CAE in Cybersecurity Symposium

November 19 | 20

CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY

CAE

★ COMMUNITY ★

Welcome

Welcome to the 2020 CAE in Cybersecurity Symposium!

Welcome!

The national cybersecurity workforce demand continues to outpace supply – a fact that is no secret to my academic colleagues in the CAE in Cybersecurity Community. Since the first CAE Community Symposium in 2013, the CAE academic institutions have grown from an average of 13,000 students nationally, to over 100,000 majoring in cybersecurity-related academic programs.

Amazing progress, but this is just the beginning. Over the next two days, you will hear about how the CAE Community and the CAE Program are launching a number of strategic initiatives to rapidly grow a quality workforce and faculty, in conjunction with key partners in industry, academia, and government. You will also have the opportunity to hear from our newly formed Communities of Practice in Cyber Defense, Research, and Operations. You will also have time to network with government partners and your regional hubs.

We know that “Zoom exhaustion” is real, so the program committee has worked hard to create a program that is informative but also keeps the collegial feeling of a community.

Contents

SAVE THE DATE

CAE Community 2022-2026 Strategic Planning Forum

December 15, 2020

Agenda

November 19, 2020 (All times EST)	
12:00pm	Welcome Logistics and Kickoff
12:15pm	NSA – Academic Partnership
12:30pm	NCAE-C Strategic Planning Overview
1:05pm	CAE Community progress and Initiatives
1:30pm	Break
1:45pm	Q&A Time with PMO
	Partner Program Updates:
2:15pm	NICE
2:45pm	CISA
3:15pm	Break
3:30pm	NSF
4:00	Closing
4:30- 5:30pm	Government Partner Meet-and-Greet

Agenda

November 20, 2020			
10:00am	Opening and Logistics Day 2		
10:15am	Communities of Practice Panel CAE-CO, R, CD		
10:55am	Break		
	CAE-CD Track	**CAE-R Track**	**CAE Candidates Meeting By Invitation Only**
11:00am	Panel	INSuRE Q&A	Candidates Meeting
11:35pm	Mini Workshops	Research opportunities at the Army Cyber Institute and The United States Military Academy at West Point	
12:45pm	Lunch		
1:15pm	Panel Presentations	DoD Panel Q&A	Candidates Meeting Continues
1:45pm	Fast Pitch and Poster Presentations		
2:00pm		Research Panel	
3:00pm	Closing		
3:15-4:00pm	CAE-C Regional Hub Meet-and-Greet		

Agenda

DAY 2 CAE-R Track	
Please visit our YouTube channel to view pre-recorded presentations prior to Friday's event	
11:00am	INSuRE Q&A – Agnes Chan, Suzanne Wetzel
11:35am	Research opportunities at the Army Cyber Institute and The United States Military Academy at West Point – Lubjana Beshaj
12:45pm	Lunch
1:15pm	DoD Panel Q&A – Cliff Wang, Reginald Cooper, Asheley Blackford, Chester (CJ) Maciag, Ryan Craven
2:00pm	Research Panel – Victor Piotrowski, James Joshi
3:00pm	Return to General Session

DAY 2 Candidates Track	
11:00am	Candidates Private Meeting
12:45pm	Lunch
2:30pm	Candidates Private Meeting, Cont.
3:00pm	Return to General Session

Agenda

DAY 2 CAE-CD Track #1	
11:00am	NCL CyberMetrics – Measuring Student Proficiencies to Launch the Cybersecurity Careers – Dan Manson, Kaitlyn Bestenheider, Meredith Kasper, Franz Payer
11:35am	Trustworthy: When Humans and Bots Are Mingled – Zhixiong Chen
11:55am	Cybersecurity Assessments in Global Public Health Involving Technology – Stanley Mierzwa
12:15pm	Social Engineer your Students Before they Social Engineer You: Teaching Human Hacking in a CAE Curriculum – Ronald Woerner, Karla Carter
12:45pm	Lunch
1:15pm	Cyber Gym: Open-Source Security Labs in the Google Cloud – Philip Huff, Sandra Leiterman
1:45pm	Escape The Breakout Room: A Set of Cybersecurity Challenges-Based Educational Game – Ankur Chattopadhyay, Meghyn Winslow
2:00pm	Cyber Ethics, Career Development, and Professional Curriculum – Stephen Miller
2:15pm	Lessons Learned in Starting a B.S. in Cybersecurity During COVID-19 Pandemic – Mark Thompson, Ram Dantu
2:30pm	Offering Continuing Education Credits in Cybersecurity for First Responders – Ram Dantu, Mark Thompson
2:45pm	The UofM Center for Information Assurance – Tony Pinson
3:00pm	Return to General Session

Agenda

DAY 2 CAE-CD Track #2	
11:35am	The CAE National Competition - Overview and Collaboration Opportunity – Jake Mihevc, Ron Sanders
11:55am	A CAE-CDE Planning for CAE-CO Designation: Curriculum Design and Content Considerations – James Robertson, Loyce Pailen
12:15pm	Got curriculum? Donate to CLARK's Plan C – Blair Taylor, Sidd Kaza
12:45pm	Lunch
1:45pm	Integrating NICE Cybersecurity Workforce Framework (NCWF) to University Career Services – Yair Levy, Emilio Lorenzo
2:00pm	An Evaluation of Cybersecurity Students' Needs for Program Improvement – Waleed Farag
2:15pm	Hackers Wanted: Building towards IT, MIS, and Cybersecurity Careers – Ronald Woemer
2:30pm	Designed Support for Student Research Avenues – Derek Sedlack
3:00pm	Return to General Session

Agenda

DAY 2 CAE-CD Track #3	
11:35am	Teaching Cybersecurity as Risk Management – Maeve Dion
11:55am	Self-regulated, Deep Learning with NIST Documents in HiEd – Maeve Dion
12:15pm	Industrial Cybersecurity Training and Education Standards - Getting the Water to the End of the Row with CYBER-CHAMP – Jade Hott, Gary Deckard, Donaven Haderlie, Shane Stailey
12:45pm	Lunch
1:45pm	Improving Cyber Security by Engaging Software Developers via Universally Applicable Security Gems – Xiuwen Liu, Mike Burmester
2:00pm	In the Covid Era - Teaching Cybersecurity Online Across the Disciplines – Debasis Bhattacharya
2:15pm	Simple tool for faculty development & support: the instructor's workbook – Maeve Dion
2:30pm	Using Wireshark in Security Classes – Wei Li
3:00pm	Return to General Session

Welcome

Thank you to the United States' educational institutions that have committed to the high standards of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) programs. The NCAE-C educators are patriots in the education and training of our Nation's Cyber First Responders!

As Commandant of the National Cryptologic School at the National Security Agency, I see the impact of what you do every day. I appreciate the NCAE-C institutions' leadership in one of the most critical, challenging academic fields today. Cyber expertise and a strong cybersecurity foundation are critical to every aspect of American life – we are seeing that now more than ever given the challenges we faced in 2020.

We thank you for your continued partnership and look forward to working with you over the next two days as we set the path for the future.

~Diane Janosek
Commandant, National Cryptologic
School, NSA

Ms. Diane M. Janosek is an award-winning cybersecurity leader and sought-after speaker. As an innovator, she has been a member of the Defense Intelligence Senior Executive Service (SES) since 2012. She currently serves as the National Security Agency's Commandant of the National Cryptologic School, which is comprised of four colleges, to include the Colleges of Cyber and Cryptology. In her role, she manages and oversees the delivery of unique courses for the U.S. intelligence workforce, both civilian and military, in the areas of cyber, network security, cyber resilience, and encryption, ensuring a strong federal workforce to defend critical national security networks.

Ms. Janosek's areas of expertise include academic leadership, privacy and technology, governance and data policy, export control, defense acquisition, information and cyber security. In her current role, she is committed to the educational, leadership, professional and practical learning needs of the nation's cyber workforce in today's dynamic threat environment.

Welcome

Welcome to the 2020 CAE Community Symposium. It’s been quite a year, but even with the challenges of COVID, telecommuting, scrambling to convert to teaching and collaborating online, and a tempestuous election, we’ve launched several creative and exciting initiatives, built a new application and program management tool, and expanded the CAE Community, the Candidates program, and resources available to all associated institutions.

We designated 25 institutions and re-designated one CAE. The success of the program, and the work of leaders within the NCAE-C schools with representatives on the Hill, has encouraged Congress to provide financial support to the program. If we are successful in our efforts over the next two years, and I’m certain we will be, I’m hopeful the Congressional support will carry us into a new period where the program will grow and flourish, and we will make a long and significant impact on the development of the cybersecurity workforce in this nation.

Your dedication, creativity, expertise and ability to motivate and inspire your students are the bedrock of this program, and are the fuel that carry us forward. We celebrate you, brag on your abilities and look forward to 2021!

~Lynne Clark
Deputy Chief, Center for Cybersecurity Education,
Innovation and Outreach, A29

Lynne is Chief of the NCAE-C program, and has responsibility for GenCyber and other NCS outreach programs. In twenty-two years at NSA, Lynne has worked in risk management and IA and managed recruiting programs for the Information Assurance Directorate. Ms Clark served in the U.S. Air Force and retired at the rank of Lieutenant Colonel in 1998. Ms. Clark’s academic credentials include a Masters in Clinical Psychology.

Speakers

Dr. Lubjana Beshaj

United States Military Academy

Dr. Lubjana Beshaj is a Cyber Fellow of Mathematics at the Army Cyber Institute and an Assistant Professor in the Department of Mathematical Sciences at West Point. Her research interests include cryptography, elliptic and hyperelliptic curve cryptography, post-quantum cryptography – more specifically isogeny based cryptography, Jacobian varieties, arithmetic of algebraic curves, and neural network cryptography.

Kaitlyn Bestenheider

Tevora

Kaitlyn “Crypto-Kait” Bestenheider is NCL’s Chief Player Ambassador, serving as champion for the NCL student players. Kaitlyn quickly became a primary advocate for NCL, developing critical resources for coaches, holding instructive and educational webinars, speaking and presenting to major audiences, and leading the adoption of NCL challenges at conferences. Kaitlyn is an Information Security Analyst at Tevora with expertise in federal governance and compliance assessments. Kaitlyn holds an M.S. in Information Systems from Pace University. Kaitlyn was the humbled recipient of the WiCyS Rising Leadership Award in 2019 and continues to grow her impact as Chief Player Ambassador for the NCL.

Dr. Debasis Bhattacharya

University of Hawai’i Maui College

Dr. Debasis Bhattacharya is currently a faculty member at the University of Hawai’i Maui College, and program coordinator for the Applied Business and Information Technology (ABIT) baccalaureate program. Dr. Bhattacharya has been working in the software industry for 32 years, having worked for large corporations such as Oracle and Microsoft. A resident of Hawaii since 2002, he has been actively researching the information security needs of small businesses since 2008. Dr. Bhattacharya holds degrees from MIT, Columbia University, University of Phoenix and NW California University School of Law. More details about Dr. Bhattacharya can be obtained at http://maui.hawaii.edu/cybersecurity.

Asheley Blackford

Air Force Research Laboratory

Ms. Asheley Blackford serves as the Program Manager for the Air Force Research Laboratory Minority Leaders Research Collaboration Program (ML-RCP). She has been a part of the Materials and Manufacturing Directorate (AFRL/RX) of the Air Force Research Laboratory since 2009. Prior to working with the MLP and RCP, Ms. Blackford was the Deputy Small Business Innovation Research (SBIR) Program Manager for AFRL/RX and has experience working with small businesses. In addition to working this program, Ms. Blackford also manages other Government contracts for her Directorate and is actively involved in the Junior Workforce Council. She is excited and eager to continue her engagement in working with her scientists and engineers as well as engaging with the universities.

Mike Burmester

Florida State University

Mike Burmester is Professor of Computer Science at the Florida State University, where he has been a faculty member since 2000. His research is in all aspects of cyber security and information assurance, with particular focus on cyber physical systems, the IoT, network security and cryptography. He is a director of the FSU Center for Security and Assurance in IT, an editor of four journals and has published over 200 publications. His research is supported by NSF and NSA/DoD.

Speakers

Karla Carter

Bellevue University

Karla Carter is an associate professor in the College of Science and Technology at Bellevue University, in Bellevue, NE. Drawing on more years than she should be admitting of information technology experience, she teaches cybersecurity, information technology ethics, and general information technology and history/civics courses. In addition to being Vice Chair for the Nebraska Chapter of the IEEE Computer Society, past Chair of ACM SIGCAS, and a member of the ACM Committee on Professional Ethics (COPE), she is curious, intense, and irreverent, and cannot resist puns. LinkedIn: https://www.linkedin.com/in/karlacarterlnkne/

Agnes Chan

Northeastern University

Professor Chan received her PhD in mathematics and joined the Northeastern University faculty in 1977. She retired from the University in 2018 and is now a Professor Emeritus. She was the Executive Director of Information Assurance and Cybersecurity programs from 2010-2018. Her research focuses on cryptography and communication security and fast, efficient mutual authentication algorithms for small mobile devices. Professor Chan holds two patents on stream ciphers. She has published widely in IEEE conferences and journals. She was awarded the Distinguished Educator Award presented at CISSE in 2016. She led the effort in establishing the Cybersecurity Research Institute in the University and designed and launched the cybersecurity programs, MS in 2005, PhD in 2010 and BS in 2017. She remains active in promoting cybersecurity education among students.

Dr. Ankur Chattopadhyay

Northern Kentucky University

Dr. Ankur Chattopadhyay is currently an Assistant Professor of CS & Cybersecurity at Northern Kentucky University (NKU). As a member of the NKU Center of Information Security and the faculty advisor of the NKU WiCyS chapter, he is actively involved in cybersecurity education & outreach programs. He is presently a Faculty Fellow at the NKU Institute for Health Innovation, and has been the principal investigator of several grant projects, including NSA/NSF GenCyber, Google IgniteCS and Microsoft TechSpark. His research interests include visual privacy, information assurance & trust in online healthcare, CS & cybersecurity education and privacy-enhancing computer vision & pattern recognition.

Dr. Zhixiong Chen

Mercy College

Dr. Z Chen is a professor and the director of Cyber Education Center at Mercy College in New York. His current research interests are centered at bots and their interaction with human beings in social application platforms. Dr. Chen has published 50 peer reviewed papers. He is a senior member of IEEE and ACM. He received PhD/MS from the University of Pittsburgh. Before joining Mercy College, Dr. Chen was a research scientist at IBM Research.

Dr. Reginald Cooper

Air Force Research Laboratory

Dr. Reginald Cooper is a Research Electronics Engineer in the Radio Frequency Electronic Warfare Branch of our AFRL Sensors Directorate and is an Air Force Research Laboratories (AFRL) Early Career Award Winner. Dr. Cooper started his career with the Air Force as a student researcher in the Minority Leaders Program developing cognitive radio networks for a dynamic wireless environment. In 2013, Dr. Cooper joined AFRL full-time. He leads a team developing war-winning electronic warfare (EW) technologies designed to detect, identify, and degrade enemy radar systems. He served as the AFRL Sensors Directorate lead for the Minority Leader-Research Collaborative Program, takes a personal interest in the students he mentors, and strives to inspire them to excel in STEM fields.

Speakers

Dr. Tony Coulson

California State University, San Bernardino

Tony Coulson, Ph.D., is the executive director of the Cybersecurity Center and professor of Information and Decision Sciences in the Jack H. Brown College at California State University, San Bernardino (CSUSB). At CSUSB, Tony has led more than 20 grant-funded cybersecurity projects totaling over $18 million. He also led the establishment of a nationally acclaimed cybersecurity program that spans business, computer science, national security studies, criminal justice, and public administration. He belongs to several boards and has won numerous academic, national, and community awards. He holds a Ph.D. in Management Information Systems from Claremont Graduate University.

Dr. Ryan Craven

Office of Naval Research

Dr. Ryan Craven is a program officer of the Cybersecurity and Complex Software Systems Program at the Office of Naval Research (ONR) in Arlington, VA. Ryan directs basic and applied science and technology efforts for the Navy and Marine Corps in the areas of systems and network security, program analysis, cyber-physical systems, and general computing. The program works with partners from across academia, small businesses, the defense industry, and federal labs. Ryan recieved his doctorate in Computer Science from the Naval Postgraduate School in Monterey, CA. His personal research has focused on network protocols, security, and internet measurement.

Dr. 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.

Dr. Gary M. Deckard

Idaho National Laboratory

Dr. Gary M. Deckard recently joined Idaho National Laboratory's Workforce Development & Training Department. Prior to joining INL, he served as the Cyber Program Director for the Atterbury-Muscatatuck Center for Complex Operations and was the driving force behind the creation of the Cybertropolis Cyber Range at the Muscatatuck Urban Training Complex. He has over 30 years of experience working in the Technology sector in the areas of Information and Operational Technology, Cyber-physical systems, Cybersecurity training, Cyber-range development, and Electronic Warfare.

Maeve Dion

University of New Hampshire

Maeve Dion teaches cybersecurity and homeland security at the University of New Hampshire, where she directs the online M.S. in Cybersecurity Policy and Risk Management. Professor Dion specializes in the policy, legal, and educational issues relating to cybersecurity, organizational resilience, and critical infrastructure. Over the past two decades, she has supported efforts of the EU, COE, OECD, NATO CCDCOE, DHS, DOD, NSTAC, and ABA, among others. Professor Dion's pedagogical emphases include constructivism, andragogy, collaborative learning, open education, and universal design for learning.

Speakers

Dr. Waleed Farag

Indiana University of Pennsylvania

Dr. Waleed Farag is a professor of Computer Science at Indiana University of Pennsylvania and the Director of the IUP Institute for Cybersecurity. Dr. Farag's research interests include cybersecurity education, network and IoT systems security, e-learning, and multimedia applications. He has published over 50 articles in recognized national and international journals and conferences. Dr. Farag has an outstanding record of securing funds to support his research and is currently the PI of several federally funded grants that support his personally founded unique initiatives contributing to the enhancement of cybersecurity education and research at IUP and the surrounding regions.

Donaven Haderlie

Idaho National Laboratory

Donaven Haderlie is a Business Specialist in the Workforce Development and Training organization within the National and Homeland Security Division at Idaho National Laboratory. He has earned a Bachelor of Science in Computer Science with an emphasis in Programming from Stevens Henager College, a Master of Science in Information Technology Management with an emphasis in Project Management from Capella University and a certificate in Digital Forensics from Capella University.

Drew Hamilton

Mississippi State University

Drew Hamilton is the Director of the Center for Cyber Innovation at Mississippi State University and a professor of computer science & engineering. Dr. Hamilton is a Fellow of the Society for Modeling & Simulation, International (SCS), Chair of the ACM Special Interest Group (SIG) on Ada and Past Chair of ACM SIG Simulation (SIGSIM). During the past ten years he has been awarded more than 70 research grants and has received more than $27M in extramural funding.

Jade Hott

Idaho National Laboratory

Jade Hott is an early-career researcher at Idaho National Laboratory (INL) who is interested in the human factors of cybersecurity as well as the field of industrial-organizational psychology. In 2019, Jade was awarded her Bachelor of Arts in Psychology with Summa Cum Laude honors from Idaho State University. Upon graduation, she completed her second internship under National & Homeland Security (N&HS) and was brought on as a regular hire at INL. Serving as her department's lead researcher, Jade has facilitated projects for N&HS outreach while conducting data analysis on current and upcoming departmental programs.

Dr. Corby Hovis

National Science Foundation

Dr. Corby Hovis is a senior program officer in the Directorate for Education and Human Resources at the National Science Foundation (NSF). He oversees the NSF-wide Research Experiences for Undergraduates (REU) Program; manages the grants focusing on cybersecurity education in the Advanced Technological Education (ATE) Program; and manages grants focusing on physics and astronomy education and interdisciplinary topics in the Improving Undergraduate STEM Education (IUSE) Program.

Speakers

Philip Huff

University of Arkansas at Little Rock

Philip Huff is an Assistant Professor of Computer Science at the University of Arkansas in Little Rock, Director of Cybersecurity Research in the Emerging Analytics Center. He has a 15-year history of working in the electric industry as Director of Critical Infrastructure Security. While at UA Little Rock, he has developed the B.S. in Cybersecurity degree program and serves on the State Board to develop the secondary school cybersecurity curriculum. His research interests include artificial intelligence for cybersecurity operations, and he has co-founded the company Bastazo to commercialize AI advancements in cybersecurity.

James Joshi

National Science Foundation

James Joshi is a Program Director at National Science Foundation's Secure and Trustworthy Cyberspace (SaTC) program. He is also a professor at the School of Computing and Information at the University of Pittsburgh. He is an elected Fellow of the Society of Information Reuse and Integration (SIRI), a Senior member of the IEEE and a Distinguished Member of the ACM. His research interests include access control models, security and privacy of distributed systems, trust management and network security. He is a recipient of the 2006 NSF CAREER award.

Robert Karas

Cybersecurity and Infrastructure Security Agency

Rob Karas came to the Cybersecurity and Infrastructure Security Agency (CISA) in 2010 and has over 28 years in the information security field and experience building nationally recognized penetration testing and security teams. He directs the Cyber Defense Education and Training (CDET) sub-division. In 2017, he was recognized by CyberPatriot as the mentor of the year. Prior to CDET, Mr. Karas stood up the red team, vulnerability scanning and penetration testing services offered at CISA. He worked in the private sector for 12 years developing security operations and penetration testing teams and 5 years at DISA, has a B.S. in Information Management from James Madison University, and maintains a variety of leadership, information assurance and technical certifications.

Meredith Kasper

Hurricane Labs

Meredith Kasper is a full-time Penetration Tester at Hurricane Labs, a managed services provider that helps companies increase their Splunk and security confidence. Meredith also specializes in vulnerability management and purple teaming–which means she utilizes both attacking and defending tactics to assess and improve proactive security posture. With a passion for cybersecurity and a zest for knowledge-sharing, Meredith's industry involvement includes organizations such as The National Cyber League (NCL) as a Lead Player Ambassador, the National Collegiate Penetration Testing Competition (CPTC), and many others.

Dr. 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. in Management Information Systems from the University of Arizona. His interests lie in cybersecurity education, data mining, and application development and he is a principal investigator on several cybersecurity education projects (towson.edu/cyber4all). He is on the ACM/IEEE/AIS/IFIP Joint Task Force on Cybersecurity Education that produced the cybersecurity curricular guidelines (cybered.acm.org). Dr. Kaza's work has been published in top-tier journals and has been funded by the National Science Foundation, National Security Agency, DOD, Intel, and the Maryland Higher Education Commission.

Speakers

Dr. 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 Curriculum Committee. 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, and user-authentication issues. He actively serves as a Board Member and the Education Section Chief of the FBI/InfraGard South-Florida chapter. He is a regularly invited keynote/guest speaker and provides media interviews on cybersecurity topics.

Dr. 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 referred journals and conferences. He is a senior member of IEEE and a member of ACM.

Sandra Leiterman

University of Arkansas at Little Rock

Sandra has over 10 years of experience teaching in STEM Education. She has taught middle school math, science, and engineering as well as university-level pre-service education courses. She currently works as the managing director of the UA Little Rock Cyber Gym, coordinating K-12 and corporate education programs, and recruitment for the Cyber Security degree program. Within STEM education, Sandra has a number of initiatives, including mentoring Girls in STEM, robotics education, education technology integration, internet safety, and project-based instruction in STEM subjects. She has a BS in Middle School Math & Science Education, a graduate certificate in K-12 Gifted Education an MSE in Digital Teaching and Online Learning, and is working on a Ph.D. in Math education.

Xiuwen Liu

Florida State University

Xiuwen Liu is Professor of Computer Science at the Florida State University, Tallahassee, Florida, USA. His main research interests are machine learning, deep learning, program and malware analysis, and cyber security education. He received the Young Investigator Award from the International Neural Network Society in 2004. He develops optimization and modeling techniques for high dimensional data and focuses recently on understanding mechanisms in deep learning. In addition, he has developed and taught software reverse engineering and malware analysis, offensive computer security, and other courses for more than ten years.

Emilio Lorenzo

Nova Southeastern University

Emilio Lorenzo is the Associate Director of Employer Relations at NSU. He graduated with a Master of Science in College Student Affairs with a concentration in Conflict Analysis and Resolution from NSU and a Bachelor of Science in Sociology & International Relations from Florida International University. In his current role, he develops unique ways to have employers and students engage with one another including career fairs, case competitions, networking events, and other innovative programs. He also develops the strategic plan in which to promote employers brand awareness on campus while ensuring students and advisors are up to date on industry trends.

Speakers

Chester (CJ) Maciag

Office of the Under Secretary of Defense, Research and Engineering

Chester (CJ) Maciag has been recognized by OASD (R&E) for outstanding contributions in developing growing collaboration and alignment within the DoD's $500M/yr Cyber Science and Technology portfolio. He conceptualized and helped launch two distinct cyber vulnerability assessment teams. From 1991-2005, Chester authored twelve refereed papers in the fields of IA and information operations, and co-authored a book chapter on live computer forensic techniques (2006). He lead engineered for the first bi-directional TS to Secret email guard for the US Air Force (1992)

Dr. Dan Manson

Cal Poly Pomona

As Commissioner of NCL, Dr. Dan Manson is a passionate advocate for helping students grow in cybersecurity by playing and learning through the NCL games. Dan was co-Principal Investigator on three National Science Foundation grants to support workforce, curriculum and professional development in cybersecurity. Dan holds a Ph.D., Management Information Systems from Claremont Graduate University, a Business, Computer Information Systems degree from California State Polytechnic University, and BA in Fine Arts from the California Institute of the Arts.

Stanley Mierzwa

Kean University

Stan is widely recognized as a leader in digital health technology and Cybersecurity. He is currently the Director, Center for Cybersecurity at Kean University where he also lectures. Previously, Stan worked at the New York Metropolitan Transportation Authority Police as the Lead Application Security. He was also the Director of Information Technology at the Population Council. He has over 12 published research publications, is a peer reviewer for the Online Journal of Public Health Informatics, and is a Certified Information Systems Security Professional (CISSP). He holds an MS in Management of Information Systems from the New Jersey Institute of Technology and a BS in Electrical Engineering Technology from Fairleigh Dickinson University.

Jake Mihevc

Mohawk Valley Community College

Jake serves as Dean of Science, Technology, Engineering and Math at Mohawk Valley Community College. He launched the college's Cybersecurity AS program in 2010 and helped it achieve the Center of Academic Excellence in Cyber Defense designation in 2014. He also serves as the PI of the CAE National Competition project for the NSA/DHS Center of Academic Excellence program. Jake is a co-founder of the Central New York Hackathon, a regional cybersecurity competition that brings over 100 students from eight cybersecurity programs together each semester to test their skills. He is an active member of the National Initiative for Cybersecurity Education Workgroup and has worked to expand cybersecurity competitions nationwide.

Stephen Miller

Eastern New Mexico University – Ruidoso

Mr. Miller is a Tenured Professor/Director/Co-PI National Cybersecurity Training and Education Center Information Systems/Cyber Security Center of Excellence Eastern New Mexico University – Ruidoso CAE-2Y. He is retired from ExxonMobil. A highlight of his career as member of the NASA Mission Control on the APOLLO Missions. He serves on many grants, committees, boards, and projects like National Cybersecurity Training and Education Center (NCyTE) Co-PI where he developed Industry Academic relationships and projects.

Speakers

Dr. Loyce Pailen

University of Maryland Global Campus

Dr. Loyce Best Pailen has more than 35 years of experience in information technology. She is currently the Sr. Director for the Center for Security Studies at UMGC, overseeing the university's DHS/CAE activities and PI for several grants. She has held director-level information technology positions at the Washington Post, Graham Holdings, and UMUC. Pailen has also provided project leadership as an Associate Provost for instructional design and subject-matter expertise for the development of major graduate, undergraduate, and community college cybersecurity curriculum development projects. Pailen is the author of a fun and enlightening series of children's books regarding cybersecurity, use of emerging technology and safety in the digital environment.

Franz Payer

Cyber Skyline

Franz Payer is the CEO of Cyber Skyline, the cloud-based platform and content provider that powers the NCL competition and games. Founded in 2014, Cyber Skyline has helped more than 100,000 students and professionals through cybersecurity competitions, candidate skills assessments, and professional development opportunities. He started his cybersecurity career as a Computer Network Operations (CNO) Software Developer and was a speaker at DEFCON 21, presenting his research on bypassing modern Digital Rights Management (DRM) security. Franz holds a BS in Computer Science from University of Maryland College Park.

Rodney Petersen

National Initiative for Cybersecurity Education

Rodney Petersen is the director of the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST). He previously served as the Managing Director and Senior Government Relations Officer in the EDUCAUSE Washington Office. He founded and directed the EDUCAUSE Cybersecurity Initiative. Previously, he worked for the University of Maryland as the Director of IT Policy and Planning. He also served as an instructor for AmeriCorps' National Civilian Community Corps. He co-edited "Computer and Network Security in Higher Education." He received his law degree from Wake Forest University and bachelors degrees in political science and business administration from Alma College. He has an Advanced Graduate Specialist in Education Policy, Planning, and Administration Certificate from the University of Maryland.

Tony Pinson

University of Memphis

A graduate of the University of Memphis, I have earned a master degree in mechanical engineering, business administration, and information systems. I'm also a licensed professional mechanical engineer and have worked for roughly 26 years in the gas utility industry. Currently, I am employed as the project coordinator for the University of Memphis Center for Information Assurance as I continue my educational interest in information technology and cybersecurity.

Dr. Victor Piotrowski

National Science Foundation

Dr. Victor Piotrowski is a Lead Program Director at the National Science Foundation (NSF), overseeing $55 million CyberCorps® SFS program, and a Program Officer in the NSF-wide Secure and Trustworthy Cyberspace (SaTC) program. He is a graduate of the Federal Executive Institute and the Harvard Kennedy School Cybersecurity Policy and Technology program. He is also a recipient of the 2015 Founder's Award by the CISSE Colloquium. In 2017, he worked as a U.S. Embassy Science Fellow in Cybersecurity in Baltic and Nordic countries.

Speakers

Dr. James Robertson

Program Director Cyber DevOps

Dr. Robertson has over twenty-five years of technical, engineering, and information systems experience in the areas of software security, cloud computing, data analysis and machine learning, software and database design and development, and modeling and simulation. He has over fifteen years of experience managing, teaching and designing courses within the Computer Science and Software Development and Security Programs for a University system. Research interests include machine learning, artificial intelligence, and secure programming in the cloud. He has authored/co-authored publications on signal and image processing, cloud computing and security. He holds Bachelor's and Master's degrees in Electro-Optical Engineering from University of Houston-Clear Lake and University of Dayton, and an Ed.D in Instructional Technology from Towson University.

Corrinne Sande

Whatcom Community College

Whatcom Community College's Director of Computer Science and Information Systems, Corrinne Sande is the director of the National Cybersecurity Resource Center funded by the NSA, and Principal Investigator for the National Cybersecurity Training & Education Center (NCyTE), a NSF–funded ATE center that works to grow and strengthen the nation's cybersecurity workforce. Ms. Sande also serves as a Co-Principal Investigator of Catalyzing Computing and Cybersecurity in Community Colleges (C5).

Dr. Ronald (Ron) Sanders

University of South Florida

Dr. Ronald (Ron) Sanders is the Staff Director for the Florida Center for Cybersecurity. He manages its staff under the leadership of the Center's Executive Director, former Director of National Intelligence J. Michael 'Mike' McConnell (VADM USN-retired). Dr. Sanders serves on the Advisory Board of the National Security Agency. From 2017 to 2020, Dr. Sanders chaired the US Federal Salary and served as Director and Clinical Professor for USF's School of Public Affairs. He led the reaccreditation of the School's flagship MPA program. Previously, he was a Vice President of Booz Allen Hamilton, where he led its human capital and wargaming practices. He was also part of the National Academy of Sciences Cybersecurity Panel and co-authored its landmark 2014 assessment of the nation's cybersecurity workforce.

Dr. Derek Sedlack

Colorado Technical University

Dr. Derek Sedlack transitioned to higher education after 20+ years direct experience with Fortune 100 companies like IBM, Dell, HP, and Citrix, and consulting interactions with AT&T, 3Com, Pratt & Whitney, Xerox, and Harris Corp in systems engineering positions through the executive board. His U.S. awarded patents are process related and reflect his organizational approach toward information security as a holistic endeavor. Dr. Sedlack defended his Ph.D. in Information Systems at Nova Southeastern University where also earned a M.Sc. in Management Information Systems. His Cybersecurity research has appeared in AMCIS, SAIC, Decision Science and international conference.

Dr. Nigamanth Sridhar

Program Officer, National Science Foundation

Dr. Nigamanth Sridhar is a program officer in the Division of Graduate Education in the Education and Human Resources Directorate at the National Science Foundation. He works on programs for cybersecurity education and workforce development and is associated with the CyberCorps Scholarships for Service (SFS) and Secure and Trustworthy Cyberspace programs. He is on an IPA appointment from Cleveland State University, where he holds a faculty appointment in computer science at the Washkewicz College of Engineering. Research interests include software engineering, programming languages, connected devices, and computer science education. He was the Dean of the College of Graduate Studies at CSU from 2017 – 2020. Dr. Sridhar holds MS and PhD degrees in Computer Science from The Ohio State University and a bachelor's degree in Information Systems from BITS Pilani in India.

Speakers

Dr. Shane D. Stailey

Senior Industrial Control Systems Cybersecurity Professional

Shane Stailey is a Senior Industrial Control Systems Cybersecurity Professional with three decades of success in learning, teaching, broadening, and applying information across multiple business streams with a spectrum of technical variety. Shane specializes in combining creative thinking, outside the box analysis, and practitioner level application to solve real world problems. As a 1st generation Master's and Doctoral level educated professional he is well aware of the value that can come from merging 'pure work,' 'consistent learning,' and 'determined perseverance,' despite life's adversities, to reach professional and personal goals and accomplishments.

Dr. Blair Taylor

Towson University

Dr. Blair Taylor is an Associate Professor in the Department of Computer and Information Sciences at Towson University. She worked with the College of Cyber at the National Security Agency on the National Cybersecurity Curriculum Program, hosted on www.clark.center. Other projects include: Security Injections @ Towson (www.towson.edu/securityinjections), which includes security modules for integrating security across the undergraduate computing curriculum and SPLASH (www.towson.edu/splash) which offers Secure Programming Logic for college credit to high school girls. Dr. Taylor has received the Fisher College of Science and Mathematics Outstanding Faculty Award and the University System of Maryland Regents award for Teaching.

Dr. 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 15 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.

Dr. Cliff Wang

North Carolina State University

Dr. Cliff Wang graduated from North Carolina State University with a PhD in computer engineering in 1996. He has done research on computer vision, medical imaging, high speed networks, and information security, and authored 60 technical papers and 3 Internet standards RFCs. Dr. Wang authored/edited 19 books on information security and holds 4 US patents on information security system development. Since 2003, he has managed extramural research portfolio on information assurance at US Army Research Office. In 2007, he was selected as the director of the computing sciences division at ARO. For the past ten years, Dr. Wang managed over $250M research funding which led to significant technology breakthroughs. He is an adjunct professor in the Department of Computer Science and the Department of Electrical and Computer Engineering at North Carolina State University.

Karen Wetzel

National Initiative for Cybersecurity Education

Karen Wetzel joined the National Initiative for Cybersecurity Education (NICE) as Manager of the NICE Framework in October 2020. As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. Karen specializes in identifying, communicating, and developing guidance around key issues, emerging trends, and opportunities of special interest. Prior to joining NICE, Karen was Director of the Community Groups and Working Groups programs at EDUCAUSE and served as Standards Program Manager for the National Information Standards Organization (NISO).

Speakers

Susanne Wetzel

Stevens Institute of Technology

I am an Associate Professor at the Computer Science Department of the Stevens Institute of Technology. I first joined the faculty at Stevens as Assistant Professor in 2002. I received my Diplom in Computer Science from the University in Karlsruhe (Germany) and my Ph.D degree in Computer Science from Saarland University (Germany) in 1998. Subsequently, I worked at DaimlerChrysler Research (Stuttgart, Germany), Lucent Technologies Bell Laboratories (Murray Hill, USA) and RSA Laboratories (Stockholm, Sweden).

Meghyn Winslow

Northern Kentucky University

Meg Winslow is currently an IT-Cybersecurity track junior at Northern Kentucky University (NKU), and the President of the NKU WiCyS student-chapter. She is a teaching assistant in the NKU Computer Science (CS) Department, and is a research assistant of Dr. Ankur Chattopadhyay. She has been teaching K-12 students for the past 5 years. A life-long love of technology and people drives her current pursuits, which includes design & development of age-appropriate & skill-based curriculum for K-12 learners and non-technical employees. As a WiCyS student leader, she is actively involved in STEM (including cybersecurity) outreach & training sessions with underserved populations.

Ron Woerner

Bellevue University

Ron Woerner, CISSP, CISM is a noted consultant, speaker and writer in the security industry. Ron established the Cybersecurity Studies program at Bellevue University, an NSA CAE-CDE where he still teaches. He has been a featured speaker for TED, (ISC)2, ISACA, and RSA conferences and numerous industry podcasts and webinars. As President and Chief Security Evangelist at Cyber-AAA (https://www.cyber-aaa.com/), he works as a Security Consultant delivering awareness, performing security risk assessments and advising small, medium, and large organizations. Ron has numerous technology degrees and is passionate about building the next generation of cyber professionals. LinkedIn: https://www.linkedin.com/in/ronwoerner/

Li Yang

National Science Foundation

Li Yang is Program Director at National Science Foundation. She is also a Guerry Professor and the Director of UTC Information Security (InfoSec) Center, a National Center of Academic Excellence in Information Assurance/Cyber Defense (CAE-IA/CD). Her research interests include secure and trustworthy Artificial Intelligence (AI), web security, intrusion detection, mobile security, big data analytics, cybersecurity education, and engineering techniques for complex software system design. She actively involves students into her research. She authored papers on these areas in refereed journal, conferences, and symposiums. She received her Ph.D. in Computer Science from Florida International University.

Presentations

Thursday 11-19 Presentation Abstracts

NCAE-C Strategic Planning Overview

Lynne Clark, Deputy Chief, Center for Cybersecurity Education, Innovation and Outreach, A29

Ms. Clark will provide an overview of NCAE-C Strategic Planning, and the upcoming Community meeting on Strategy on 15 December. Despite COVID, there has been significant growth in 2020, and the program continues to enjoy support from Congress, while concern for the future of the cybersecurity workforce in the United States continues to grow. Before the Program Office commits the NCAE-Cs to a strategic path for the next five years, there is a commitment to garnering input from the members of the CAE Community.

CISA Update

Robert Karas, Associate Director, Cyber Defense Education and Training

Rob Karas will provide a brief introduction to the Cybersecurity and Infrastructure Security Agency (CISA), a co-sponsor of the CAE-C program. Rob is the Associate Director of the Cybersecurity Defense Education and Training (CDET) subdivision of CISA. With CDET, CISA is establishing a model that seeks to strengthen our current cybersecurity workforce and pipeline, as well as cultivate a non-traditional cybersecurity workforce to help reduce the national cybersecurity workforce shortage. He will speak about his vision as the leader of this exciting new subdivision, how CISA's programs and initiatives intersect with the mission of the CAE program, and the benefits that will affect the CAE community for years to come.

NSF Update

Dr. Nigamanth Sridhar, Program Officer in the Division of Graduate Education in the Education and Human Resources Directorate at the National Science Foundation

Dr. Corby Hovis, Senior Program Officer in the Directorate for Education and Human Resources at the National Science Foundation

Dr. Victor Piotrowski, Lead Program Director at the National Science Foundation

Li Yang, Program Director at the National Science Foundation

NSF update on cybersecurity education and workforce development initiatives at NSF, as well as cover programs of CyberCorps SFS, Security and Trustworthy Cyberspace (SaTC), and Advanced Technology Education (ATE).

Presentations

CAE-R Presentation Abstracts

INSuRE Q&A

Agnes Chan
Suzanne Wetzel, Associate Professor at the Computer Science Department of the Stevens Institute of Technology

INSuRE (Information Security Research and Education) has been an important activity within the CAE-R community, yet it remains unknown to many institutions. In this talk, we will present the history of the program, its evolution and its current state. We will discuss the values and the challenges INSuRE faces and its future directions.

Research opportunities at the Army Cyber Institute and The United States Military Academy at West Point

Dr. Lubjana Beshaj, Assistant Professor in the Department of Mathematical Sciences at West Point

The Army Cyber Institute (ACI) is a national resource for interdisciplinary research, advice and education in the cyber domain, engaging DoD, Army, Government, academic and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective army cyber defense and cyber operations. The ACI focuses on exploring the challenges facing the Army (and likewise the Nation) within the cyber domain in the next 3-10 years. Using our multi-disciplinary, mission focused team of professionals as well as leveraging the United States Military Academy faculty and our various partners, we expand the body of knowledge and advise senior military and government officials. Our vision is to develop intellectual capital and impactful partnerships that enable the nation to outmaneuver our adversaries in cyberspace.

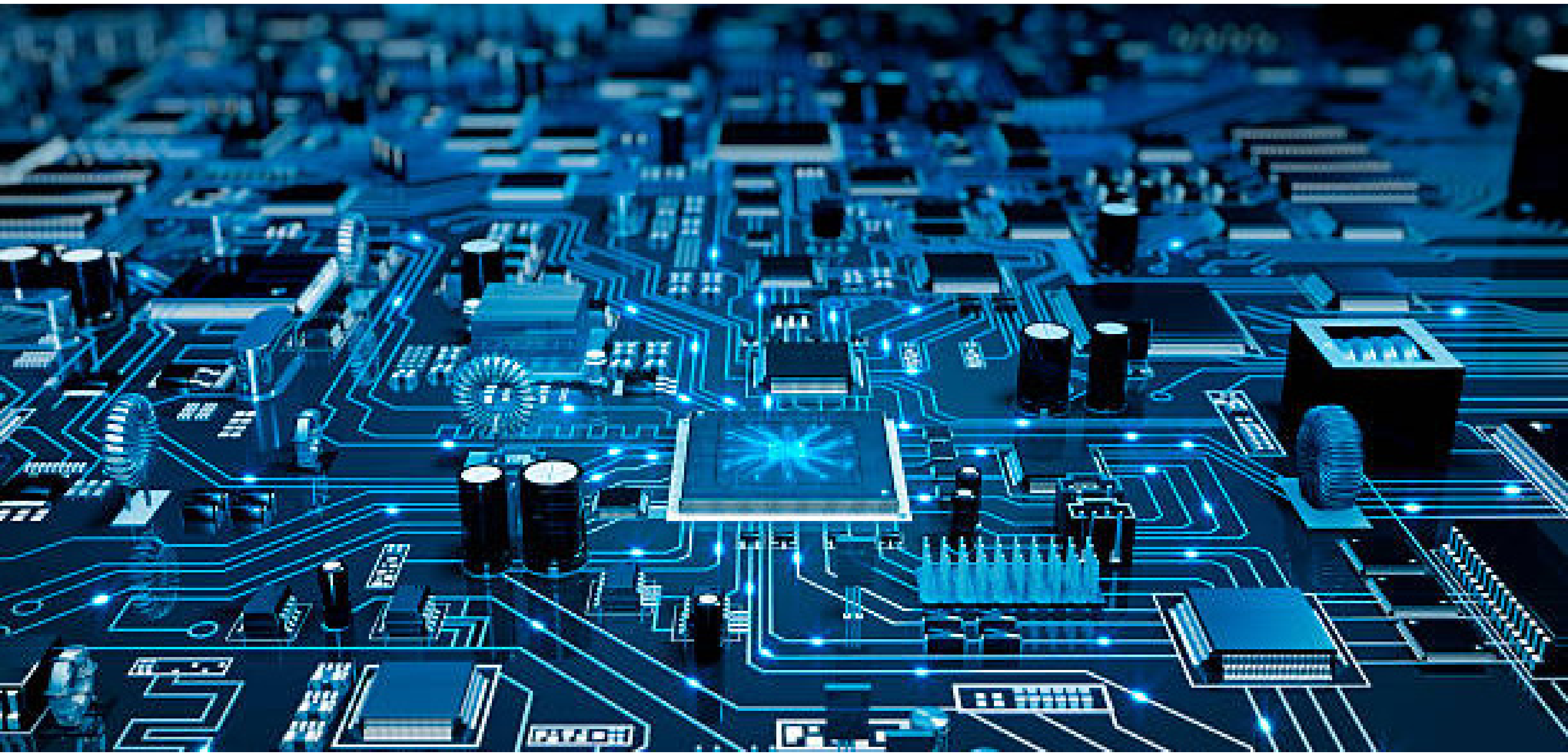
Presentations

Secure and Trustworthy Cyberspace Program and Federal Cybersecurity R&D Priorities

Dr. Victor Piotrowski, Lead Program Director at the National Science Foundation

James Joshi, Program Director at National Science Foundation's Secure and Trustworthy Cyberspace (SaTC) program

The Army Cyber Institute (ACI) is a national resource for interdisciplinary research, advice and education in the cyber domain, engaging DoD, Army, Government, academic and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective army cyber defense and cyber operations. The ACI focuses on exploring the challenges facing the Army (and likewise the Nation) within the cyber domain in the next 3-10 years. Using our multi-disciplinary, mission focused team of professionals as well as leveraging the United States Military Academy faculty and our various partners, we expand the body of knowledge and advise senior military and government officials. Our vision is to develop intellectual capital and impactful partnerships that enable the nation to outmaneuver our adversaries in cyberspace.



Presentations

CAE-CD Track #1 Presentation Abstracts

NCL CyberMetrics – Measuring Student Proficiencies to Launch the Cybersecurity Careers

Dr. Dan Manson, Emeritus Professor, Computer Information Systems, Cal Poly Pomona

Kaitlyn Bestenheider, Information Security Analyst

Franz Payer, CEO of Cyber Skyline

Meredith Kasper, Penetration Tester

With many “entry-level” positions in the cybersecurity industry requiring 3-5 years of experience, numerous students and recent graduates find themselves at a loss on how to launch their careers in this field with an ever-growing need for professionals. The question becomes, “How can students take their knowledge from curriculum to career?”

The National Cyber League (NCL) does just that in a way that makes learning feel like playing. The NCL vision is to provide an ongoing virtual training ground for students to develop, practice, and validate their cybersecurity knowledge and skills using next-generation, high-fidelity simulation environments, based on industry-relevant learning objectives. This offensive and defensive cybersecurity capture-the-flag (CTF) game is based on the CompTIA Security+ and maps to the NIST NICE Framework and NSA CAE Knowledge Units so that the comprehensive, individualized Scouting Reports each player receives provides metrics that matter!

Join this panel led by NCL Assistant Chief Player Ambassador, Kaitlyn “CryptoKait” Bestenheider, and supported by NCL Commissioner, Dan Manson, NCL Lead Player Ambassador and professional penetration tester, Meredith Kasper, and the NCL Game Maker from Cyber Skyline, Franz Payer. The panel will discuss the importance of creating on-ramps for students to launch their cybersecurity careers, the NCL integration with CAE Knowledge Units, and how NCL supports schools CAE accreditations.

Presentations

Trustworthy: When Humans and Bots Are Mingled

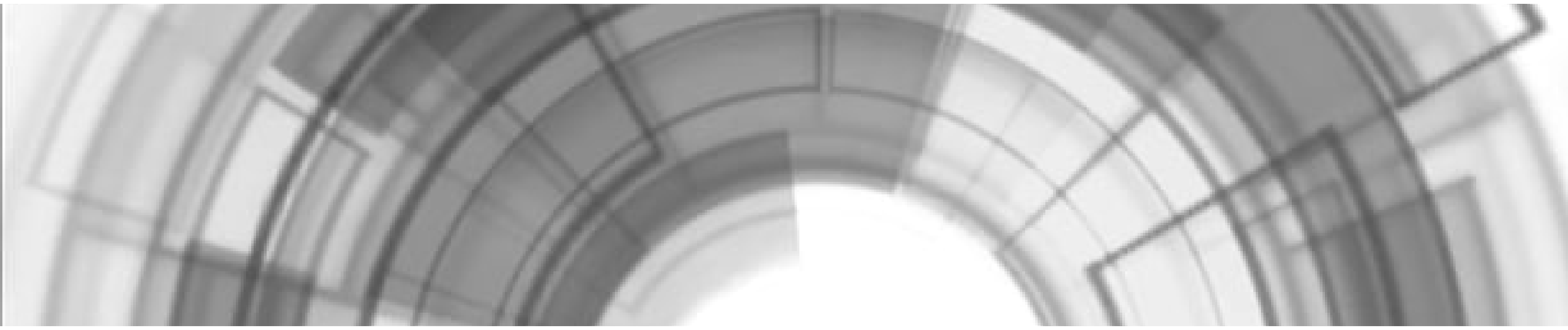
Zhixiong Chen, Professor and Director of the Cyber Education Center, Mercy College

This presentation is about to identify conversational bots using blockchain technology, a first step to address trustworthy challenging when social media applications are mixed with human users and social bots. Internet persona or account user profile for social bots usually is hardly being used to distinguish conversational bots from other human users. PASS (Personal Archive Service System) using blockchain technology has built in the Proof of X mechanism. The usage of such built in feature into bot identification makes users aware of bot interaction which could mitigate the threat of disinformation by social bots. Moreover, in practice, we add feedback bot score, called syn points stored in the chain during the process of registration, verification and lifecycle monitoring.

Cybersecurity Assessments in Global Public Health Involving Technology

Stanley Mierzwa, Director, Center for Cybersecurity at Kean University

Over the last decade, many public health research efforts have included information technologies such as Mobile Health (mHealth), Electronic Health (eHealth), Telehealth, and Digital Health to assist with unmet global development health needs. This presentation provides a background on the lack of documentation on cybersecurity risks or vulnerability assessments in global public health areas. This presentation suggests existing frameworks and policies be adopted for public health. We also propose to incorporate a simple assessment toolbox and a research paper section intended to help minimize cybersecurity and information security risks for public, non-profit, and healthcare organizations. - Further slides will be provided prior to the event to be shared.



Presentations

Social Engineer your Students Before they Social Engineer You: Teaching Human Hacking in a CAE Curriculum

Ron Woerner, Technology Instructor

Karla Carter, Associate Professor

As long as we have people, social engineering is a threat. Hacking the human element has only gotten worse with most people working, playing and communicating online. With its prominence, shouldn't this be a part of all cyber defense and operations curriculum?

In this session, you will learn techniques for teaching it either as its own class or within other classes. Everyone in security needs to understand human weaknesses and the best ways to protect and defend against human threats and vulnerabilities. Attendees will learn the importance of human factors, psychology, and leadership for security professionals. The session leaders will show how security controls may be bypassed by a person's intentional or unintentional acts and methods for reducing the cyber risks associated with human error and social engineering. Attendees will leave with a firm grasp of social engineering techniques and how the laws of influence can be used to breach security controls. The techniques discussed here are taken from books such as, "Influence, The Art of Persuasion", "How to Win Friends and Influence People," and "Social Engineering, The Science of Human Hacking." The objective isn't to make attendees paranoid, but aware of their surroundings and how they may be vulnerable to the power of human hacking.

Learn how social engineering and human hacking is incorporated into a cybersecurity curriculum as one of its most popular classes. All cyber instructors need to learn how to social engineer their students before they social engineer you.

Cyber Gym: Open-source Security Labs in the Google Cloud

Philip Huff, Director of Cybersecurity Research, University of Arkansas in Little Rock

Sandra Leiterman, Managing Director of the UA Little Rock Cyber Gym

The open-source cyber gym provides a hands-on Google cloud learning environment flexible for both instructors and students. Instructors have access to custom-built workouts mapped to skills in the NICE Framework and Security+ Standards or instructors can create their own workouts. When ready, an instructor initiates a system build for the number of students or teams in their class. From here students have access to independently control their workout both in the class and outside of the class.

This session will explore the experience in deploying this technology to over 500 students in the state of Arkansas and show the cloud costs for various workouts. We will also walk participant through the setup and live build from the viewpoint of the instructor and demonstrate the automated assessment reported back to the instructor. This material is based upon work supported by the National Science Foundation under Grant No. 1623628. The project is available at https://github.com/emerginganalytics/ualr-cyber-gym.

Escape The Breakout Room: A Set of Cybersecurity Challenges-Based Educational Game

Ankur Chattopadhyay, Assistant Professor of CS and Cybersecurity

Meghyn Winslow, Cybersecurity Student, Northern Kentucky University

Existing literature show that Escape The Room themed games have not been used much in cybersecurity education and outreach. In this fast pitch talk, we will present an original Escape The Room themed cybersecurity educational game, which consists of a set of nifty cybersecurity challenges in the form of beginner's puzzles on a variety of introductory cybersecurity topics, including cryptographic ciphers, social engineering-based phishing attacks, online fake web certificates, and ransomware attacks. We have specifically developed this cyber educational game as an experiential learning activity that is driven by realistic scenario-based cybersecurity challenges, and can be played in teams. We have successfully implemented this game as a team learning exercise that can be offered in a virtual learning setting. We will share our experience (including lessons learned and takeaways) of hosting this game as part of a virtual cybersecurity educational summer camp for a high school audience, where remote learners participated in this game in "Breakout Room" teams within a Zoom meeting session. Our presentation will include an overview of this novel "Escape The Breakout Room" game, and a discussion on hosting this game over Zoom as part of a virtual cybersecurity education camp, or a virtual introductory cybersecurity class. Under the current COVID-19 pandemic situation, when cybersecurity education is going virtual, this new instance of an Escape The Room themed cybersecurity educational game and its experiential team learning approach would be of interest & relevance to the CAE community, including all cybersecurity educators, who are particularly looking for engaging, competitive virtual learning activities at a beginner's level.

Presentations

Cyber Ethics, Career Development, and Professional Curriculum

Stephen Miller, Professor/Director Cybersecurity Center of Excellence

This Fastpitch covers Eastern New Mexico University-Ruidoso IS258 Cyber Ethics, Career Development, and Professional course curriculum developed and endorsed jointly by an advisory team from ExxonMobil, DOD U.S. Navy, Academia, New Mexico Workforce Development. The rationale for student taking this course was to provide students with the necessary understanding and abilities to apply ethics in the cyber world. This course prepares students to apply cyber ethics in the workplace and in furthering their careers.

Lessons Learned in Starting a B.S. in Cybersecurity During COVID-19 Pandemic

Mark Thompson, Senior Lecturer, University of North Texas

Ram Dantu

UNT's new B.S. in Cybersecurity was formally approved by the Texas Higher Education Coordinating Board (THECB) in March 2020 with an implementation date starting in the Fall 2020 semester. Given the rapidly changing and often unchartered environment that cybersecurity operates in, the B.S. in Cybersecurity was created to provide a high quality, academically challenging, and career-enriching educational program that is responsive to industry trends, changing standards, and employer needs. Approved only a few months before the program launch, we will discuss the lessons learned in the design and implementation of this new, high demand interdisciplinary degree program. In particular, we would like to share the technical, logistic, and marketing opportunities and challenges that we faced during this past year as we worked to get our new program off the ground, especially as we were met with further obstacles of social distancing and remote learning requirements due to COVID-19.

Presentations

Offering Continuing Education Credits in Cybersecurity for First Responders

Ram Dantu

Mark Thompson, Senior Lecturer, University of North Texas

As we become a more digital society, it imperative that first responders, including EMS and law enforcement, become well-versed in the role that technology plays in their field and understand the security implications demanded in this changing environment. Most existing continuing education (CE) credits, however, are only offered specifically for technical job requirements, such as de-escalation techniques and airway management training for law enforcement and EMS certified personnel, respectively. We propose offering CE credits in cybersecurity and forensics for first responders, working with the applicable agencies such as the Texas Commission on Law Enforcement (TCOLE) and the National Registry of Emergency Medical Technicians (NREMT) for approval. The training modules for EMS personnel would, for example, include hands-on experiments focusing on securing first responder operations, devices, and privacy such as securing mobile applications and sharing emergency information via mobile devices and HIPAA-compliant confidentiality protection of patient data such as vital signs (e.g., blood pressure, heart rate, respiration rate, blood oxygen). We will discuss our novel interdisciplinary training approach and then review the process from creating our curriculum to getting approval from the appropriate agencies.

The UofM Center for Information Assurance

Tony Pinson, Project Coordinator, Center for Information Assurance, University of Memphis

A brief summary of the educational, research, and community outreach activities conducted by The University of Memphis Center for Information Assurance.

Presentations

CAE-CD Track #2 Presentation Abstracts

The CAE National Competition- Overview and Collaboration Opportunity

Jake Mihevc, Dean, Science, Technology, Engineering, and Math

Ron Sanders, Staff Director for the Florida Center for Cybersecurity

The first CAE National Competition will be held throughout the 2021-2022 academic year and is designed to increase student and faculty engagement with competitions throughout the CAE program. The competition is oriented towards students who are new to cybersecurity competitions, and will include an extensive training and practice environment, regional competitions, and the National Finals to be held at the 2022 CAE Executive Leadership Forum. The challenges within the competition will be CAE-sourced to allow each of the unique facets of cybersecurity education to be components of the competition. This presentation will provide an overview of the project as well as the challenge submission and compensation framework that encourages CAE faculty to collaborate and contribute to the project.

A CAE-CDE Planning for CAE-CO Designation: Curriculum Design and Content Considerations

James Robertson, Program Director Cyber DevOps

Loyce Pailen, Sr. Director for the Center for Security Studies at UMGC

The University of Maryland Global Campus (UMGC) is developing a robust graduate degree program in Cyber Operations (CO). The program was designed from the beginning to ultimately obtain an NSA/DHS CAE-CO designation. With this in mind, the subject matter experts and curriculum designers focused on the required knowledge units and built in the artifacts to meet other CAE criterion like explicit focus on CO, integration of CO into the foundational courses, and content currency. This session will also review the faculty and student involvement as well as research concerns required for the designation and how the institution approached these concerns. While the UMGC program has not yet been designated as a CAE-CO, this session is valuable to those who are considering a program and for those who may face re-designation hurdles.

Presentations

Got Curriculum? Donate to CLARK's Plan C

Blair Taylor, Professor, Towson University

Sidd Kaza, Chairperson of the Department of Computer and Information Sciences at Towson University

Covid-19 has created tremendous challenges for academia. Last spring, faculty across the U.S. moved suddenly and completely to virtual teaching. This fall, as many of us continue to teach primarily online, we are developing quality resources, including videos and other materials that facilitate learning in this new environment.

As a result of the pandemic, the role of the CAE community is more important than ever. Cyber attacks have increased, as hackers are exploiting the new vulnerabilities posed by the massive migration to work-from-home across all industries.

CLARK, funded by NSA (grant# H9830-17-1-0405), hosts over 750 free cybersecurity learning objects under the creative commons non-commercial license. CLARK's Plan C is an opportunity to gather cybersecurity resources developed during these trying times and expedite publication on the CLARK (www.clark.center) platform.

During this workshop, the CLARK team will work with faculty to upload their curriculum content to the Plan C collection, fine-tune their learning outcomes with the "Blooming Onion" app, and map to CAE knowledge units. By contributing curriculum, the CAE community can help faculty across the country teach cyber in their online classes. Participants will receive a small stipend for each contribution.

Integrating NICE Cybersecurity Workforce Framework (NCWF) to University Career Services

Dr. Yair Levy, Professor of Cybersecurity and Director of CIPhER

The use of NICE Cybersecurity Workforce Framework (NCWF) is critically important to ensure consistency across cybersecurity jobs in government, industry, and academia. Nova Southeastern University (NSU) has been a leader in cybersecurity education for many years and was among the first in the state of Florida to receive CAE designation. NSU received the initial CAE designation in March 2005 and received CAE re-designation in 2009 and 2014. Over the past several months the faculty and staff of College of Computing and Engineering (CCE) at NSU has been working with the NSU Career Development Office (CDO) staff (https://www.nova.edu/career/) on the integration of the NCWF into the student advising process. The CAE 2020 Fastpitch presentation provides an overview of the collaboration model between the CCE and CDO at NSU that includes exposure of the framework to the career advisors, the relevant job roles for the NSA/DHS designated cybersecurity programs offered by the CCE, the creation of a Career Development Newsletter specifically for computer science and engineering students, as well as the development of sample student resumes specifically aligned with the NSA/DHS designated NSU cybersecurity programs.

Presentations

An Evaluation of Cybersecurity Students' Needs for Program Improvement

Waleed Farag, Professor of Computer Science at Indiana University of Pennsylvania

This proposal discusses the findings of an interesting research study with the objective of identifying writing and communication challenges faced by both cybersecurity students and professionals in the field and proposing effective solutions to address these challenges. This research study was part of a comprehensive project (funded by the NSA) intended to enhance cybersecurity education in western PA. To achieve the project's objectives, we designed and conducted a QUAN-QUAL mixed-method study which collected survey data from students enrolled at two US-based institutions, and interview data from 27 professionals working in the cybersecurity field within the US and elsewhere. This proposal discusses results related to the quantitative component of our research while briefly commenting on the related findings of the qualitative component. To better understand the backgrounds and needs of the study participants, and attempt to capture various challenges they face in the area of communication skills, the employed quantitative instrument was designed to primarily address the following two research questions: • Which courses did aspiring cybersecurity professionals identify as valuable? Are there group differences? • How did undergraduate students describe their present attitudes and skill level in terms of writing and oral communication? This presentation will expound our research findings including an identified gap of high school courses that prepare students to succeed in the field, and differences in perception of the importance of writing and communication skills among various student groups. The presentation will also provide recommendations and lessons learned from implementing an effective educational service to address the identified challenges.

Hackers Wanted: Building towards IT, MIS, and Cybersecurity Careers

Ron Woerner, Technology Professor, Bellevue University

The ultimate goal of an educator is to build students towards a successful career outside the classroom. The top careers today focus on technology, from software development to IT management to cybersecurity, yet businesses often struggle to find qualified people to fill these positions. This session provides actionable solutions for teachers and school administrators for teaching critical computing, cybersecurity, and technical troubleshooting skills. The presenter will share tips, tools, and techniques for building our next generation of cyber experts in ways that build critical technology skills while remaining fun and accessible to all students. He will share ideas for getting technology into the classroom, finding mentors to help with instruction, and engaging students to learn through cyber clubs, camps, and competitions. One of the biggest challenges is influencing students to enter fields that lead to technology careers. He does this by hacking; not the evil kind, but the type defined in the Hacker Dictionary as “one who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.” The techniques discussed in this session allow students to use their native curiosity to better and more safely use the technology around them. This session also covers teaching cyber safety, security, and ethics. Successful careers all start in our schools. Join me in building the next generation of cyber employees to solve the technical problems of today and tomorrow. This session is based on the TED talk, “Hackers Wanted.” https://www.ted.com/talks/ron_woerner_hackers_wanted

Designed Support for Student Research Avenues

Dr. Derek Sedlack, Associate Professor, Colorado Technical University

We propose a designed growth path for emerging researchers that does not currently exist. When Ph.D.’s defend, it is expected that their directed training and research focus will provide clear direction for impactful future work, but that assumption has not been realized. We propose an entry path for graduate students to better understand and contribute to research and administration publication functions that should enhance their academic prospects and help them add to scientific solutions business desperately needs.

Presentations

CAE-CD Track #3 Presentation Abstracts

Teaching Cybersecurity as Risk Management

Maeve Dion, Assistant Professor, University of New Hampshire

Cybersecurity requires technical expertise to create, implement, and maintain the security and resilience of our infrastructure and data. However, cybersecurity also requires organizational and behavioral expertise to manage the risks arising from misaligned policy and practices. NIST has emphasized such matters in the evolution of its guidance on managing cyber risks and integrating cybersecurity with enterprise risk management (ERM). Further, it is important to educate our students for employment with small and mid-sized businesses, not just in large agencies and organizations with existing know-how and resources for ERM. U.S. businesses are primarily small and mid-sized organizations with less in-house expertise in ERM and cybersecurity. These businesses are just as reliant on technology and thus should also be managing their cyber risks; we need to be educating our students on how to integrate cybersecurity with risk management for all types and sizes of organizations. How do we teach the risk management aspects of cybersecurity? One approach is to have a specialized class for our STEM cybersecurity programs. Another approach is to create a program focused on how to bring cybersecurity concepts into the operational management and risk management of organizations. This presentation gives an overview of teaching policy and risk management for cybersecurity and offers some best practices. Some common challenges are addressed, as well as a few solutions and ongoing struggles. This presentation also suggests how organizational policy and risk management can be woven into a variety of classes.

Self-regulated, Deep Learning with NIST Documents in HiEd

Maeve Dion, Assistant Professor, University of New Hampshire

Cybersecurity professionals must remain aware and up to date in dynamic situations and environments. The professions demand lifelong learners who can efficiently and effectively troubleshoot new situations and customize solutions that improve our resilience and agility. NIST standards and guidance documents range from broad, big-picture overviews to extensively detailed criteria. These documents are academically authoritative and practicable (encouraging learning based on professional requirements), but how can we integrate NIST documents into our curricula so as to foster lifelong learning skills? In Higher Education, especially in cases of online or remote learning, skills for self-regulated learning are critically important. Self-regulated learning can promote more effective and efficient study skills and encourage study strategies that last long beyond the degree completion. Similarly, we know that certain kinds of learning activities can support deep learning and the enhancement of higher-level cognitive skills such as critical examination, synthesis, and evaluation. Prof. Maeve Dion shares examples of how an aligned teaching approach and learning activities can support our students' engagement with NIST documents while enhancing self-regulated learning and higher-level cognitive skills. Ideally, our cybersecurity graduates should know not only how to apply these documents in a variety of circumstances, but also how to critically analyze, customize, and improve on these guidance documents for the betterment of employer organizations and also for contributions back into our cybersecurity communities of interest.

Industrial Cybersecurity Training and Education Standards - Getting the Water to the End of the Row with CYBER-CHAMP

Jade Hott

Dr. Shane D. Stailey, DCS-IA, Senior Industrial Control Systems Cybersecurity Professional

Donaven Haderlie, Business Specialist

Gary M. Deckard, PhD, MBA, CISSP, PMP, Industrial Control System Cybersecurity Professional

There is a pervasive talent deficit in cybersecurity that prevents employers from being able to find qualified job applicants. In a recent survey of cybersecurity professionals, most report that their teams are at least somewhat understaffed with open positions remaining unfilled. Many tools are available to bridge the educational gap for the cybersecurity workforce, but these tools do not take a holistic approach to security by addressing both operational technology (OT) and information technology (IT). With the recent convergence of IT and OT systems, vulnerabilities that were previously limited to IT have been introduced into the industrial environment. Therefore, it is vital to integrate industrial security concepts into current and future cybersecurity curriculum offerings. During this workshop, participants will learn about the CYBER security – Competency Health and Maturity Progression (CYBER-CHAMP©) model. CYBER-CHAMP was initially created as a tool for organizations to understand the security competency gaps in their workforce, but the model can also be utilized to inform academia and cybersecurity training providers. The model offers a methodology to increase security across an organization, which includes all work roles within a company and the best practices employees are expected to perform. Once these target roles are identified, the roles can be mapped to education and training options by identifying the everyday tasks an individual performs. This same mapping method can be used to reverse-engineer the education and training offerings that can be provided for students, the current workforce, veterans, and individuals in other disciplines who are interested in growing their knowledge of cybersecurity.

Presentations

Improving Cyber Security by Engaging Software Developers via Universally Applicable Security Gems

Xiuwen Liu, Professor, Florida State University

Mike Burmester, Professor of Computer Science at the Florida State University

As the majority of jobs in Computer Science are software development oriented, Computer Science curricula have shifted towards producing software more efficiently. As a result, low-level concepts such as computer instructions, assembly programming and calling conventions that are fundamental to cyber security are only covered marginally. Ultimately the security of cyberspace depends on the programs we use; increasing their robustness to vulnerabilities will enhance cyber security greatly. How to engage software developers in secure coding and other cyber security practices becomes a fundamental challenge. At the same time, in order to handle the ever-increasing complexity of malware and other programs, cyber security analysts heavily depend on specialized tools. This makes it even more difficult for typical software developers to comprehend the cyber security impacts. Without an intuitive grasp of the impacts of software vulnerabilities, it is difficult for software developers to get interested in the inherent cyber security threats. To overcome the challenges, we have developed universally applicable small programs that illustrate the importance of cyber security mechanisms. The programs are designed so that they can be tried using only commonly available tools such as compliers to maximize their reach. These simple programs overcome the barriers to most cyber security issues that rely on specialized tools. By relating these programs to fundamental issues in cyber security, software developers gain first-hand experience of the potential impacts of cyber attacks and therefore increase the awareness of cyber security importance. To illustrate the effectiveness of the approach, we have developed several examples. We have used variations of the tools in intro-level computer organization and programming courses, that have raised curiosity and interests to cyber security substantially.

In the Covid Era - Teaching Cybersecurity Online Across the Disciplines

Debasis, Bhattacharya, Assistant Professor, University of Hawaii Maui College

Cybersecurity has become a prevalent topic in many colleges, but how it should fit into the overall educational process is still not fully understood. A cybersecurity project at the University of Hawaii Maui College (UHMC), funded by the NSF ATE program, spans multiple disciplines and targets women and minorities. The goal of this project is to ensure that a broad audience of faculty, students and practitioners get trained in the fundamentals of cybersecurity. This is especially challenging during a pandemic, when all education is online. This project also targets students in middle and high schools, who are drawn to cybersecurity by the mass media but are not educated in the field or aware of future careers in cybersecurity.

Presentations

Simple Tool for Faculty Development & Support: The Instructor's Workbook

Maeve Dion, Assistant Professor, University of New Hampshire

Learn how a program management process and a single document can support your faculty and also your course/program reviews. Elevate the instructor's workbook into a tool that not only provides situational awareness and pedagogical foundations, but also helps to connect remote faculty and capture ideas and experiences in a hectic and demanding environment. Presuming that all faculty are experts in a course's subject matter, the workbook does not focus on substantive knowledge. Rather, it helps to blend practical resources, pedagogical foundations, and experiential tips from prior teachers and students. Since Spring 2019, faculty in UNH's online M.S. Cybersecurity Policy & Risk Management courses have utilized our workbooks and related processes. Our faculty especially value the workbook's support with pedagogy and the learning management system, as well as the workbook's accessibility and inclusion features that encourage each instructor to add comments and suggestions for improvement. In this Fastpitch Session, Prof. Maeve Dion provides an exemplar workbook, highlights the core features, and shares how the workbooks are utilized as part of our collaborative curriculum development and course review processes. Whether full-time academics or full-time practitioners, our faculty's lives are busy and complicated. The COVID-19 situation has increased the complexity: more learning is remote, and instructors are delving more deeply into the functionalities of our learning management systems/tools and the best practices for online learning and teaching. Raise your concept of a workbook to a new level and explore how you might want to adapt it for your course or program.

Using Wireshark in Security Classes

Wei Li, Professor, College of Computing and Engineering at Nova Southeastern University

This presentation is intended to discuss the promotion of security tools in general, and Wireshark in particular, in security-related classes at Nova Southeastern University (NSU). As a pioneer in cybersecurity education, NSU was striving to introduce students with hands-on experience in classroom settings. Wireshark is one of the most widely used tools in computer networking for deep packet analysis and has been used widely in several courses. In this presentation, we will cover a brief Wireshark introduction, and demonstrate a step-by-step process on how to set up and deploy the tool, identify protocols and payload, and perform analysis on security protocols such as SSL. Through this presentation, we hope to raise awareness, foster new ideas, and share the best practices in teaching hands-on skills within the CAE community.