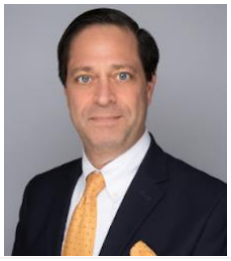
This publication was partially supported by CAE Community at the California State University, San Bernardino (CSUSB), under National Security Agency (NSA) award number H98230-22-1-0316

Table of Contents

CD Track Program Committee Co-Chairs



Tobi West	Yair Levy	Anne Kohnke
Coastline College, CA	Nova Southeastern University, FL	University of Detroit Mercy, MI
twest20@coastline.edu	levyy@nova.edu	kohnkean@udmercy.edu

CD Track Program Committee Members

Name	Affiliation	State
Hosam Alamleh	University of North Carolina Wilmington	North Carolina
Jim Alves-Foss	University of Idaho	Idaho
Vijay Anand	University of Missouri, St. Louis	Missouri
Julia Armstrong	The Ohio State University	Ohio
Syed Badruddoja	California State University, Sacramento	California
Shankar Banik	The Citadel	South Carolina
Ayad Barsoum	St. Mary's University	Texas
Debasis Bhattacharya	University of Hawaii Maui College	Hawaii
Matt Bishop	University of California, Davis	California
Gretchen Bliss	University of Colorado Colorado Springs	Colorado
Rakesh Bobba	Oregon State University	Oregon
Stephan Bohacek	University of Delaware	Delaware
Katie Bowers	Purdue University Northwest	Indiana
David Breeding	ECPI University	Virginia
Prasad Calyam	University of Missouri	Missouri
Zechun Cao	Texas A&M University-San Antonio	Texas
Anna Carlin	Fullerton College	California
Rohit Chadha	University of Missouri	Missouri
Eric Chan-Tin	Loyola University Chicago	Illinois
Zhixiong Chen	Mercy University	New York
Kristine Christensen	Moraine Valley Community College	Illinois
Bei-Tsengm "Bill" Chu	UNC Charlotte	North Carolina
Ulku Clark	University of North Carolina Wilmington	North Carolina
Haley Crabtree	Terra State Community College	Ohio
Deanne Cranford-Wesley	North Carolina Central University	North Carolina
Jun Dai	Worcester Polytechnic Institute	Massachusetts

Ram Dantu	University of North Texas	Texas
Thomas Devine	West Virginia University	West Virginia
Dennis Dias	United States Naval Academy	Maryland
Eva Dring	SANS Technology Institute	Maryland
Eman El-Sheikh	University of West Florida	Florida
Adel Elmaghraby	University of Louisville	Kentucky
Mohamed Elwakil	United States Coast Guard Academy	Connecticut
Waleed Farag	Indiana University of Pennsylvania	Pennsylvania
Armando Fernandez	Columbus State University	Georgia
Paige Flores	Towson University	Maryland
Zoe Fowler	Norwich University	Vermont
Guillermo Francia III	University of West Florida	Florida
Bill Gardner	Marshall University	West Virginia
Tirthankar Ghosh	University of New Haven	Connecticut
Nicklaus Giacobe	The Pennsylvania State University	Pennsylvania
William Glisson	Louisiana Tech University	Louisiana
Greg Gogolin	Ferris State University	Michigan
Max Gorbachevsky	Utica University	New York
Maanak Gupta	Tennessee Tech University	Tennessee
Rachelle Hall	Glendale Community College	Arizona
Seth Hamman	Cedarville University	Ohio
Jason Hammon	Western Governors University	Utah
Derek Hansen	Brigham Young University	Utah
Mathew Heath Van Horn	Embry-Riddle Aeronautical University	Florida
Randy Hinrichs	Norwich University	Vermont
Fenecia Homan	Dakota State University	South Dakota
Robert Honomichl	University of Arizona	Arizona
Behzad Izadi	Cypress College	California
Caroline Jennings	SANS Technology Institute	Maryland
Jiri Jirik	Moraine Valley Community College	Illinois
Jenny Ju	City University of Seattle	Washington
Andrew Kalafut	Grand Valley State University	Michigan
Bilge Karabacak	University of North Carolina Wilmington	North Carolina
Siddharth Kaza	Towson University	Maryland
Tahir Khan	Western Illinois University	Illinois
Denise Kinsey-Bergstrom	Franklin University	Ohio
Yesem Kurt Peker	Columbus State University	Georgia
Mark Lawrence	New Mexico State University	New Mexico
Sandra Leiterman	University of Arkansas at Little Rock	Arkansas
Michelle Lewis	Oregon State University	Oregon
Wei Li	Nova Southeastern University	Florida
Xiuwen Liu	Florida State University	Florida
Dan Manson	Cal Poly Pomona	California

Samah Mansour	Grand Valley State University	Michigan
Jim Marquardson	Northern Michigan University	Michigan
Daniel McIntosh	Laramie County Community College	Wyoming
Rachel Meyers	Purdue University Northwest	Indiana
Stanley Mierzwa	Kean University	New Jersey
Jake Mihevc	Mohawk Valley Community College	New York
Jason Mitchell	Lansing Community College	Michigan
Mike Morris	Western Governors University	Utah
Dave Nevin	Oregon State University	Oregon
Laxima Niure Kandel	Embry-Riddle Aeronautical University	Florida
Casey O'Brien	University of Illinois Urbana-Champaign	Illinois
Joel Offenberg	Howard Community College	Maryland
Loyce Pailen	University of Maryland Global Campus	Maryland
Abhishek Parakh	Kennesaw State University	Georgia
Rebecca Passmore	University of Arkansas at Little Rock	Arkansas
Justin Pelletier	Rochester Institute of Technology	New York
Bryan Preti	University of Advancing Technology	Arizona
Michael Ramage	Murray State University	Kentucky
Lydia Ray	Columbus State University	Georgia
Chris Rondeau	Bossier Parish Community College	Louisiana
Michael Ruth	Roosevelt University	Illinois
Arthur Salmon	College of Southern Nevada	Nevada
John Sands	Moraine Valley Community College / NCyTE	Illinois
Michael Sauer	Northern Michigan University	Michigan
Suzanna Schmeelk	St. John's University	New York
Christian Servin	El Paso Community College	Texas
Filipo Sharevski	DePaul University	Illinois
Chris Simpson	National University	California
Jia Song	University of Idaho	Idaho
Mirco Speretta	Fairfield University	Connecticut
Stuart Steiner	Eastern Washington University	Washington
Majd Tahat	Louisiana Tech University	Louisiana
Hondo Tamez	Johnson County Community College	Kansas
Cara Tang	Portland Community College	Oregon
Albert Tay	Brigham Young University	Utah
Blair Taylor	Towson University	Maryland
Chip Thornsburg	Northeast Lakeview College	Texas
James Tippey	Excelsior University	New York
Erald Troja	St. John's University	New York
Michael Tu	Purdue University Northwest	Indiana
Cihan Tunc	University of North Texas	Texas
Prem Uppuluri	Radford University	Virginia
Paul Wagner	University of Arizona	Arizona

Mary Wallingsford	Anne Arundel Community College	Maryland
Lixin Wang	Columbus State University	Georgia
Ping Wang	Robert Morris University	Pennsylvania
Michael Whitman	Kennesaw State University	Georgia
Xin Xing	University of Nebraska Omaha	Nebraska
Jacob Young	Bradley University	Illinois
Holly Yuan	University of Wisconsin-Stout	Wisconsin
Morgan Zantua	City University of Seattle	Washington
David Zeichick	CSU, Chico	California
Junjie Zhang	Wright State University	Ohio
Yu Zhang	University of Kentucky	Kentucky
Dmitry Zhdanov	Illinois State University	Illinois

Proceedings Editorial Preface

2025 CAE in Cybersecurity Community Symposium
National Centers of Academic Excellence in Cybersecurity (NCAE-C)
Charleston, SC

In 1999, the National Security Agency (NSA) launched the Center of Academic Excellence in Information Assurance Education program and over the years we have seen many changes to make the program stronger. Now under the direction of the Department of Defense (DoD) Office of the Chief Information Officer (CIO) - Cyber Academic Engagement Office (CAEO), the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program is a collaborative effort that includes academic institutions across the Nation that establishes ongoing rigorous criteria for cybersecurity curriculum. Over 480 institutions all over the Nation hold at least one designation in Cyber Defense (CAE-CD), Cyber Research (CAE-R), and/or Cyber Operations (CAE-CO). Hundreds of dedicated faculty members and administrators work together with a commitment to produce cybersecurity professionals who will reduce vulnerabilities in our national infrastructure. This focused commitment includes mentoring and coaching new and redesignating institutions to validate their programs, providing feedback and recommendations in the form of pre-submission reviews, and conducting peer-reviews of Program of Study (PoS) Validation and CAE Applications.

At the direction of the NSA's Program Management Office (PMO), many dedicated faculty members and administrators collaborate to help develop and document the CD, R, and CO programs criteria following the established requirements; support the ongoing updates of the NCAE-C Knowledge Units (KUs); support platforms to share cybersecurity curriculum and valuable resources, design and support the software application used to capture all applications and annual reports; and support the infrastructure to make the process of newly designating institutions and redesignation possible. Additionally, this unique NCAE-C Community brings together government, industry, and educational institutions to collaborate on critical projects of national importance, projects that support the K-12 educational space, bring educational and certificate programs to veterans, and many other programs that support and strengthen the overall NCAE-C program.

This year has marked another milestone for the NCAE-C Community. The vision for this year's community symposium was to organize an academic double-blind peer-review process using the EasyChair platform of presentation, mini workshops, lightning talk, and poster submissions and produce a proceedings book to document all the hard work by community members. We strongly believe in the value of coming together to share best practices, stories of successful collaborations, lessons learned, future directions, and solutions to community-wide issues. In addition to a formal call for submissions, we provided author's guidelines, organized three peer-reviews for each submission, and developed a first ever Proceeding for this event. This was no small amount of work and special thanks goes to Dr. Tobi West for her dedication and meticulous work ethic to keep everything brilliantly organized. This year the Program Committee (PC) accepted 56

Presentations, seven Mini Workshops, 24 Lightning Talks, and 17 Posters. We would also like to thank Dr. Tony Coulson, Amy Hysell, and their team at the *CAE in Cybersecurity Community National Center* (https://caecommunity.org/) for supporting the *CAE Community of Practice in Cyber Defense (CoP-CD)* (https://caecommunity.org/community-of-practice/cyber-defense) and the 2025 CAE in Cybersecurity Community Symposium. We would also like to thank Dr. Diba Azizi Hadi, Principal Director, DoD CIO - CAEO, Renae P. Weathers, NCAE-C Chief/Program Manager, for their leadership and Annie Becker, NCAE-C PMO for the support of the program and the CoP-CD. It is an honor to serve this exceptional community of scholars, government, and industry professionals as we collaborate to strengthen our nation and programs in order to address the critical need to educate and build up the next generation of cybersecurity professionals. Finally, we would like to thank all 126 PC members listed in pp. 1-4 for their outstanding scholarly reviews and dedicated quality feedback to the authors. This year, the PC members and co-chairs have completed 376 peer-reviews.

The 2025 CAE Community Symposium - CD Track Program Committee Co-Chairs,

Tobi West, Ph.D.	***Yair Levy, Ph.D.***	***Anne Kohnke, Ph.D.***
Coastline College, CA	Nova Southeastern University, FL	University of Detroit Mercy, MI

Refereed Extended Abstract Proceedings for Presentations

Generative artificial intelligence (AI) in knowledge discovery and generation for cyber defense

[Presentation]

Ping Wang, Robert Morris University, PA, wangp@rmu.edu

Extended Abstract

Knowledge discovery through pentesting is a critical step in cyber defense to learn and manage security vulnerabilities. Fast growing generative artificial intelligence (AI) technologies have the potential to improve the efficiency, productivity, and accuracy in knowledge discovery and generation. Inspired by the knowledge principles and defense strategies from Sun Tzu's classic work *The Art of War*, this research explores the role and moderating effects of generative AI and its limitations in security knowledge discovery for cyber defense. The study focuses on the strategies of discovering and knowing the cybersecurity vulnerabilities of oneself and one's opponents, which may be enhanced by generative AI and Large Language Model (LLM) solutions such as ChatGPT. The proposed AI-moderated knowledge discovery model for cyber defense is tested and illustrated with prompts and output from the interactive ChatGPT tool trained with security data from virtual network simulations for pentesting. This study explores and discusses the positive impacts as well as limitations and challenges of generative AI in pentesting for security knowledge discovery in cyber defense. The goal of the study is to contribute an AI-moderated knowledge discovery model and empirical data for cyber defense to inform further research on comparing generative AI and human intelligence and creativity in the cybersecurity domain. This research presents an adapted model of AI-moderated Knowledge Discovery for cyber defense based on the classic defense strategies in *The Art of War*. The model is tested and illustrated using a virtual network pentesting simulation for data collection to train the LLM-based AI tool of ChatGPT on various network vulnerabilities such as backdoors, DoS, and brute force. Subsequent queries and generated answers from ChatGPT indicate efficient knowledge and information on the vulnerabilities with suggested strategies for mitigation. The knowledge from pre-trained ChatGPT shows that AI solutions may enhance the pentesting process for cyber defense. The simulation test also shows some limitations of the AI tool.

Keywords: Generative AI, The Art of War, cyber defense, knowledge, pentesting, ChatGPT.

Infusing cybersecurity across any discipline

[Presentation]

Denise Kinsey-Bergstrom, Franklin University, OH, denise.bergstrom@franklin.edu

Extended Abstract

Developing cybersecurity curriculum can be difficult. Adding cyber concepts to non-IT courses can be more challenging. Often, cybersecurity faculty are tasked with developing curriculum with little or no direct experience in the topic to satisfy a school or department of education mandate. As academics and professionals, we tend to approach the problems of how to start, what topics to include, where to put each topic, how to assess learning, as ominous. The reason is that each discipline is different: some are applied, others are taught theoretically. How a patient receives care is different than the way a critical manufacturing problem is solved. Or is it? What if there was an easy, repeatable way to infuse cybers concepts and a security mindset across every discipline? And after infusing cyber, take some of the concepts inherent in those disciplines and use each to provide context in cybersecurity courses? It is possible. This presentation offers an overview of a method for including cybersecurity topics and infusing those in context-specific and appropriate ways without having to be an expert in every other discipline. This simple and repeatable process aids in providing context to the student, resources to the faculty, and more readily understood content to the student. The more easily they understand the more likely the student is to retain that information. After the overview, the attendees will be offered the chance to have their curriculum specific needs address (as time allows). The three approaches for infusing cybersecurity essential knowledge into any discipline are shared including steps for repeating each with the attendees' own curriculum.

Keywords: Cybersecurity, curriculum, development, awareness, context-driven, repeatable process.

NMU's cybersecurity collaboration with the DoD's Exercise Northern Strike

[Presentation]

Michael Sauer, Northern Michigan University, MI, msauer@nmu.edu

Jim Marquardson, Northern Michigan University, MI, jimarqua@nmu.edu

Extended Abstract

Northern Michigan University (NMU) recently became the first higher education collaborator in the 12-year history of Northern Strike, one of the Department of Defense (DoD)'s largest joint military readiness exercises held at the largest National Guard training facility in the country. Eight NMU information assurance/cyber defense students had a rare opportunity to work alongside military cybersecurity teams from the United States (U.S.) and the North Atlantic Treaty Organization (NATO) ally Latvia. Their mission was to regain control of a network used for communications and war command that had been compromised by a foreign adversary, determine how the network was infiltrated and remediate the vulnerability. Another first in the exercise was using offensive cybersecurity to increase the war fighting capability and situational awareness of troops while they were performing a ground-based mission of breaching and securing a building containing critical infrastructure. The presentation will cover:

- How the engagement with military and political leaders was facilitated
- Mission briefing and overview of the cyber exercise
- Skills and tools used in the mission
- Student reflection and experiences on working alongside military troops
- A live video of the strike force that breached and secured the building
- Building on the collaboration to increase higher education participation and capabilities in future missions

Exercise Northern Strike is a Joint National Training Capability (JNTC) accredited, Army sponsored, National Guard Bureau program conducted twice a year (winter and summer) within the 4-season National All Domain Warfighting Center's contested multi-domain operating environment. Northern Strike trains for joint operations and decisive action missions. Northern Strike 24-2 took place at Camp Grayling's National All-Domain Warfighting Center. This year's summer iteration of the annual exercise incorporated training scenarios involving homeland security, cybersecurity, and defense against unmanned aerial systems.

Keywords: DoD, national security, collaboration, military, cyber warfare.

Designing a Linux-focused digital forensics course for undergraduate students

[Presentation]

Lydia Ray, Columbus State University, GA, ray_lydia@columbusstate.edu

Extended Abstract

Digital Forensics is a constantly evolving field that needs periodic review to replace obsolete facts with new knowledge. A Digital Forensics course required in an undergraduate Applied Computer Science and Cybersecurity curriculum must provide an in-depth knowledge of hardware and file systems for a variety of reasons. Forensics software may have bugs. During litigation and cross-examination, investigators with an in-depth knowledge of hardware, hard drive and Operating System (OS) have an advantage. Additionally, such in-depth knowledge helps students find out-of-box solutions. We explored several textbooks and found that they lack in-depth knowledge and effective hands-on activities on important areas such as Windows Registry analysis, and on newly developed areas such as solid-state drives (SSD). Most of these books require students to use Windows-based digital forensics tools which are either expensive or slow and limited (such as Autopsy). The easy-to-use designs of these Windows-based tools obscure the fundamentals of OS and file systems, preventing students from acquiring in-depth knowledge. We also explored "Practical Linux Forensics" by Bruce Nikkel. While this book uses Linux based forensics techniques, it only covers forensics of modern Linux based systems. To that end, we have designed a Digital Forensics course, with interesting hands-on labs and case-based projects designed from scratch based on Linux-based open-source tools. This course aligns with the skills and competencies of International Association of Computer Investigative Specialists (IACIS) Certified Forensic Computer Examiner (CFCE) Program (IACIS, 2024). Thus, completing this course will prepare students for taking the test for this certification. Linux-based forensic tools will allow students to gain in-depth knowledge of analysis of traditional hard drives and SSDs with file systems File Allocation Table (FAT) 32 and New Technology (NT) File System (NTFS). Students will use Linux virtual machines as their own digital forensics labs to investigate case files. Thus, this course will dramatically reduce the material cost for the students since it will phase out the current $140 eBook in favor of our materials. In this presentation, we will present the key features of this new course with some of the novel hands-on activities and the capstone case to demonstrate the pedagogical benefits described above. We will also present mid-semester student feedback on the effectiveness of this course.

Keywords: Digital forensics, education, pedagogy, Linux.

Reference:

International Association of Computer Investigative Specialists (IACIS). (2024). *BCFE/CFCE core competencies.* https://www.iacis.com/wp-content/uploads/2024/10/BCFE-CFCE-Core-Competencies.pdf

Teaching automobile hacking with the instrument cluster simulator

[Presentation]

Jim Marquardson, Northern Michigan University, MI, jimarqua@nmu.edu

Michael Sauer, Northern Michigan University, MI, msauer@nmu.edu

Extended Abstract

As vehicles become increasingly connected and autonomous, the importance of automotive cybersecurity education cannot be overstated. This presentation highlights the critical need for teaching automotive cybersecurity in academic and professional settings, emphasizing the role of hands-on learning in preparing students and practitioners to address emerging threats. One of the primary challenges in this field is working with physical automotive hardware, which can be cost-prohibitive and logistically complex. The Instrument Cluster Simulator (ICSim) provides a practical and accessible alternative for simulating in-vehicle network behavior that overcomes these barriers. ICSim creates a virtual controller area network (CAN) in which a simulated car can be manipulated using graphical user interface controls or via direct transmission of CAN messages using command-line applications. This session will offer an overview of ICSim by exploring its functionality and applications in cybersecurity training. Attendees will learn about the benefits of using simulations, including reduced costs, increased accessibility, and the ability to create controlled learning environments. The presentation will also include a step-by-step guide to setting up ICSim within a Kali Linux virtual machine, ensuring participants can replicate the setup in their environments. Finally, curriculum examples will be shared to demonstrate how ICSim can be integrated into courses to teach core concepts such as CAN bus analysis, message injection, and vulnerability testing. By the end of the session, attendees will have a deeper understanding of the tools and strategies available for teaching automotive cybersecurity effectively and affordably. These tools have been used in GenCyber summer camps with high school students and as part of ethical hacking courses at the university level. Experiences from the instructors and tips for effectively using these tools will be shared.

Keywords: Automotive cybersecurity, simulation, controller area networks.

Hacking for good: Red teaming as an experiential service-learning opportunity in cybersecurity education

[Presentation]

Jacob Young, Bradley University, IL, jayoung@fsmail.bradley.edu

Angelica Fanti, Bradley University, IL, afanti@fsmail.bradley.edu

Extended Abstract

This presentation explores a unique approach to cybersecurity education that bridges academic learning with community impact. Using a service-learning model, our cybersecurity capstone course employs red teaming principles to provide students with hands-on experience in conducting comprehensive security assessments for local small business clients. Our course is structured around three distinct phases—Planning, Execution, and Reporting. In the planning phase, students work in teams to define assessment goals, gather open-source intelligence (OSINT), and outline strategies to evaluate vulnerabilities across multiple domains, including physical security, network defenses, organizational policies, and social engineering threats (Young, 2020; Young et al., 2017). In the execution phase, students operate as a red team, mimicking adversarial techniques to identify weaknesses while adhering to strict ethical and legal guidelines, including white hat and non-disclosure agreements. Weekly team updates and detailed activity reports ensure accountability, progress monitoring, and iterative feedback. These tasks also prepare students for the CompTIA PenTest+ certification, fostering technical competence alongside applied experience. The final reporting phase emphasizes professional communication. Students synthesize findings into actionable insights, delivering a formal report and presentation to the client. This capstone activity enhances students' ability to translate technical results into business-relevant recommendations, underscoring the importance of clear, client-focused communication. Our course demonstrates how integrating red teaming into undergraduate curricula can create a powerful synergy between learning and community service, not only preparing students for professional success, but also addressing real-world security challenges. Attendees will gain insights into implementing similar service-learning models in cybersecurity education to enhance student engagement and community collaboration. We will provide a detailed overview of the course design, learning outcomes, and demonstrate the measurable impact of our innovative pedagogical approach.

Keywords: Security assessment, red team, social engineering, service learning, cybersecurity.

References:

Young, J. A. (2020). Teaching tip: The development of a red teaming service-learning course. *Journal of Information Systems Education*, *31*(3), 157–178.

Young, J. A., Campbell, K. N., Fanti, A. N., Johnson, S. M., Sells, Z. S., & Sutter, A. M. (2017). The development of an applied ethical hacking and security assessment course. *Proceedings of the 2017 Midwest Association of Information Systems (MWAIS)*. http://aisel.aisnet.org/mwais2017/40

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Stepping-stone intrusion upstream detection by exploring the distribution of network traffic

[Presentation]

Jianhua Yang, Columbus State University, GA, yang_jianhua@ColumbusState.edu

Extended Abstract

Most professional intruders prefer to make use of stepping-stone to launch their attacks. There have been many approaches developed to detect stepping-stone intrusion since 1995. The primary idea to detect stepping-stone intrusion is to estimate the length of the connection chain from an intruder's host to the victim as shown in Figure 1. A Sensor is defined as a stepping-stone host in which a detection program can run. Most detection approaches focus on downstream detection that is to estimate the length of the connection chain from the Sensor to the Victim. This may introduce false-positive detection error since the upstream length, which is from the Sensor to the Intruder' host, was not counted.

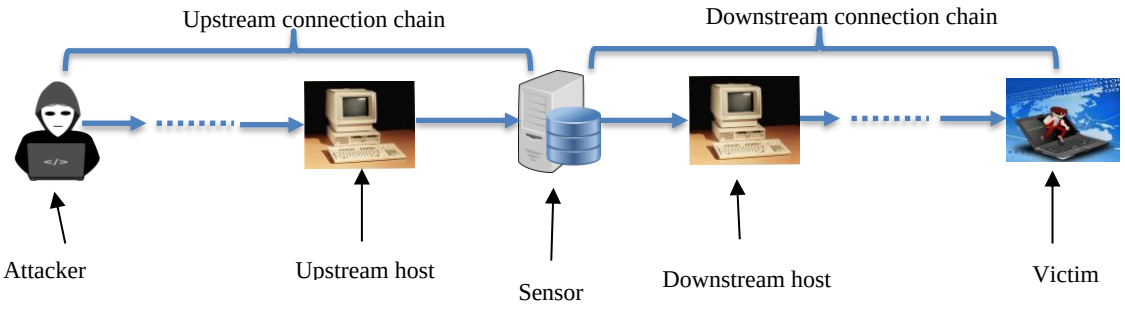


Figure 1: Model of Network based Detection

In order to reduce false-positive detection error, counting the length of the upstream connection chain plays a key role for successful intrusion detection. More important, if it is possible to conduct stepping-stone upstream detection, the detection sensor can be the Victim, other than a stepping-stone host. In this project, our team is exploring an approach to use the distribution of network traffic to conduct upstream stepping-stone intrusion. The detection mechanism was based on an observation: the longer a connection chain, the more deviation of network traffic from its original distribution. In our research project, we use intra-packet (TCP/IP packet) time gap distribution to modelling network traffic. In the Attacker's host, one study shows the distribution follows Poisson distribution. At the victim side, the original distribution is changed since it passes through a connection chain. The longer the connection chain, the higher deviation from its original distribution. Some experimental results support the statement, but more experiments under different situation are needed and underway.

Keywords: Stepping-stone, upstream detection, network distribution, poisson distribution.

An effective approach for stepping-stone intrusion detection resistant to intruders' Chaff-Perturbation via packet crossover

[Presentation]

Lixin Wang, Columbus State University, GA, wang_lixin@columbusstate.edu

Extended Abstract

Today's intruders usually launch cyberattacks to a target system through several stepping-stone hosts, to reduce the chance of being detected. Using stepping-stone intrusion (SSI), the intruder's identity is very difficult to discover as it is concealed by a long interactive connection chain of hosts. An effective approach for SSI detection (SSID) is to determine how many connections are contained in a connection chain. This type of method is called network-based SSID. Most existing network-based SSID only worked for network traffic without intruders' session manipulation. These known SSID algorithms are either weak to resist intruders' chaff attacks or have very limited capability in resisting attacker's session manipulation. This paper develops a novel network-based SSID algorithm resistant to intruders' chaff-perturbation by using packet crossover. Through well-designed network experiments, we verified that for a given connection chain, the downstream sub-chain length strictly increases with the obtained packet crossover ratio. Our SSID approach was designed based on this observation as follows: 1) Set up a connection chain A→S1→S2→S3→V of 5 hosts, where host S1 serves as the sensor, host A the attacker, and host V the victim; 2) Run an attacker script on a terminal in host A for a couple of minutes, and capture 10 datasets of the network packets from the connection S1→S2 at S1; 3) then calculate the intrusion threshold crossover ratio which is the average packet crossover ratio among the 10 captured datasets; 4) At the same time, we capture 10 datasets at S1 from another outgoing link from S1 and calculate the average packet crossover ratio over all the 10 captured datasets; 5) If the average packet crossover ratio obtained at Step 4 is not less than the one obtained at Step 3, it is most likely that this out-going link is used by a hacker for malicious SSI; 6) Repeat Step 4 for every outgoing link from S1 to see whether it is used by a hacker for malicious SSI. The SSID approach proposed in this paper is simple and easy to implement as the number of packet crossovers can be easily computed. Our proposed algorithm is verified by rigorous technical proofs as well as well-designed network experiments. Our experimental results show that the proposed SSID algorithm works effectively and perfectly in resisting intruders' chaff-perturbation up to a chaff rate of 50%.

Keywords: Connection chain, session manipulation, chaff-perturbation, packet crossover, stepping-stone intrusion.

An innovative and immersive Chinese language pilot summer program for cybersecurity college students

[Presentation]

Waleed Farag, Indiana University of Pennsylvania, PA, farag@iup.edu

Extended Abstract

The ongoing globalization and open access trends necessitate a workforce of cybersecurity professionals that not only understand the technical aspects of the field but also possess knowledge and skills in various areas including critical foreign languages. This proposal describes the design, implementation, and lessons learned from offering a one-of-a-kind project developing Chinese language skills in a select group of highly motivated and accomplished cybersecurity students from across the United States (U.S.). Throughout different phases of this project, we have collaborated with numerous National Centers of Academic Excellence in Cybersecurity (NCAE-C) to recruit participants, identify and hire qualified instructors, invite guest speakers, and deliver program contents and follow-up activities. Our Chinese language program was carefully designed to provide an immersive, enjoyable, and inspiring experience for its participants to expand their Chinese language skills and learn how to apply these skills to a cybersecurity career. The 10-week program held in summer 2024 began with a two-week virtual orientation focused on program requirements, expectations, and language skill assessment, followed by eight weeks on-site at our main campus with additional online follow-up activities during Academic Year (AY) 2024-25. The project started with a nationwide recruitment campaign that resulted in submission of more than 80 applications, representing 49 universities from 28 states. 15 highly qualified applicants were selected (40% of which were female), representing 15 different universities from 12 states. We recruited and hired 10 instructors and assistants from major universities across the nation and delivered the summer 2024 program with a student-to-teacher ratio of 1.5. The over 200 hours of provided instruction included daily hands-on activities, group practice, one-on-one sessions, cumulative weekly projects, and 10+ cultural events. We used formative and summative assessment to measure the achievement of learning outcomes and project objectives. The program also organized a two-day trip to the National Security Agency (NSA) in which all participants were given distinctive opportunities to learn from and connect with language, cybersecurity, and career experts at the agency. Throughout AY 2024-25, we continue engaging our participants in language immersion via follow-up synchronous instruction (monthly three-hour sessions for eight months) as well as required one-on-one speaking sessions, asynchronous activities, and assignments. This proposal will also discuss the positive impact of this pilot program demonstrated by the excellent feedback we received from our participants and collaborating partners. Additionally, we will share valuable lessons and best practices learned, including the need for thorough candidate background assessment, how to thoughtfully group participants based on skill levels, and how to purposely implement immersive activities and handle various academic and logistical challenges.

Keywords: Chinese language, immersive activities, engaging curriculum for cybersecurity students.

Confidence and capability: The impact of participating in cybersecurity competitions on career development

[Presentation]

David Zeichick, Chico State, CA, dzeichick@csuchico.edu

Extended Abstract

This presentation investigates the career impacts of participating in a cybersecurity competition. It assesses the effect of such competitive experiences on job interview opportunities, interview performance, and the practical application of skills learned in the competition to professional roles. Data was collected through a survey of cybersecurity competition participants. To recruit participants for the survey we utilized LinkedIn to identify individuals who had mentioned a cybersecurity competition in their skills section and held a current position within the cybersecurity field. We then sent out connection requests on LinkedIn and successfully established connections with 62 professionals. We received completed surveys from 34 individuals in the group, a 55% response rate. The survey consisted of 35 questions; it included 27 quantitative queries using a Likert scale, five open-ended qualitative inquiries, one binary yes/no question, and two queries for consent to disclose their identity, followed by a prompt for their name and email address. The survey was conducted online via Survey Monkey, with each response's start and end times, as well as their IP address, being logged. An individual's belief in their capability to succeed is a crucial element in pursuing a career in cybersecurity and, according to cybersecurity competition alumni that completed our survey, there is a strong consensus that participating in a cybersecurity competition enhanced their confidence. They indicated that participating in the competition not only positively enhanced their understanding of cybersecurity but also motivated them to learn more about it. But did competing in the cybersecurity competition get them their current job? There wasn't consensus to this question. Less than half reported that they talked about the cybersecurity competition during their job interview. For those that did, many reported that they were the ones that brought it up. During their interview they used the cybersecurity competition as a talking point, pointing out their ranking and the practical hands-on skills acquired which they felt help compensate for their lack of prior work experience. Overall, the cybersecurity competition improved the competence and confidence of past participants now in the cybersecurity field. To bridge the existing skills gap and expand the pool of cybersecurity professionals, it's imperative to engage a younger audience with cyber competitions.

Keywords: Competition, training, education, hiring.

Building cybersecurity AI expertise: A tiered approach at ECPI University

[Presentation]

David Breeding, ECPI University, NC, dbreeding@ecpi.edu

Extended Abstract

Artificial intelligence (AI) has become an essential tool in addressing modern cybersecurity challenges, from detecting advanced persistent threats (APTs) to automating incident response. To meet the industry's demand for AI-literate cybersecurity professionals, ECPI University has developed a comprehensive, multi-level AI curriculum that seamlessly integrates AI concepts into its cybersecurity programs. This tiered approach ensures that students progressively build the skills needed to leverage AI for cyber defense while fostering critical thinking and ethical considerations. ECPI's AI curriculum is structured into five distinct levels, each designed to support specific learning outcomes and applied skills within cybersecurity courses:

1. Cybersecurity AI Use Cases: Introduces real-world AI applications and ethical considerations, integrated into introductory cybersecurity courses.
2. Cybersecurity AI Prompting: Teaches prompt engineering for tasks like log analysis and incident response through targeted learning modules.
3. Cybersecurity AI Tools: Provides hands-on practice with AI-enabled tools like AWS Security Hub and CrowdStrike, embedded in practical lab exercises.
4. Cybersecurity AI Model Design: Guides students in building and training AI models using Jupyter Notebooks, incorporated into advanced security analytics courses.
5. Cybersecurity AI Deployment: Offers practical experience deploying AI systems in real-world environments, culminating in capstone projects.

Each of these levels is integrated within the broader cybersecurity curriculum rather than being stand-alone courses, ensuring that students gain AI competencies alongside their core cybersecurity training. This approach aligns with National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CD) objectives by equipping graduates with skills relevant to industry certifications such as AWS Cloud Practitioner and CompTIA Security+. The hands-on methodology ensures students are workforce-ready, addressing the critical gap in AI-trained cybersecurity professionals.

Keywords: Artificial intelligence, cybersecurity education, AI tools, AI model deployment, certification alignment.

Digital badging: Celebrating student competencies

[Presentation]

Chip Thornsburg, Northeast Lakeview College, TX, ithornsburg@alamo.edu

Extended Abstract

The 20-minute presentation share how Northeast Lakeview College in San Antonio, Texas, uses digital skills badges to address the students' challenge of explaining competency-based work during interviews. The Competency in Cybersecurity Education working group developed a definition of competency and a framework for writing competency statements, bridging the gap between higher education and employers. The National Security Agency (NSA) – National Centers of Academic Excellence in Cybersecurity (NCAE-C) program has adopted the ABCDE framework and the inclusion of competency-based projects in NCAE-C recognized programs. During four years of meetings, the question of "how can students improve their resumes and/or create digital portfolios to relay project-based work to potential employers repeatedly surfaced." The group acknowledged the need to improve student resumes and documentation but felt this was beyond the scope of its charge. In the handbook developed by the working group, the Situation, Task, Action, and Result (STAR) method is suggested to assist students in explaining competency-based work to potential employers (Nestler & Fowler, 2023). This still places much of the burden on the student to recall the essential elements of the projects and how they might relate to specific work roles. Digital badging platforms allow for the integration and automated publishing of project details between online Learning Management System (LMS and social media platforms, including LinkedIn. Digital Badges enable employers to view the project requirements, including the tasks, skills, and knowledge required to perform a work role according to the NICE framework. Several digital skill badge examples will be shared from the Cyber Defense program at Northeast Lakeview College.

Keywords: Digital badges, skill-based learning, competency, student resumes.

Reference:

Nestler, V. & Fowler, Z. (2023) Competency in cybersecurity education: A handbook for educators at NCAE-C designated institutions. *Norwich University*.

Changing undergraduate cybersecurity instruction

[Presentation]

Mathew J. Heath Van Horn, Embry-Riddle Aeronautical University-Prescott, AZ, heathvam@erau.edu

Extended Abstract

The National Cybersecurity Education Colloquium (NCEC) in October 2024 revealed a mismatch between cybersecurity employers and academics. Employers expressed a need for graduates who can perform skills, whereas academics focus on graduates mastering theory. We present three mechanisms that have helped us blend these goals into productive graduates. Cybersecurity theory-based instruction has become somewhat routine, whereas cybersecurity hands-on instruction is still trying to find traction. Textbooks that focus on just theory can be used for years, but when they offer labs, they can quickly become obsolete due to the pace of cyberspace innovation. An inordinate amount of time can be spent initiating, writing, testing, polishing, and assessing hands-on instruction compared to typical theory assessments. We use three mechanisms to enhance cybersecurity instruction. The first mechanism is leveraging students to develop hands-on instruction materials. Our students bring their internship, employment, and personal knowledge exploration experience to identify needed hands-on learning labs. The students create labs bundled into a textbook covering three cyber networking areas: building, defending, and attacking networks. Second, we prioritize active learning by completing theory-based labs and hands-on assessments. Students report that most classes, even Science, Technology, Engineering, and Mathematics (STEM)-based ones, have a lecture-to-practice ratio of 80/20, with assessments still grounded firmly in multiple-choice exams. We reversed the ratio to 20/80, and assessments are based on student demonstration of skill. The third mechanism is specifications grading, which makes it simple to assess students without jeopardizing the rigor of the grading process. Students have clear expectations, and learning objectives are articulated. This reduces anxiety and frees up the instructor's time to develop course instructional content continuously. Furthermore, students perform continuous self-reflection, which allows them to deepen their learning experiences. Finally, we collected course feedback in Fall 2024, and students reported favorably on implementing the three mechanisms. Students also attributed their success at job interviews to the enhanced focus on hands-on learning because they could now demonstrate their learned abilities. To develop more scientific results, we use instruments from other STEM fields to assess student perceptions of grading specifications and hands-on learning. The initial data collection should be completed by 1 April 2025. We hope this initial effort will support longitudinal studies in the future where we can focus data collection on the unexpected findings discovered in this effort.

Keywords: Cybersecurity, undergraduate, hands-on learning, specifications grading.

Practical cybersecurity toolkit using Python

[Presentation]

Akhtar Lodgher, Texas A&M San Antonio**,** TX, alodgher@tamusa.edu

Izzat Alsmadi, Texas A&M San Antonio, TX, ialsmadi@tamusa.edu

Extended Abstract

A practical cybersecurity toolkit is developed in Python by undergraduate students, designed for real-world applications in network analysis, forensics, system information gathering, and more. This abstract expands upon the initial prototype, discussing the design, implementation, and experimental results of key features, including encoding and decoding files, port scanning, password cracking, retrieving vulnerability information from Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) and Common Vulnerabilities and Exposures (CVE) databases, metadata extraction, and handling large log files. The toolkit has been used in various scenarios, demonstrating how students can conceptualize and build practical cybersecurity applications using Python in an easy-to-use educational framework. Design and Implementation: The toolkit consists of multiple modules, each focusing on a specific cybersecurity function:

- Port Scanning: Utilizes socket and NMAP for network scanning, supporting both internal and external scans with varying levels of detail.
- File Integrity and Hashing: Implements SHA-256 hashing to detect duplicate or tampered files.
- Password Hashing and Cracking: Uses Password-Based Key Derivation Function (PBKDF2) and Argon2 for secure password storage and cracking experiments. PBKDF2 and Argon2 are both password-based key derivation functions (KDFs) used for password hashing
- Metadata Extraction: Extracts and modifies image file metadata using the EXIF library.
- Vulnerability Assessment: Retrieves real-time vulnerability data from CISA KEV and CVE databases.
- Large File Handling: Efficiently process log files and other large data sets.

Experimental Setup and Results: To evaluate the toolkit, we conducted experiments in controlled environments for port scanning (compared scan times and accuracy), file integrity checks (tested effectiveness in identifying duplicate files and detecting modifications), password hashing (measured time and security strength of PBKDF2 and Argon2 hashing), meta data extraction (verified accuracy in extracting and modifying image metadata). Results indicate that the toolkit provides reliable and efficient cybersecurity functionalities, making it a valuable resource for students learning to solve problems and develop software as emerging professionals. Conclusion and Future Work: The toolkit has been used in cybersecurity training programs, and academic research. Students have extended the toolkit capabilities for penetration testing, forensic analysis, and vulnerability detection. Future work includes using a graphical user interface (GUI), AI-driven threat detection, and expanded forensics capabilities.

Keywords: Cybersecurity toolkit using Python, vulnerabilities.

Evolution of GenAI in the classroom - Beyond chatbots and prompts

[Presentation]

Debasis Bhattacharya, University of Hawaii Maui College, HI, debasisb@hawaii.edu

Extended Abstract

The launch of ChatGPT in November 2022 ushered in a new era of conversational chatbots using user prompts to converse with large language models (LLMs). Two years of rapid adoption have led to a global usage of LLMs for conversations using chat interfaces from OpenAI, Google, Anthropic, Meta, and other large companies. These chat interfaces have been adopted in classrooms worldwide to perform educational tasks such as existing content summarization, new content creation, coding exercises, augmented search and discovery, and other academic exercises. Prompt Engineering has evolved, with larger context sizes in the chatbots, to enable extended conversations that can be complex. This presentation highlights the evolving GenAI tools and technologies and how they are expected to contribute to cybersecurity education and workforce development (e.g., secure prompt engineering, AI-assisted cyber defense training, risk mitigation using RAG). This presentation also provides insights into pedagogy and teaching strategies to include GenAI tools as virtual assistants in cybersecurity education.

Keywords: Generative AI, artificial intelligence, prompt engineering, agentic AI, retrieval augmented generation.

Building bridges: A multi-university cybersecurity clinic model for CAE-CD community impact

[Presentation]

Chris Simpson, National University, CA, csimpson@nu.edu

Teresa Macklin, California State University San Marcos, CA, macklin@csusm.edu

Extended Abstract

Three California universities have partnered with a regional cyber-focused nonprofit organization to develop an innovative regional cybersecurity clinic model, supported by a $1 million grant from Google's Cybersecurity Clinics Fund. As one of the first multi-institution cybersecurity clinics in development, this collaborative effort demonstrates how academic partnerships can maximize impact and operational efficiency in serving underserved communities while providing students with hands-on cybersecurity experience. Our free clinic model offers students practical cybersecurity experience by completing real-world projects addressing the cybersecurity needs of underserved organizations. This model enables students from graduate and undergraduate programs in cybersecurity, homeland security, and computer science to work directly with small businesses, nonprofits, and community organizations to address real-world cybersecurity challenges. Under faculty supervision, students conduct real-world security assessments, develop mitigation strategies, and provide practical recommendations, creating a win-win scenario where organizations receive needed cybersecurity support while students gain invaluable practical experience. The clinics are free for customers and vary in length based on the customer's needs. The presentation will share practical insights and lessons learned during the clinic's initial development phase, focusing on key challenges and solutions in establishing cross-institutional collaboration. Topics will include developing shared student training protocols, standardizing service delivery across institutions, coordinating resources, and managing centralized client intake processes. Presenters will discuss both successes and obstacles encountered while building partnerships between diverse academic programs and departments. This session is particularly relevant to the National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CD) community as it provides a practical roadmap for institutions considering similar collaborative ventures. The presenters will share their experiences in real time, offering insights into the ongoing process of building a multi-institution clinic from the ground up. They will also highlight how each institution integrates the clinic into its respective curriculum. By highlighting both challenges and innovative solutions in establishing a regional cybersecurity clinic, this presentation will help other institutions develop more efficient and effective models for academic cybersecurity clinics serving their communities.

Keywords: Cybersecurity education, multi-institutional collaboration, community outreach, clinical model, service learning, regional partnership, capacity building.

Addressing trust and safety challenges in neural network-powered modern AI: A call for broader awareness and action

[Presentation]

Gongbo Liang, Texas A&M University-San Antonio, TX, gliang@tamusa.edu

Xin Xing, University of Nebraska Omaha, NE, xxing@unomaha.edu

Yu Zhang, University of Kentucky, KY, yuzh03@gmail.com

Extended Abstract

Despite the remarkable progress of neural network (NN)-powered artificial intelligence (AI), a fundamental question remains: Can we trust them? While research has often prioritized performance, it has frequently overlooked critical aspects like uncertainty quantification, leading to *miscalibration*, a mismatch between a model's confidence and its actual accuracy (Liang et al., 2020). Imagine a miscalibrated autonomous vehicle confidently declaring a clear path despite an obstacle, illustrating this potentially catastrophic risk. Furthermore, the rise of generative AI highlights issues like model *bias*, where these models can perpetuate societal biases by unfairly associating certain demographics with specific professions. Beyond these issues, modern NNs also struggle with *generalization* (Wang et al., 2020), *robustness* (Deanda et al., 2025), and *unstable feature learning*, further eroding trust in their safety and reliability. This deficit is also mirrored in education. While introductory machine learning courses may briefly introduce NNs, they often lack depth, leaving students with a superficial understanding. Dedicated undergraduate NN courses are absent from most universities' curricula. For instance, in South Texas, a region with approximately five million inhabitants and served by 13 universities and 11 colleges, only one institution offers an undergraduate course dedicated to NNs. This presentation examines some underlying causes of neural networks' trustworthiness and safety concerns. We also showcase our proposed probabilistic embedding solutions designed to mitigate these challenges, thereby fostering a foundation for informed discussion and future research. Our objective is to broaden the discourse beyond the immediate NN and AI research communities and engage a wider audience. By raising awareness and promoting collaborative efforts, we aim to contribute to developing a more robust and trustworthy AI ecosystem.

Keywords: Neural network, artificial intelligence (AI), NN trustworthiness and safety concerns.

References:

Liang, G., Zhang, Y., Wang, X., & Jacobs, N. (2020). Improved trainable calibration method for neural networks on medical imaging classification. In *31st British Machine Vision Conference (BMVC)*. BMVA, 2020.

Wang, X., Liang, G., Zhang, Y., Blanton, H., Bessinger, Z., & Jacobs, N. (2020). Inconsistent performance of deep learning models on mammogram classification. *Journal of the American College of Radiology*, 17(6), 796-803.

Deanda, D., Alsmadi, I., Guerrero, J., & Liang, G. (2025). Defending mutation-based adversarial text perturbation: a black-box approach. *Cluster Computing*, 28(3), 196.

Addressing the critical need for experiential learning within cybersecurity education

[Presentation]

Paul Wagner, University of Arizona, AZ, paulewagner@arizona.edu

Robert Honomichl, University of Arizona, AZ, rjhonomichl@arizona.edu

Extended Abstract

Cybersecurity threats are evolving at an exponential rate with industry and educational institutions struggling to keep up. Traditional educational methods often leave a significant gap in practical experience among graduates. Cybersecurity education often emphasizes theory over practice. While theoretical knowledge forms the foundation of cybersecurity education, the lack of hands-on experience limits students' ability to address real-world challenges. Students frequently lack opportunities to apply concepts practically, resulting in a workforce underprepared to tackle dynamic cybersecurity threats and organizational needs. Additionally, employers are increasingly dissatisfied with recent graduates' ability to perform the required tasks for their job roles. Experiential learning emphasizes learning through action and application allowing students to engage in simulated environments, hands-on labs, and real-world projects. Experiential learning bridges the gap between theory and practice, developing critical thinking, problem solving, and technical proficiency. Traditional options for experiential learning include labs, simulations, Capture the Flag (CTF) events, bootcamps, workshops, internships, and case studies. Two innovative approaches to experiential learning are cybersecurity clinics and institutional Security Operations Centers (SOC) providing services to clients within university communities. Services may include cybersecurity education and awareness training, risk and vulnerability assessments, and continuous monitoring. Participating students develop technical, critical thinking, and research skills in a real-world context. By engaging with stakeholders to identify specific needs, students must adapt to changing situations and develop written and verbal communication skills. Under-resourced organizations benefit by better understanding their operational and cybersecurity risk and having support to improve their risk posture. These solutions are important to the National Centers of Academic Excellence in Cybersecurity (NCAE-C) – CAE Community for several reasons. First, ensuring students are job-ready is a key tenet of educational programs. Second, understanding innovative options, their development, administration, and outcomes fosters institutional development. Finally, supporting under resourced organizations enhances national security by protecting the vulnerable. Although the Arizona cybersecurity clinic and regional Security Operations Centers (SOCs) are in the early stages of implementation, examples and comparisons of these learning experiences will be discussed, including current status, lessons learned, challenges, student learning outcomes, and a collaborative statewide model involving multiple NCAE-C schools.

Keywords: Experiential learning, cybersecurity education, cybersecurity clinics, security operations centers.

NCTA's role in credentialing high school teachers to expand availability and access to high school cybersecurity courses

[Presentation]

Sandra Leiterman, University Arkansas at Little Rock, AR, saleiterman@ualr.edu

Melissa Dark, Dark Enterprises, USA, melissa.dark@darkenterprisesinc.com

Paul Wagner, University of Arizona, AZ, paulewagner@arizona.edu

Filipo Sharevski, DePaul University, IL, fsharevs@cdm.depaul.edu

Jun Dai, Worcester Polytechnic Institute, MA, jdai@wpi.edu

Extended Abstract

The National Cybersecurity Teaching Academy (NCTA) was launched in 2021 with support from the National Centers of Academic Excellence in Cybersecurity (NCAE-C) to DePaul University, University of Arkansas at Little Rock (UALR), University of Louisville, and DARK Enterprises. In 2022, with continued NCAE-C support, California State University-Sacramento joined the NCTA coalition. NCTA provides scholarships for qualified high school teachers to complete a cybersecurity graduate certificate that integrates both technical content knowledge and cybersecurity pedagogy. The goals were to increase teachers' cybersecurity content knowledge in order to expand dual enrollment options at United States (U.S.) high schools. Initially designed as a 12-credit-hour program, the graduate certificate was expanded to 18 credit hours to meet dual enrollment requirements. Since its inception, 64 teachers who matriculated in 2022 have successfully completed the program, 20 are projected to graduate in summer 2025, and 38 teachers who started in summer 2024 are on track to complete their studies in summer 2026. Building on this success, in 2024 the coalition expanded to include Dakota State University, University of Arizona, University of Maryland Global Campus, and Worcester Polytechnic Institute and formed the National Cybersecurity Teaching Coalition (NCTC). NCTC will continue to offer NCTA graduate certificates with 175 scholarships available in 2025 and another 175 scholarships in 2026. Additionally, NCTC will develop an early-entry program for pre-service teachers. Further, NCTC will identify and develop educational licensing and endorsements for cybersecurity like computer science or Career Technical Education (CTE) endorsements. Given NCTA's emphasis on dual credit courses, the Early College Credit in Cybersecurity (E3C) initiative within NCTC developed a supplement to the ACM CSEC Curriculum Guidelines of foundational content for Cyber 1 and 2. Cyber 1 will be piloted at four high schools as early college credit in Arkansas beginning in the fall of 2025. This initiative benefits the CAE in Cybersecurity Community by identifying pathways for graduate-level cybersecurity education aligned with NCTA, promoting E3C opportunities and articulation agreements across institutions, and developing cybersecurity pathways for students.

Keywords: Cybersecurity education, dual enrollment, early college credit, cybersecurity teacher credentialing.

CyberLearN: A collaborative model for sustainable workforce development

[Presentation]

Sandra Leiterman, University Arkansas at Little Rock, AR, saleiterman@ualr.edu

Becky Passmore, University Arkansas at Little Rock, AR, rpassmore@ualr.edu

Extended Abstract

The Arkansas Cyber Learning Network (CLN) is designed to create a sustainable ecosystem for cybersecurity education by aligning curriculum and resources across institutions. The network's stackable certificate model offers pathways from the Certificate of Proficiency (CP) to the Advanced Technical Certificate (ATC) and ultimately to a Bachelor's (BS) degree. By providing students with credentials at each stage of their educational journey, the CLN increases access and equity, ensuring students can enter the workforce early while continuing toward advanced degrees. To enhance flexibility, all CLN courses are transitioning to a competency-based education (CBE) model. This approach allows students to progress at their own pace, emphasizing mastery over seat time. Additionally, Prior Learning Assessments (PLAs) recognize work and life experiences, creating multiple entry and exit points that support nontraditional learners balancing education with other commitments. A key feature of the CLN is its shared faculty and cross-institutional enrollment system, addressing the nationwide adjunct faculty shortage. By pooling faculty resources, the network ensures students receive high-quality instruction without geographic limitations while promoting pay equity across institutions. Additionally, CLN is expanding into high schools, piloting concurrent cybersecurity courses taught by National Cybersecurity Teaching Academy (NCTA) graduates, reducing transportation barriers and providing early access to cybersecurity education. Employer engagement is central to CLN's workforce development efforts. Industry partners collaborate to ensure curriculum relevance, support internship and apprenticeship programs, and provide hands-on experience. Additionally, scalability efforts include standardizing credit transfer policies across institutions to ensure course quality and seamless articulation between credentials. By addressing staffing shortages, transportation barriers, employer collaboration, and credit transfer challenges, the Arkansas CLN provides a replicable framework for sustainable regional cybersecurity education networks.

Keywords: Workforce development, shared resources, competency-based education, cybersecurity training, employer collaboration.

Cyber 1 & 2: Foundations of cybersecurity CSEC update

[Presentation]

Melissa Dark, Dark Enterprises, USA, melissa.dark@darkenterprisesinc.com

Philip Huff, University of Arkansas at Little Rock, AR, pdhuff@ualr.edu

Cara Tang, Portland Community College, OR, cara.tang@pcc.edu

Jun Dai, Worcester Polytechnic Institute, MA, jdai@wpi.edu

Matt Bishop, UC Davis, CA, mabishop@ucdavis.edu

Extended Abstract

Cybersecurity education has grown since Cybersecurity Curricula 2017 was released. Today, there are ~385 universities and 384 community colleges with a cybersecurity Classification of Instructional Programs (CIP) code for bachelor's degrees and associate degrees (Tims et al., 2024). Another recent study of cybersecurity programs at 446 National Centers of Academic Excellence in Cybersecurity (NCAE-C) schools found 803 degrees at these 446 institutions (Dark & Daugherty, 2024). In addition to this growth, cybersecurity courses/pathways are being included at the secondary level. A 2022 study found that 15% of the 23,882 public high schools in the United States offer a cybersecurity course (CyberSupply, 2023). This number will grow as the new College Board AP Career Kickstart Cybersecurity program rolls out in coming years (The College Board, 2025). This growth makes educational articulation, which has long been important in other disciplines, newly important in cybersecurity. Articulation can help students move between educational institutions or programs without losing credits or having to repeat work. This can save students time and money. Articulation can help educational institutions build more seamless learning pathways in an effort to bridge students more effectively from high school to college and among colleges and universities. A committee created a supplement to the Cybersecurity Curricula 2017 guidelines that includes learning outcomes and instructional guidance to support foundational collegiate-level courses and upper-level high school cybersecurity offerings, i.e., Cyber 1 and 2. Support for this work was provided by NCAE-C grant and the ACM. This supplement was recently by published by ACM. The authors will present the work and discuss next steps to support adoption of the guidelines and therefore early college credit in cybersecurity.

Keywords: Cyber 1, curriculum guidelines, articulation, ACM CSEC supplement.

References:

CyberSupply (2023). *Cybersecurity education: Availability & access in public high schools.* https://cybersupply.org/

Dark, M., & Daugherty, J. (2024). E3C – Teach Cyber: https://teachcyber.org/e3c/

Tims, J. L., Tucker, C. S., Weiss, M. A., & Zweben, S. H. (2024). Student enrollment and retention in 2022--23 U.S. undergraduate computing programs. *ACM Inroads, 15*(4), 20–46. https://doi.org/10.1145/3700774

The College Board (2025). *Career kickstart.* https://apcentral.collegeboard.org/about-ap/outreach-and-collaborations/career-kickstart

On teaching and learning industrial control systems security using Open Platform Infrastructure (OPI)

[Presentation]

Guillermo Francia, III, University of West Florida, FL, gfranciaiii@uwf.edu

Extended Abstract

The introduction of virtualization ushered the emergence of microservices to facilitate efficient ways to deploy and manage containerized applications. Further, these so-called Open Platform Infrastructures (OPI) provide a system with which lightweight containers can securely run in isolation on a given host. We leveraged this valuable feature of Docker to create an environment for a practical Industrial Control Systems (ICS) training platform. In this presentation, we endeavor to share our work in advancing the security of ICS through a four-pronged approach: i) provide a safe training infrastructure for ICS security; ii) present an effective avenue for ICS security testing without operational disruption; iii) implement ICS digital twins to enable ICS security training; and iv) facilitate the design, implementation, and evaluation of ICS security tools. To realize these objectives, we demonstrate the effective utilization of Open Platform Infrastructure (OPI) with Docker technologies to deploy virtualized Programmable Logic Controllers (PLCs), also known as softPLCs, and Human Machine Interfaces (HMIs) that can emulate or act as digital twins of ICS. We describe the creation of a cost-effective and realistic laboratory setup for teaching and learning ICS security that includes hands-on activities such as reconnaissance, vulnerability assessment, penetration testing, intrusion detection, ICS forensics analysis, threat analysis, ladder logic programming, and HMI development. In addition, the emulation of a typical Information Technology (IT) and Operation Technology (OT) networks running on Docker containers will illustrate the viability and affordability of such implementations for teaching, learning, and testing of ICS security. All tools used in the OPI system are either free or open-sourced. The complete OPI system can be installed in a Windows, MacOS, or Linux operating system. As an enticement, we offer suggestions for future enhancements that can further drive this teaching and learning system for the benefit of the security community. A complete fifteen-week undergraduate curriculum utilizing this system will be published at the CLARK System (https://clark.center/home) security curricula repository.

Keywords: Digital twins, Human Machine Interface (HMI), Industrial Control Systems (ICS) Security, Information Technology/ Operational Technology (IT/OT) Networks, Open Platform Infrastructure (OPI), Programmable Logic Controllers (PLCs).

Building an AI-Enabled cybersecurity workforce

[Presentation]

Eman El-Sheikh, University of West Florida, FL, eelsheikh@uwf.edu

Extended Abstract

The rapid advancement of Artificial Intelligence (AI) is transforming industries and reshaping the future of work. The growing adoption of AI, particularly generative AI, presents both challenges and opportunities for cybersecurity professionals. This presentation explores the evolving landscape of AI in cybersecurity and strategies to build a workforce equipped to leverage AI for cyber defense while mitigating AI-driven threats. The cybersecurity industry faces an increasing demand for skilled professionals, with AI playing a dual role in augmenting cyber capabilities and introducing new security vulnerabilities. This presentation will discuss key industry trends, essential AI-related cybersecurity skills, and education frameworks to develop an AI-enabled cybersecurity workforce. We outline a three-tiered model for AI competency in cybersecurity education:

1. **AI Generalist:** All individuals should have a fundamental understanding of AI's evolution, benefits, risks, and tools.
2. **AI Professional:** In addition to the above, all working professionals should be able to leverage AI tools to enhance different domains and professional productivity.
3. **AI Cyber Professional:** An AI-enabled cybersecurity professional should be able to leverage AI to enhance cybersecurity, as an **AI-Cyber Specialist**, plying AI methods and tools to support cybersecurity, or as a **Secure AI Developer**, developing secure AI frameworks and systems.

The presentation outlines a phased approach that institutions can adopt to integrate AI across programs, leveraging national frameworks and resources such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework and the National Science Foundation (NSF)/National Security Agency (NSA) CyberAI Project. By fostering AI proficiency in cybersecurity professionals, the National Centers of Academic Excellence in Cybersecurity (NCAE-C) - CAE Community can build a resilient, AI-enabled workforce ready to defend against evolving threats while harnessing AI's potential to enhance security operations.

Keywords: Artificial intelligence, machine learning, cybersecurity education, workforce development, AI-enabled cybersecurity, curriculum and program development.

Challenges and future path for valid research in the human factor of cybersecurity

[Presentation]

Yair Levy, Nova Southeastern University, FL, levyy@nova.edu

Extended Abstract

Over the past four decades, computing researchers have been working very hard to develop advanced systems to help protect organizations and mitigate risks of cybersecurity attacks. These advanced cybersecurity systems include Intrusion Detection/Intrusion Prevention Systems (IDS/IPS), sophisticated spam filtering applications, Artificial Intelligence (AI) augmented firewall systems, and malicious network traffic detection, to name a few. However, with all these advanced systems, data breaches and network compromises still occur in increasing numbers, as well as the majority of these are caused by social engineering as the initial entry point to organizational networks (Verizon, 2024). Social engineering is defined as an attack developed to manipulate, deceive, and persuade individuals to perform an activity (e.g. click on a link or attachment, provide their credentials) that then allows adversaries to gain access to the network or run malicious software. Research into the human factor of cybersecurity is not new. However, some research streams have been heavily relying on self-reported surveys, and when it comes to areas such as information security compliance, social engineering, or cybersecurity skills and competencies, such self-reported measures are invalid if assessing intentions instead of actual behavior. This presentation will discuss those challenges and provide recommendations for future research based on the work done in the Levy CyLab (https://infosec.nova.edu/cylab/) at Nova Southeastern University over the past two decades. Specifically, the presentation will start with several examples of why self-reporting in cybersecurity research may pose significant challenges, especially when it comes to social engineering and cybersecurity compliance when replying on intentions rather than actual behaviors. Then, an overview of the foundational theory behind the research done in the Levy CyLab, which was developed by the 2002 Nobel laureate Kahneman (2011) known as the "System 1/System 2 thinking" will be discussed. Following, examples of several field experiments using commercially off-the-shelf (COTS) phishing platforms like KnowBe4.com™ will be discussed, along with several mobile device applications that we have developed to simulate email applications and assess phishing attacks will be presented. Discussions about overcoming Institutional Review Board (IRB) restrictions and following the guidelines will also be presented. This presentation will conclude with open discussions to encourage early-career faculty members who wish to pursue research related to social engineering and the human factor in cybersecurity.

Keywords: Human factor in cybersecurity, social engineering research, challenges of self-reported surveys in cybersecurity, experimental and developmental research in cybersecurity.

References:

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Verizon (2024). 2024 data breach investigations report. Verizon Business.

Building cybersecurity excellence: AI-driven collaborative learning and ethical reasoning in NCAE Co-Op Centers

[Presentation]

Randy J. Hinrichs, Norwich University, VT, rhinrich@norwich.edu

Extended Abstract

The cybersecurity field increasingly demands professionals with both technical expertise and social cybersecurity skills such as ethical reasoning. As threats evolve, ethical dilemmas surrounding privacy, data security, and equitable access require professionals to navigate high-stakes decisions aligned with legal and moral standards. This proposal enhances "CyberEd in a Box," a component of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) Co-Op program at Norwich University. Funded by Grant H98230-22-1-0329, the initiative integrates artificial intelligence (AI) with the National Institute of Standards and Technology (NIST)/NICE Cybersecurity Workforce Framework. It improves personalized learning, strengthens cognitive skill development, and fosters ethical decision-making through a cooperative learning model. This proposal addresses this demand by leveraging AI to help students identify their career pathways, engage in targeted skill development, and work on specific tasks such as ethical reasoning through AI-driven guidance tailored to their learning needs. This presentation will explore how AI-driven tools, including CyberGEN.IQ, ChatGPT, Gemini, and Perplexity, enhance cybersecurity training by providing adaptive feedback and aligning students with industry certifications and career pathways. It will highlight AI's role in personalized training, ethical decision-making, and mapping students to NICE Framework roles. Additionally, the session will showcase real-time AI feedback integration, micro-credentialing, and immersive cybersecurity training using cyber ranges and virtual Security Operation Center (SOC) environments. Ethical reasoning will be emphasized through structured frameworks that instill accountability, fairness, transparency, and trust in real-world decision-making scenarios. Metrics show a 20% rise in scenario performance scores and a 30% boost in ethical reasoning. AI-driven assessments track cognitive and ethical development through adaptive analytics, interactive simulations, and real-world case studies. CyberWallet enables credential tracking with AI-powered verification, dynamic skill assessments, and real-time competency mapping. The program scales across NCAE-C Co-Op Centers, linking academia, industry, and government through structured internships. Key challenges include resource constraints, faculty training, and accreditation alignment. Neuroplasticity-based learning reinforces cognitive adaptability, decision-making, and ethical reasoning. This presentation will highlight best practices in AI-enhanced cooperative learning, real-time AI feedback integration, adaptive ethical training techniques, and future developments in cybersecurity education. By merging advanced educational technology with ethical cybersecurity training, "CyberEd in a Box" addresses workforce gaps and prepares students for modern cybersecurity roles.

Keywords: AI-driven personalization, ethical reasoning, cybersecurity education, NIST/NICE framework, NCAE Co-Op centers, cognitive assessments.

Integrating ethics and societal impact into cybersecurity education in online learning

[Presentation]

James Tippey, Excelsior University, FL, jtippey@excelsior.edu

Extended Abstract

The rapid evolution of cybersecurity threats demands more than just technical expertise from professionals. As digital security becomes integral to all facets of modern life, it is crucial to instill ethical reasoning and societal awareness in cybersecurity education. This abstract explores the imperative of integrating ethics and societal impact into cybersecurity curricula, focusing on online learning environments and the National Centers of Academic Excellence in Cybersecurity (NCAE-C) - CAE in Cybersecurity Community. Traditional cybersecurity education has predominantly focused on developing technical skills to identify and mitigate security risks. However, cybersecurity actions' increasing ethical dilemmas and societal consequences call for a broader educational approach. Students must learn to critically assess the implications of their work, balancing privacy, security, accessibility, and equity in their decision-making processes. Incorporating ethical and societal considerations into online cybersecurity education is uniquely challenging but vital for preparing responsible cybersecurity professionals. The CAE in Cybersecurity Community, cybersecurity education leaders, can advance this integration by adopting pedagogical frameworks that address ethical and societal dimensions. This presentation outlines practical strategies for embedding these elements into the online curriculum, including case studies, discussion prompts, and project-based learning. For example, students can engage in scenario-based learning that simulates real-world ethical dilemmas, requiring them to navigate complex decisions about privacy rights, algorithmic biases, or surveillance ethics. Additionally, ethical reflection activities can be integrated into cybersecurity assignments to promote deeper consideration of societal impacts. The presentation will provide examples of a NCAE-C institution successfully integrating ethical elements into its courses. The proposed strategies are designed to enhance engagement in online learning, promote critical thinking, and prepare students to tackle the ethical challenges they will face in their professional careers.

Keywords: Cybersecurity curriculum, online learning, ethics integration, societal.

Navigating cloud security and forensics: Addressing emerging threats and challenges

[Presentation]

Becky Passmore, University of Arkansas at Little Rock, AR, rpassmore@ualr.edu

Sandra Leiterman, University of Arkansas at Little Rock, AR, saleiterman@ualr.edu

Extended Abstract

As cloud adoption accelerates, organizations face increasingly complex cybersecurity threats and forensic challenges. This presentation explores the rapid expansion of cloud applications, the rise of multi-cloud and hybrid environments, and the evolving attack landscape. A key focus is on the Shared Responsibility Model, highlighting security gaps and accountability in cloud environments. Emerging cloud threats such as ransomware, misconfigurations, account hijacking, and data leaks are examined, along with insider threats and Application Programming Interface (API) vulnerabilities that compromise supply chains. The challenges of cloud forensics, including limited data access, legal constraints, and multi-tenancy concerns—are discussed in the context of digital investigations. Artificial intelligence (AI) is a game-changer in cloud security and forensics, offering capabilities for threat detection, anomaly identification, and automated incident response. AI-driven solutions, including User and Entity Behavior Analytics (UEBA), Security Orchestration, Automation, and Response (SOAR), and Natural Language Processing (NLP) for log analysis, enhance investigative efficiency and forensic integrity. Through real-world case studies and cutting-edge research, this presentation underscores the importance of AI in mitigating cloud security risks, streamlining forensic investigations, and fortifying defenses against evolving cyber threats.

Keywords: Cloud environments, cloud forensics, cybersecurity, artificial intelligence, data protection, cybersecurity workforce.

Detecting vulnerabilities in PHP-Based web programs using graph models

[Presentation]

Junjie Zhang, Wright State University, OH, junjie.zhang@wright.edu

Extended Abstract

The ability to detect vulnerabilities is essential for ensuring the security of web servers. However, the development and deployment of detection mechanisms often lag the discovery of new vulnerabilities. This delay is largely attributed to the significant syntactical diversity inherent in web programs. Furthermore, traditional program representations—such as source code, abstract syntax trees (ASTs), and intermediate representations (IRs) like single static assignment (SSA)—are primarily designed to facilitate compilation rather than security analysis. To address these challenges systematically, we propose a novel graph-based program representation called the heap graph, specifically tailored to enhance the effectiveness of vulnerability detection. Specifically, A heap graph is generated by symbolically interpreting the AST of a PHP program. It captures the immediate data and control dependencies among all objects in a program, where each object represents the evaluation result of an expression in the analyzed program. This representation enables efficient exploration of information flows between any pair of objects by simply traversing the graph. As a result, many security analyses can be seamlessly transformed into graph operations. To this end, we have built three security applications using the heap graph, including UQuery (Huang et al., 2024), UChecker, and UFuzzer (Huang et al., 2021). Specifically, UQuery uses graph queries to implement scalable taint analysis. UChecker derives three symbolic satisfiability constraints to jointly model both the reachability and the exploitability of the move_upload_file() API, which can be misused by attacker for arbitrary file uploading. UFuzzer performs lightweight fuzzing by identifying, preserving, and refactoring only the code relevant to the targeted vulnerabilities. Together, these systems have successfully identified over 50 previously unknown vulnerabilities, resulting in 11 assigned Common Vulnerabilities and Exposures (CVEs). Our work has great potential to build novel educational modules to develop students' skills in program analysis, software security, and vulnerability detection.

Keywords: Software security, vulnerability, program analysis, symbolic execution.

References:

Huang, J., Zhang, J., Liu, J., Li, C., & Dai, R. (2024, September). UQuery: Static security analysis of php-based web programs using graph models. *Proceedings of the IEEE Conference on Communications and Network Security (CNS)* (pp. 1-9). IEEE.

Huang, J., Zhang, J., Liu, J., Li, C., & Dai, R. (2021, October). Ufuzzer: Lightweight detection of php-based unrestricted file upload vulnerabilities via static-fuzzing co-analysis. In Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 78-90).

Using fine-tuned LLMs to grade homework

[Presentation]

Stephan Bohacek, University of Delaware, DE, bohacek@udel.edu

Aishah Aseeri, University of Delaware, DE, aaishah@udel.edu

Extended Abstract

Large Language Models (LLMs) have the potential to automatically grade homework and give students hints, and therefore significantly improve education. However, as explained in this talk, due to hallucinations and general lack of capabilities, using LLM for grading and giving hints has mixed results. The performance of LLMs can be improved by using methods such as prompt engineering, Retrieval-Augmented Generation (RAG), and fine-tuning. In this talk, we explore the possibility of using fine-tuned LLMs to grade and give hints. In fine-tuning, the weights of a fully trained LLM are adjusted so that it provides better results for a specific problem. The advantage if fine-tuning is that the massive training data sets and expense to build a general purpose LLM is leveraged for a specific purpose. The fine-tuning method requires providing a moderate-sized set of training data for the specific problem or problems. In this talk, we demonstrate a system that can be used for automatic grading and fine-tuning. We explore the performance of a fine-tuned system and an unfine-tuned system. In addition, we explore the performance of using a single fine-tuned system to grade similar problems and the performance of using different fine-tuned systems for each problem. We find that fine-tuning is labor intensive, but, for problems where the unfine-tuned LLMs perform poorly, fine-tuning is a viable option.

Keywords: AI, education, automatic grading, fine-tuning LLMs.

ORTSOC: A clinical rotations approach to professional cybersecurity education

[Presentation]

Dave Nevin, Oregon State University, OR, dave.nevin@oregonstate.edu

Rakesh Bobba, Oregon State University, OR, rakesh.bobba@oregonstate.edu

Michelle Lewis, Oregon State University, OR, Michelle.Lewis@oregonstate.edu

Extended Abstract

ORTSOC - The Nation's First Cybersecurity Teaching Hospital is the heart of the academic program in Cybersecurity at Oregon State University. Adapted from the clinical rotation model long used by our nation's teaching hospitals, ORTSOC provides experiential learning opportunities for students through a year-long program which is embedded into the curriculum. Guided by experienced professionals, students in the program hone their cybersecurity skills by providing managed cybersecurity services to a consortium of under-served organizations across the region. For students seeking to start careers in cybersecurity operations, the clinical program offers a carefully structured opportunity to build an experiential bridge between the classroom and professional practice. During this talk, the co-founders of the ORTSOC will share an overview of the program, present education and service goals, and discuss the pros and challenges of a security operations center (SOC)-based clinical rotations model for cybersecurity education. The talk will begin with a history of the program that led to the development of ORTSOC, an overview of Oregon State University's cybersecurity program and how the teaching hospital model of cybersecurity education differs from traditional models such as cyber ranges and internships. Talk will cover the pros and challenges of a SOC-based clinical rotations model for cybersecurity education including: some early success statistics, approaches to attracting and building relationships with stakeholders, addressing liability concerns. etc. We'll also briefly touch upon funding and staffing required. We'll end the session with an open discussion with the audience with the hope of developing potential partnerships with other organizations who may be interested in similar approaches.

Keywords: Experiential learning, clinical rotations, teaching hospital model, cybersecurity education, computer science.

A transdisciplinary approach to maritime transportation system cybersecurity education, and capability development

[Presentation]

Ulku Clark, University of North Carolina Wilmington, NC, clarku@uncw.edu

Jeff Greer, University of North Carolina Wilmington, NC, greerj@uncw.edu

Geoff Stoker, University of North Carolina Wilmington, NC, stokerg@uncw.edu

Kasey Miller, University of North Carolina Wilmington, NC, millerkc@uncw.edu

Hosam Alamleh, University of North Carolina Wilmington, NC, alamlehh@uncw.edu

Bilge Karabacak, University of North Carolina Wilmington, NC, Karabacekb@uncw.edu

Extended Abstract

The National Infrastructure Protection Plan (NIPP) outlines a tiered cyber risk management strategy for protecting sixteen interconnected, life-sustaining critical infrastructure sectors. This presentation focuses on the Maritime sub-sector, which is part of the larger transportation system sector, and includes both ships and ports. The NIPP defines a role for academia in supporting the cybersecurity of critical infrastructure, specifically through workforce development and technology innovation. University of North Carolina Wilmington (UNCW) is currently addressing NIPP needs by offering specialized applied maritime cybersecurity classes. It is also conducting applied Research and Development (R&D) to develop new maritime cybersecurity solutions. This presentation provides an update on a new learning environment being developed for classroom use. It will also provide a brief status update on a novel, proof-of-concept engineering workstation being developed for both student and professional use when designing an enterprise cyber risk management strategy. A transdisciplinary approach is being used in the classroom and for the conduct of applied R&D. This became necessary because of the broad range of knowledge, skills, and abilities needed for managing maritime cyber risk. Knowledge domains being covered in the virtual learning environment and workstation, include maritime, systems engineering, and safety engineering, and cybersecurity engineering. Work completed to date suggests the boundaries that define traditional academic disciplines need to be reconsidered to better address critical infrastructure operator work force training and technology needs.

Keywords: Maritime, system engineering, safety engineering, cybersecurity.

Central Illinois high school cyber defense competition

[Presentation]

Dmitry Zhdanov, Illinois State University, IL, dzhdano@ilstu.edu

Yousra Javed, Illinois State University, IL, yjaved@ilstu.edu

Extended Abstract

Central Illinois High School Cyber Defense Competition (CIHSCDC) is a multi-year tradition organized by Illinois State University. 2024 was the biggest event yet, and the 2025 competition is scheduled for April 2025. We would like to share with the National Center of Academic Excellence in Cybersecurity (NCAE-C) CAE in Cybersecurity Community our insights about organizing and running the competition. The 2024 competition comprised a red team, ten blue teams, and a white team. The blue teams were formed by a total of 63 high school students from Central Illinois High Schools. The red team included cybersecurity professionals from State Farm and Illinois State University, whereas the white team consisted of Cybersecurity faculty, student volunteers, and staff who managed the competition and judged the blue teams. The blue team's goal was to complete short tasks assigned by the white team and keep critical services running while dealing with attacks from the red team. Plaques were distributed to the top three blue teams. The competition provided an opportunity for high school students to interact with cybersecurity faculty and students, as well as the penetration testing professionals in our red team, to gain valuable technical skills. We will discuss both technical and organizational aspects of the competition, as well as the industry collaboration behind it. This talk will benefit the CAE in Cybersecurity Community members looking to organize similar events at their locations.

Keywords: Cybersecurity competition, high school.

Building the next generation of cybersecurity faculty: The National Community College Cybersecurity Fellowship Program

[Presentation]

Kristine Christensen, Moraine Valley Community College, IL, christensen@morainevalley.edu

John Sands, Moraine Valley Community College, IL, sands@morainevalley.edu

Michele Robinson, NCyTE, WA, MRobinson@whatcom.edu

Christian Servin, El Paso Community College, TX, cservin1@epcc.edu

Extended Abstract

The rapid growth of cybersecurity threats has created an urgent need for qualified professionals while exposing a critical educator shortage. A 2024 survey of National Centers of Academic Excellence in Cybersecurity (NCAE-C) - Cyber Defense (CD) institutions showed 78% are actively recruiting faculty, with 76% facing industry competition for talent. With student demand high in 74% of institutions and expected to increase in 89% over the next three to five years, this shortage presents a significant challenge (Morris et al., 2024). The National Community College Cybersecurity Fellowship Program helps to address this shortage through a community-centered approach. By recruiting students in their final year or recent graduates with bachelor's or graduate degrees from 4-year NCAE-C institutions and placing them at 2-year NCAE-C institutions, we foster a collaborative relationship that benefits both institutions. The program also actively engages diverse stakeholders and will include business and industry professionals and retiring or recently separated military personnel with security expertise in this year's cohort. The fellowship program follows an integrated training curriculum that includes a 4-hour virtual orientation, a 16-hour Microsoft 21st Century Skills Workshop, a 32-hour Cybersecurity Educator Fundamental Bootcamp, and a 60-hour teaching assistantship, enabling participants to develop comprehensive lesson plans, instructional materials, and practical hands-on activities. Fellows are paired with experienced educators at NCAE-C 2-year colleges and are mentored and supported with resources and professional development throughout their experience. Fellows complete their training with an authentic classroom teaching experience where they put their skills into practice. This multifaceted approach not only addresses the faculty shortage but also sustains a dynamic ecosystem for developing cybersecurity educators within the CAE in Cybersecurity Community. Fellowship alumni have transitioned into roles such as full-time faculty, adjunct instructors, teaching assistants, and K-12 substitute teachers.

Keywords: Cybersecurity education, faculty development, community college.

Reference:

Morris, M., Hammon, J., Anderson, K., Vikayanon, K., Coombs, L., Spragg, A., Giwamogorewa, O., Jirapanjavat, S., & Ilges III, C. L. (2024). Help wanted: Cybersecurity educators - How NCAE institutions are responding. *NICE Community Coordinating Council, Transform Learning Process Working Group.*

Cybersecurity Curriculum Task Force 2.0

[Presentation]

Cara Tang, Portland Community College, OR, cara.tang@pcc.edu

Tobi West, Coastline College, CA, twest20@coastline.edu

Blair Taylor, Towson University, MD, btaylor@towson.edu

Sidd Kaza, Towson University, MD, SKaza@towson.edu

Extended Abstract

Funded by the National Security Agency (NSA) through the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, the mission of the National Cybersecurity Curriculum Task Force was to catalog and create high-quality and relevant curricula on emerging cybersecurity topics, mapping to curricular and workforce guidelines, and make them freely available. That mission was accomplished, including (1) a comprehensive search of available curricula in cybersecurity repositories, directories, and among the community; (2) gap analysis identifying high-need areas for a cyber-ready workforce; and (3) development of high-impact, high-value curricula for the community. Curriculum from this project has been made freely available on Cybersecurity Labs and Resource Knowledge-base (CLARK) (n.d.) and with over 100 learning objects produced in topics such as zero trust security, ransomware, quantum-resistant cryptography, and software supply chain security. As the field of cybersecurity continues to change and grow, as adversaries update their techniques, as new topics emerge, and as Artificial Intelligence (AI) enters the scene in a big way, there is a need for innovative solutions in cybersecurity education and more support for cybersecurity curriculum for the CAE in Cybersecurity Community and beyond. Cybersecurity Curriculum Task Force 2.0 will build upon the successful foundation and processes from the previous task force to develop and implement high-quality, relevant curricula focusing on AI (aligned with the new CyberAI Knowledge Units (KUs)), Secure Coding, and at least two additional cybersecurity areas. The project will serve as a conduit for the existing NCAE-C centers, supporting all curriculum efforts within the CAE in Cybersecurity Community and beyond to meet the growing cyber workforce demand. This presentation will give a summary report on the first curriculum task force, including an overview of the curriculum produced and where to find it freely available on CLARK. The presentation will then introduce Cybersecurity Curriculum Task Force 2.0, including its mission and goals, expected products, and opportunities to participate.

Keywords: Cybersecurity curriculum, CLARK, emerging topics, secure coding, artificial intelligence.

Reference:

Cybersecurity Labs and Resource Knowledge-base. (n.d.). https://www.clark.center

Experiential learning competencies: How hackathons intersect cybersecurity education competencies using industry partnerships

[Presentation]

Christian Servin, El Paso Community College, TX, cservin1@epcc.edu

Jonathan J. Childress, Microsoft, CA, jonathan.childress@microsoft.com

Nadia V. Karichev, El Paso Community College, TX, nmerzlya@epcc.edu

Extended Abstract

Hackathons, commonly utilized for experiential learning through capture-the-flag competitions or challenge-based activities, serve as effective platforms to bridge educational requirements and industry needs. However, institutions—whether two-year community colleges or four-year universities—often face constraints such as limited course contact hours, insufficient resources, and challenges in faculty mentoring and project development. These limitations challenge the delivery of authentic and comprehensive experiences for students pursuing cybersecurity degrees, ultimately impacting their ability to meet industry and workforce requirements. The National Centers of Academic Excellence in Cybersecurity (NCAE-C) - Cyber Defense (CD) mandate that programs of study integrate competencies aligned with cybersecurity workforce roles, as outlined in the NICE and DCWF frameworks. While these frameworks identify tasks, knowledge, and skills, they often lack alignment with practical program needs. Experiential learning opportunities, such as hackathons, capture-the-flag competitions, and national challenges, provide a unique avenue to address these gaps. Despite their potential, logistical and institutional barriers frequently restrict the frequency and depth of such activities within academic semesters. This work presents a set of competencies rooted in the Essential Elements (ABCDE) model (Nestler & Fowler, 2023), implemented through experiential learning at a community college. It outlines a three-day hackathon format designed to foster collaboration between academia and industry professionals, with active participation from industry partners. The approach incorporates coaching to enhance the learning experience, leveraging work-based learning opportunities such as mentoring, cooperative work experiences, and service learning. Furthermore, the work highlights the integration of adversarial thinking as a vital element, enriching the educational impact of these events and addressing the dynamic needs of cybersecurity education.

Keywords: Competencies, experiential learning, industry partnerships.

Reference:

Nestler, V., & Fowler, Z. (2023). *Competency in cybersecurity education: Handbook for Educators at NCAE-C designated institutions*. CAE in Cybersecurity Community.

Cybersecurity informed engineering: An interdisciplinary opportunity

[Presentation]

Sharon Hamilton, Norwich University, VT, shamilto@norwich.edu

Shankar Banik, The Citadel, SC, baniks1@citadel.edu

Colin Chinn, Savannah River National Laboratory, SC, colin.chinn@srnl.doe.gov

Extended Abstract

Given the current and increasing criticality of digital control systems within critical energy infrastructure, there is a priority gap that the cybersecurity and engineering communities and the nation must address. The technicians who support the engineering process often lack training, a body of knowledge, and other reinforcement of cybersecurity practices to effectively address cyber threats in energy infrastructure. The current reliance on the external application of cybersecurity measures by specialized practitioners late in the system implementation lifecycle reduces the systems' overall resilience and cost competitiveness. The result is an increased risk of high-consequence cyber-enabled impacts that threaten national and economic security or public health and safety. Enhanced education is essential to overcoming the shortfall in our nation's cybersecurity informed engineering (CIE) professional capabilities and citizen awareness. The three presenters will introduce current United States (U.S.) national strategies and implementation guides to use as a roadmap for cybersecurity and engineering faculty to integrate more cybersecurity into engineering education, requirements, and practices to develop interdisciplinary cybersecurity curriculum materials, standards, and demonstration projects. The goal is to advance security by design for cyber-physical systems. This interactive session will introduce educational initiatives for CIE. The presenters, representing the CAE in Cybersecurity Community and the Department of Energy National Research Labs, will explore options and initiatives for an educational roadmap that can be used to mature our graduates, in all fields, with CIE awareness and application fundamentals. The presenters will seek to challenge the CAE in Cybersecurity Community, suggest some incremental initiatives that can be taken, and encourage academic, Federal, and business communities to embrace these initiatives as essential to business and organization continuity.

Keywords: Cybersecurity, engineering, infrastructure, interdisciplinary.

Empowering lifelong learning: Digital wallets

[Presentation]

Mike Morris, Western Governors University, UT, mike.morris@wgu.edu

Extended Abstract

The modern workforce faces a rapidly evolving landscape driven by technological advancements and shifting market demands, necessitating a paradigm shift towards lifelong learning. Western Governors University (WGU)'s Achievement Wallet, developed in collaboration with key partners like iQ4, Credential Engine, IBM, and others, and supported by the Lilly Endowment Inc. and Walmart Foundation, directly addresses this need by providing a learner-owned, comprehensive digital record of educational achievements and skills. This platform moves beyond the limitations of traditional transcripts and resumes, offering a nuanced representation of an individual's capabilities and emphasizing the importance of continuous skill development in a digital age where adaptability is crucial. By utilizing linked open data standards like the Credential Transparency Description Language (CTDL), the Achievement Wallet fosters transparency and empowers individuals to curate a verifiable record that effectively showcases their evolving expertise. The Achievement Wallet effectively bridges the persistent gap between education and employment by offering a dynamic solution to the pervasive skills gap challenge. Traditional hiring practices often rely on outdated criteria and fail to recognize the full spectrum of a candidate's abilities, particularly soft skills, which are increasingly vital for success. This platform enables learners to articulate both hard and soft skills acquired through diverse learning experiences, providing employers with a holistic view of their potential.

Keywords: Lifelong learning, skills gap, digital credentials, soft skills, achievement wallet.

Co-developing the pathways tool within the CAE Cyber Competition Atlas

[Presentation]

Jake Mihevc, Mohawk Valley Community College, NY, jmihevc@mvcc.edu

Extended Abstract

Cybersecurity competitions have become a significant part of a holistic cybersecurity education, and student participation in competitions is a requirement for a program to earn and retain CAE designation. The number of competitions has grown dramatically, and it is difficult for students and faculty to identify the best competition, or sequence of competitions, for their program and career goals. The *CAE Cyber Competition Atlas* is embedded within the CAE in Cybersecurity Community website and serves as a visual tool that provides critical information about the competition landscape to prospective competitors. The competitions displayed in the Atlas are the result of National Centers of Academic Excellence in Cybersecurity (NCAE-C) Annual Report data, and the visualization displays the level of NCAE-C engagement as well as linkages between competitions. The *CAE Cyber Competition Atlas* is currently effective in informing students and faculty about the characteristics of individual competitions. Students and faculty need additional functionality and information on common sequences of competitions that students follow to suggest a learning and competition plan for future students, clubs, and programs. The Atlas contains a beta version of the competition pathways tool, and faculty and student input on its conceptual framework can enhance its usefulness, and ultimately the level of NCAE-C engagement it realizes. The goal of this session is to solicit feedback on, and encourage engagement with, the co-development of the pathways tool within the *CAE Cyber Competition Atlas* to maximize its usefulness for students and faculty. The presenter will demonstrate the existing functionality of the Atlas and its underlying data sources and discuss options for the co-development of the pathways tool in the year to come.

Keywords: Cybersecurity competitions, CAE Cyber Competition Atlas, competitions pathways tool, student engagement.

Expanding the K-12 cybersecurity teacher pathway

[Presentation]

Morgan Zantua, City University of Seattle, WA, zantuamorgan@cityu.edu

Jenny Ju, City University of Seattle, WA, jujenny@cityu.edu

Robert Honomichl, City University of Seattle, WA, rjhonomichl@arizona.edu

Marc Dupuis, University of Washington Bothell, WA, marcjd@uw.edu

Extended Abstract

The Cybersecurity High School Innovations (CHI) program offers a replicable model to address the critical shortage of cybersecurity professionals by equipping secondary educators with the skills and resources needed to teach cybersecurity. Based on teaching training programs over three years, 2022 to 2024, the CHI program demonstrates that training more teachers increases the number of students pursuing cybersecurity careers. CHI open-source curriculum aligns with government and industry standards, ensures relevance and adaptability across diverse educational settings. A tiered approach, trains teachers in introductory cybersecurity, Security+ certification preparation, and cyber competitions. Modular content enables educators to introduce content across a wide range of school environments including in urban, rural, tribal, and on-line high schools. Hands-on learning, a cornerstone of CHI, models for teachers how-to engage students through labs, real-world simulations, and interactive activities like capture-the-flag competitions. These practical experiences make complex concepts accessible and foster problem-solving and critical thinking skills essential in cybersecurity. In summers in-person summits teachers meet with corporate, government, and military professionals through virtual and in-person panels, workplace visits, and collaborative activities. Teachers gain insight and advice from cybersecurity professionals learning how to prepare students for cybersecurity careers. The inclusion of cyber competitions increases engagement and exposes teachers with strategies to introduce and engage students to real-world skills applications. CHI's success lies in its scalability and inclusivity as the program bridges gaps in teachers' technical expertise, builds connections to cybersecurity professionals from multiple sectors, and promotes diversity. This adaptable framework serves as a replicable model for other regions and institutions. There have been discussions with other regions and institutions about replicating the framework and model of CHI; however, at this time, it has not been replicated. Since 2022, CHI has trained 99 teachers from 16 different states. During the presentation, more details of the CHI framework, challenges, curriculum, best practices, and lessons learned over the past three years will be discussed, as well as the program's future work.

Keywords: K-12 teacher training, hands-on, open-source curriculum, competitions.

Partnering for cybersecurity: A community college's journey to become a state DHS-based regional SOC

[Presentation]

Rachelle Hall, Glendale Community College, AZ, rachelle.hall@gccaz.edu

Drew Nichols, Glendale Community College, AZ, drew.nichols@gccaz.edu

Extended Abstract

The growing demand for a skilled cybersecurity workforce has prompted innovative partnerships between academia and government agencies. This presentation shares the journey of how a community college collaborated with the state Department of Homeland Security (DHS) to become a Regional Security Operations Center (RSOC). This initiative provides students with a paid, hands-on internship opportunity in a live Security Operations Center (SOC) bridging that gap between academia and employment in the field. The RSOC serves as a vital hub for monitoring, detecting and informing rural municipality clients of potential cyber threats. Rural municipality clients are critical infrastructures across the state that fall within cybersecurity poverty, they are in need of cybersecurity services, but do not have the resources to provide it. The RSOC interns provides cybersecurity services for the municipalities at no cost to them. The partnership integrates DHS resources and expertise with the college's cybersecurity curriculum to provide the opportunity for students to gain real-world experience. This presentation will outline the building of the partnership, aligning educational outcomes with workforce needs and address legal and operational challenges. Through this partnership, the RSOC not only is addressing the national cybersecurity skills gap, it also is empowering students to transition into full-time security positions. It is training a pipeline of job-ready cybersecurity professionals and is a model that can be replicated.

Keywords: Cybersecurity, Department of Homeland Security (DHS), internship, workforce development, community college, regional security operations center.

GPS spoofing: Challenges, detection strategies, and training through real scenarios

[Presentation]

Laxima Niure Kandel, Embry-Riddle Aeronautical University, FL, niurekal@erau.edu

Bhawana Devkota Poudel, Embry-Riddle Aeronautical University, FL, poudelb2@my.erau.edu

Daniel Diessner, Embry-Riddle Aeronautical University, FL, diessned@erau.edu

Extended Abstract

Global Positioning System (GPS) signal spoofing is a sophisticated attack method in which adversaries broadcast false GPS signals to mislead receivers into calculating incorrect Position, Navigation, and Timing (PNT) information. The repercussions of such attacks can be significant, potentially disrupting critical sectors such as aviation, military operations, and financial services. Traditional detection methods, including signal strength analysis and cryptographic techniques, often fall short against advanced spoofing strategies. To address these challenges, our efforts focus on both detection techniques and the development of educational/training materials. On the research front, we investigate the use of Machine Learning (ML), particularly a Random Forest Multiclass Classifier (RFMC), to effectively detect and distinguish between genuine and spoofed GPS signals. To enhance trust and confidence in detection systems, Explainable AI (XAI) methods are employed to provide feature-specific explanations, offering greater transparency and understanding of the decision-making process. In addition to research, hands-on training initiatives are underway to demonstrate GPS spoofing techniques. These efforts leverage the Center of Aerospace Research Systems (CARS) integrated King Air flight deck test benches as part of the Aviation Cyber Initiative (ACI) Cyber Rodeo initiative. Using these test benches with integrated flight simulation capabilities, interactive, pilot-in-the-loop cyber scenarios are developed.

Keywords: GPS spoofing, GPS spoofing detection, GPS spoofing detection using ML/AI, pilot training.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Growing the cybersecurity workforce: Enhancing career guidance through professional development for advisors and counselors

[Presentation]

Kristine Christensen, Moraine Valley Community College, IL, christensen@morainevalley.edu

John Sands, Moraine Valley Community College, IL, sands@morainevalley.edu

Jiri Jirik, Moraine Valley Community College, IL, jirik@morainevalley.edu

Michele Robinson, NCyTE, WA, MRobinson@whatcom.edu

Extended Abstract

Although the cybersecurity sector employs over 1.2 million professionals in the United States, it faces a workforce gap of approximately 450,000 unfilled positions. A significant barrier to addressing this gap is the lack of understanding of cybersecurity work roles. While funding efforts have been allocated for developing robust cybersecurity curricula and programs, there are limited resources and training opportunities available for career counselors, academic advisors, and educators to help them confidently guide students into cybersecurity career pathways. This research examined how targeted professional development for academic advisors and career counselors enhances their ability to connect with and guide students effectively toward cybersecurity careers and pathways. This study employed a quasi-experimental design with 61 participants, including K-12 counselors, advisors, faculty, and administrators, as well as their community college and four-year college counterparts. It assessed participants' baseline knowledge, delivered a Cybersecurity Career Awareness Workshop, and evaluated outcomes through pre- and post-workshop surveys. The workshop provided participants with a toolkit containing information about the cybersecurity career landscape, academic pathways, industry certifications, and resources such as the NICE Workforce Framework and Cyberseek.org. Key findings indicate significant improvements in participants' confidence and knowledge. Pre-workshop surveys revealed that over 70% of participants felt either "slightly confident" or "not confident at all" in advising students about cybersecurity pathways. Post-workshop evaluations demonstrated a 25% increase in confidence, with over 60% of participants reporting feeling "somewhat confident" or higher levels. The most substantial improvement was observed among participants who were initially slightly confident, with some reaching "very confident" after the training. The results demonstrate that the training positively impacted participants' confidence in guiding students on cybersecurity career paths and counseling students on the necessary knowledge, skills, and abilities to succeed in various cybersecurity roles. Most importantly, by improving career guidance resources and preparedness among counselors and advisors, this initiative can help address the critical cybersecurity workforce gap and build a more diverse cybersecurity workforce.

Keywords: Cybersecurity workforce, academic advising, career counseling, career pathways.

Guiding your students to new heights in space cybersecurity

[Presentation]

Anna Carlin, Fullerton College, CA, acarlin@fullcoll.edu

Tobi West, Coastline College, CA, twest20@coastline.edu

Extended Abstract

As space exploration and technology continue to advance, the need for robust cybersecurity measures in the space industry has become increasingly critical. Imagine a day without GPS to help with navigation or to find your missing device. As educators, we can encourage students to understand and contribute to the rapidly evolving field of space cybersecurity. Cybersecurity challenges faced by space missions, satellites, and communication networks are especially different when identifying differences between space and terrestrial cybersecurity. A key challenge to furthering space cybersecurity is the limited sharing about space cyberattacks which inhibits conducting a post-mortem analysis of vulnerabilities exploited, incident response steps taken, and measures taken to strengthen cyber resiliency (Neher et al., in press). The ability to fix security issues requiring physical access to space systems on orbit is nearly impossible as its mission could be for several years or decades before retirement. Numerous opportunities are available to engage students through internships and scholarships where students can gain hands-on experience in the field. Sharing these opportunities is key to inspiring the next generation of cybersecurity experts safeguarding the future of space exploration.

Keywords: Space cybersecurity, space internships, U.S. Space Force, Air Force Research Laboratory (AFRL), SMART scholarships.

Reference:

Neher, S., Groves, D., Yune, H., Rodriguez, R., Broaddus, S., & Cheng, E. (*in press*). Associated attack surfaces and vulnerabilities of space vehicle autonomous functions. *Proceedings of the 2025 IEEE Aerospace Conference.*

Share the spark: Advancing the development of new and early-career faculty in the CAE community

[Presentation]

Paige Zaleppa Flores, Towson University, MD, pzaleppa@towson.edu

Gretchen Bliss, University of Colorado, Colorado Springs, CO, gbliss@uccs.edu

Extended Abstract

As the demand for skilled cybersecurity professionals continues to grow, it is critical to build a strong pipeline of educators who are equipped to prepare the next generation of cybersecurity experts. Addressing this need, the *CAE-CD New and Early Career Faculty Initiative* **(**National Centers of Academic Excellence in Cybersecurity, n.d.) is dedicated to supporting emerging educators by fostering connections within the CAE in Cybersecurity Community through virtual workshops, networking opportunities, and resource-sharing. To date, this initiative has hosted 10 workshops, attracted over 170 registrants and has garnered more than 650 views on YouTube (YouTube, n.d.). By focusing on new and early-career faculty development, this initiative aims to equip educators with the tools and knowledge needed to provide high-quality cybersecurity education aligned with industry standards and workforce needs. This presentation will provide an in-depth overview of the initiative's previous workshops and activities, highlighting successful strategies and key takeaways that have supported new and early-career faculty. In addition to reflecting on past efforts, the session will introduce new ideas for future workshops and professional development activities designed to address the evolving challenges faced by early career educators in cybersecurity. These proposed ideas will focus on topics such as innovative teaching methods, useful resources, and getting involved with extracurricular opportunities for students. Throughout the session, attendees will have multiple opportunities to provide feedback on the presented ideas and strategies. Participants will also be invited to share their insights and suggest additional topics or approaches that could further strengthen the support provided to new and early-career faculty in the CAE in Cybersecurity Community.

Keywords: Faculty development, early-career faculty, professional development, workshops.

References:

National Centers of Academic Excellence in Cybersecurity. (n.d.). *CAE-CD new and early- career faculty members*. Retrieved January 15, 2025, from https://caecommunity.org/cae-cd-new-and-early-career-faculty-members

YouTube. (n.d.). *New and early-career faculty members playlist*. YouTube. Retrieved March 10, 2025, from https://www.youtube.com/playlist?list=PLo3yqKgTfZlNHAYUJZUMDf8EN4R7FEzvl

Securing student futures: Working with career services as a critical partner in cybersecurity education

[Presentation]

Caroline Jennings, SANS Technology Institute, MD, cjennings@sans.edu

Extended Abstract

Discover how SANS Technology Institute (SANS.edu)'s undergraduate programs have redefined success by embedding career outcomes into their program metrics—achieving industry-leading results.

- Over 70% of the job seeking Bachelor in Applied Cybersecurity students at SANS Technology Institute have jobs prior to graduation. Of those who earned a role in cybersecurity after program completion, 0% took longer than six months to earn a job offer. The median starting salary for those job seeking graduates was about $114,000.
- SANS Technology Institute adopted an intrusive academic and career advising style, and career outcomes are central to ongoing curriculum and program evaluation. Career Services' integration into the curriculum and ongoing student support has led to such high outcomes, leaving us with some lessons learned.

This session will unpack the strategies behind these outcomes and explore how you can partner with your campus Career Services office to enhance your students' career trajectories. Additionally, gain insights into what Career Services may need (but might not know to request) from cybersecurity faculty and take a deep dive into the realities of today's job market.

- Career Services and faculty should be aligned on what a cybersecurity resume looks like and what hiring managers are looking for. Faculty and Career can also collaborate on common base information, including critical skills, certifications, and even the tangible value of experiential and co-curricular experiences.
- Gain insight to reinforce Career Services messaging on best practices in job searches, including how to pass ATS screenings, key free or existing university resources to prepare resumes and mock interviews.

Learn how to adapt your curriculum, assignments, and projects utilizing some suggested resources to better equip your students for success in their cybersecurity career journeys.

Keywords: Cybersecurity career outcomes, career services integration, job market readiness.

Proposed CAE CoP-CD "Rural CAEs" initiative

[Presentation]

Debasis Bhattacharya, University of Hawaii Maui College, HI, debasisb@hawaii.edu

Gary Sparks, Metropolitan Community College, NE, GSparks@mccneb.edu

Stu Steiner, Eastern Washington University, WA, ssteiner@ewu.edu

Extended Abstract

This proposed National Centers of Academic Excellence in Cybersecurity (NCAE-C) - Community of Practice in Cyber Defense (CoP-CD) initiative includes quarterly workshops and a list of resources to be shared on the CoP-CD page. Its goal is to address the challenges facing NCAE-C in Cyber Defense (CD) institutions in rural United States (U.S.) locations.

These may include issues such as:

- Addressing the limited job opportunities for graduates from a NCAE-C in a rural location
- Addressing the limited or lack of local chapters of professional associations and federal groups (e.g., Information Systems Audit and Control Association (ISACA), Information Systems Security Association (ISSA), Federal Bureau of Investigation (FBI) affiliated InfraGard)
- Addressing the lack of incoming student enrollment in NCAE-C cybersecurity programs

The goal is also to develop a working list of resources and tools rural NCAE-C institutions can use to alleviate some of the abovementioned challenges. The Co-Chairs will have open discussions and solicit feedback from the CAE in Cybersecurity Community to select committee members for this initiative.

Keywords: Rural academic institutions, cybersecurity, NCAE-C Community of Practice in Cyber Defense (CoP-CD) initiative.

Partnerships in action: A collaborative approach to launching community college students into cyber careers

[Presentation]

Eva Dring, SANS Technology Institute, MD, edring@sans.edu

Kim Kafka, SANS Technology Institute, MD, kkafka@sans.edu

Caroline Jennings, SANS Technology Institute, MD, cjennings@sans.edu

Extended Abstract

The growing demand for cybersecurity professionals presents a significant opportunity for higher education institutions, particularly community colleges, to play a leading role in preparing students for these critical roles. This presentation explores a partnership model developed by the SANS Technology Institute (SANS.edu), which enables students to transition from foundational coursework at community colleges to advanced, industry-aligned cybersecurity training and professional certifications, culminating in a Bachelor's Degree in Applied Cybersecurity (BACS). The partnership is designed to be both scalable and resource-efficient, integrating community college coursework into an upper-level degree. Students pursuing an Associate of Applied Science (AAS) in Cybersecurity can directly apply their credits to the SANS Technology Institute Bachelor's program, but earned credits from any associate degree can be also be transferred, providing broad accessibility and flexibility. Students complete up to 70 transferable credits at their community college before advancing to SANS Technology Institute for 50 credits of specialized training. Like community colleges, SANS Technology Institute has a large population of students who are also working professionals, and all of the programs offered are designed to accommodate this. The learning model emphasizes practical, hands-on learning through flexible delivery, with students earning nine industry-recognized Global Information Assurance Certification (GIAC) certifications, ensuring they are workforce-ready upon graduation. Community colleges have excellent track records of getting students into the workforce and being incredibly attuned to workforce needs; SANS Technology Institute can help provide additional tools to accelerate advancement throughout their careers. This case study will present data and outcomes from existing partnerships, demonstrating the significant career benefits for students, including an average starting salary of $110,000 for job-seeking graduates. It will also address how community colleges can enhance their institutional reputation and student success metrics through this collaboration, all while maintaining a low barrier to implementation. By highlighting the successes of this partnership and offering a roadmap for replication, this session aims to inspire community college representatives to consider similar opportunities to strengthen their programs and improve student outcomes in the high-demand field of cybersecurity.

Keywords: Collaboration, partnership, community college, careers in cybersecurity, flexible learning, lifelong learning.

Challenges and opportunities at the intersection of AI and cybersecurity

[Presentation]

Greg Gogolin, Ferris State University, MI, gogoling@ferris.edu

Isaac Gogolin, Michigan State University, MI, gogolini@msu.edu

Extended Abstract

This presentation will describe some of the challenges and opportunities with integrating AI into the cybersecurity landscape from both an offensive and defensive perspective. Topics include data and model quality issues (particularly in temporal environments), appropriate use, and best practices in detecting and responding to cybersecurity threats with Artificial Intelligence (AI). A case study overview of integrating an ABET accredited National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CD) degree with an undergraduate AI degree will be described. This will include some of the challenges that intersect opinion, experience, theory and practicality, which will point to the number one cybersecurity threat that nobody seems to be talking about. This will be further supported by looking at data leakage challenges and reproducibility failures described by Kapoor and Narayanan (2023), as well as workforce considerations. An overview of some ways that AI can be used within cybersecurity will include the use of a Large Language Model (LLM) that incorporates Metasploit in cybersecurity reconnaissance and penetration testing. Additional factors such as deployment considerations will further illustrate some of the challenges and opportunities that exist at the intersection of AI and cybersecurity, including cybersecurity of AI.

Keywords: Artificial Intelligence, cybersecurity, LLM, Metasploit, education, cybersecurity threats.

Reference:

Kapoor, S., & Narayanan, A. (2023). Leakage and the reproducibility crisis in ML-based science. *Patterns, 4*(9), 100779. https://doi.org/10.1016/j.patter.2023.100779

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Educating offensive AI model security experts: Challenges, opportunities, and viable pipelines

[Presentation]

Xiuwen Liu, Florida State University, FL, liux@cs.fsu.edu

Mike Burmester, Florida State University, FL, burmester@cs.fsu.edu

Extended Abstract

Offensive computer security has played a critical role in improving cyber security. Focusing on software vulnerabilities and exploits has led to the developments of common weakness enumerations and associated tools to identify them. The associated educational and research programs have trained offensive cybersecurity experts. Collectively, they have greatly improved security of numerous applications, resulting in secure coding practices with a broad impact. Pretrained, large foundation models play a central role in the recent surge of artificial intelligence, resulting in finetuned models with remarkable abilities when measured on benchmark datasets and standard exams. Due to their inherent complexity, these models are poorly understood. While the existence of small adversarial inputs to such models is well known, the structures of the representation space are not well characterized despite their fundamental importance. At the same time, as such models are being integrated with more and more applications, securing such AI models and applications is becoming critically important. How to train the future experts who have the necessary understanding and knowledge of inner workings of Artificial Intelligence (AI) models and hands-on skills to test and secure them is an emerging frontier in cybersecurity education. Building on our understanding of the fundamental principles and extensive experience working in both AI and cyber security, we have developed a viable and effective pipeline to produce offensive AI model security experts. For the students in the selected group, they would take a deep and reinforcement learning course we offer in their senior year to learn the fundamental principles underlying the current AI models. Then these students are given opportunities in various classes to apply such models to solving cybersecurity problems such as penetration testing and program analysis. With their insights, the developed models tend to work much better than other existing solutions. In addition, the students are encouraged to understand and analyze the inner workings and inherent limitations of these models to further their skills and knowledge and develop offensive AI security techniques. In this talk, we will discuss how our pipeline is implemented, how we overcome the practical challenges our students face, and how our pipeline can be adopted more broadly. Furthermore, we will discuss broader challenges in the emerging offensive AI model security and ways to overcome them collectively. Together, we think the CAE in Cybersecurity Community can develop effective pipelines to meet the emerging needs and challenges produced by the large foundation AI models.

Keywords: Offensive AI, LLMs, AI security, offensive computer security.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Cybersecurity education vs. AI: Designing labs that prioritize thinking over tooling

[Presentation]

Sebastian Hayes, Brigham Young University, UT, Sebastian_hayes@byu.edu

Albert Tay, Brigham Young University, UT, albert_tay@byu.edu

Extended Abstract

As Artificial Intelligence (AI) technologies advance, educational environments face an increasing challenge: maintaining rigorous, authentic assessments that effectively teach applicable skills. Nowhere is this challenge more pronounced than in fields like cybersecurity, where hands-on labs and assignments are essential for skills acquisition. The growing accessibility and sophistication of AI tools have introduced a paradox. While these technologies provide invaluable support to professionals, they may also undermine the critical learning process for students, who might rely on AI-generated solutions instead of actively engaging with the material. This presentation aims to address these challenges by providing educators with strategies and principles for designing cybersecurity lab assignments that are resilient to complete AI-generated solutions. By implementing these methods, instructors can ensure students engage in critical thinking, hands-on practice, and genuine learning experiences. The goal is not to eliminate AI tools from the classroom but to establish a framework where its use complements, rather than undermines educational objectives. The most effective strategy we have found is carefully wording lab instructions. While humans can interpret ambiguous terms in context, AI models often misinterpret them, leading to unintended consequences. In one malware removal lab, the instructions stated: "These are the known hash values of malicious files. However, hackers may alter files to create hashes we are unaware of." A student input these instructions into an AI model, which generated seemingly valid code. However, the model misinterpreted "hashes we are unaware of" to mean any unlisted hash, causing the script to indiscriminately delete all system files, rendering the machine unusable. Although the AI-generated code was technically functional, the student failed to verify its logic before execution. While we recognize that AI is a valuable tool in a cybersecurity professional's arsenal, it should enhance—not replace—the learning process. By resisting the over-reliance on AI tools and fostering critical thinking, we can equip students with the skills they need in an increasingly AI-driven world.

Keywords: Cybersecurity, AI tools, critical thinking, skill acquisition.

A dynamic learning object framework for quantum security workforce development

[Presentation]

Abhishek Parakh, Kennesaw State University, GA, aparakh@kennesaw.edu

Mahadevan Subramaniam, University of Nebraska Omaha, NE, msubramaniam@unomaha.edu

Extended Abstract

The emerging fields of quantum computing, communications, and networking present unique educational challenges due to their highly transdisciplinary nature, spanning quantum mechanics, computer science, cryptography, and network engineering. Traditional educational approaches are inadequate for teaching these complex subjects, while the scarcity of quantum infrastructure limits hands-on learning opportunities. This poses a significant challenge for the Cyber Defense community, which needs a well-trained workforce capable of understanding and securing quantum communications and networks. In this presentation, we describe QUINTET, which addresses these challenges by providing an innovative experiential learning platform that automatically generates personalized learning paths based on student needs and time constraints. The platform utilizes a modular architecture built around Learning Objects (LOs) - self-contained educational units that include interactive simulations, coding exercises, assessment tools, and small educational games (gamelets) focused on quantum concepts. These LOs are organized into three categories: foundational knowledge units, bridge knowledge units connecting different disciplines, and interdisciplinary knowledge units integrating multiple domains. The platform employs a novel fractional knapsack algorithm to synthesize optimal learning sequences that maximize educational value within specified time constraints while ensuring prerequisite knowledge is covered. Learning paths are delivered through Jupyter notebooks that integrate with quantum computing platforms from IBM, Microsoft, and Amazon, allowing students to gain practical experience with quantum programming. What distinguishes QUINTET is its ability to adapt content delivery based on student prerequisites and learning objectives while incorporating hands-on experimentation through virtual labs, interactive simulations, and educational gamelets. The platform includes comprehensive modules covering quantum cryptography, quantum key distribution, quantum routing protocols, and quantum network security principles - topics crucial for developing a quantum-ready cybersecurity workforce. This approach significantly advances quantum education solutions by providing an integrated, experiential learning environment that connects theoretical concepts with practical applications. The platform's ability to automatically generate customized curricula while maintaining pedagogical coherence makes it particularly valuable for workforce development in quantum cybersecurity, where practitioners must acquire interdisciplinary expertise quickly. Initial feasibility testing suggests QUINTET effectively addresses the challenges of quantum education through its adaptive, hands-on approach. This project is partly funded by NSF awards 2324924 and 2324925.

Keywords: Experiential learning, quantum education, quantum internet, learning objects.

Recruiting transitioning veteran and first responder students for cybersecurity work roles

[Presentation]

Justin Pelletier, Rochester Institute of Technology, NY, jxpics@rit.edu

Brock Wagehoft, Rochester Institute of Technology, NY, bewics@rit.edu

Mary Wallingsford, Anne Arundel Community College, NY, mewallingsford@aacc.edu

Extended Abstract

Recruiting military veterans and first responders for cybersecurity roles presents a unique opportunity to address the workforce gap. According to the *2024 Cybersecurity Workforce Study* by International Information System Security Certification Consortium (ISC2, 2024), the global cybersecurity workforce shortage has grown by 19%, leaving a 4.8 million worker deficit. Veterans and first responders possess mission-critical training, strategic thinking, adaptability, and crisis management skills that make them well-suited for cybersecurity careers, particularly in Governance, Risk, and Compliance (GRC), incident response, and threat mitigation. Additionally, some veterans already have security clearances and are familiar with defense-related technologies that can accelerate their transition into cybersecurity roles. Many possess leadership and teamwork capabilities and a desire to continue serving even after they are no longer able to meet the physical demands of their previous professions. However, recruiting this specific population comes with its own challenges, including competing home and work responsibilities, financial barriers, and a shortage of entry-level cybersecurity positions. Additionally, transitioning veterans and first responders may struggle with confidence and finding a sense of purpose in civilian careers. Successful recruitment strategies include leveraging networks such as the Veterans of Foreign Wars (VFW), American Legion, Veterans Upward Bound, veteran services offices, and government transition assistance programs (TAP). Direct marketing via phone, email, and social media, along with outreach at veteran events and workforce development offices, has proven effective. A coalition of institutions has developed a pilot workforce program to create pathways for veterans and first responders into cybersecurity careers. Recruiting from this largely untapped pool of talent whose skills and values align with the core demands of cybersecurity can be effective. Securing GI Bill funding for non-vocational programs and partnering with organizations such as the Veteran's Administration will enhance sustainability and impact. By prioritizing tailored support, including financial assistance (tuition and stipends), structured training and mentorship, educational institutions can increase enrollment and success rates, ultimately strengthening the cybersecurity workforce.

Keywords: Governance, Risk, and Compliance (GRC), scholarship, veteran, recruit.

Reference:

ISC2. (2024, October). *2024 ISC2 cybersecurity workforce study*. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

Homomorphic encryption and statistical confidentiality

[Presentation]

Yeşem Kurt Peker, Columbus State University, GA, peker_yesem@columbusstate.edu

Rahul Raj, Columbus State University, GA, raj_rahul@students.columbusstate.edu

Extended Abstract

Statistical confidentiality is the protection of data while ensuring it can be used for statistical purposes *(*European Union - Eurostat, n.d.*)*. It involves reducing the risk of identifying individuals from data collected for research or statistical analysis and ensures that data collected for statistical purposes is used exclusively for those purposes. Statistical confidentiality provisions enable aggregate statistical analysis while preserving the anonymity of data subjects. Data collectors use techniques such as encryption, access control, anonymization, and differential privacy to comply with statistical confidentiality requirements. While these methods provide varying levels of protection, they often have limitations, particularly when plain data, though not directly linked to individuals, remains accessible. Homomorphic encryption allows computations on encrypted data without revealing it to anyone other than an authorized collector. When combined with other techniques, homomorphic encryption offers an ideal solution for ensuring statistical confidentiality. Fast Torus Fully Homomorphic Encryption (TFHE) is a fully homomorphic encryption scheme that supports efficient homomorphic operations on Booleans and integers. In this study, we investigate the use of TFHE for conducting statistical analysis on encrypted data. We utilize Zama's Concrete Compiler (*Zama.ai*, n.d.) to execute basic statistical operations within a Docker environment with limited resources (eight Central processing unit (CPUs) and eight GB memory) on a system with an 11th Gen Intel Core i5 processor and 16GB RAM. The results show that basic tasks like calculation of mean and finding min/max work well for small datasets while keeping data encrypted. However, more complex tasks like calculation of median and variance slow down dramatically as datasets get larger due to the compiler's limitations in handling decimals, dynamic logic and performing division. While this work confirms the theoretical viability of Fully Homomorphic Encryption (FHE) for statistical analytics, practical implementation demands substantial optimizations to make it viable for real-world applications.

Keywords: statistical confidentiality, homomorphic encryption, privacy, TFHE.

References:

European Union - Eurostat. (n.d.) *Statistical confidentiality and personal data protection.* https://ec.europa.eu/eurostat/web/microdata/statistical-confidentiality-and-personal-data-protection

Zama.ai (n.d.). *Concrete.* https://docs.zama.ai/concrete

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Agentic workflows for cybersecurity education

[Presentation]

Tianyu Wang, Mercy University, NY, twang4@mercy.edu

Nianjun Zhou, IBM Watson Research, NY, jzhou@us.ibm.com

Zhixiong Chen, Mercy University, NY, zchen@mercy.edu

Extended Abstract

This work-in-progress presentation introduces a multi-agent learning framework designed to enhance cybersecurity education by leveraging large language models (LLMs) technologies with rich peer-reviewed cybersecurity resources from the CAE in Cybersecurity Community, including the Cybersecurity Labs and Resource Knowledge-base (CLARK) digital library. Cybersecurity education faces distinct challenges, including the rapid evolution of threats and tools, the need for industry-relevant skill development, and the balance between theoretical knowledge and practical application. Additionally, educators must continuously update curricula to reflect emerging cybersecurity trends while ensuring accessibility and engagement for learners at different proficiency levels. The platform employs a Retrieval-Augmented Generation (RAG) architecture, enabling dynamic access to curated learning resources such as slides, quizzes, lab exercises, and videos. This modular structure ensures content relevance while offering learners targeted and comprehensive educational experiences. The intelligent integration of these resources supports continuous learning and helps instructors customize materials for diverse learning needs. The framework operates through a structured multi-agent workflow. Users initiate learning by submitting queries to the interactive Query Agent, which invokes a Retrieve Agent. The Retrieve Agent searches and compiles relevant content. To reinforce learning, an Evaluation Agent generates exercises for users based on retrieved content, assesses responses, and provides adaptive feedback. By integrating active learning strategies and explicitly mapping content to cybersecurity skill sets and career pathways, the system bridges the gap between academic education and workforce readiness. Furthermore, its adaptive learning capabilities empower students to progress at their own pace while receiving personalized guidance tailored to their goals. The ability to track learner progress and adjust content dynamically enhances engagement and retention, making cybersecurity education more effective. This framework represents a step toward scalable, AI-driven cybersecurity education, aligning with CAE objectives to enhance workforce preparedness through innovative, evidence-based learning methodologies. Future work will focus on refining agent coordination and expanding the framework's capabilities to better serve educators and learners in the cybersecurity field.

Keywords: Cybersecurity education, CLARK, Large Language Models (LLMs), Retrieval-Augmented Generation (RAG), multi-agent, agentic workflow.

Immersive Cybersecurity Workforce Development Program to prepare current and future workforce in critical infrastructure

[Presentation]

Tirthankar Ghosh, University of New Haven, CT, tghosh@newhaven.edu

Tobi West, Coastline College, CA, twest20@coastline.edu

Ram Dantu, University of North Texas, TX, ram.dantu@unt.edu

Debasis Bhattacharya, University of Hawaii Maui College, HI, debasisb@hawaii.edu

Maanak Gupta, Tennessee Technological University, TN, mgupta@tntech.edu

Extended Abstract

The Immersive Cybersecurity Workforce Development Program is a new coalition led by the University of New Haven to develop a sustainable, skills-based, competency-focused workforce development program to educate and train existing and future workforce in four critical infrastructure sectors - energy, government facilities, finance, and telecommunications. The coalition partners are geographically diverse and will lead efforts as described below: *University of New Haven* (CAE-CO) will work with regional and state financial institutions, state and local governments to create and offer pathways for AI in Cybersecurity and Cyber Threat Intelligence for Finance. *Tennessee Technological University* (CAE-CD) will create pathways for the energy sector for first responders and transitioning military in collaboration with national labs such as Oak Ridge National Lab and Pacific Northwest. *University of Hawaii - Maui College* (CAE-CD) will complement the Good Jobs Hawaii initiative to create introductory cybersecurity certificates for state and local employees, small businesses and non-profits. *Coastline College* (CAE-CD) will extend the workforce development work done through the state-funded California Cybersecurity Apprenticeship Program (CCAP) to offer a Cybersecurity Fundamentals certificate for the telecommunications sector. *University of North Texas* (CAE-CD & CAE-R) will develop and pilot a workforce readiness assessment tool to map participants' skills and knowledge to work roles, tasks and job descriptions that would augment employer's efficacy for their hiring process. The program was funded through a $2.47 million grant from National Security Agency (NSA) – National Centers of Academic Excellence in Cybersecurity (NCAE-C) and will target existing workforce to upskill them and help them transition into cybersecurity jobs. Additionally, the program will prioritize recruitment of veterans, transitioning military, first responders and military spouses to help them transition into cyber workforce with entry-level training and pathways. The coalition will develop and pilot a tool that will map participants' skills and knowledge to cybersecurity work role tasks from job descriptions that will assist employers in assessing applicants' competencies and augment the process of efficient hiring.

Keywords: Workforce development, workforce readiness, skills mapping.

AI-driven cyber defense for drone mission recovery at the tactical warfighting edge

[Presentation]

Prasad Calyam, University of Missouri-Columbia, MO, calyamp@missouri.edu

Rohit Chadha, University of Missouri-Columbia, MO, chadhar@missouri.edu

Vijay Anand, University of Missouri-St. Louis, MO, vijay.anand@umsl.edu

Reshmi Mitra, Southeast Missouri State University, MO, rmitra@semo.edu

Extended Abstract

Drones play a vital role at the Tactical Warfighting Edge (TWE), supporting reconnaissance, logistics, and situational awareness at the edge. However, ensuring the security and safety of these drones, particularly when they lose connection with their control stations on the ground due to physical or malicious causes, remains a significant challenge. Adaptive navigation and secure communication of drones are critical for mission success in contested environments with intermittent connectivity and adversarial threats. This is an important topic for the CAE in Cybersecurity Community because it addresses modern cyber threats on constrained edge devices such as drones equipped with cameras and sensors, which need to be handled with low-overhead zero trust solutions that are well established in unconstrained data center networks. Further, this topic is of high interest to Department of Defense (DoD) community and can foster collaborations between academia in the CAE in Cybersecurity Community and various DoD stakeholders for furthering both research and education initiatives. In this presentation, we outline an Artificial Intelligence (AI)-driven security framework that integrates different security components such as an Intelligent Drone Trajectory Management (IDTM) model based on the Q-Learning algorithm, designed to ensure resilience and security in degraded network conditions via drone guidance optimization. Specifically, the IDTM enables the drone to continue its mission, divert to a fallback location, or return to base when network connectivity with the Google Cloud Storage (GCS) node is lost. By leveraging hardware and software integrations, the framework enables continuous monitoring, dynamic authentication, microsegmentation, and other security controls to protect drone communications and operations from network and physical attack threats in TWE settings. We detail a realistic testbed for both simulation and experimentation in a tactical grid environment to evaluate the framework's performance under conditions simulating electronic warfare, hijacking, and network intermittence. Simulations use a realistic grid environment with obstacles, no-fly zones, and dynamic threats, while physical testbeds with drones and development boards validate real-world performance. Through simulation results, we demonstrate that the proposed AI-driven framework achieves a mission success rate at high reward ratio with minimal safety trade-offs when combined with Trust Zone Enforcement. We also demonstrate how the hardware testbed validation results show that our approach enhances drone survivability and ensures resilient computation and communication operations in contested environments, even under Global Positioning System (GPS) spoofing and signal jamming conditions.

Keywords: Edge network attacks, tactical warfighting edge, drone mission guidance, reinforcement learning, network microsegmentation.

Refereed Extended Abstract Proceedings for Mini-Workshops

Computer squad detectives: A digital forensics case exemplifying social justice

[Mini Workshop]

Denise Dragos, St. John's University, NY, dragosd@stjohns.edu

Suzanna Schmeelk, St. John's University, NY, schmeels@stjohns.edu

Extended Abstract

This mini workshop proposal showcases and compresses a digital forensics intervention based on a real-life public social justice case in the Northeast New York on which the author worked. The workshop's curricular design and IRB-approved participant feedback of a digital forensics workshop curriculum (Dragos & Schmeelk, 2023) is designed for the audience to engage in the case and become real-life computer squad detectives. The authors' curricula design can be a standalone learning experience, integrated within a forensics component of a cyber security course (e.g., Network Perimeter Security), or expanded into other settings. The workshop showcases skills needed for foundational digital forensics (DFR) fieldwork and explains pedagogical techniques and successful environments for building inclusive classrooms that have been successful as reported by heterogeneous students. Forensics topics in the curriculum are selected from the following areas found in a foundational digital forensics course: data acquisition; processing crime/incident scenes; information retrieval from Windows, Macintosh, and Linux systems; recovering graphical, Word, Acrobat, and other file types; virtual machine forensics; investigating emails; examining social media data; writing investigation reports; studying the importance of ethics for expert witnesses; and, understanding expert testimony in digital investigations (Cooper et al., 2010; Roy et al., 2019). The anticipated skills covered in the mini workshop are components of a full semester course which covers the basics for cybercrime and cyber-incidents to prepare students for interaction with law enforcement agencies, interaction with organizational forensic teams, and further digital forensic courses (e.g., Advanced Digital Forensics, Mobile Device Forensics, Incident Response, Malware Analysis, and Management of Digital Evidence).

Keywords: Digital forensics education, DFR, social justice, legal cases, crime solving skills, IRB-participant feedback, mini workshop.

References:

Cooper, P., Finley, G. T., & Kaskenpalo, P. (2010). Towards standards in digital forensics education. *Proceedings of the 2010 ITiCSE Working Group Reports, 87–95*. https://doi.org/10.1145/1971681.1971688

Dragos, D., & Schmeelk, S. (2023). Foundational digital forensics skills and learning: Exemplifying social justice. *Proceedings of the 2023 IEEE Frontiers in Education Conference (FIE)*, College Station, TX, USA, 2023, pp. 1-6. https://doi.org/10.1109/FIE58773.2023.10343015

Roy, S., Wu, Y., & LaVenia, K. N. (2019). Experience of incorporating NIST standards in a digital forensics curricula. *Proceedings of the 7th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS.2019.8757533

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Leveraging local LLMs for custom cybersecurity tool development: A hands-on workshop

[Mini Workshop]

Vincent Nestler, California State University, San Bernardino, CA, vnestler@csusb.edu

Extended Abstract

As artificial intelligence becomes increasingly integrated into cybersecurity practices, educators face the challenge of incorporating AI tools while maintaining security and privacy. This workshop introduces a practical approach to utilizing local Large Language Models (LLMs) for developing custom cybersecurity tools, offering a secure and cost-effective alternative to cloud-based Artificial Intelligence (AI) services. Through hands-on demonstration using Ollama and Open-WebUI, participants will learn how to leverage local LLMs like Llama, Nemotron, and Mistral to create specialized security tools for vulnerability scanning, penetration testing, and network monitoring. The workshop showcases real implementations from an ethical hacking course, where students successfully developed custom tools without the constraints of cloud-based AI services' community guidelines or rate limits. This approach addresses critical concerns in cybersecurity education: maintaining data privacy, ensuring unlimited access to AI resources, and preparing students for enterprise environments where local AI deployment is preferred. Participants will gain practical knowledge of the complete workflow - from concept development and prompt engineering to code generation and refinement - enabling them to immediately implement these techniques in their classrooms. This session bridges the gap between AI capabilities and cybersecurity education needs, providing educators with a secure, practical, and pedagogically sound approach to tool development.

Keywords: Local LLMs, cybersecurity education, tool development, artificial intelligence, practical pedagogy, ethical hacking, hands-on learning.

Delivering cyber education content in Browser-Based Virtual Machines (BBVMs)

[Mini Workshop]

Nicklaus A. Giacobe, Penn State University, PA, nxg13@psu.edu

Matthew A. Ruff, Oregon State University, OR, matt.ruff@oregonstate.edu

Extended Abstract

Cyber educators are often faced with the financial challenge of where to host virtual machines to teach our students the basics of computers. The current options are expensive or add unhelpful complexity. Some use desktop hypervisors, which are difficult to manage for large groups of students with diverse hardware. Others host virtual machines on bare-metal hypervisors in data centers, but that can be expensive. A third option is hosted labs provided by textbook publishers and others. However, those can be expensive, and limit flexibility of content provided. Browser-Based Virtual Machines (BBVMs) provide technology educators with constrained operating systems and without back-end hypervisors. The BBVM is delivered via Apache or nginx, and runs completely inside the web browser in JavaScript using the student computer Central Processing Unit (CPU). In this session, we will provide detailed instructions to implement the v86 project to deliver BBVMs, and the BrowserVM project to create custom Buildroot .iso files with instructor-developed content. BBVMs seem to have started from Bellard's jslinux, as early as 2011 and includes a few different distros of Linux, with text and X Window interfaces. Bellard's work is self-published but is difficult to reproduce. However, the x86 emulation he created allows a full virtual machine to run inside of the browser's JavaScript Virtual Machine (VM). This means that once the VM is delivered to the end-user's web client, it runs locally, rather than on a remote server. Fabian (copy.sh)'s x86 project extends Bellard's work with multiple distros of Linux, Windows and other operating systems. We extend the work of Ruff and Giacobe (2022) to update instructions from v86 to deliver the BBVMs and from BrowserVM to create a v86 compatible Buildroot .iso file. Buildroot's, embedded Linux is a useful choice for cyber educators to use as a BBVM because of its very small size, and simple command-line interface. We will present how to configure both projects, installing on a typical web server, and creating custom .iso images. These custom images will make it obvious how instructors can populate and deliver their own content to their students. We will conclude with example .iso images for basic exercises of file system navigation and manipulation with command-line Linux which should be familiar to most cyber professionals.

Keywords: Browser-based virtual machines, cyber education, virtual machines.

Reference:

Ruff, M., & Giacobe, N. A. (2022, March). Leveraging browser-based virtual machines to teach operating system fundamentals. *Journal of The Colloquium for Information Systems Security Education, 9*(1), pp. 1-7.

Machine learning applications in cybersecurity: From development to deployment

[Mini Workshop]

Holly Yuan, University of Wisconsin-Stout, WI, yuanh@uwstout.edu

Extended Abstract

The evolving landscape of cyber threats has made machine learning an essential tool in network security, yet many cybersecurity programs struggle to incorporate hands-on Maching Learning (ML) training effectively. This workshop provides a structured, hands-on introduction to practical machine learning applications in cybersecurity, designed for educators with basic Python programming knowledge and fundamental understanding of network security concepts. During this hands-on workshop, participants will implement machine learning techniques for network intrusion detection using real-world Internet of Things (IoT) traffic data. The workshop begins with an overview of why machine learning can be used for network security applications. Participants will then engage in guided exercises using provided Python notebooks and Amazon Web Services (AWS) Sagemaker environments or Visual Studio (VS) Code to minimize setup time. The hands-on portion focuses on three key areas: data preprocessing and feature engineering specific to network traffic analysis, model development using scikit-learn for Random Forest implementation, and practical deployment strategies using AWS Sagemaker endpoints. Using a prepared IoT dataset, participants will develop models to detect various attack patterns, including Distributed Denial of Service (DDoS) attempts, port scanning, and malware traffic. Special attention is given to security considerations during model deployment, including Identity and Access Management (IAM) policies and secure Application Programming Interface (API) endpoints. The workshop materials include ready-to-use Jupyter notebooks, sample datasets, and complete documentation that educators can immediately adapt for their classrooms. To ensure effective time management in the 20-minute format, participants will receive pre-workshop setup instructions and access to a GitHub repository containing all necessary materials. While the workshop demonstrates the complete development cycle, it focuses on the most critical aspects of ML implementation in cybersecurity, with additional resources provided for deeper exploration. This practical approach equips educators with both the technical foundation and teaching materials needed to incorporate machine learning effectively into their cybersecurity curriculum, addressing the growing demand for ML-enhanced security expertise in the workforce.

Keywords: Machine learning, network security, cloud deployment, IoT security, hands-on workshop, cybersecurity education.

Building effective cybersecurity pipelines from the ground up

[Mini Workshop]

Rachel Meyers, Purdue University Northwest, IN, raweaver@pnw.edu

Katie Bowers, Purdue University Northwest, IN, katie.bowers@pnw.edu

Michael Tu, Purdue University Northwest, IN, Michael.Tu@pnw.edu

Extended Abstract

In this presentation, we will explore the essential strategies for building a strong pipeline between educational institutions and K-12 schools to foster student engagement, alignment with academic pathways, and career readiness in the field of Cybersecurity. Broad strategies will be shared that can be implemented or modified to align with your strategic needs, and we will share our process to illustrate how this can be done. Key steps in the process that will be discussed include: connecting with potential partners, what to include in your introductory email template, securing buy-in from school partners, development of partnership Memorandum of Understandings (MOUs), navigating state code, modality of potential early college courses (e.g., dual enrollment, concurrent enrollment, Advanced Placement (AP)), curriculum alignment, student enrollment and registration, student engagement and outreach, and, finally, the transition from high school to college. While codes differ from state to state, we will suggest strategies to understand your unique state requirements. A significant focus will be placed on innovative approaches to engage students and teachers through dynamic in-school presentations and interactive games that promote awareness of current and future cybersecurity educational opportunities. By effectively showcasing upcoming summer courses, camps, and other academic programs, we will illustrate how to maintain student enthusiasm and motivation throughout their cybersecurity journey. This session will provide valuable insights into developing sustainable partnerships and fostering long-term student success. Attendees will learn actionable strategies to build partnership pipelines from the ground up.

Keywords: Partnerships, engagement, curriculum, concurrent enrollment, pipeline.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Teaching with VAPOR: A graphic modeling language for cybersecurity attack scenarios

[Mini Workshop]

Derek L. Hansen, Brigham Young University, UT, dlhansen@byu.edu

Ben Schooley, Brigham Young University, UT, ben_schooley@byu.edu

Malaya Canite, Brigham Young University, UT, mcanite@byu.edu

Ethan Richmond, Brigham Young University, UT, eman0202@byu.edu

Zac Maughan, Utah State University, UT, a02317571@usu.edu

Spencer Smith, Brigham Young University, UT, s9302@byu.edu

Extended Abstract

This mini workshop introduces a novel diagraming language called Visualizing Attack Patterns and Operational Risk (VAPOR) that is explicitly designed to model and characterize adversarial cyber-attack scenarios. VAPOR includes a set of black and white icons of different types (Actors, Things, Actions, and States), as well as rules for creating diagrams using them (e.g., always include an attacker, vulnerability, and Confidentiality, Integrity, and Availability (CIA) triad triangle; use directed lines to connect objects). VAPOR was designed by the authors to help learners (1) understand attack patterns and weaknesses (e.g., MITRE's Common Weakness Enumerations (CWEs) and Common Attack Pattern and Enumeration (CAPECS)), (2) plan cybersecurity attacks, and (3) understand historical cyber-attack cases (e.g., Stuxnet, WannaCry). We used an iterative design process to develop VAPOR, making improvements based on feedback from students who used it in multiple individual and group assignments as part of our sophomore Adversarial Mindset class for 3 consecutive semesters. Student interviews, classroom observations, and assignment analysis showed evidence that VAPOR helps students gain a more concrete and procedural understanding of the interactions involved in a cyberattack, from initial access to impact. By diagramming scenarios, students developed a thorough understanding of attacks, being able to identify attacker goals, CIA violations at every stage, and weaknesses that enabled the attack. Using VAPOR required students to manually build diagrams with specificity due to the creative nature of creating visualizations, preventing students from relying solely on AI tools. Finally, professors were able to efficiently identify and address student misunderstandings that came to the forefront in their VAPOR visualizations. We believe it will be useful for other educators teaching adversarial tactics. During the workshop session, researchers will introduce VAPOR, provide assignment examples for implementing VAPOR in the classroom, and give time for attendees to create diagrams. To introduce VAPOR, researchers will provide a rulebook for creating standardized VAPOR diagrams and briefly overview the icons available in the icon library. After, researchers will demonstrate how to implement VAPOR as individual and group assignments to facilitate student understanding of CAPECs and case studies, showing student-created examples.

Keywords: Adversarial thinking, diagramming language, VAPOR, graphical modeling language, cybersecurity visual language.

Addressing critical shortage of cybersecurity instructors

[Mini Workshop]

Ram Dantu, University of North Texas, TX, Ram.Dantu@UNT.edu

Cihan Tunc, University of North Texas, TX, Cihan.Tunc@UNT.edu

Extended Abstract

There is a growing concern in the field of cybersecurity especially due to integrated cyberspace (including but not limited to smart cities, smart and autonomous vehicles, and critical infrastructures) and the development and integration of Artificial Intelligence (AI) in these environments. Addressing the cyber-threats requires a highly skilled workforce who have expertise both in theory and practice. We observe a shortfall in the cybersecurity workforce, with over 750,000 open positions globally, 21% of which are entry-level. Unfortunately, this gap is also observed for the cybersecurity instructors. This workshop aims to address the urgent need for cybersecurity instructors and workforce through three strategic approaches: (1) Transitioning professionals to academia: Mid-career and senior-level professionals in industry and federal agencies can bring invaluable real-world experience and knowledge to train next-generation cybersecurity workforce, which can also increase the interest in this field. (2) Empowering current instructors with advanced degrees: Instructors without a Ph.D. are keen to enhance their knowledge with advanced degrees. However, they face multiple challenges like geographical immobility, existing work requirements, work – personal-life – Ph.D. triangle, and financial aid. (3) Increasing awareness in the cybersecurity field. There is a lack of awareness in the cybersecurity field unless the companies face major failures or breaches. Similarly, many students are not aware of cybersecurity and its potential job market, which causes them to wander around in different topics affecting the cybersecurity workforce readiness. This workshop will provide actionable solutions to these challenges by discussing possible strategies to address identification and support for prospective instructor candidates, balancing work and Ph.D. pursuits, navigating degree completion challenges, industry-academia skill transfer, residency requirements compliance, federal agency collaboration, etc. This workshop is designed for especially community college and 4-year university instructors, industry professionals, and employees from federal agencies who are directly impacted by or can contribute to resolving the shortage of qualified cybersecurity instructors. During the workshop, we will discuss the concerns interactively, and share some resources, and we will also try to create a Ph.D. matchmaking session where the prospective Ph.D. students and prospective Ph.D. supervisors can introduce themselves.

Keywords: Cybersecurity, workforce, readiness, student, advanced degrees, awareness.

Refereed Extended Abstract Proceedings for Lightning Talks

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Feasibility of creating a non-profit and non-governmental organization cybersecurity incident reporting and dataset repository using OSINT

[Lightning Talk]

Stanley Mierzwa, Kean University, NJ, smierzwa@kean.edu

Iassen Christov, Kean University, NJ, hristovj@kean.edu

Extended Abstract

Organizations of all types are prone to cybersecurity and information security attacks. Non-Profit Organizations (NPOs) and Non-Governmental Organizations (NGOs) are not exempt from using information technology solutions and, thus, have been the recipient victims of cyber attackers. There exist many areas and venues where data are collected to report back annually on the status and numbers of cybersecurity attacks against many sectors of our society. The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) catalogs sixteen critical sectors that are considered vital to the United States. However, it is not easy to find where the NPO and NGO community should reside with regard to a categorized sector. In order to provide a catalog method, using the CISA sixteen critical sectors was utilized. One opportunity for the CISA critical sectors, is to pursue adding NPOs and NGOs as potential critical sectors. Many NPOs and NGOs provide critical services to areas of underserved communities, and as such, provide critical services to their communities. The cybersecurity incident data collected by many agencies does place a focus on the sixteen sectors. This presentation will focus on the NPO and NGO community and provide the process followed to research and create the data repository, create categorization of attacks or taxonomy, fields captured, outlets, and areas where data that is relevant to historical cybersecurity incidents in these types of agencies is available. In addition, the beginning of a running log and dataset for the NPO and NGO community will emerge to determine if this activity is feasible and can continue. A desired outcome for this effort is to make available a dataset that can be referenced by researchers, students, and leaders investigating cybersecurity risk management and analysis of the NPO and NGO sectors.

Keywords: Cybersecurity research, threat intelligence, open-source repository, feasibility, work role competency.

Bringing different disciplines and competitions in your classroom

[Lightning Talk]

Eric Chan-Tin, Loyola University Chicago, IL, dchantin@luc.edu

Mohammed Abuhamad, Loyola University Chicago, IL, mabuhamad@luc.edu

Extended Abstract

It is well-known that cybersecurity does not belong only to computer science/engineering. Other disciplines such as Psychology, Criminal Justice, Sociology, and Political Science can have a great impact in cybersecurity research and education. Students taking only courses are at a disadvantage and should be encouraged to participate in cybersecurity competitions to obtain real-world skills. This lightning talk will look at incorporating two aspects in an interdisciplinary cybersecurity program/curriculum: 1) different disciplines and majors such as Psychology, Criminal Justice, Political Science, Sociology into the cybersecurity program; and 2) including cybersecurity competitions as an integral part of the cybersecurity classroom and curriculum. Incorporating many disciplines reach a wider audience and also increase diversity of knowledge. Cybersecurity competitions are an applied method to the classroom environment. Ways to get started, how to engage faculty from other disciplines, and which competitions to get started in, will be covered. This session will be interesting to instructors who are starting or are interested in starting a new interdisciplinary cybersecurity program. The learning outcomes from this session are 1) How to engage with other disciplines and include them in the curriculum; 2) How to incorporate cybersecurity competitions into the classroom. The authors have mentored over 50 students in the past five years and are teaching in a small to mid-sized cybersecurity program with 100-150 enrolled students. The general flow of this lightning talk is as follows:

- Intro to Loyola cybersecurity program
- Benefits of being interdisciplinary?
- How to collaborate with others?
- What are cybersecurity competitions? and why?
- Which competitions are useful for interdisciplinary students?

Keywords: Cybersecurity education, interdisciplinary, competitions, curriculum.

Practicum projects in cybersecurity education

[Lightning Talk]

Jason Mitchell, Lansing Community College, MI, mitch24@lcc.edu

Extended Abstract

The growing demand for skilled cybersecurity professionals highlights the need for educational programs that effectively prepare students for real-world challenges. Community colleges play a crucial role in this effort, providing hands-on, experiential learning opportunities that bridge the gap between theory and practice. Practicum projects are a vital component of these programs, immersing students in real-world cybersecurity tasks while being evaluated by industry professionals. In this session, I will present the practicum-based approach used in our Cybersecurity A.A.S. degree, detailing how these projects provide students with the technical and soft skills necessary for workforce readiness. For example, in CITS 125 (Computer Support A+ Cert Prep), students enter a classroom where individual computer components are laid out and must assemble a functional system, install an operating system, configure a wireless network, and complete maintenance tasks. In CITS 225 (Networking for PC Technicians), students act as network consultants, designing and building networks using Cisco Packet Tracer, then presenting their solutions to industry professionals who evaluate their decisions on security, scalability, and troubleshooting. These projects go beyond simulations by incorporating real-world problem-solving, decision-making, and employer engagement. Our Business Industry and Leadership Team (BILT) members, who represent the employers hiring our graduates, review and assess student projects, ensuring they align with industry expectations. By embedding practicum projects into cybersecurity curricula, we enhance students' ability to apply concepts, use industry-standard tools, and develop critical thinking and communication skills. For the National Center of Academic Excellence in Cybersecurity (NCAE-C) - Cyber Defense (CD) community, integrating practicum projects into cybersecurity education is essential for developing a highly skilled workforce. This session will provide concrete examples of how to structure, implement, and evaluate practicum projects, offering insights for educators, administrators, and industry partners looking to strengthen experiential learning in cybersecurity programs.

Keywords: Cybersecurity education, practicum projects, hands-on learning, real-world application, experiential learning, skill development.

Exploring NCAE cyber competencies under ABET student outcomes framework

[Lightning Talk]

Erald Troja, St. John's University, NY, trojae@stjohns.edu

Suzanna Schmeelk, St. John's University, NY, schmeels@stjohns.edu

Extended Abstract

There has been a well-documented shortage of cybersecurity professionals in the United States. This deficiency has triggered a well-funded National cybersecurity education effort both from the part of the National Security Agency (NSA) and Department of Defense (DoD). The most successful cybersecurity educational movement is highlighted by the NSA effort to create National Centers of Academic Excellence in Cybersecurity (NCAE-C). There are currently over 400 such designated NCAE-Cs in the United States and all of them have excellent programs to train the next generation of cybersecurity professionals. Recent changes in the NCAE-C re-designation criteria revolve around building and assessing cybersecurity competencies which can be thought of as the ability of a student to perform a task within the context of a work role. In this talk, we explore some efficient ideas and methods in order to allow cybersecurity NCAE-Cs, who also hold an ABET accreditation in cybersecurity, to be able to build and assess cybersecurity competencies in a manner that can be seamlessly used towards ABET program assessment.
A program coordinator (PC)/program director (PD) who oversees an NCAE-C validated cybersecurity Program of Study (PoS) that is also accredited by ABET will be tasked with measuring/assessing the defined cyber competencies, as well as ABET performance indicators, in order to utilize assessment results as part of the internal improvement cycle. Unfortunately, between the minimum 10 cybersecurity competencies and at least six ABET student outcomes, this might lead to over assessment, and it might soon be seen as detrimental as 'analysis paralysis'. In this talk we provide best practices on how a PC/PD can cleverly (i) define cyber competencies based on already defined ABET performance indicators (ii) exploit mutual assessment opportunities as to satisfy both NCAE-C and ABET requirements. We provide a case study on the methods utilized on our B.S. in Cyber Security Systems PoS which is both a validated NCAE-C PoS as well as ABET-accredited. We hope that NCAE-C validated cybersecurity program coordinators/directors whose program is also ABET-accredited will benefit the most from the ideas and practices shared on this talk.

Keywords: ABET, cyber competencies, assessment, continuous improvement.

Leveraging AI tools for assessment: A case study in computer science education

[Lightning Talk]

Ayad Barsoum, St. Mary's University, TX, abarsoum@stmarytx.edu

Extended Abstract

Artificial Intelligence (AI) is transforming numerous industries, and education is no exception. For faculty members, grading exams —particularly free-response assessments— can be a time-consuming task, especially in institutions where policies restrict the use of graduate assistants for final exam grading or such assistance is unavailable. While multiple-choice exams can be graded quickly using automated tools, free-response exams present unique challenges due to the diversity of student answers and the absence of binary solutions. Free-response assessments require students to generate their own answers rather than selecting from predefined options, as in multiple-choice tests. Common types of free-response exams include, but are not limited to, code writing, essay questions, short-answer questions, and problem-solving tasks. In the Fall 2024 semester, we explored the potential of AI to streamline grading in one of our courses, where the final exam required students to write programs to solve problems. Using ChatGPT, we submitted the exam questions, model answers, and a detailed grading rubric. Initially, we tested ChatGPT's understanding by comparing its grading of past student submissions against our own manually graded results. The variance was minimal—only three points on average—demonstrating an acceptable level of accuracy. Through iterative fine-tuning, which involved questioning the AI's grading rationale and providing targeted feedback, we optimized its performance. Once confident in its reliability, we graded current student submissions using ChatGPT, significantly reducing the time required. While the AI provided accurate and detailed evaluations, we retained the final decision on grades by conducting a quick review of each assessment and verifying the deducted points. This use case highlights the value of AI tools as virtual "graduate assistants," providing efficient and effective support for grading free-response exams. However, the ultimate responsibility and decision-making remain with the professor, ensuring fairness and academic rigor.

Keywords: Artificial Intelligence (AI), virtual graduate assistants, assessment.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Enhancing credit transfer efficiency and accuracy through knowledge unit (KU) mapping

[Lightning Talk]

Michael Ruth, Roosevelt University, IL, mruth@roosevelt.edu

Extended Abstract

This proposal introduces an approach to streamline and enhance the accuracy of the credit transfer process between National Centers of Academic Excellence in Cybersecurity (NCAE-C) institutions, particularly when courses are not directly comparable. As part of the program of study designation, all NCAE-Cs are required to align individual courses to Knowledge Units (KUs) and we propose to use those alignments to enable institutions to determine whether a student's coursework from one NCAE-C designated institution satisfies course requirements at another. Although KU alignments are not public, accessing this information from NCAE-C Point of Contacts (POCs) has been successful. This approach addresses the time-intensive nature of manual course evaluations encountered when accepting transfer students. Variability in course scope and content can be attributed to differences in the way institutions structure and deliver their programs. Some institutions offer Cybersecurity and Computer Science degrees while others are more IT-centric, offering Cybersecurity and Information Technology degrees. For example, one institution might offer two specialized cybersecurity courses where all core KUs are aligned to these courses where another institution may offer several cybersecurity courses where the same KUs might be in different courses along with other optional KUs. In these instances, it is time consuming and error prone to discover the relationships between individual courses much less across several courses. However, our proposed approach of using KU alignments in the transfer matchmaking process allows for greater flexibility by considering the full scope of KUs covered by a combination of courses, rather than requiring a one-to-one course substitution in a very efficient and consistent manner. Consider two CAE institutions: Institution A, a smaller teaching-focused college with a cyber security concentration, and Institution B, a larger, IT-focused university with a broader range of networking and security courses. Institution A offers course 101 that covers KUs X and Y and course 102 which covers KUs W and Z. Institution B offers 110 that covers KUs X, W and a 112 that covers Y and Z. Together, these courses all cover the same content. But due to differences in course titles, structure, and syllabi, it's not immediately clear how the courses correspond between institutions. However, using KU alignments, we can identify that the courses 101 and 102 at institution A are identical in KU coverage to the courses 110 and 112 at institution B. In addition to simplifying the review process, using KU alignments reduces subjective differences in course reviews between institutions. The NCAE-C approved KU alignments provide a consistent, community-vetted resource for evaluating transfer credits. While challenges remain, such as differences in course levels (e.g., introductory versus senior-level classes) and restrictions related to community college credits, implementing policies informed by KU alignments can help students fulfill degree requirements, even when transferred credits do not directly align with course levels.

Keywords: Cybersecurity credit transfer, Knowledge Units (KUs) alignment.

Graduate student cyber capstone design: A real-world cybersecurity analysis of VPN mobile applications

[Lightning Talk]

Suzanna Schmeelk, St. John's University, NY, schmeels@stjohns.edu

Denise Dragos, St. John's University, NY, dragosd@stjohns.edu

James Dermezis, St. John's University, NY, james.dermezis20@my.stjohns.edu

Andre Duchatellier, St. John's University, NY, andre.duchatellier20@my.stjohns.edu

Tomas Medina, St. John's University, NY, tomas.medina24@my.stjohns.edu

Charles Orbezo, St. John's University, NY, charles.orbezo20@my.stjohns.edu

Jared Reid, St. John's University, NY, jared.reid19@my.stjohns.edu

Extended Abstract

In an age where online risks are at an all-time high, there is an increased need for a virtual private network (VPN) (Cruz, 2024). This talk first provides a curricular design of a graduate student capstone research course where students are given real-world data to analyze as well as timely topics. We then report on one graduate student small group analysis of 27 freely available VPN mobile applications selected using a Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) for transparency and reproducibility. The applications metadata were compiled with results from a *Mobile Security Framework (MobSF)* analysis (Klein, 2021). We are examining the application code to give aggregated insights and recommendations into the state of cybersecurity of the mobile VPN applications. The results show that the applications analyzed varied significantly in many instances, including security from external threats, intrusiveness of required permissions, and data collection. Insecure practices were also detected, including the use of insecure random number generators and the logging of sensitive data. The authors report on useful mitigation needs and improvements for the future of secure mobile application development. The talk concludes with lessons learned from the research curricular design that fosters real-world security analysis in a world where artificial intelligence offers many benefits as well as challenges to research designs.

Keywords: Android applications, Virtual Private Networks, VPN, mobile application security, static analysis, mobile security framework.

References:

Cruz, B. (2024, September 26). *VPN consumer usage, adoption & shopping study: 2020*. Security.org. https://www.security.org/resources/vpn-consumer-report-annual

Klein, J. (2021). A journey through android app analysis: Solutions and open challenges. *Proceedings of the 2021 International Symposium on Advanced Security on Software and Systems*, 1–6. https://doi.org/10.1145/3457340.3458298/

Bridging the gap: Leveraging Microsoft Learn to enhance cybersecurity education

[Lightning Talk]

Hondo Tamez, Johnson County Community College, KS, atamez@jccc.edu

Extended Abstract

With cybersecurity threats growing rapidly, the need for industry-aligned education is more critical than ever. This session introduces how Microsoft Learn for Educators empowers academic institutions to bridge the gap between classroom learning and professional certification. In just 10 minutes, we'll explore how integrating Microsoft's Security, Compliance, and Identity Fundamentals (SC-900) and other security-related learning paths into coursework provides students with hands-on skills and certification readiness. This presentation will highlight key resources available to educators, including ready-to-use teaching materials (n.d.), free or discounted certification vouchers, and strategies for incorporating Microsoft Learn content to enhance student engagement and employability. Additionally, we'll discuss how these certifications align with in-demand cybersecurity roles, emphasizing practical tools to help students grasp complex concepts like identity management, threat protection, and cloud security. Beyond the benefits, we will also address potential challenges, such as accessibility for institutions without Microsoft resources and balancing certification-based learning with broader cybersecurity pedagogy. By considering these factors, we aim to provide a realistic perspective on integrating Microsoft learn while ensuring equitable access to cybersecurity education. Attendees will walk away with actionable steps for leveraging Microsoft Learn to enhance their cybersecurity curriculum, empowering students to gain both academic knowledge and industry-recognized credentials.

Keywords: Cybersecurity, education, Microsoft Learn, certification, curriculum, employability.

References:

Microsoft. (n.d.). Microsoft Learn Educator Center. https://learn.microsoft.com/en-us/training/educator-center/

Microsoft. (n.d.). Microsoft Certification Poster. https://query.prod.cms.rt.microsoft.com/cms/api/am-binary/RE2PjDI

Competition competencies: Four key employability findings

[Lightning Talk]

Dan Manson, California State Polytechnic University, Pomona, CA, dmanson@cpp.edu

Morgan Zantua, City University of Seattle, WA, zantuamorgan@cityu.edu

Extended Abstract

Cybersecurity talent appears to be constantly growing in demand (CyberSeek, 2025). However, there continues to be a mismatch between supply and demand. Most entry-level cybersecurity jobs require several years of experience. What students do outside the classroom is as important as what they do in the classroom. The more you do outside the classroom helps students understand what they need to be doing in the classroom. According to Outlook in ONET On-Line Cybersecurity jobs openings are ranked as having a Bright Outlook, and Cyberseek.org continues to list over 500,000 US job openings as of June 1, 2024 (National Center for O*NET Development, 2025). On closer examination, the entry level positions require at least three years of experience. Despite this hot job market, recently minted cybersecurity college graduates have a hard time securing their first "entry-level" because they don't meet the minimum requirements. Based upon alumni experience and interviews conducted through evidencing competencies research, students can demonstrate up to three years of experience by participating in competitions and other extracurricular activities. Students who distinguish themselves by developing a track record outside of the classroom have more employment options at higher wages. Four themes emerged through forty interviews of high performing cybersecurity student competitors. The most surprising recurring theme was empathy. Through the course of the interview process students continually emphasized the importance of knowing your audience in presenting their reports during competitions. A consistently strong theme students mentioned was how important it was to build a team in lieu of having individual star performers. Finally, transferring cybersecurity skills to employability proved the students' ability to convince hiring managers of their ability to do the work when hired.

Keywords: Teamwork, empathy, knowing your audience, employability.

References:

National Center for O*NET Development (2025). *O*NET OnLine.* https://www.onetonline.org

CyberSeek (2025). https://www.cyberseek.org

Securing air-gapped industrial control systems: Mitigating wireless threats through proactive defense strategies

[Lightning Talk]

Hosam Alamleh, University of North Carolina Wilmington, NC, alamlehh@uncw.edu

Ulku Clark, University of North Carolina Wilmington, NC, clarku@uncw.edu

Bilge Karabacak, University of North Carolina Wilmington, NC, karabacakb@uncw.edu

Kasey Miller, University of North Carolina Wilmington, NC, millerkc@uncw.edu

Extended Abstract

Critical infrastructure systems, including power grids and maritime navigation, face increasing cyber threats that extend beyond traditional internet-based attacks. While air-gapping and Information Technology/ Operational Technology (IT/OT) segmentation are widely used security measures, adversaries have developed advanced methods to remotely activate dormant malware within isolated environments. This paper investigates wireless-based remote activation techniques that exploit vulnerabilities in communication systems such as Global Positioning System (GPS), Automatic Identification System (AIS), Radio Frequency (RF), and pager networks. Attackers can manipulate these signals to trigger pre-installed malware, bypassing conventional defenses. Two real-world case studies highlight the risks of such attacks. The first examines how AIS spoofing can be used to remotely activate malware onboard maritime vessels, leading to navigation system failures and potential operational disruptions. The second explores GPS-based time synchronization manipulation in power grids, where attackers can destabilize energy infrastructure by injecting malicious timing signals. To mitigate these threats, this paper proposes strategies such as secure firmware development, signal authentication, and anomaly detection. Strengthening wireless security and implementing advanced intrusion detection systems are essential to counter these evolving attack vectors. This study emphasizes the need for a comprehensive cybersecurity approach that accounts for non-internet-based threats, ensuring the resilience of critical infrastructure against emerging cyber risks

Keywords: Air-gapped industrial control systems, mitigating wireless threats, IT/OT.

Pipeline pressure: The rising need for cybersecurity educators at CAE schools

[Lightning Talk]

Jason Hammon, Western Governors University, UT, jason.hammon@wgu.edu

Extended Abstract

The cybersecurity job market remains in demand and students are responding. As students ask for more courses, universities struggle to find people to teach them (Morris et al., 2024). The research shared in this lightning talk connects the cybersecurity educator shortage to the broader historical challenges faced by computer science departments. As the cybersecurity discipline matures and new programs are created, the lag in developing qualified educators is amplified (Computing Research Association, 2023; National Academies of Sciences, Engineering, and Medicine, 2018). This creates a cyclical challenge: expanding the professional talent pipeline further increases the demand for instructors. In this talk, I will share a literature review with key resources to inform the community at large about the issues along with the current state gained from Integrated Postsecondary Education Data (IPED) and Taulbee Survey data. In 2024, our research team conducted a survey of program leaders from National Center of Academic Excellence in Cybersecurity (NCAE-C) schools. Through 100 responses from 42 states, the survey reveals that while institutional leadership prioritizes cybersecurity education, efforts to expand teaching capacity remain localized and small in scale. Student demand is surging, but hiring efforts are hindered by a limited candidate pool and resource constraints. Join me in this lightning talk to learn about the current challenges and survey results, a reading list for informing yourself about the issues, and potential strategies moving forward.

Keywords: Educator workforce gap, cybersecurity education, talent pipeline, strategic planning, workforce development, training, careers.

References:

Morris, M., Hammon, J., Anderson, K., Vikayanon, K., Coombs, L., Spragg, A., Giwamogorewa, O., Jirapanjavat, S., Ilges, C. (2024). *Help wanted: Cybersecurity* educators. *How NCAE institutions are responding. NICE Community Coordinating Council.* https://www.nist.gov/system/files/documents/2024/12/19/Cybersecurity%20Educators%20Wanted%20White%20Paper%20%28December%202024%29_508compliant.pdf

National Academies of Sciences, Engineering, and Medicine (2018). Assessing and responding to the growth of computer science undergraduate enrollments. *The National Academies Press.* https://doi.org/10.17226/24926

Computing Research Association. (2023). *The CRA Taulbee survey*. http://cra.org/resources/taulbee-survey/

The Cybersecurity Canon: The best list of go-to cybersec books

[Lightning Talk]

Julia Armstrong, The Ohio State University, OH, armstrong.798@osu.edu

Helen Patton, Cisco, CA, helen.patton@gmail.com

Extended Abstract

Cybersecurity is a broad field, with a large contingent of skills in addition to the knowledge to apply to routine and unique situations. The best educators strive to bridge the gap by providing both up to date technical information integrated with experiential learning to develop our future practitioners. To support students of all levels, educators must source material that is academically rigorous and accepted by the cybersecurity community. Our talk will provide information on a resource that satisfies both needs - the Cybersecurity Canon. The Cybersecurity Canon is a project that facilitates cybersecurity professionals reviewing cybersecurity books and curating the best of them so that aspiring and mature professionals alike can easily access cyber wisdom, not just cyber noise. The international cannon committee is composed of experienced and highly respected professionals. The Canon started over 10 years ago when the Chief Information Security Officer (CISO) for Palo Alto Networks realized how hard it was for cyber professionals, like himself, to keep up with cybersecurity knowledge. He brought a group of professionals together to start curating a list of books which provided timeless, meaningful cyber wisdom. When the CISO left Palo Alto Networks, the project needed a new home. At the time, the CISO of The Ohio State University, Helen Paton, was a Canon committee member and co-founder of Ohio State's Institute for Cybersecurity and Digital Trust (ICDT) (Patton, 2020). The Canon provides all these reviews as resources to the community through Ohio State's website. As of January 2025, there are over 200 book reviews on the website, and over 50 books inducted in the "Cybersecurity Canon Hall of Fame". These are searchable on keywords, so the viewer can more easily find specific books, authors or topics. Review pages also include links on where to obtain each book. Ways other educators could use this resource are both individual and group studies. In addition to reading reviews and finding books for personal or class use, some professors have started discussing a book club for students and/or community practitioners. Future potential engagement with schools and professionals may be hosted and organized by Ohio State and ICDT. Programs to be described and discussed include book clubs and book club resources; toolkits to incorporate reading and writing reviews into curriculums and teacher material; opportunities to partner with the Canon to bring authors to the schools as speakers.

Keywords: Cybersecurity Canon, book reviews, best books, book clubs, cybersecurity hall of fame.

Reference:

Patton, H. (2020, August 6). Cybersecurity Canon: A resource for security professionals comes to higher education. *Ohio State - Institute for Cybersecurity and Digital Trust.* https://icdt.osu.edu/about-cybersecurity-canon

Providing students with hands-on experience in a SOC environment

[Lightning Talk]

Mirco Speretta, Fairfield University, CT, msperetta@fairfield.edu

Henry Foss, Fairfield University, CT, hfoss@fairfield.edu

Extended Abstract

A Security Operations Center (SOC) is a cybersecurity function that is usually implemented in medium and big organizations. Its purpose is to detect and respond to cybersecurity incidents in real time. Successful SOC analysts (i.e., employees in the SOC) must have a broad experience that usually starts from a technical background and also implement soft skills for effective cross-team communication. The students in higher education who are in technical fields such as Computer Science and of course cybersecurity, would greatly benefit from the experience of working in a SOC. Moreover, the security teams of many higher education institutions often have to battle with the lack of resources. Two years ago, the School of Engineering and Computing at Fairfield University started a collaboration with their internal Information Technologies Services team. The goal was twofold: the creation of a facility where students from the Computer Science department could experience hands-on experience in Cybersecurity and the support of the cybersecurity activities at Fairfield University. The result of that collaboration was an internal SOC where students could work while gaining experience in the field. In this presentation we will share our journey to establish an internal SOC that is accessible to students. We will discuss our experience over the activities related to its maintenance: the recruitment and the onboarding of the students, the organization of the activities within the SOC including that cybersecurity tools that we use. We will also share the outcomes and the benefits for the students in learning industry standard tools and in their job search.

Keywords: Security Operations Center (SOC), experiential learning.

Creating hackers to build better defenders

[Lightning Talk]

William Bradley Glisson, Louisiana Tech University, LA, glisson@latech.edu

Madj Tahat, Louisiana Tech University, LA, mtahat@latech.edu

Extended Abstract

The world continues to be fascinated with malware, ransomware, and attacks. This attraction presents a viable mechanism to entice participants into cybersecurity, computer science, and Science, Technology, Engineering, and Mathematics (STEM). This enticement led to a Department of Defense (DoD) grant submission to develop a cybersecurity gaming environment called the Cyber Assault Competition (CAC). Participants can scan networks, attack, and perform tasks that would typically raise red flags in real-world production environments. Easy points are assigned to entry-level breaches, and more advanced points are assigned to difficult breach scenarios. Attackers must identify flags and submit them for points. The initial idea simulates networks consisting of Virtual Machines. However, after a round of testing, it was evident that the overhead for that configuration impeded performance. At this point, the development pivoted to docker containers as an architecture simulation method. The CAC system intercepts incoming connection requests on protocols like Secure Shell (SSH), creates lab infrastructure on demand, and then routes the remote connections to the new temporary infrastructure. The system uses the same methodology as similar 'infrastructure as code' tools and accepts a configuration file in Yet Another Markup Language (YAML) format. This makes creating competition labs easier for administrators, as they can specify all the scenario details and networking in advance and replicate the environment any number of times using the same configuration file. When the participants' infrastructure is successfully spun up and ready, the system executes the equivalent of a 'docker attach' command to the newly created user/host container, Kali Linux, for access to attack tools. The system generates environments on demand and is highly configurable to meet the specific needs of targeted environments. CAC creates a fun and safe environment for students to learn about network attacks. CAC has been integrated into the University's Risk Assessment, Advanced Networks, and Cybersecurity classes. It has been demonstrated at the University's Research & Partnerships Week, deployed at two high schools, and demonstrated for a research group at another University. From a research perspective, the infrastructure provides the foundation for future work that investigates the design, development, and quantification of a scalable, modular infrastructure for malware detection that can capture data from multiple activities, clean appropriately, and be used as input for various machine learning and AI algorithms.

Keywords: Cybersecurity, hacking, attack, gaming.

Breaking barriers: A comprehensive study on challenges faced by women in cybersecurity

[Lightning Talk]

Samah Mansour, Grand Valley State University, MI, mansours@gvsu.edu

Andrew Kalafut, Grand Valley State University, MI, kalafuta@gvsu.edu

Extended Abstract

The existence of a significant gender gap in the technology industry is well-known. Women are vastly underrepresented across all sectors, including cybersecurity. Even after entering the workforce, women face significant challenges to inclusion and equity. This study investigates the status of gender dynamics within the cybersecurity industry, focusing on the challenges and opportunities for professional women, as revealed through a targeted survey. Despite some advancements, women remain underrepresented, particularly in leadership roles, constituting just a quarter of the cybersecurity workforce. This underrepresentation contributes to the growing global shortage of cybersecurity professionals. Our analysis utilized a survey distributed among professional women in various cybersecurity roles across the United States. The survey examined aspects such as leadership, networking, work-life balance, sexism, and gender bias. The survey responses, drawn from 51 participants, were analyzed using quantitative and qualitative methods and considered age, years of work experience, and education level. Findings highlight persistent issues such as significant gender bias, pay disparities, sexual harassment, and discrimination, which not only hinder women's career progression but also affect their work environment and overall job satisfaction. Challenges in work-life balance and limited networking opportunities further increased the barriers faced by women in this field. Based on the survey's findings, the study proposes several actionable recommendations to promote gender diversity and inclusion within the cybersecurity industry. These include establishing targeted mentorship programs, flexible work arrangements, regular pay audits to address compensation disparities, and comprehensive training to fight unconscious bias and sexual harassment. Additionally, creating networking groups and events specifically for women could strengthen a sense of community and support professional growth.

Keywords: Women, cybersecurity, career, barriers, survey, gender gap, inclusion.

Decrypting cyber careers: Helping students navigate career paths with NICE and DCWF using Try Cyber Challenges

[Lightning Talk]

Paige Zaleppa Flores, Towson University, MD, pzaleppa@towson.edu

Extended Abstract

This lightning talk will highlight an innovative lesson designed to expose students taking an introductory cybersecurity course at a 4-year institution to the diverse range of career opportunities within cybersecurity. The presentation highlights the ways that the NICE Framework and the Department of Defense (DoD) Cyber Workforce Framework (DCWF) can be leveraged to guide students in exploring and understanding diverse cybersecurity work roles and career paths. By connecting industry-recognized frameworks to practical learning experiences, the lessons bridge the gap between academic knowledge and cybersecurity careers. The in-class portion of the lesson engages students through interactive in-class activities and hands-on challenges using the *Try Cyber* platform (TryCyber, n.d.) that simulate tasks in various work roles, providing practical experience that connects classroom concepts to real-world cybersecurity tasks. These activities help students visualize the daily responsibilities of various cybersecurity careers and develop a deeper understanding of the skills required for success in those roles. Complementing the hands-on activities, the homework assignment prompts students to reflect on their personal interests and abilities. Students evaluate which cybersecurity roles align with their current skills, explore roles that spark their interest, and identify the knowledge and skills they need to develop to successfully pursue those career paths. This reflective component fosters self-awareness and supports informed decision-making as students begin to map out potential career paths in cybersecurity. Attendees will discover how integrating structured frameworks, hands-on experiences, and reflective learning can empower students to confidently pursue meaningful careers in the dynamic field of cybersecurity. This session will provide educators with innovative, student-centered strategies to inspire and equip the next generation of cybersecurity professionals with the skills and knowledge needed to thrive in the ever-evolving cyber landscape. The lesson materials will also be shared through the Cybersecurity Labs and Resource Knowledge-base (CLARK) platform (Flores, 2025).

Keywords: Career exploration, NICE Framework, DCWF, hands-on learning, student engagement, reflective learning.

References:

Flores, P. (2025). *Exploring cybersecurity careers with CISA try cyber challenges.* Retrieved February 26, 2025, from https://clark.center/details/pzalep1/09ae8f70-4b6d-46b9-b4bf-ce4f2bbc5867/0

TryCyber. (n.d.). *Interactive cybersecurity learning platform.* Retrieved January 15, 2025, from https://trycyber.us

2025 cybersecurity alumni workforce study: Where are they now?

[Lightning Talk]

Tobi West, Coastline College, CA, twest20@coastline.edu

Extended Abstract

Cybersecurity educators are essential in preparing students for careers in the field. While some graduates actively share their career paths and the influence of their education, others transition into the workforce with minimal feedback to educators on their experiences or outcomes. The 2025 Cybersecurity Workforce Study by National Cybersecurity Training and Education Center (NCyTE) examined the career trajectories of cybersecurity graduates from higher education institutions, including community colleges (NCyTE, 2024). The study underscores the growing impact of these programs in mitigating workforce shortages and aligning graduates with NICE cybersecurity work roles. Key survey findings, including the most common work roles, certifications earned, and other insights, will be presented to highlight these programs' contributions. The study gathered responses from over 200 alumni who completed cybersecurity programs at various educational levels—associate, bachelor's, master's, and doctorate—across the United States. It examined the influence of extracurricular activities, such as internships, student clubs, and cybersecurity competitions, in strengthening practical skills and improving employability. The findings provide insights into alumni career paths, highlighting the roles they have pursued, their job responsibilities, and the extracurricular experiences they consider crucial for securing employment in the cybersecurity and technology sectors. What distinguishes this study is its focused examination of how National Centers of Academic Excellence in Cybersecurity (NCAE-C) programs contribute to addressing the global shortage of cybersecurity professionals. This study will explore emerging trends and uncover opportunities for cybersecurity education programs to enhance extracurricular offerings and incorporate new materials into their curricula. The findings highlight the critical role of academic programs in equipping graduates with the skills and credentials needed to secure careers in cybersecurity and related technology fields, providing valuable insights for educators, employers, and aspiring professionals.

Keywords: Alumni, cybersecurity workforce, NICE Framework, career pathways.

Reference:

NCyTE Center. (2024). *Workforce study: Cybersecurity alumni. Where are they now?* https://www.ncyte.net/academia/faculty/faculty-resources/2024-workforce-study-community-college-cybersecurity-alumni

Superpowers in action: How neurodivergent minds excel in cybersecurity

[Lightning Talk]

Bill Gardner, Marshall University, WV, bill.gardner@gmail.com

Extended Abstract

This literature review explores the intersection of neurodiversity and cybersecurity higher education, focusing on the unique strengths, challenges, and needs of neurodivergent students. Neurodivergent individuals—including those with Autism Spectrum Disorder (ASD) and Attention Deficit Hyperactivity Disorder (ADHD)—possess exceptional abilities, or "superpowers," that are highly relevant to the field of cybersecurity. These include heightened pattern recognition, exceptional attention to detail, and strong problem-solving skills. Additionally, individuals with ASD often demonstrate remarkable resistance to social engineering tactics, such as phishing scams, due to their ability to detect inconsistencies and anomalies. Similarly, individuals with ADHD may excel in multitasking and thrive in dynamic, fast-paced environments. Despite these strengths, neurodivergent students frequently encounter challenges in traditional educational settings, particularly with abstract concepts, group work, and communication. To address these barriers, researchers advocate for hands-on learning experiences, flexible instructional approaches, and accommodations tailored to individual needs. For instance, Universal Design for Learning (UDL) principles offer inclusive strategies that support diverse learning styles. Furthermore, mentorship and networking opportunities provide neurodivergent students with guidance and professional growth, helping them transition into the workforce. By embracing the superpowers of neurodivergent individuals and creating supportive, inclusive educational environments, educators and institutions can bridge the cybersecurity skills gap while fostering innovation and diversity. Neurodivergent students' contributions not only enrich the field but also offer invaluable perspectives that address emerging challenges in cybersecurity.

Keywords: Neurodiversity, cybersecurity education, Universal Design for Learning (UDL), accommodations, mentorship.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Generative AI classroom exercise: Incident response

[Lightning Talk]

Joel D. Offenberg, Howard Community College, MD, joffenberg@howardcc.edu

Extended Abstract

What to do for the last class session before the Thanksgiving holiday? It's been a long semester, and students are ready and willing to skip class…after all, people will be traveling or preparing for the holiday. They might hope that class will be cancelled, or we will show videos or something?! Meanwhile, many instructors seek how to best to incorporate Artificial Intelligence (AI) into their coursework. Prohibit it? Embrace it? Use it for assignments? After 2024 CAE in Cybersecurity Community Symposium and NICE Conference, the author was inspired to incorporate an AI exercise into a class. But how? First, the author asked ChatGPT for examples of how AI is being used in cybersecurity…and ChatGPT said that institutions were using Generative AI (GenAI) to run incident response simulations. As it happened, the author was reviewing Incident Response right before the holiday in the Security+ class. Next, the author found several institutions had pioneered the use of GenAI to conduct Incident Response simulation exercises---not as a classroom exercise but as a table-top exercise for evaluating a real-world Incident Response plan (mWISE Conference, 2024, Mardock, A. 2024). The author replicated this exercise in class, with students as incident responders. The opening prompt, on ChatGPT, is similar to Mardock's: *Let's play an incident response simulation game. You will be the storyteller and tell us what the incident response team sees. I will be the incident response team and tell you our responses and what we find.* ChatGPT responded with a realistic scenario involving a software company. The students working as a team responded based on the incident response practices in the CompTIA curriculum. As the students said what they would investigate or which actions they would take, the AI developed the scenario. The goals were to incorporate using AI for cybersecurity in a classroom exercise while providing a realistic incident response learning experience for students without relying on pre-fabricated labs or the instructor's creativity while encouraging students to come to class (16 out of 22 did). Students reported they felt they applied the principles from class in a realistic, dynamic environment; learning would have been enhanced if the exercise was conducted in smaller groups. Replicability is limited because ChatGPT responds with different scenarios in response to the prompt above. A future classroom exercise could be in smaller teams, using different AI platforms.

Keywords: Artificial Intelligence, incident response, classroom exercise, lessons learned.

References:

Mardock, A. (2024, January). *Prompting for cyber incident response practice- a generative AI example.* https://www.linkedin.com/pulse/prompting-cyber-incident-response-practice-ai-april-mardock-cissp-kb7uc/

mWISE Conference (from Mandiant). (2024, October). *Generative AI cyber incident response tabletop exercise.* [Video]. YouTube. https://www.youtube.com/watch?v=w5mpUs29JSI

CAE-CD community outreach competition: Four years of experience

[Lightning Talk]

Wei Li, Nova Southeastern University, FL, lwei@nova.edu

Xiuwen Liu, Florida State University, FL, liux@cs.fsu.edu

Extended Abstract

The *CAE-CD Outreach Competition* initiative was established by the National Centers of Academic Excellence in Cybersecurity (NCAE-C) - Community of Practice– Cyber Defense (CoP-CD) to: 1) to encourage and promote cybersecurity awareness and online safety practices by taking advantage of the cybersecurity outreach CAEs do throughout the year; and 2) to maximize the impacts of the NCAE-C institutions on their local communities. The initiative was originally motivated by the October cybersecurity awareness month and was extended to cover the efforts of the entire calendar for each cycle. A Committee was formed for the *CAE-CD Outreach Competition* initiative that then established a set of criteria and rules. Impact measures include the number of groups and organizations that are being impacted, the total number of attendees, the durations and frequencies of the events, and the effectiveness of outreach materials. Range of measures include the number of different kinds of groups, the inclusion of underrepresented groups in the cybersecurity profession spectrum of the age groups. Effort measures include: 1) evidence of NCAE-C institutions to promote and engage in the outreach events; 2) total number of outreach events provided in the NCAE-C institutions; and (3) Level of NCAE-C resources and dedicated effort to coordinate, plan, execute, and follow through with the activities. Rules specify the qualified events, which must be active, sustained, and/or well-designed engagement on cybersecurity-related promotions outside the NCAE-C institution, and unqualified events such as in-reach activities, activities not focused on cybersecurity, collaboration among NCAE-C institutions. The Competition started in year 2021 with the first cycle results presented in the 2022 CAE in Cybersecurity Community Symposium; the results for year 2024 will be released during this Symposium. The presentation will cover the lessons learned, the impacts it has had, and other relevant details. Obviously, the Committee cannot be successful without the strong support of the CAE in Cybersecurity Community. We will encourage more NCAE-C Institutions to engage well-designed outreach activities to their communities with high impacts, document their efforts, and submit to this Committee for recognition.

Keywords: Cybersecurity, community outreach, security awareness.

Cyber sexual assault: A growing challenge in the digital age

[Lightning Talk]

Arthur Salmon, College of Southern Nevada, NV, Arthur.salmon@csn.edu

Extended Abstract

One of the largest issues is when discussing cyber sexual assault is the lack of definition. In my presentation I will be discussing ways to define and handle obstacles in this discussion and research in this area. There is a lack of research and a lack of clarity, this presentation will aid in developing a working definition between the present and the audience. Data from the College of Southern Nevada will be presented. Actional items will be addressed as awareness components. Cyber sexual assault has become a pervasive issue in the digital era. As technology continues to evolve so do the methods by which perpetrators exploit online platforms. Despite its prevalence, the subject of cyber sexual assault remains under-researched, primarily due to the sensitive nature of the topic and the societal stigma associated with it. This issue is particularly relevant to educational institutions, where K-12 and higher education. One of the most significant challenges in addressing cyber sexual assault is the lack of research. The sensitive nature of the subject matter discourages victims from coming forward. In educational settings, this lack of research is even more pronounced, as discussions surrounding online sexual violence are often avoided due to concerns about appropriateness or backlash. This lack of information creates a gap in understanding the full impact of cyber sexual assault on students, faculty, and the educational system. Additionally, the absence of awareness about what these crimes exacerbates the issue. Digital literacy programs tailored for students, educators, and administrators can empower individuals to protect themselves online by teaching safe internet practices. Raising awareness about cyber sexual assault encourages accountability from online platforms and organizations, prompting them to create safer digital environments. Collaborative efforts among governments, educational institutions, and technology companies can lead to more effective prevention strategies and resources for victims, fostering a safer learning environment for all. Cyber sexual assault is a complex and deeply troubling issue that demands immediate attention. By fostering greater understanding, promoting education, and advocating for stronger legal protections, society can work toward creating safer online spaces for all.

Keywords: Cyber sexual assault, digital safety, consent, prevention, and victim support.

The 3 c's - Engaging and training cybersecurity students

[Lightning Talk]

Mary Wallingsford, Anne Arundel Community College, MD, mewallingsford@aacc.edu

Noell Damron, Community College of Baltimore County, MD, cdamron@ccbcmd.edu

Vinitha Nithianandam, Community College of Baltimore County, MD, vnithiana@ccbcmd.edu

Extended Abstract

College students are vital for expanding the cadre of information assurance professionals who safeguard critical government infrastructure. Cybersecurity programs provide foundational concepts, tools, and techniques for configuring, monitoring, and hardening systems and networks. However, employers demand work experience even for entry-level positions, posing a challenge for new graduates. With limited internships and apprenticeships, students must supplement classroom learning by engaging in clubs, competitions and/or certifications (3C's) to enhance their practical skills and strengthen their resumes. A survey of 2-year and 4-year institutions offers detailed insights into these activities and their funding. Competitions provide skills for a resume even with no prior experience. Some demand teamwork and are used as class assignments while others are independent learning exercises or implemented in clubs. Categories such as cryptography, network traffic analysis, password cracking and forensics allow students to explore a variety of work roles through hands-on learning. Most of the funding comes from departmental budgets, industry/corporate sponsors or student self-pay. Certifications are industry recognized and validate skills providing students with a credential that highlights proficiency even without work experience. Although most schools reported students self-fund or pay courses lab fees, funding from programs such as Perkins grants, industry and corporate sponsors and college budgets can be used to provide students with discount vouchers. This serves as an equity tool allowing underserved and minority populations an opportunity to earn the certification that they may not otherwise be able to afford. Cybersecurity related clubs provide opportunities to network, take field trips, learn from guest speakers and work with hands-on projects and competitions to practice skills and expand classroom instruction. Hands-on cybersecurity projects and games such as Backdoors and Breaches, Jeopardy, Bingo, and escape rooms expand skillset and reinforce education. More than half of the schools reporting indicate funding for activities comes from student activity fees although institutional and department budgets and industry sponsorships were also utilized. Other extracurricular opportunities identified include Cyber Ranges, internships, apprenticeships, graduate assistants, on-campus employment, resume reviews, and mock interviews. Facilitating student engagement in these activities is essential for institutions and faculty, as they play a crucial role in enhancing students' skills, expanding their professional competencies, and increasing their employability. Adequate support and funding for these initiatives are imperative to ensure students have access to meaningful experiential learning opportunities that align with workforce demands.

Keywords: Clubs, competitions, certifications, careers, cybersecurity.

LLMs for mapping KSATs to job postings and predict DCWF work roles

[Lightning Talk]

Ram Dantu, University of North Texas, TX, ram.dantu@unt.edu

Arup Datta, University of North Texas, TX, arupdatta@my.unt.edu

Alexis Blackwell, University of North Texas, TX, alexisblackwell@my.unt.edu

Thomas Trebat, University of North Texas, TX, thomastrebat@my.unt.edu

Extended Abstract

A crucial part in today's rapidly changing labor market for both companies and job seekers is accurately determining skills needed for a particular job. Job descriptions include a wealth of information about the duties, abilities, and credentials required to carry out a particular job. This information can be extremely difficult to extract. Additionally, the extracted data is frequently unstructured leading to problems in the usability of the information. The standardized Department of Defense (DoD) Cyber Workforce Framework (DCWF) can assist job searchers in locating condensed and organized data on the Knowledge units, Skills, Abilities, and Tasks (KSAT) that must be completed to be successful in that position. However, there are no current effective approaches available that can truly extract information from job postings and map to the KSATs specified in the DCWF. Previous research primarily focuses on matching job descriptions to candidate resumes. The task of extracting skills from a job description can be made simpler by a few traditional Natural Language Processing (NLP) tools and techniques, but those technologies are unable to identify implicit talents. In this work, we aim to close the gap and develop a method that does not concentrate on the keywords that were taken from the job posting, which loses the latent information when mapping it with the DCWF KSATs. Large Language Models (LLMs) with their vast knowledge base and ability to be expanded to handle nearly any task without any training. LLMs can learn from examples given in the input context and use that knowledge to perform similar tasks. Therefore, LLMs can be utilized by providing a few-shot examples together with the reasoning behind the chain of thought. In addition, LLMs save a great deal of time compared to manually annotating many training examples. Furthermore, training and testing the model is faster as LLMs are simple to use and do not require any training. This research work aims to fill the skill extraction and mapping gap by leveraging the reasoning capabilities of LLMs to provide an effective method to identify explicit and implicit skills and align them with the DCWF framework. The DCWF contains around 72 work roles, and the total number of KSATs is around 3089. However, it is not possible to pass all 3089 KSATs to LLMs for relevancy as it would be too expensive given the current capacity of the models. So, instead, we have successfully narrowed it down to around 400 (to fit a low-end LLM model) eliminating the need for significant data annotation and model training and holds the potential for streamlining curriculum design and job-role analysis.

Keywords: DCWF Framework, Large Language Model, KSAT, Zero-shot prompting, few-shot examples.

STORM Cybersecurity Career Development Program at Coastline College

[Lightning Talk]

Tobi West, Coastline College, CA, twest20@coastline.edu

Extended Abstract

The STORM Cyber program at Coastline College is a key component of a national coalition aimed at addressing the growing need for skilled professionals in cybersecurity, in partnership with the University of New Haven, Tennessee Technological University, University of Hawaii - Maui College, and University of North Texas. This partnership leverages a collaborative approach, bringing together CAE educational institutions, industry leaders, and government agencies to develop a workforce prepared to defend against emerging cyber threats. As part of this national coalition, the STORM Cyber program benefits from shared resources, expertise, and research initiatives, enhancing its ability to provide cutting-edge education. The STORM Cyber program is a comprehensive initiative designed to prepare community college students for careers in cybersecurity through hands-on skills development and an early research opportunity. The program emphasizes practical skills development, enabling participants to effectively address real-world cyber threats and challenges. The program provides a strong foundation in key areas such as the fundamentals of cybersecurity, programming, computer networking, operating systems, and network security, ensuring that graduates are well-equipped to secure digital environments in both private and public sectors. A significant feature of the STORM Cyber program is its immersive learning environment, which includes virtual labs and simulated cyberattacks. These experiences allow participants to apply theoretical knowledge in realistic scenarios, enhancing their problem-solving and critical-thinking abilities. Additionally, the program integrates certifications such as CompTIA Security+, CompTIA Network+, and Certified Defensive Security Analyst (HTB CDSA) into the curriculum, making it a valuable choice for individuals aiming to stand out in the competitive cybersecurity job market. By blending technical expertise with practical application, the STORM Cyber program bridges the gap between academic learning and professional readiness. Another notable aspect of the STORM Cyber program is its emphasis on collaboration and mentorship. Participants work closely with mentors and peers, fostering a community of learning and innovation. Regularly scheduled workshops and guest lectures provide networking opportunities and insights into the latest cybersecurity trends and practices. Additionally, the program addresses the growing demand for skilled professionals in cybersecurity, aligning its objectives with industry needs and global security standards. The STORM Cyber program equips students with the tools and knowledge needed to prepare for in-demand cybersecurity careers providing no-cost tuition and textbooks, certification exam vouchers, Hack-the-Box and TestOut subscriptions, and a research stipend. This one-year program culminates in a research symposium to showcase the efforts of students in the STORM Cyber program.

Keywords: Cybersecurity, early research, community college, workforce readiness.

Refereed Extended Abstract Proceedings for Posters

A strategic approach to harden network security using the NIST framework for small technical skilling organization

[Poster]

Sarath Chandra Reddy Chowtukuri, Nova Southeastern University, FL, sc3597@mynsu.nova.edu

Yair Levy, Nova Southeastern University, FL, levyy@nova.edu

Extended Abstract

A strong network security planning is essential for reducing risks, ensuring long-term profitability, and supporting safe remote work. It protects sensitive data, helps meet regulatory requirements, and ensures business continuity. By implementing effective cybersecurity practices, organizations can minimize financial losses from cyberattacks, enhance their reputation, and build trust with consumers. An integrated security framework is crucial for defending against network threats and maintaining organizational resilience. The National Institute of Standards and Technology (NIST) recently updated the Cybersecurity Framework 2.0 (2024), which provides a creditable and easy-to-follow framework, especially for small to medium companies. Protecting network information and infrastructure is vital to ensuring stable operations and mitigating threats to network systems' integrity. This poster leveraged current network security technologies to enhance the organization's cybersecurity posture, protecting its data and systems against unauthorized access and ensuring stronger, resilient operations in cyberspace. This project aimed to integrate network security hardening practices and technical management controls into a cohesive network security infrastructure for a small technical skilling organization in the southeastern United States to enhance its current limited security network settings. This project included an assessment of the top relevant cybersecurity risks associated with the current network infrastructure and set a risk management plan to address the top risks. Cybersecurity controls were proposed following the NIST Cybersecurity Framework 2.0 (2024), including a proposal for the cost of implementing the project. Recommendations on the benefits of the project to enhancing the network security posture of the organization are outlined.

Keywords: Network security hardening, network infrastructure protection, resilient operations, NIST Cybersecurity Framework for small organizations, risk mitigation, cybersecurity best practices.

Reference:

The National Institute of Standards and Technology (NIST) (2024). *Cybersecurity framework 2.0*. https://www.nist.gov/cyberframework

Implementing information security policies and compliance plan to mitigate the risks posed by remote work at a small law firm

[Poster]

Alex Corral, Nova Southeastern University, FL, ac3575@mynsu.nova.edu

Jomariel Castillo, Nova Southeastern University, FL, jc5224@mynsu.nova.edu

Yair Levy, Nova Southeastern University, FL, levyy@nova.edu

Extended Abstract

Remote work became increasingly popular in working society during the COVID-19 pandemic as a means for businesses to continue operating during perilous times. A survey conducted by the Pew Research Center in 2023 revealed that 14%, or roughly 22 million, of employed adults, work from home full-time in a post-pandemic society. Consequently, the suddenness of the favored remote work modality has presented new cyber threats and unidentified risks to organizations that host remote work infrastructure. Some cyber risks include phishing, vulnerable network security, endpoint security, and data protection. With employees working from home on their personal devices, network security configurations can be different amongst employees. For example, the telecommunications company Zoom discovered in 2024 that their 5.15.5 and older versions of their Zoom Desktop Client, Virtual Desktop Infrastructure (VDI) Client, Rooms Client, and Meeting Software Development Kit (SDK) for Windows were all vulnerable to privilege escalation from unauthenticated users via network access. As Zoom was widely used during the pandemic, this put Zoom and thousands of companies at risk. Remote work risks are relevant to addressing cybersecurity, and these cyber risks are further perpetuated due to how hastily remote work was adopted globally. Due to the convenience and need for remote work in the recent past, postponed or overlooked risks have surfaced as remote work was hastily adopted despite companies' unprepared information systems. The goal of this project was to mitigate the risks surrounding remote work through Information Security Policies (ISPs) and compliance plan implementation for a small law firm in South Florida. This project identified the top cyber risks surrounding remote work and provided actionable steps as to how the firm can mitigate them effectively following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (2024). Recommendations for the company's cybersecurity posture tier elevation following the NIST Cybersecurity Framework (2024) and costs associated with implementing the project are provided.

Keywords: Information security policies, cybersecurity compliance plan, NIST Cybersecurity Framework for small organizations, risk mitigation, cybersecurity best practices.

References:

Pew Research Center (2023). *About a third of U.S. workers who can work from home now do so all the time.* https://www.pewresearch.org/short-reads/2023/03/30/about-a-third-of-us-workers-who-can-work-from-home-do-so-all-the-time/

The National Institute of Standards and Technology (NIST) (2024). *Cybersecurity framework 2.0.* https://www.nist.gov/cyberframework

Advancing cybersecurity education in collaboration with industry

[Poster]

Behzad Izadi, Cypress College, CA, bizadi.cypresscollege@gmail.com

Rassoul Alizadeh, Cypress College, CA, ralizadeh@cypresscollege.edu

Noah Terpening, Cypress College, CA, nterpening@cypresscollege.edu

Extended Abstract

The Cybersecurity program at Cypress College successfully completed a three-year NSF-ATE-funded grant, *Pathway to Advancement in Cybersecurity Education (PACE).* This initiative established a structured dual enrollment program, introduced cybersecurity college courses to students as early as the 10th grade, and provided cybersecurity training and competition opportunities for elementary, middle, and high school students. As a result of PACE, comparing the 2018–2019 academic year (prior to PACE) to the 2022–2023 academic year (the final year of PACE), high school student enrollment in our Cybersecurity certificate program increased from 28 to 60 (+114%), college student enrollment rose from 5 to 42 (+740%), and total Cybersecurity certificate completions grew from 23 to 69 (+200%). Recently, our program was awarded a second three-year NSF-ATE grant, *Advancing Cybersecurity Education in Collaboration with Industry.* This new initiative aims to expand the cybersecurity workforce through industry collaboration by adopting the Business & Industry Leadership Team (BILT) model and engaging youth and underrepresented populations. The BILT model, a proven NSF-based framework, fosters effective industry collaboration by identifying the knowledge, skills, and abilities (KSAs) required by employers and incorporating them into the curriculum. Additionally, industry partners participate in project activities such as internships and mentorship programs. A key focus of the new NSF project is increasing female participation in the program by training faculty and providing female mentors. The project also seeks to expand dual enrollment partnership agreements with neighboring high schools. This poster summarizes the outcomes of PACE and highlights the objectives of the newly funded NSF grant.

Keywords: NSF-ATE grant, industry collaboration, Business Industry Leadership Team, BILT, cybersecurity pathway, dual enrollment, underrepresented populations.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Leveraging DevSecOps tools to hit the top 10 in cyber competitions

[Poster]

Brendan McShane, Penn State University, PA, BrendanMcShane@psu.edu

Nicklaus A. Giacobe, Penn State University, PA, nxg13@psu.edu

Donwon Lee, Penn State University, PA, dongwon@psu.edu

Extended Abstract

In cyber education, many National Centers of Academic Excellence in Cybersecurity (NCAE-C) institutions augment classroom instruction with participation in cyber competitions. Preparation for high-engagement, often in-person, competitions is critical to success. Current cyber competition teams need to practice building, defending, and attacking target networked computer systems that are similar in scope to what is in the competitions. They need a place to make that happen. In this poster, we present our current cyber-range-in-a-cart, and how our students use open source, cloud computing DevSecOps tools to fabricate environments suitable for training in-person competition teams. This tool has helped us train, which has led us to top-10 placements in Collegiate Cyber Defense Competition (CCDC Regional), United States (U.S.) Department of Energy CyberForce, and Collegiate Penetration Testing Competition (CPTC). Other competitions (e.g. National Cyber League) are suitable for initial immersion. These are often Capture the Flag (CTF)-style where participants are expected to figure it out as they go. These competitions are designed to challenge the new competitor to learn by doing, often just-in-time. These entry-level competitions engage new competitors, but preparation on behalf of the participant can be limited. Once students get a taste of the excitement of competition, we provide additional training run by experienced students on our club platform. More senior competitors (students) develop target systems, use the cloud computing tools (e.g. Heat Template) to deploy them. They provide access to dozens of trainees, who, through repeated engagements, can increase their skillsets to compete for seats for the in-person competition team. As a secondary outcome, the student builders and maintainers of the infrastructure benefit independently. Infrastructure development uses tools like Kubernetes, OpenStack, and Helm charts. OpenStack's Heat enables rapid deployment of Virtual Machines (VMs) with preconfigured settings defined through Yet Another Markup Language (YAML). These students develop a skillset that is valued by employers. Components include four Cisco UCS (768 GB RAM, 2x16 Core Intel Xeon); 2x Cisco UCS (256 GB RAM, 2x8 Core Intel Xeon); 24x 500 GB SSD;10G Switch, 8 port; 1G Switch, 24 port; 5x 1G Tabletop Switch; Mikrotik router; 2x UPS (1540 Watt); 16U rolling network rack. Acknowledgement: This work was supported under NSF CyberCorps Scholarship for Service - NSF Award Number 1663343.

Keywords: Cyber range, competitions, DevSecOps, cloud.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Transitioning from survey-based risk assessment to risk intelligence model for maritime cybersecurity

[Poster]

Bilge Karabacak, University of North Carolina Wilmington, NC, karabacakb@uncw.edu

Ulku Clark, University of North Carolina Wilmington, NC, clarku@uncw.edu

Hosam Alamleh, University of North Carolina Wilmington, NC, alamlehh@uncw.edu

Extended Abstract

This poster introduces a survey-based cybersecurity risk assessment method designed to actively engage maritime stakeholders, including policymakers and leaders. The poster is divided into four key sections. First, it presents the findings of an extensive critical literature review that analyzed over 30 maritime cybersecurity guidelines developed by Non-Governmental Organizations (NGOs), governments, and international organizations. This review highlights the fragmentation and gaps in existing guidelines and establishes the need for a unified approach to cybersecurity in the maritime sector. Second, it addresses the identified gap by introducing Cybersecurity Risk Assessment Method for Maritime Transportation Systems, a method tailored to incorporate the International Maritime Organization's (IMO) safety criteria. Third, it showcases the application of the method through a survey of 80 maritime professionals, providing insights into their perception of cybersecurity risks, and revealing varied risk levels across different operational contexts. Lastly, the poster explores the potential to scale and enhance the method using artificial intelligence. It outlines a roadmap for transitioning from the survey-based method into a Maritime Risk Intelligence Model, an AI-powered approach to streamline cybersecurity risk assessments and deliver actionable insights to maritime stakeholders. This transformation aims to address the sector's dynamic challenges, enabling more efficient, scalable, and adaptive risk assessments.

Keywords: Cybersecurity risk assessment, Maritime Transportation Systems (MTS), Artificial Intelligence (AI), maritime cybersecurity, risk intelligence model.

Auburn University's Ethical Hacking Club

[Poster]

Farah Kandah, Auburn University, AL, farah-kandah@auburn.edu

Luke Robinson, Auburn University, AL, ler0064@auburn.edu

Extended Abstract

Auburn University's Ethical Hacking Club (AUEHC), a student-run chapter, meets weekly to discuss fundamental cybersecurity concepts such as network security, penetration testing, digital forensics, host security, and cyber-physical security. The club's mission is to create a platform for individuals passionate about cybersecurity to acquire essential knowledge and skills. To enrich discussions and provide valuable insights, AUEHC actively invites guest speakers, including cybersecurity and Machine Learning (ML)/Artificial Intelligence (AI) professors at Auburn University and industry professionals. Beyond regular meetings, AUEHC organizes various competitions to engage and challenge its members. These include Los Alamos National Laboratory (LANL) Cyber Fire Puzzles and student-organized events like War Driving and social engineering experiments. Additionally, the AUEHC forms and trains teams to participate in external competitions, such as the Department of Energy (DoE)'s CyberForce competition, the Southeastern Collegiate Cyber Defense Competition, and the National Cyber League. These competitions provide opportunities for members to showcase their skills and collaborate as a team. Notably, AUEHC recently achieved a commendable 15th place in CyberForce and ranked 12th among nearly 5,000 teams in the National Cyber League (NCL). AUEHC organizes competition training sessions to enhance participants' skills and foster team building. These sessions offer hands-on experience and practical exercises that enable members to acquire essential cybersecurity knowledge and apply it in real-world scenarios.

Keywords: Student activities, ethical hacking club, cybersecurity competitions.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Defending backdoor attacks in real-time image recognition systems using morphological filter

[Poster]

Bashar Najah Allwza, California State University, Sacramento, CA, basharallwza@csus.edu

Syed Badruddoja, California State University, Sacramento, CA, badruddoja@csus.edu

Ram Dantu, University of North Texas, TX, ram.dantu@unt.edu

Extended Abstract

A backdoor attack is one of the common model poisoning attacks, where the attacker implants a backdoor for the future to trigger a prediction. Investigators found that the neural networks suffered a low prediction accuracy of 45.42% and 14.61% in brain tumor detection due to injected trojan-based poison attacks. Moreover, another research introduced a malfunctioning malware detection platform that allowed malware through the network at an 89.5% success rate using class-activation mapping-based deep neural network poisoned attacks. Furthermore, researchers discovered that a trained patch can misbehave as desired by the attacker with 99% prediction accuracy in Very Deep Convolutional Networks (VGG), MobileNet, and Resnet Convolutional Neural Network (CNN) architectures, deeming the model poisoning attacks to be precarious to many applications in healthcare, economy, and social applications. Additionally, attackers employ other strategies to compromise the model's integrity, such as injecting phony samples and establishing adversarial instances. Existing defenses against model poisoning attacks face multi-faceted challenges due to the nature of the attack, damage to the reputation, and size of the impact. Furthermore, most defense strategies involve repairing the training dataset, retraining the Artificial Intelligence (AI) model, or keeping the data secure. However, this type of repair requires the model to be retrained and damages the business continuity of applications. We propose a novel defense mechanism utilizing morphological filters to defend against backdoor attacks in real-time. We add a 3x3 morphological filter to clean the poisoned data before it can pass through the poisoned model and apply morphological operations. The images are eroded and dilated to remove the poison from the poisoned record and reflect its original shape. Once the filter is applied to the image in erosion operation, the pixel value in the new resulting image will be the minimum value of the pixels that landed on the white area of the filter. Furthermore, the dilation operation makes the objects more prominent, so the pixels around the targeted pixel are replaced with the maximum value of the surrounded pixel, which helps restore the shape to its original size. The experiment was conducted using Modified National Institute of Standards and Technology (MNIST) digit recognition dataset with 60000 samples using neural network. The defense mechanism has maintained the model's accuracy of 90% and made the correct label prediction even when the number of poisoned records was significantly high. Moreover, the F1-score was stable at 0.96 with up to 5000 poisoned records. Furthermore, when we evaluated our defense mechanism with the increasing size of the poisoned pixels, it maintained a stable high prediction accuracy of around 90% and an F1 score of 0.95. In the near future, we will expand our work to study the efficacy of our method.

Keywords: Neural networks, artificial intelligence, security, backdoor attacks.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Randomizing forger selection to improve decentralization in proof of stake consensus protocol

[Poster]

Sasi Kanduri, California State University, Sacramento, CA, sasikanduri@csus.edu

Syed Badruddoja, California State University, Sacramento, CA, badruddoja@csus.edu

Extended Abstract

Proof of Stake (PoS) emerged as an efficient consensus protocol, selecting validators for new blocks based on their cryptocurrency holdings and "stake". For decentralized applications in Decentralized Finance (DeFI) industry. However, PoS promotes centralization and inadvertently leads to a concentration of control among a few participants, potentially threatening the decentralized nature of the blockchain. Conversely, liquid staking pool platforms such as Lido help users pool their assets for staking on PoS networks and incentivize users with liquid tokens, making participation more accessible. However, these pools lead to centralization, with a few large pools dominating staking, concentrating validation power and governance influence. This undermines decentralization by creating reliance on a small number of entities, increasing risks of collusion or censorship. Proof of Stake and Activity (PoSA) protocol, one of the solutions, addresses centralization by rewarding validators based on both stake capital and their business contributions, promoting decentralization. However, they fail to address the centralization due to algorithmic limitations and do not entirely address the randomness and fairness factors of the selection process. In this research, we expand stake-based consensus mechanisms to the selection level to improve decentralization using a hash power-based proof of stake (hPoS) consensus protocol. The stakes and timestamps are used to calculate hash powers (a value that determines the probability of selection) that can be used to improve randomness in the validator selection process. The simulation was executed in a pilot blockchain infrastructure using 50 nodes. Moreover, we executed the coinage-based and hash power-based consensus protocol in two scenarios - one where the stakes are totally random among all the nodes and another where a fixed group of nodes has higher stakes than all others. The observed result proves that our algorithm yielded high randomization compared to the Coinage-based implementation. Since the validity of each stake expires after a certain period of time, the node selection is based on the stake average over a certain range of stakes, which increases the randomness of the protocol. Moreover, our results show that the participation opportunities are more equitably distributed than the coinage protocol. Furthermore, we assessed the fairness and entropy of hPoS consensus protocols versus the Coinage protocol. The fairness factor increased from 0.11 to 0.45, and entropy increased from 0.51 to 0.80 for the hash power-based protocol compared to the Coinage. Our findings empower the cybersecurity community to advance consensus protocols by leveraging improved randomization for enhanced decentralization and security in blockchain systems.

Keywords: Proof of Stake, consensus protocol, blockchain, decentralization.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

INDRA: A drone penetration testing platform for cybersecurity education

[Poster]

Thomas Devine, West Virginia University, WV, thomas.devine@mail.wvu.edu

Simon Dalton, West Virginia University, WV, sad00013@mix.wvu.edu

Chloe Johnson, West Virginia University, WV, cmj00004@mix.wvu.edu

Visnu Pandian, West Virginia University, WV, vsp00002@mix.wvu.edu

Raekwon Thomas, West Virginia University, WV, rnt00002@mix.wvu.edu

Extended Abstract

Closing the cybersecurity skills gap requires hands-on education that puts students in realistic scenarios to prepare them for the challenges faced by cybersecurity professionals. As the accessibility and capabilities of drones and small Unmanned Aerial Vehicles (sUAV) have evolved, they are increasingly used in a diverse range of professional applications, making them a tempting target for cyber-attacks. This poster details an ongoing experiment in hands-on cybersecurity education at the undergraduate level to test the cybersecurity of sUAVs. To gain hands-on experience in ethical drone hacking, we created INDRA: Sky Commander, a penetration testing platform for sUAVs. INDRA is built, maintained, and evolved by undergraduate students as an ongoing capstone senior design project. INDRA, the Interceptor for Neutralization and Drone Remote Access, is a platform for improving the security posture of sUAVs by conducting penetration tests to probe and exploit the attack surface of sUAVs. We designed INDRA to be easy to use and easy to extend with a simple and intuitive interface and modular design to facilitate the development and integration of new ethical hacking modules, allowing the platform to evolve over time with new generations of students. The first generation of students designed the software architecture and implemented the initial graphical user interface (GUI), basic Wi-Fi scanning functionality, and a Wi-Fi deauthentication attack module. The second generation consisted of two groups that focused on performing radio frequency (RF) jamming attacks on Wi-Fi drones and migrating the platform to the cloud. The RF jamming module utilizes software-defined radios (SDRs) and USB-based WiFi devices to deny availability to Wi-Fi drones and the cloud migration group successfully ported the application to the cloud so that any laptop with an SDR and appropriate USB Wi-Fi adapter could perform the deauthentication attack, though RF Jamming was limited by latency issues. The third generation implemented an eavesdropping attack module. By sniffing and decoding packets, they covertly intercepted images from the drone's video feed to display on the GUI. The two groups in the fourth generation are currently designing additional reconnaissance features and attempting to extend RF Jamming to work on non-Wi-Fi drones.

Keywords: Drone penetration testing platform, deauthentication attack, radio frequency (RF) jamming attacks.

Jericho: A cyber city for enhancing cyber operations education

[Poster]

David Reid, Cedarville University, OH, dreid@cedarville.edu

Jacob Grady, Cedarville University, OH, jgrady@cedarville.edu

Logan Miller, Cedarville University, OH, loganmiller216@cedarville.edu

Kaicheng Ye, Cedarville University, OH, kaichengye@cedarville.edu

Seth Hamman, Cedarville University, OH, shamman@cedarville.edu

Extended Abstract

Cyber operations create effects in physical space as well as cyberspace, but most cybersecurity education exercises are confined to cyberspace. Jericho helps drive home the real impact of cyber operations and cyber-insecurity by incorporating physical space effects into cyber operations education. Jericho is a physical table-top cyber city that incorporates critical infrastructure elements. It blends a traditional cyber range experience with a physical range. Existing cyber physical ranges are rare and prohibitively expensive. Jericho is a model for how ranges can be constructed inexpensively. It is constructed using an extensible crate model using off-the-shelf electromechanical components like motors, speakers, and Light Emitting Diodes (LEDs) wired to a microprocessor such as Raspberry Pi Zeros. It models how missions can be created on the range by placing students in the role of cyber operators charged with the attack or defense of critical infrastructure. Students gain access to the cyber city's network over a Virtual Private Network (VPN) and begin their mission in a sandboxed virtual machine environment similar to many cyber education exercises. In one mission, students find and exploit vulnerabilities as they pivot through a mock city's cyberspace infrastructure with the goal of commandeering the city's traffic lights. The mission is accomplished when the physical traffic lights in the miniature city change at the will of the students.

Keywords: Critical infrastructure, cyber city, cyber operations education, cyber physical range, microprocessor, Raspberry Pi.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Welcome to WannaCry: A case study and model for cybersecurity education

[Poster]

Eli Creek Richmond, West Virginia University, WV, ecr00012@mix.wvu.edu

Thomas Devine, West Virginia University, WV, thomas.devine@mail.wvu.edu

Extended Abstract

In cybersecurity education, there is a notable deficit in comprehensive, hands-on training for malware analysis conducted within an ethical framework. This research addresses this gap by introducing an educational module that immerses students in both dynamic and static analysis of the WannaCry ransomware, fostering active learning and critical thinking while emphasizing responsible practices. The module consists of a web application to be hosted by the instructor and two virtual machines (VMs) to be downloaded by the student or hosted in a cyber-range. The VMs are pre-configured with all necessary tools and files for both static and dynamic analysis of the malware. Students access detailed instructions and walkthroughs through the web application, which guides them through each phase of conducting the analysis on the VMs. Within the controlled, isolated VM environment, students utilize modern, open-source tools such as Ghidra for reverse engineering and Cuckoo Sandbox for behavioral analysis. This setup enables them to observe malware behavior, dissect its code and structure, and analyze its propagation methods, all while ensuring safe handling of malicious software. As an educational module, the expected learning outcomes include proficiency in malware analysis methodologies, identification of obfuscation techniques, and enhanced problem-solving skills pertinent to cybersecurity. For assessment, the walkthroughs are accompanied with questions whose answers require the students to perform the analysis themselves. All questions are auto-graded with a report accessible to the students at the end of the activity that can be submitted as the deliverable for the assignment. By engaging directly with real-world malware in a controlled setting, students gain practical experience that bridges theoretical knowledge and real-world application. The Welcome to WannaCry educational module is currently being beta-tested by senior-level undergraduates at a National Centers of Academic Excellence in Cybersecurity (NCAE-C) institution and we intend to release the module to the CAE in Cybersecurity Community after addressing the concerns raised during testing.

Keywords: Hands-on malware analysis, cybersecurity education module, WannaCry ransomware training.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Detection of smart contract vulnerabilities using AST-transformer

[Poster]

Harshith Sai Veeraiah, California State University, Sacramento, CA, harshithveeraiah@csus.edu

Syed Badruddoja, California State University, Sacramento, CA, badruddoja@csus.edu

Ram Dantu, University of North Texas, CA, ram.dantu@unt.edu

Extended Abstract

The Solidity programming language has become a cornerstone for developing decentralized finance (DeFi) applications using smart contracts, thriving as blockchain technologies experience unprecedented growth. However, these smart contracts are exposed to significant security vulnerabilities, as even minor coding flaws can lead to catastrophic financial losses and reputational damage. Existing methods for vulnerability detection, including static analysis tools and AI-based approaches like Recurrent Neural Networks (RNNs), often fail to adequately address the complexity and contextual nuances of smart contracts. This research introduces an innovative vulnerability detection methodology that leverages Abstract Syntax Trees (ASTs) combined with transformer-based models. By parsing Solidity-based smart contracts into ASTs, this approach captures a hierarchical representation of the code, revealing intricate relationships between elements such as variables, functions, and control dependencies. The use of transformer models further enhances detection by capturing long-range dependencies and complex contextual interactions, surpassing the limitations of rule-based and earlier AI-driven approaches. The proposed transformer-based methodology outperformed the RNN-based model in both accuracy and robustness, highlighting its superiority in vulnerability detection. The transformer model achieved a state-of-the-art accuracy of 99.89%, with a stable F1-score of 0.96, perfect precision of 1.00, and strong recall of 0.92, showcasing its ability to detect vulnerabilities like Integer Overflow with high precision and minimal false positives. In contrast, the RNN-based model demonstrated an accuracy of 92.58% and a precision of 0.84 but lagged in recall at 0.61, resulting in an F1-score of 0.71. While the RNN model exhibited general effectiveness, its lower recall indicates a limitation in capturing all vulnerabilities within the dataset. The transformer-based approach's capacity to sustain high performance even under challenging conditions, combined with its superior precision and recall, establishes it as a more reliable and practical solution for enhancing smart contract security. This comparison underscores the importance of leveraging advanced transformer architectures for achieving state-of-the-art results in the evolving landscape of vulnerability detection. This work not only advances the field by addressing the shortcomings of existing tools but also provides a scalable and adaptable solution tailored to the dynamic and evolving threat landscape of blockchain ecosystems. By integrating cutting-edge machine learning techniques with structural code analysis, the proposed framework represents a significant step forward in safeguarding decentralized applications and fostering trust in DeFi platforms.

Keywords: Smart contracts, security, artificial intelligence, solidity.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Advancing IT accessibility, enrollment, and workforce readiness through hybrid education models

[Poster]

Daniel McIntosh, Laramie County Community College, WY, DMcIntosh@LCCC.WY.edu

Troy Amick, Laramie County Community College, WY, TAmick@LCCC.WY.edu

Extended Abstract

The growing Information Technology (IT) workforce demand exceeds the available talent pool, particularly in cybersecurity, data center management, and network administration. Traditional education models struggle to address these shortages due to reliance on high school pipelines, limited outreach to rural areas, and lack of mentorship and networking opportunities for students. This initiative integrates multiple strategies under a comprehensive workforce development program to expand access to IT and cybersecurity education. A hybrid education model ensures geographically isolated students receive industry-aligned training through virtual labs and online resources, bridging the accessibility gap. Early exposure initiatives, including high school outreach and the Strategies for Success Course, introduce students to IT and cybersecurity concepts, increasing confidence and enrollment. To enhance preparedness, summer bootcamps in IT and cybersecurity offer hands-on experiences before students enter formal programs. These bootcamps, along with faculty-led mentorship programs, have contributed to a 30% increase in enrollment from underserved students in rural areas. Additionally, professional development efforts equip educators with inclusive teaching methodologies, ensuring a supportive learning environment. Key accomplishments include the expansion of virtual labs, industry partnerships, and student networking platforms such as Tau Epsilon Kappa (TEK), the IT Professional Club, and The Cyber Defense Team. These efforts collectively strengthen cybersecurity literacy, enhance workforce readiness, and create an inclusive talent pipeline. By addressing systemic barriers and evolving industry needs, this model offers a scalable approach to IT and cybersecurity workforce development.

Keywords: Higher education, training and lifelong learning in cybersecurity, K-12 cybersecurity, student club activities.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Internet of Drone Things (IoDT) simulation for resiliency through Large Language Models (LLMs)

[Poster]

Cihan Tunc, University of North Texas, TX, Cihan.Tunc@UNT.edu

Fatima Shibli, University of North Texas, TX, Fatima.Shibli@UNT.edu

Extended Abstract

The simultaneous expansion of the Internet of Things (IoT) and drone technologies has led to the development of the Internet of Drones Things (IoDT), with the aim of combining sensor-enhanced and communication-capable drones with IoT devices. The collaboration between these systems has enormous potential to instigate substantial change across multiple sectors, including disaster management, surveillance, search and rescue, and smart agriculture. Despite their potential, the IoDT ecosystem is still in its infancy, facing significant and complex challenges, including but not limited to cyberattacks (and even physical attacks), resiliency, scheduling, management, and integration. This is primarily a concern when unpredictable dynamic environmental conditions present significant complexity (e.g., transient obstacles and weather conditions). Therefore, we must overcome these challenges to realize the full potential of IoDT systems while remaining optimistic about future developments. Resiliency for IoDT management using static algorithms faces challenges when responding to dynamic real-time environments, especially when safety is a concern. Therefore, to address these challenges, our research focuses on developing and analyzing a lightweight IoDT simulator that utilizes Large Language Models (LLMs) to improve resiliency through task management and decision-making. We created a lightweight simulator that uses path-planning algorithms like Dijkstra, A*, and D*, enabling drones to independently select the best routes based on energy use and environmental danger by dynamically reallocating tasks to functioning drones when certain drones experience failures or cyberattacks. We also leverage cutting-edge LLMs like GPT-4 and Llama 3 for resilient decision making that generates and assigns tasks to drone swarms by analyzing current environmental conditions and adjusting each drone's specific abilities. The proposed work offers great performance (compared to traditional methods) across different environmental conditions in different real-world scenarios. The findings demonstrate that LLM integration into IoDT systems improves drone swarm resilience while establishing foundations for smarter adaptive drone-IoT operations.

Keywords: Internet of Drone Things, resiliency, large language models, LLM, cybersecurity, simulator, drones.

2025 CAE in Cybersecurity Symposium – Charleston, South Carolina
Refereed Proceedings – CAE in Cyber Defense (CD) Track

A Publication of the CAE in Cybersecurity Community National Center

Micro-transcript generation using detailed knowledge units for workforce readiness

[Poster]

Cihan Tunc, University of North Texas, TX, cihan.tunc@unt.edu

Fatima Shibli, University of North Texas, TX, fatimashibli@my.unt.edu

Ram Dantu, University of North Texas, TX, ram.dantu@unt.edu

Alexis Blackwell, University of North Texas, TX, alexisblackwell@my.unt.edu

Thomas Trebat, University of North Texas, TX, thomastrebat@my.unt.edu

Extended Abstract

Despite growing support for cybersecurity, recent incidents have shown that current cybersecurity solutions, expertise, and the workforce still need further development to effectively protect cyberspace. There is still a large gap between the knowledge and skills taught in cybersecurity programs and those needed in the cybersecurity workforce due to several factors, such as the constantly evolving nature of the field and the inclusion of soft skills—such as communication, problem-solving, and critical thinking—alongside technical skills. Another reason for this gap is that the same course may be taught differently across institutions or by different instructors. Therefore, a major concern for the cybersecurity workforce is the significant gap between the required knowledge and skills, what is taught in cybersecurity education programs, and how well students master individual topics. Our aim is to strengthen the cybersecurity pipeline by building more robust educational programs to expand the pool of qualified candidates for future employment, thereby advancing the nation's cybersecurity capabilities. To achieve this goal, we created a solution that rigorously assesses cybersecurity students in preparation for cybersecurity workforce applications. Our solution comprises the Work-Skills Readiness (WSR) tool, which allows Knowledge Units (KUs) defined in the National Center of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CD) document to be directly incorporated into the learning outcomes of a course in a Learning Management System (LMS). Using the WSR tool, an instructor selects relevant KUs that pertain to the course curriculum, which can be directly imported into assignment rubrics for grading and evaluation of students based on official NCAE-C - CD KUs. Once assignment submissions have been received and graded, a micro-transcript is generated that displays the KU scores obtained directly from assignment submissions. The micro-transcript lists the KU topics, the number of topics covered within the KU, and up to three distinct scores for each topic (Basic, Intermediate, and Advanced). These scores indicate the proficiency level of the student with the competency statements as used by NCAE-C designated academic institutions. The micro-transcript can help students more effectively apply for career opportunities in the cybersecurity field, since it succinctly conveys their knowledge and skills to potential employers. In summary, by utilizing this solution, instructors can ensure that their course material more closely aligns with industry standards, and students can contribute to creating a highly skilled national cybersecurity workforce.

Keywords: Micro-transcript, knowledge units, LLM, workforce readiness.

NCAE Cyber Games: Technology and methodology

[Poster]

Jake Mihevc, Mohawk Valley Community College, NY, jmihevc@mvcc.edu

Nick Doerner, NCAE Cyber Games, NY, ndoerner@ncaecybergames.org

Extended Abstract

This poster highlights the technology and methodology that have contributed to the success of the *NCAE Cyber Games* project over the last five years. The *NCAE Cyber Games* is a competition that includes both Red versus Blue infrastructure defense and Capture The Flag (CTF) challenges. The competition is designed for students that are new to cybersecurity competitions, and over 1,000 students from 100 unique National Centers of Academic Excellence in Cybersecurity (NCAE-C) institutions participated in 2024. The technology platform that brings the *NCAE Cyber Games* to life is the result of 10,000 hours of development and is open-sourced to facilitate broad adoption. This poster details the different technologies employed within the platform, their functions, and how they interact to produce robust virtual networks, cohesive visualizations, real-time scoring, and a red-team dashboard that depicts the status of vulnerabilities and exploits within team systems. The methodology of the *NCAE Cyber Games* leads to an engaging student experience as evidenced by a student satisfaction rating higher than 90% in each year of the competition. This poster illustrates the approaches and methodologies that make the *NCAE Cyber Games* unique. The team registration system is fully automated and student-driven, thereby teaching students valuable leadership and organizational skills. Team and competition-wide communications are facilitated by the Discord platform, and the NCAE-C Discord server is structured to enable supportive communications, real-time learning assistance, and the infusion of humor into the experience. The reward structure of the event celebrates learning, improvement, and teamwork to create a welcoming environment for all students regardless of how important competition is to their personal goals.

Keywords: Cyber competitions, NCAE Cyber Games.

US Coast Guard Academy (USCGA) eCTF 2025

[Poster]

Joshua West, US Coast Guard Academy, CT, joshua.c.west@uscga.edu

Dominic Gilbert, US Coast Guard Academy, CT, dominic.s.gilbert@uscga.edu

Wyatt Duthu, US Coast Guard Academy, CT, wyatt.j.duthu@uscga.edu

Juan Garcia, US Coast Guard Academy, CT, juan.a.garcia@uscga.edu

Mohamed Elwakil, US Coast Guard Academy, CT, mohamed.m.elwakil@uscga.edu

Extended Abstract

This poster presents the design of a hardened security satellite TV system developed for the 2025 MITRE Embedded Capture the Flag (eCTF) competition by the United States Coast Guard Academy (USCGA) team. The system aims to safeguard that only authorized decoders with valid subscriptions can decode television (TV) frames while protecting against potential attacks. The architecture comprises five main components: the uplink, which initiates data transmission of raw TV frames; the encoder, responsible for encoding these frames; the satellite, which acts as a broadcast mechanism forwarding encoded frames to connected decoders; the host computer, managing interactions between the decoder and the satellite; and the decoder itself, which maintains active subscriptions and decodes received frames. The system must fulfill three key functional requirements: the system build, which establishes a consistent build environment and generates global secrets; the encoder, which encodes TV frames using secure methods; and the decoder, which processes commands, updates subscriptions, and decodes frames while ensuring integrity and authenticity. To achieve this, the design incorporates stringent security measures, including unique channel keys derived from deployment-specific secrets to prevent unauthorized access, secure key exchange utilizing RSA encryption for subscription updates, frame authentication through Message Authentication Codes (MACs) to verify integrity, and monotonic timestamps to ensure frames are processed in the correct order, rejecting mis-ordered frames.

Keywords: Hardened security satellite TV, MITRE eCTF 2025, system design, security requirements.

Reference:

MITRE. (n.d.). *Embedded capture the flag (eCTF) competition.* https://ectfmitre.gitlab.io/ectf-website/index.html