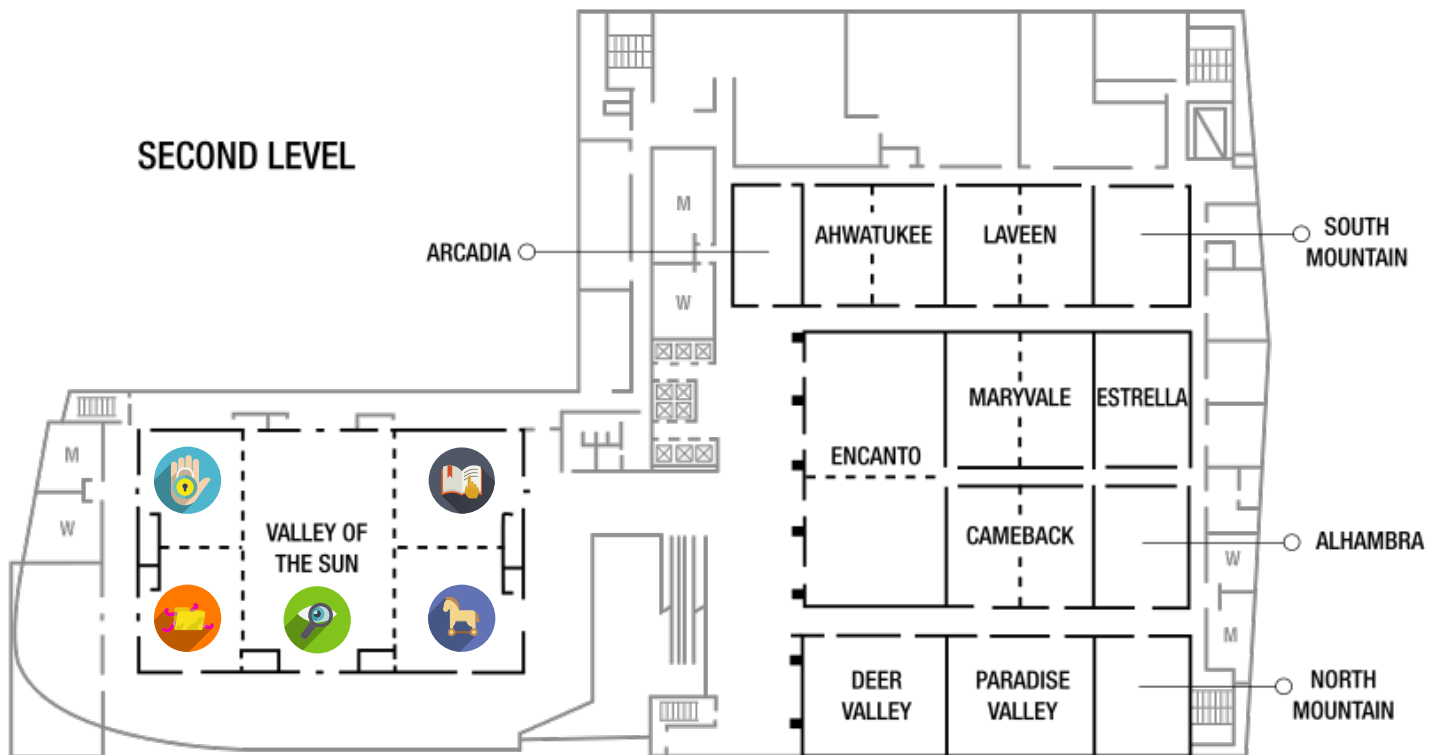
Friday, November 22nd, 2019			
CAE-CDE Track		CAE-R Track	
7:30am	Registration (Breakfast on your own)		
8:00am	Special Interest Groups (see page 7 for schedule)  	INSuRE: History and Highlights 	
9:00am	Presentations (see page 7 for schedule)  	Expansion of INSuRE (9:00am-9:45am)  Planning for Future CAE-R Symposium Organization (9:45am-10:00am) 	
10:00am	Morning Break		
10:15am	Presentations (see page 7 for schedule)   	Planning for Future CAE-R Symposium Organization (cont.) (10:15am-10:30am)  CAE-R Research Support Discussion (10:30am-11:00am) 	
11:00am	CRRC Regional Meeting Time/Networking Time    		
12:00pm	Working Lunch: Preview the New Tool – CAE-C Program Office		
1:00pm	Program Office: Details on New Program Guidelines 		
2:00pm	Afternoon Break		
Breakout Sessions			
2:15pm	Community College Discussion Questions  	BA & Graduate Program Discussion Programs 	CAE-R Discussion and Questions 
3:30pm	Question Period Recap 		
4:15pm	Discussion 		
5:00pm	Dismissal (Dinner on your own)		

Use these icons to navigate the CAE in Cybersecurity Symposium.



Agenda

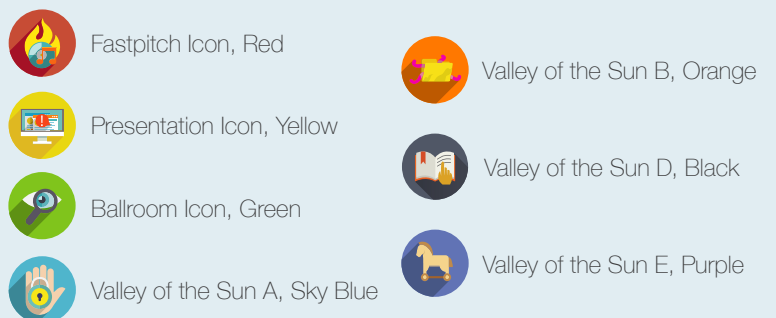
Fastpitch Schedule		
Thursday, November 21		
3:00pm-3:10pm	Community College Cyber Pilot (C3P) Program	 
3:10pm-3:20pm	International Opportunities for Cybersecurity Faculty	 
3:20pm-3:30pm	An Innovative Approach Using Mixed Reality to Improving Career Readiness	 
3:30pm-3:40pm	Pathway for Community College Students to an ABET-Accredited Degree in Cybersecurity	 
3:40pm-3:50pm	Teach Cyber Now: Ask Me How	 
3:50pm-4:00pm	ACM Cybersecurity Curriculum Guidelines Mapping to CAE Knowledge Units	 



Agenda

Special Interest Group Schedule (Friday)	
8:00am-9:00am	Integrating Professional Cybersecurity Certification Preparation into Fundamentals Course 
	Developing a Professional Society for Cybersecurity Education 
Presentation Schedule (Friday)	
9:00am-9:30am	Promoting Cybersecurity Competitions at Nova Southeastern University 
	Using Devops Tools to Deploy Cybersecurity Labs in Cloud Computing Environments 
9:30am-10:00am	Reach to Teach: Using Videos to Prepare Cybersecurity Adjunct Faculty 
	Matching Employer Cyber-Skill Needs with Students' Assured Skills 
10:15am-11:00am	Hands-on Learning Experiences for Cyber Threat Hunting Education 
	High School CCF (Cybersecurity Curriculum Framework) 
	WIN-Cyber: Work (role) Insight Network Online Competency & Pathway Tool 

Use these icons to navigate the CAE in Cybersecurity Symposium.



Welcome

Welcome and Thank You!



Thank you to the United States' educational institutions that have committed to the high standards of the CAE-C programs. The educators at the CAEs are patriots... the professionals who educate and train our nation's Cyber First Responders! Our nation thanks you.

As Commandant of the National Cryptologic School at the National Security Agency, I see the impact of what you do every day. I am proud of the work the Centers of Academic Excellence in Cybersecurity schools are doing, leading the way in one of the most critical, challenging fields in this nation today. Cyber expertise, and cybersecurity in particular, is critical to every aspect of American life, and we are critically short of qualified workforce.

We look forward to working with you this week and in the coming months to improve the program management processes, and to continue to grow and advance cybersecurity education.

~Diane Janosek
Commandant, National Cryptologic
School, NSA

Diane M. Janosek is a senior executive and leader whose career spans legal, policy and executive management positions in the U.S. Government at the National Security Agency (NSA), the Pentagon and the White House. Her expertise in cyber education, privacy and technology, information security, cyber/fiscal law, data governance and information security, export control/foreign military sales, resource management and inclusion/diversity has informed all her work.

Currently an NSA Commandant of the National Cryptologic School, Ms. Janosek leads five colleges that deliver offerings for the nation's civilian/military intelligence global workforce in the areas of signals intelligence, cyber/network security, cyber resilience, and encryption, and teaches courses in the Graduate Program of the National Intelligence University.

Ms. Janosek led legal/compliance review of privacy controls of key intelligence programs as Chief Legal Officer, Privacy and Civil Liberties Oversight Board, She served as chief ethics officer and as primary advocate for declassification of key facts on controversial collection programs.

Previously, as Deputy Associate Director, Policy and Records and leading export control, CFIUS, Foreign Military Sales, classification and cyber policy, she ensured NSA corporate governance, assisted with enhancing information sharing/transparency and served as NSA's senior official to the Pentagon on export control matters.

Before joining the NSA, Diane was Assistant to General Counsel of the Navy and served as an attorney at the White House Counsel's Office.

Welcome



NSA launched the Center of Academic Excellence in Information Assurance (now Cyber Defense) Education program in 1999. The program was envisioned to contribute to the growing demand for cybersecurity expertise in the intelligence community workforce. Over the years, as it became clear cyber defense would become an integral element of national security, the program's objectives expanded to support the nation's need for cybersecurity workforce development.

The program has evolved over the years, most recently merging with NSA's CAE in Cyber Operations Program, but the focus will continue to be promoting higher education and research in cybersecurity and producing professionals with cybersecurity expertise in order to reduce vulnerabilities in our national infrastructure and develop a cyber-ready workforce for the intelligence community.

Cybersecurity is an ever-evolving field and we cannot do this without you. The expertise that you bring to the table is unique and we greatly appreciate your time and expertise as we work to shape the cybersecurity workforce of the future.

~Lynne Clark
Deputy Chief of the Center for Education, Innovation,
and Outreach in NSA's National Cryptologic School

Lynne Clark is the Deputy Chief of the Center for Education, Innovation, and Outreach in NSA's National Cryptologic School.

Prior to this assignment, Ms Clark was Deputy Chief of Workforce Resources, Education and Development for NSA's Information Assurance Directorate (IAD). This included responsibility for IAD's hiring and intern programs, education and professional development for IAD personnel.

From 1993 to 2012, Ms Clark was assigned to the Interagency OPSEC Support Staff, where she had responsibility for Operations Security (OPSEC) Training and Program Development consultation to all Federal Departments and Agencies with a national security mission. During her tenure at the IOSS, she participated in several interagency working groups, most notably as Chair of the National Security Policy Board's OPSEC and Risk Management Working Group.

Prior to her tenure at the IOSS, Lynne was on active duty with the U.S. Air Force with worldwide assignments in airspace management, radar operations and risk management; she retired at the rank of Lieutenant Colonel in 1999.

Ms. Clark's academic credentials include a Masters in Clinical Psychology from the Fielding Institute, and a B.A. in Community Development from Baldwin-Wallace College.

Panels

Executive Leadership Panel



Paul J. Maurer, Ph.D.
President
Montreat College



Lawrence Rose
Dean, JHBC
California State University,
San Bernardino



Dr. Ryan Carstens
President, ENMU
Ruidoso Branch
Community College



Randy VanWagoner
President
Mohawk Valley
Community College

CAE National Resource Center Panel



Margaret Leary
CAE-CNRC Peer Review



Corinne Sande
CAE-CNRC Candidates Program



Art Conklin
CAE-CNRC KU Dvelopment



Tony Coulson
CAE-CNRC CAE Community

Program Committees



Amelia Estwick – Excelsior College – CAE-CDE Track

Dr. Amelia Estwick is the Director for the National Cybersecurity Institute and Faculty Program Director for the School of Graduate Studies Cybersecurity program at Excelsior College (a CAE-CDE school). Prior to her academic position, Dr. Estwick spent 17 years with the National Security Agency and held multiple technical leadership positions, including Technical Director within NSA's Cyber Threat Operations Center. Dr. Estwick earned her Doctorate and Master's degrees in Computer Science from The George Washington University and her Bachelor's degree in Computer Information Systems from Southern University at New Orleans. Prior to her academic and professional pursuits, she served eight years in the United States Army (INFOSEC) and is a Gulf War veteran.

Faisal Kaleem – Metropolitan State University – CAE-CDE Track

Faisal Kaleem (CISSP, CEH, Security+, MCT, CCLO, and CCPA) is a professor in the Department of Computer Science and Cybersecurity at Metropolitan State University. Dr. Kaleem's research work includes cybersecurity learning activities and privacy through the use of Augmented Reality, cybersecurity and forensic curriculum development, computer and network security, mobile device security and forensics, and mobile malware analysis and attribution. Dr. Kaleem has also established MN Cyber—a statewide institute for cybersecurity and forensics research and education. He is currently serving as the Executive Director of MN Cyber. He is also the co-founder and executive member of Minnesota Cyber Career Consortium (MNC3).



Kim C. Muschalek – San Antonio College – CAE-CDE Track

Kim C. Muschalek, has over 24 years of higher education experience in computer applications management and computer science. She is a Microsoft Operations Specialist and Certified Adobe instructor and is qualified to teach Cisco Networking Certification classes. Kim has experience teaching client operating systems (Windows and Linux), TCP/IP, network design and architecture, and hardware configuration and software integration. In 1995, Kim joined the faculty at San Antonio College. As a 6-year mentor to the San Antonio College/ Information Technology and Security Academy (ITSA) CyberPatriot Team, she taught cyber security concepts and team strategies aimed at solving real-world cyber security issues. Kim has been the Computer Information Systems/Computer Science program coordinator since 2016. She is currently the PI for the NSF Scholarship for Service C3P Pilot Program and the Director of the South Central CAE Regional Resource Center.



Agnes Hui Chan – Northeastern University – CAE-R Track

Professor Chan received her PhD in mathematics and joined the Northeastern University faculty in 1977. She retired from the University in fall 2018 and is now Professor Emeritus in the Khoury College of Computer and Information Science at Northeastern. Her research focuses on cryptography and communication security. She works on fast, efficient authentication algorithms for small mobile devices. Professor Chan holds two patents on stream ciphers. She was awarded the Distinguished Educator Award presented at CISSE in 2016. Professor Chan is active in promoting women in sciences, participating as an invited speaker at NSA's "Women in Mathematics" and "Alumni Mathematicians" at Smith College.



Dongwan Shin – New Mexico Tech – CAE-R Track

Dr. Dongwan Shin is an Associate Professor of Computer Science and Engineering department at New Mexico Tech. Since joining the department in 2005, Dr. Shin has been involved in a variety of research and educational projects funded by various government agencies, national labs, and industry partners on cybersecurity. He has been involved in many departmental activities related to cybersecurity and programming competitions jointly supported by Sandia labs, Los Alamos lab, and ACM International Collegiate Programming Contest. He was named Orr Endowed Chair of Computer Science and Engineering department while serving as the department chair from 2015 to 2018.



Jennifer Cutler – Texas A&M – CAE-R Track

Jennifer Cutler has been with the Texas A&M Cybersecurity Center for over 3 years. She currently serves as Program Manager, with her focus on student engagement, industry partnerships, and professional development. She is the administrator and advisor for the Texas A&M Cyber Leader Scholar Program, which includes the CyberCorps®: Scholarship for Service and DoD CySP Scholarships. She is Staff Advisor for the Texas A&M Cybersecurity Club, as well as, serving as the Texas A&M representative for the Cyber Alliance Committee of the RELLIS Campus Academic Alliance, a consortium of the eleven Texas A&M System Schools to foster and facilitate Cybersecurity research, education, and training. Jennifer received her Bachelor's degree in Anthropology and History from Texas A&M University in 2001.



Speaker Bios

Agnes Hui Chan

Northeastern University

Professor Chan received her PhD in mathematics and joined the Northeastern University faculty in 1977. She retired from the University in fall 2018 and is now Professor Emeritus in the Khoury College of Computer and Information Science at Northeastern. Her research focuses on cryptography and communication security. She works on fast, efficient authentication algorithms for small mobile devices. Professor Chan holds two patents on stream ciphers. She was awarded the Distinguished Educator Award presented at CISSE in 2016. Professor Chan is active in promoting women in sciences, participating as an invited speaker at NSA's "Women in Mathematics" and "Alumni Mathematicians" at Smith College.



Bei-Tseng "Bill" Chu

University of North Carolina at Charlotte

Dr. Bei-Tseng "Bill" Chu is a Professor at the Department of Software and Information Systems, University of North Carolina at Charlotte and the associate director of the Center for Configuration Analytics and Automation. He is the point of contact for UNC Charlotte's NSA/DHS recognized Center of Academic Excellence in Cyber Defense Education, and Center of Academic Excellence in Research. He is the PI of the SFS program at UNC at Charlotte and has received several cybersecurity education grants from the NSA and NSF. He received his BS in Electrical Engineering and Ph.D. in Computer Science from the University of Maryland, College Park.



Ram Dantu

University of North Texas

Dr. Ram Dantu has 20 years of industrial experience in the networking industry, where he worked for Cisco, Nortel, Alcatel, and Fujitsu and was responsible for advanced technology products from concept to delivery. He is a Professor in the Department of Computer Science and Engineering and the founding director of the Network Security Laboratory and the Center for Information and Computer Security at the University of North Texas. He has received several NSF awards in collaboration with Columbia University, Purdue University, the University of California, Davis, Texas A&M University, and Massachusetts Institute of Technology. In addition to over 200 research papers, he has authored 25 patents.



Melissa Dark

Dark Enterprises, Inc.

Melissa Dark has been a leader in cybersecurity education for 20 years. She has pioneered a number of initiatives in cybersecurity curriculum, instruction, assessment, and research. She is currently focused on building capacity in high school cybersecurity education to help fill the cybersecurity workforce pipeline.



Jason Denno

University of Arizona

Jason Denno is the Director of Cyber, Intel and Information Operations at the University of Arizona. Mr. Denno's experience includes over 20 years of designing, developing, deploying, and operating intelligence and cyber systems across the globe. His professional experience includes senior level positions in both large and small defense contracting companies, the Director of the Battle Command Battle Lab for Fort Huachuca, and he is a former US Army Infantry and Signals Intelligence officer. In addition to an MS in Cyber Operations, MBA, and a BA in Political Science, Mr. Denno possesses multiple GIAC certifications in Cyber Operations.



Speaker Bios



Yingfei Dong

University of Hawaii at Manoa

Yingfei Dong received his B.S degree and MS degree in Computer Science from Harbin Institute of Technology in 1989 and 1992, respectively, his doctor degree in engineering from Tsinghua University in 1995, and his PhD degree in Computer and Information Science from the University of Minnesota in 2003. He joined the Department of Electrical and Computer Engineering in the College of Engineering at University of Hawaii as an assistant professor in August, 2003. His main research interests are in the areas of computer and network security and privacy, computer networks, Internet services and distributed systems.



Daniel Dougherty

Worcester Polytechnic Institute

Daniel J. Dougherty is Professor of Computer Science at WPI, having held previous faculty positions at Dartmouth College and Wesleyan University. The broad theme of my research is the development of software tools to help people understand the properties satisfied by their systems, especially security policies and cryptographic protocols. A recent focus has been on lightweight tools grounded in logic but accessible even to end-users. Our slogan is: "You need not be a logician to use formal methods."



Guillermo Francia, III

University of West Florida

Dr. Guillermo A. Francia, III received his Ph.D. in Computer Science from New Mexico Tech. His research interests include embedded and industrial control systems security, vehicular network security, machine learning, and unmanned aerial vehicle security. He is a two-time recipient of a Fulbright award related to cybersecurity projects (Malta, 2007/UK, 2017) and is the 2018 winner of the National CyberWatch Center Innovations in Cybersecurity Education Award. In July 2019, he received an appointment as Commissioner of the Computing Accreditation Commission of ABET. Currently, Dr. Francia is serving as Faculty Scholar and Professor at the UWF Center for Cybersecurity.



Shelly Heller

George Washington University

Computer Science Professor Shelly Heller holds a Ph.D. from the University of Maryland. Her research interest is in the area of computers in educational settings and the impact of interactive multimedia on learning in these environments. Of particular interest is how students learn to use educational software, including the development of courseware for new application areas, the integration of the computer into existing educational settings and public spaces, and in-service and pre-service teacher training. Her efforts in women's leadership include her research grants and her role as the director of the Elizabeth Somers Women's Leadership Program. Dr. Heller is currently the Director of the newly formed School of Engineering and Applied Sciences Center for Women in Engineering.



Kyle Jones

Sinclair College

Mr. Jones holds a CompTIA Strata, A+, Network+, Security+ certification as well as an ITIL Foundations. He holds an Associate's in Network Engineering from Southern State, a Bachelor's of Business from Wilmington College, and a Master's degree in Information Assurance and Security from American Public University. He is a CAE2Y Principal Investigator and serves as the coordination and curriculum specialist for Sinclair's CIS 2640 Network Security class. Recently, he participated in a round table discussion hosted by the Dayton Business Journal on the present landscape of cybersecurity, and he was featured on WDTN Dayton-Channel 2 in a vignette about "Good Cyber Hygiene."

Speaker Bios

Faisal Kaleem

Metropolitan State University

Faisal Kaleem (CISSP, CEH, Security+, MCT, CCLO, and CCPA) is a professor in the Department of Computer Science and Cybersecurity at Metropolitan State University. Dr. Kaleem's research work includes cybersecurity learning activities and privacy through the use of Augmented Reality, cybersecurity and forensic curriculum development, computer and network security, mobile device security and forensics, and mobile malware analysis and attribution. Dr. Kaleem has also established MN Cyber—a statewide institute for cybersecurity and forensics research and education. He is currently serving as the Executive Director of MN Cyber. He is also the co-founder and executive member of Minnesota Cyber Career Consortium (MNC3).



Sidd Kaza

Towson University

Dr. Sidd Kaza is the Chairperson of the Department of Computer and Information Sciences at Towson University. He received his Ph.D. degree in Management Information Systems from the University of Arizona. He is a principal investigator on several cybersecurity education projects. He is also on the ACM/IEEE/AIS/IFIP Joint Task Force on Cybersecurity Education that produced the four-year cybersecurity curricular guidelines (cybered.acm.org). Dr. Kaza's work has been published in top-tier journals and conferences and has been funded by the National Science Foundation, National Security Agency, Department of Defense, Intel, and the Maryland Higher Education Commission.



Wei Li

Nova Southeastern University

Dr. Wei Li is a professor in the College of Computing and Engineering at Nova Southeastern University. His research interests include attack modeling and simulation, intrusion detection, firewall management, role-based access control, and the application of AI techniques in various security problems. He has published over two dozen papers in refereed journals and conferences. He is a senior member of IEEE and a member of ACM.



Mark Loepker

Cyber Center for Education & Innovation/National Cryptologic Museum

Mark S. Loepker is the Senior Advisor and Education Lead at Cyber Center for Education & Innovation, home of the National Cryptologic Museum. Mark is a master practitioner in Information Assurance and International Partnerships with over 39 years of government experience. He worked closely with congressional members and staff on emerging cybersecurity issues and legislation. Mr. Loepker was the Director, National Information Assurance Partnership, established between the National Institute of Standards and Technology and the NSA to evaluate information technology product conformance to international standards.



Yair Levy

Nova Southeastern University

Yair Levy, Ph.D. is a Professor of IS and Cybersecurity at Nova Southeastern University (NSU), the Director of the Center for Information Protection, Education, and Research (CIPhER), and chair of the Cybersecurity Faculty Group at the college. He earned his BS.c. in Aerospace Engineering (Technion) and MBA and Ph.D. in MIS from Florida International University. He heads the Levy CyLab (<http://CyLab.nova.edu>), which conducts innovative research in cybersecurity, social engineering, user-authentication issues, and privacy. He actively serves as a Board Member and the Education Section Chief of the FBI/InfraGard South-Florida chapter.



Speaker Bios



Allen Parrish

Mississippi State University

Allen S. Parrish is Associate Vice President for Research and Professor of Computer Science and Engineering at Mississippi State University. Dr. Parrish works with internal and external university constituencies to facilitate research collaboration and to enhance MSU's research portfolio. Dr. Parrish was previously Professor of Cyber Science and Founding Chair of the Department of Cyber Science at The United States Naval Academy, where he helped to start the cyber operations program. Dr. Parrish received a Ph.D. in Computer and Information Science from The Ohio State University.



Portia Pusey

Portia Pusey provides educational research, evaluation, and research development services for projects which improve our national preparedness to protect our digital infrastructure through education. Her research interests center on enriching the engagement and professional skills of cybersecurity learners and professionals, cybersecurity competitions as a sport and the potential of competitions to function as professional development, learning environments, and assessment. She specializes in leading the design, conducting and performing analysis of research which strengthens practice in formal and informal cybersecurity learning situations. She also designs outreach experiences which promote cybersecurity careers and awareness for all k-career stakeholders.



Dongwan Shin

New Mexico Tech

Dr. Dongwan Shin is an Associate Professor of Computer Science and Engineering department at New Mexico Tech. Since joining the department in 2005, Dr. Shin has been involved in a variety of research and educational projects funded by various government agencies, national labs, and industry partners on cybersecurity. He has been involved in many departmental activities related to cybersecurity and programming competitions jointly supported by Sandia labs, Los Alamos lab, and ACM International Collegiate Programming Contest. He was named Orr Endowed Chair of Computer Science and Engineering department while serving as the department chair from 2015 to 2018.



Chris Simpson

National University

Chris Simpson is the Director of the National University Center for Cybersecurity and is the Academic Program Director for the Master of Science in Cybersecurity program at National University. He has developed innovative curriculum and labs in ethical hacking, pentesting, and incident response. Mr. Simpson holds a Bachelor of Sciences degree in Computer and Information Science (CIS) from the University of Maryland and a Master of Science degree in Information Security and Assurance from George Mason University. He is currently a Doctoral student at Dakota State University.



Cara Tang

Portland Community College

Cara Tang is a faculty member and department chair in the Computer Information Systems department at Portland Community College (PCC), and chair of the Association for Computing Machinery Committee for Computing Education in Community Colleges (ACM CCECC). She chairs the Cyber2yr Task Group creating curriculum guidelines for two-year cybersecurity programs.

Speaker Bios

Mark Thompson

University of North Texas

Dr. Mark Thompson earned his Ph.D. from Louisiana Tech University in Computational Analysis and Modeling, an interdisciplinary program in mathematics, computer science, and statistics with a focus in cybersecurity. He has been teaching in the computer science field for over 14 years and is affiliated with the Center for Information and Computer Security (CICS) at the University of North Texas (UNT). Mark has over 15 years industry experience at Bell-Northern Research, the research and development arm of Nortel Networks, on all phases of development as a senior programmer and systems architect on large, real-time telecommunications systems.



Vincent Urias

Sandia National Laboratory

Vincent Urias is a computer engineer, and Principal Member of Technical Staff in Sandia's Cyber Analysis Research Development Department continuing to make major contributions to Sandia's cyber defense programs, especially in the simulation of complex networks, in developing innovative cybersecurity methods, and in designing exercise scenarios that test the limits of current network security. This work is helping Sandia's customers anticipate current and emerging security threats and make critical decisions about their investments.



Paul Wagner

University of Arizona

Paul is currently an Assistant Professor of Practice for the University of Arizona's Cyber Operations Program. Prior to working with the University of Arizona, Paul spent 20 years in the Army where he developed his knowledge in computer networking and designing robust network architectures to support global operations in support of national and joint operations. He has almost ten years of direct experience as a Signal Officer supporting combat operations for combat units, combat support hospitals, and satellite communications units. His expertise is in establishing diverse architectures in environments with limited or no organic networking and communication resources or infrastructure.



Jinpeng Wei

University of North Carolina at Charlotte

Dr. Jinpeng Wei is an Associate Professor in the Department of Software and Information Systems at the University of North Carolina at Charlotte. His research focuses on theory, methods, and tools that enhance the security of widely used systems software in a broad spectrum of computer systems, from OS kernels, to file systems, to cloud platforms. He has worked on several important topics, including active cyber defense, malware analysis, cyber threat hunting, cloud computing security, and systems software vulnerabilities. He is the winner of three best paper awards and the AFRL Visiting Faculty Research Program Award.



Deanne Cranford-Wesley

Forsyth Technical Community College

Dr. Deanne Cranford-Wesley is currently Associate Dean of the Davis iTEC/Cyber Security Center at Forsyth Technical Community College. She also teaches cybersecurity and computer forensics in the cybersecurity program. Dr. Cranford-Wesley previously worked as Department Coordinator and Associate Professor in the 4 year space for 12 years. She currently is and executive board member for the NC TECH Association an Executive Board member and for the NC Chamber. Dr. Cranford-Wesley has vast experience in curriculum design, grant writing, and program evaluation. She is a published author of various technology related articles. She has a Ph.D. in Education Leadership.



Speaker Bios/Fastpitch Abstracts



Zachary Zaccagni
University of North Texas

Zach Zaccagni is a second year Ph.D. student in the department of Computer Science and Engineering at the University of North Texas (UNT). His research investigates uses and applications of blockchains beyond cryptocurrency, with an emphasis on new consensus protocols. He is a research assistant to Dr. Ram Dantu in the Network Security Laboratory at UNT. He holds a Master's in Computer Science from Wichita State University of Wichita, Kansas, that investigated autonomous robotic decision making in task scheduling. Zach worked as an instructor concurrently teaching in-person and online classes for the duration of his master's program.



Corby Hovis

Corby Hovis is a senior program officer at the National Science Foundation (NSF) in Alexandria, Virginia, where he oversees the NSF-wide Research Experiences for Undergraduates (REU) Program and manages grant opportunities focusing on cybersecurity education in community colleges, including those sponsored by the Advanced Technological Education (ATE) Program. Before coming to NSF, Dr. Hovis served on the faculty of Valparaiso University (Valparaiso, Indiana) and as science editor at Encyclopædia Britannica (Chicago, Illinois). He earned his graduate degrees (Ph.D., M.S., M.A.) from Cornell University and his undergraduate degree from Wake Forest University. During 2009-2010, he spent a year as an American Council on Education (ACE) Fellow in the Office of the President at The Ohio State University.



Fastpitch Abstracts

Community College Cyber Pilot (C3P) Program



Kyle Jones, Sinclair College

In 2018, NSF awarded a group of community colleges funding to establish a standalone CyberCorps®: Scholarship for Service program. These community colleges received funding for student scholarships, tuition and related costs. The session will briefly review the recruiting and selection process, the different curriculum pathways and describe the target audience to receive these scholarships. The fast pitch will also discuss how the institutions have collaborated to establish a cohort of students across multiple institutions.

Fastpitch Abstracts

International Opportunities for Cybersecurity Faculty



Guillermo Francia, III, University of West Florida

This presentation will cover international opportunities for cybersecurity faculty to expand their technical and cultural vision of the discipline. Its purpose is to share experiences gained and to entice other academic or professional experts in cybersecurity to conduct research, pursue professional development, assist in curriculum development, and/or assess cyber best practices at international institutions through the Fulbright program. The Fulbright award, administered by the Council for the International Exchange of Scholars for the US State Department, provides generous stipend to cover travel, food and lodging, and other personal expenses incurred during the duration of the award which ranges from 3 to 6 months. Depending on the selected program, dependents may also be supported with modest allowances to enable them to join the award recipient during the entire duration. It is indeed a rewarding experience towards understanding cultural and technical diversity!

An Innovative Approach Using Mixed Reality to Improving Career Readiness



Mark Thompson and Ram Dantu, University of North Texas

The lack of soft skills such as communication, diversity, leadership, and work ethics being taught in programs reduces the effectiveness of cybersecurity experts as organizations across all industry sectors become targets of increasingly complex and debilitating attacks. We propose a program to improve career-readiness of future workforce by increasing soft skill competencies, encouraging engagement through experiential learning, and providing opportunities for learning and networking through professional development using mixed reality tools and other novel activities.

Pathway for Community College Students to an ABET-Accredited Degree in Cybersecurity



Mark Thompson and Ram Dantu, University of North Texas

To meet the ever-growing demand for well-trained, ethically responsible cybersecurity professionals, we looked to programs and students at community colleges in the Dallas-Fort Worth area as input for our new degree in cybersecurity. Then we applied curricular guidelines from CAE, NICE, ABET, and ACM to develop a high quality, academically challenging, and career-enriching ABET-accredited pathway for community college students to a degree in cybersecurity that is responsive to industry trends, changing standards, and employer needs.

Teach Cyber Now: Ask Me How



Sidd Kaza, Towson University, and Mark Loepker, National Cryptologic Museum

The global cybersecurity crisis has challenged academic institutions to build and grow cybersecurity programs to help produce a skilled and knowledgeable cyber workforce. The current state of cybersecurity education is faced with three intersectional challenges: 1) a dire shortage of faculty and teachers, 2) a rapidly evolving field, and 3) limited access to quality curricular materials. While addressing the shortage of faculty requires a long-term solution, it has been shown that high quality curricula not only helps institutions build programs, but also improve student learning outcomes. Increasing access to better curricula is a relatively inexpensive, yet impactful intervention. To help meet these challenges, the National Security Agency funded the CLARK Cybersecurity Curriculum Library (www.clark.center). CLARK hosts over 700 quality-assured learning objects from over 70 institutions organized as collections, including the NSA National Cybersecurity Curriculum Program (NCCP) and the National Science Foundation C5 (c5colleges.org) collections.

This fastpitch will introduce the highlights of CLARK and provide examples of high-quality cyber learning objects that can be immediately deployed in the classroom.

Fastpitch/Special Interest Group Abstracts

ACM Cybersecurity Curriculum Guidelines Mapping to CAE Knowledge Units



Cara Tang, Portland Community College

In 2017 the ACM (the world's largest educational and scientific computing society), with the Joint Task Force on Cybersecurity Education, published Cybersecurity Curricula 2017 (CSEC2017), guidelines for baccalaureate programs in Cybersecurity.

The ACM CCECC (Committee for Computing Education in Community Colleges) is developing curriculum guidelines for associate degree programs, based on CSEC2017, with expected publication in early 2020. These guidelines, code-named Cyber2yr, map to the CAE knowledge units for two-year programs.

Note also that the ACM CSEC2017 and Cyber2yr guidelines, respectively, are the basis for the ABET program criteria for Cybersecurity four-year programs, and the currently-under-development ABET program criteria for Cybersecurity two-year programs.

This fastpitch session will present an overview of the ACM Cybersecurity curriculum guidelines with focus on the forthcoming Cyber2yr guidelines for two-year programs, and how they map to the CAE knowledge units for two-year programs. The Cyber2yr guidelines can be used to develop or update a two-year Cybersecurity program that includes the CAE foundational and technical core knowledge units.

Integrating Professional Cybersecurity Certification Preparation into Fundamentals Course



Yair Levy, Nova Southeastern University, and Eric G. Berkowitz, Roosevelt University

Careers in cybersecurity and information technology (IT) require professional certifications along with academic degrees. The challenge most students are faced with is that some cybersecurity certifications require significant knowledge, skills, and abilities (KSAs) and personal recommendations for years of industry experience. However, there are several great opportunities for students to obtain entry level cybersecurity certifications that are well accepted by the industry as part of their academic degree program. Moreover, such cybersecurity certificates are required by thousands of cybersecurity entry level jobs and can greatly help students even to finance their education immediately after completing such professional certifications.

This presentation will discuss the integration of such entry level cybersecurity professional certification preparation as part of the virtual lab component that of Fundamental of Cybersecurity course at the graduate program that is mainly focused on career changers. The presentation will provide the background for the selection of the specific platform (LabSim) along with the experience our college had over the past two years in using it. Moreover, the discussions will cover some of the linking of the Fundamental Knowledge Units (KUs) to the course and the specific assignments to assess the relevant KU objectives.

The presentation will also include cases of success story of students who completed the course, went to pursue the professional cybersecurity certification (Security+), and the impressive impact it had on their cybersecurity career path. The presentation will conclude with open discussion and Q&A session.

Presentation/Special Interest Group Abstracts

Developing a Professional Society for Cybersecurity Education



Allen Parrish and Sidd Kaza, Mississippi State University and Towson University

The CAE Community continues to do an outstanding job in supporting and facilitating a community for cybersecurity education for US programs that have the CAE designation. However, this approach is limited to US-based programs, and admission to the community requires employment at an institution that holds a CAE credential. A professional society for cybersecurity educators that is strictly based on individual interest and qualification would be a more typical approach in other academic areas of computing. Such an approach has been discussed at several different meetings of cybersecurity educators, and we feel that further engagement and discussion is needed to assess the potential of such an approach. As such, we propose this Special Interest Group to assess the level of interest in this idea, and to facilitate the organization of an effort to develop a charter and to plan an organizational approach.

Promoting Cybersecurity Competitions at Nova Southeastern University



Wei Li, Nova Southeastern University

This presentation is intended to cover the promotion of cybersecurity competitions by the Center of Academic Excellence (CAE) at Nova Southeastern University (NSU). NSU first received its CAE designation in March 2005 amongst the first in the State of Florida and was redesignated in October 2014. The promotion of cybersecurity competition has long been in our agenda but was challenging, primarily due to the nature of students as many of them are working professional students. In this presentation, we will cover the recent practices at NSU with a focus on the engagement of working professionals and online students in cybersecurity competition.

- National cybersecurity competitions currently being promoted
- Faculty support of cyber competitions
- Programs/Courses promotions of cyber competitions
- Outcomes/Benefits of cyber competitions
- Future steps Through this presentation, we hope to raise awareness, foster new ideas, and share the best practices in promoting cybersecurity competitions within the CAE community.

Using Devops Tools to Deploy Cybersecurity Labs in Cloud Computing Environments



Chris Simpson, National University

Hands-on cybersecurity labs are an excellent way to teach cybersecurity and for students to demonstrate knowledge. There is a large body of research on cybersecurity labs that provide examples of excellent lab environments. Due to the use of proprietary software and other factors like significant hardware requirements and large file sizes, it can be difficult to replicate these lab environments. The emergence of low cost cloud computing resources and the automated deployment of infrastructure using Devops tools make it easier to share and deploy lab resources. There are several open source projects that provide excellent lab environments that can be easily deployed in cloud computing environments.

This presentation will provide a short overview and demonstration of using Devops tools to automate the deployment of open source cybersecurity labs into cloud computing environments. The talk will highlight some of the possible tools and how they can be used across cloud computing platforms. During the demonstration an open source lab environment will be deployed in Amazon Web Services.

This presentation is based off of a paper from the presenter that was presented at the AMCIS 2019 conference. The presentation at the CAE conference will focus on the practical aspects if using Devops tools to deploy cybersecurity labs.

Presentation Abstracts

Reach to Teach: Using Videos to Prepare Cybersecurity Adjunct Faculty



Shelly Heller, George Washington University

There is a capacity issue in the educational system preparing cyber security experts in this high-demand area: students cannot readily be added to the education system, especially at the Community Colleges level, because trained faculty to accommodate expanded sections are scarce. The weak link in the cybersecurity workforce supply chain is often the inability to find faculty who can be effective and can provide proper encouragement to the students to join the cyber workforce.

GW has developed one way to address this capacity issue by preparing a way to tap cybersecurity experts, with an initial emphasis on graduates of the NSF-sponsored CyberCorps program, as adjunct faculty. Such cybersecurity experts in the workforce have the potential to fill the need for part-time cybersecurity faculty at the Community College level. By tapping into the pool of working cybersecurity experts and retired individuals whose background fits the typical qualifications, a viable long-term strategy can be developed. The challenge is to outfit these technology-savvy individuals with pedagogical insights and skills, usually not present in this chosen population.

The Reach to Teach project, funded by the Department of Defense, was developed over the last two years with input from educators at both 2 year and 4 year institutions to explore this potential. The research effort engaged current faculty, as well as education experts, and resulted in a pilot Reach To Teach online course that was piloted in several workshops including the 2018 3CS Conference in Portland, OR. Reach to Teach includes six brief video sessions that can be viewed by prospective adjunct faculty, each of which includes the following content: introduction to community colleges, ethics, and pedagogy. The pedagogic content includes the general structure of a course, crafting goals and objectives, techniques for moving explanations from the concrete to the abstract, using group work using case studies, and using discussions in classes.

Reach to Teach is now ready to be used by the academic community. The program can be found at <https://blogs.gwu.edu/seas-reachtoteach/>. There is no fee or cost associated with program adoption. For more information contact Principal Investigator Shelly Heller (sheller@gwu.edu) or co-Principal Investigator Costis Toregas (toregas1@gwu.edu).

Matching Employer Cyber-Skill Needs with Students' Assured Skills



Zachary Zaccagni and Ram Dantu, University of North Texas

We present a novel way to help match employers' cybersecurity skill requirements with students' knowledge using a blockchain to assure students' credentials and records. This approach applies micro-accreditation of topics and rigor scores to students' courses and associated tasks, making it easier for employers to explore students' records to verify their success in specific skills. In turn, this allows employers to make better hiring decisions, conferring a solid way for students to prove the quality of their skills. Future work includes mapping courses from CAE to NICE framework, fine-tuning transaction times, and developing a better consensus model for peer-reviewed rigor.

Presentation Abstracts

Hands-on Learning Experiences for Cyber Threat Hunting Education



Jinpeng Wei and Bei-Tseng "Bill" Chu, University of North Carolina at Charlotte, and Deanne Cranford-Wesley, Forsyth Technical Community College

Cyber threat hunting has emerged as a critical part of cyber security practice. However, there is a severe shortage of cybersecurity professionals with advanced analysis skills for cyber threat hunting.

Sponsored by NSA, the University of North Carolina at Charlotte (UNC Charlotte) and Forsyth Technical Community College (Forsyth Tech) have been developing hands-on teaching materials for cyber threat hunting that will expand our current strong educational programs in cybersecurity. UNC Charlotte is designated as a Center of Academic Excellence in Information Assurance Education-Cyber Defense, and a Center of Academic Excellence in Information Assurance Research by NSA and DHS, and has an NSF funded IUCRC in Configuration Analytics and Automation. Since 2001, UNC Charlotte has run the Carolina Cyber Defender Scholarship Program, one of the largest such programs in the United States, with funding from NSF and NSA. Forsyth Tech has been re-designated as a Center of Academic Excellence in Cyber Defense Education in May 2019. It has established the Davis ITEC Cybersecurity Center and with the support of a grant from Department of Education, it has been building a Security Operation Center Student Lab since December 2018, to strengthen the future workforce in cyber security through hands-on learning.

We have developed freely-available, hands-on teaching materials for cyber threat hunting suitable for use in two-year community college curriculum, 4-year universities curriculum, as well as for collegiate threat hunting competitions. To the best of our knowledge, there are not such open source material online for educational purposes.

Our project fits into the theme of "Innovations in Cybersecurity Education, Training, and Workforce Development," with a focus on "Accelerate Learning and Skills Development" defined by the NICE Strategic Plan.

The objectives of our project are twofold: (1) develop hands-on learning experiences that cover two important areas in threat hunting: threat analysis and security data analytics, and (2) build institutional capacity by integrating at least seven hands-on labs on threat hunting into existing curricula at two participating institutions: UNC Charlotte and Forsyth Tech.

Our hands-on labs focus on exercising a set of essential technical skills (called the threat hunting skill set) in an enterprise environment and they are modeled after real-world scenarios. Our lab environment contains real threats (e.g., malware) against real software (e.g., Operating Systems and applications), and real security datasets. These labs are designed to help a student learn how to detect active and dormant malware, analyze its activities, and assess its impact. These labs also teach a student how to search and probe for anomalies in a variety of datasets using multiple analytical skills, such as statistical analysis. Our labs are designed at different difficulty levels suitable for use by two-year community college students, 4-year university students, as well as for collegiate threat hunting competitions.

We plan to present the design and implementation of our hands-on labs, and we will offer an interactive learning session in which we will walk the participants through some of our labs on their computers.

Presentation Abstracts

High School CCF (Cybersecurity Curriculum Framework)



Melissa Dark, Dark Enterprises, Inc., and Mark Loepker, National Cryptologic Museum

A team of educators has been working on a cybersecurity curriculum framework (CCF). The purpose of the framework is to express a set of standards that stakeholders can use to develop a dedicated cybersecurity course for high schools. While computer science ideas and work are present in the framework, the CCF clearly delineates cybersecurity as its own topic. In the next phase of this project, the team hopes to develop methods for dual-credit and/or advanced placement so that students who take the course in high school can earn college credit for it. This session at the CAE community meeting would be focused on sharing the framework and investigating the pros and cons of dual-credit or advanced placement from the perspective of CAE principals.

WIN-Cyber: Work (role) insight network online competency & pathway tool



Faisal Kaleem and Portia Pusey, Metropolitan State University

Employers in Minnesota are participating in the development of an NSA-funded K-18 cybersecurity education pathway and a tool that facilitates mapping and reports on the intersection of certifications, cybersecurity workforce frameworks, and cybersecurity course objectives of MN higher education.

The cybersecurity education community needs an online interactive mapping tool and resource for all stakeholders that will remain current through changes in the field. When educational programs are mapped to the frameworks and certifications, analyses can be conducted to understand gaps and redundancies in curriculum and facilitate the availability of prior learning credit based on certifications.

Within the landscape of cybersecurity education and professional development, there are several frameworks which can be used to guide curriculum development and evaluation. These include the NSA Center of Academic Excellence Knowledge Units, NICE Framework, and CSEC 2017. In addition, cybersecurity certifications are a key element in the cybersecurity education ecosystem. However, the potential mapping combinations between and among domains and objectives of the frameworks and certifications are in the millions of connections.

This presentation will describe the development, testing and deployment of the first iteration of the WIN Cyber tool. The innovation of the WIN Cyber Tool is the multiple algorithmic supports for recommend mapping connections between the elements in frameworks, certifications, and courses. The demonstration will show (1) algorithmic support for mapping, (2) data collection, retrieval, and the development of topic trees, and (3) prior learning credit analysis function. We will conclude by collecting input on future use-cases and functionality of the tool.



Thank you for attending the CAE in
Cybersecurity Community Symposium!

All materials from the symposium will be available to view and download on the CAE in Cybersecurity Community website. If you have any questions, comments, or concerns please see our contact us at info@caecommunity.org