Session 1: Cybersecurity Curriculum Development and Pedagogy

November 13th at 10:15 AM

Bridging the Cybersecurity Skills Gap: Aligning Educational Programs with Industry Needs

Joshua Ball, Maura Lyons, Kendra Evans

This paper examines the widening cybersecurity skills gap and its implications for organizations, highlighting the inadequacies in current educational and training programs. Through a comprehensive survey of 200 senior executives responsible for cybersecurity strategy, we identify the most valued technical and non-technical skills, the perceived deficiencies in new hires, and the role of practical experience and industry-academia collaboration.

Building on existing research, this paper highlights the relative importance of skills, the value of practical experience, and the benefits of industry-academia collaboration. The results reinforce existing literature while offering new perspectives essential for addressing the cybersecurity workforce challenges.

We found that organizations that collaborate with educational institutions report higher satisfaction with new hires but also experience significant gaps in practical experience and industry-specific best practice knowledge among new hires. Cluster analysis revealed distinct patterns in organizational priorities, challenges, and characteristics, suggesting that tailored educational approaches may be necessary.

November 13th at 10:35 AM

Project-Based Learning in K12 Cybersecurity Education

Sandra Nite, Wesley Brashear, Trenton Gray, Dhruva Chakravorty

Teaching adolescents can be challenging, and cybersecurity education is no different. Teachers need to find ways to engage students in the learning by providing some incentive, such as encouraging a sense of curiosity about something in the world around them. In this paper, we discuss one model of teaching, the 5E Model, that has been effective in helping teachers engage students so they have a desire to learn the material. We will also discuss the Project-Based Learning method of teaching in which students learn the necessary information for the project as they work on the project. Students' incentive to learn is based on the need for the learning in order to solve the problem and complete the project. We combined these two ideas and integrated them into some of the activities in the summer camp as well as the project for the week. We will describe two camp activities and how the 5E Model was used to plan the activities. Then we will describe the final project and how the 5E Model was used as the students developed their projects throughout the week, learning more and more about the cybersecurity concepts around which the camp was focused. We hope to give others who work with adolescents in informal learning some ideas to help keep students engrossed in the learning opportunities provided to them.

November 13th at 10:55 AM

Mentoring Cybersecurity Students in Online Degree Programs

Herbert Mattord, Michael Whitman

This paper examines the design, implementation, and continuous improvement of a successful mentoring program integrated into cybersecurity capstone courses at a Southern University, aimed at bridging the gap between academic learning and real-world experience. Faced with a need to implement experiential outcomes for cybersecurity graduates, the university introduced a structured mentoring initiative involving industry executives and technical leads to enhance students' professional development, networking opportunities, and practical skills. The program's remarkable success, attributed to several key factors: the careful selection of mentors, comprehensive mentor training, and the assignment of multiple mentors to minimize disruption caused by potential withdrawals, has significantly enhanced student outcomes. A continuous improvement process, anchored by after-action reviews at the end of each semester, allows the program to evolve in response to participant feedback, ensuring alignment with educational goals and addressing diversity, equity, and inclusion (DEI) challenges in the field. The paper concludes that this mentoring initiative enhances student outcomes and underscores the importance of integrating experiential learning opportunities within academic curricula. Recommendations for institutions adopting similar programs include prioritizing mentor selection and training, implementing continuous feedback loops, and emphasizing mentor commitment to maximize student benefits.

November 13th at 11:15 AM

Cybersecurity High School Innovations: A Path for Educators to Teach Cybersecurity Courses in their Schools

Marc Dupuis, Robert Honomichl, Morgan Zantua, Jenny Ju

There remains a significant unmet demand for cybersecurity professionals nationwide. Many solutions have been forwarded, but more are needed. Improving opportunities within higher education institutions is important and a critical component of addressing this unmet need, but may do too little too late for many potential cybersecurity professionals. This paper examines the development of an innovative program designed to address this challenge by providing opportunities to secondary educators of all backgrounds. Participants are given an opportunity to learn about cybersecurity and how to bring what they learn back to their own schools and teach it to their students as a standalone course. The program provided a remote component in preparation for an intensive in-person summer summit where participants were brought together at one or more locations. During that time, they would hear from experts in academia, industry, and the military, as well as have an opportunity to practice what they learned through various hands-on labs and activities. Participants from the first year were invited back the second year for a more challenging and advanced experience. During the third year, first and second year participants were invited back such that there were three levels of participants. This paper reports on the findings of this innovative program and provides recommendations for future iterations of similar programs based on lessons learned.

November 13th at 11:35 AM - Virtual

Empowering Youth in the Digital Age: A Curriculum Proposal Informed by Welsh High School Teachers' Perspectives on Cybersecurity Education

Maha Alotaibi, Yulia Cherdantseva, Omar Rana, Catherine Teehan

As cyber threats increasingly target vulnerable youth, the need for comprehensive cybersecurity education has become more critical. Integrating cybersecurity into secondary school curricula offers a promising solution, equipping students with the necessary skills to identify and mitigate cyber risks. Despite the increasing number of cyber risks targeting young people, cybersecurity education in secondary schools is still in its early stages. This study investigates the perspectives of 27 Welsh secondary school teachers on incorporating cybersecurity education into their curricula through semi-structured interviews. The qualitative insights gathered reveal key challenges and opportunities, including a lack of resources, age-appropriate materials, and pedagogical support for teaching cybersecurity. Our findings underscore the need for targeted educational reforms and collaboration between schools and cybersecurity professionals. Based on these results, we provide practical recommendations for educators, school administrators, and cybersecurity practitioners to enhance youth cybersecurity education.

Session 2: AI and Cybersecurity Education

November 13th at 1:15 PM

Teaching Generative AI for Cybersecurity: A Project-Based Learning Approach

Nate Mathews, Christopher Schwartz, Matthew Wright

In the Spring 2024 semester, we introduced an elective course titled “Generative AI and Cybersecurity” for MS and upper-division BS students specializing in cybersecurity at our university. The course was designed to equip students with a foundational understanding of Generative AI, particularly large language models (LLMs) like GPT-4, and explore their applications within the field of cybersecurity. Through a combination of classroom instruction, hands-on projects, and industry guest lectures, students engaged with the technical, ethical, and legal dimensions of AI in cybersecurity. The course emphasized practical learning, with students gaining experience in AI tools such as ChatGPT, as well as developing skills in prompt engineering and API usage. While some students were eager for even more technical AI content, they appreciated the hands-on learning, insights from industry guest speakers, and the chance to see how the more powerful models like GPT-4 could be usefully applied to cybersecurity problems.

November 13th at 1:35 PM

Empowering the Next Generation: A Strategic Roadmap for AI in Cybersecurity Education

Vahid Heydari, Kofi Nyarko

The integration of artificial intelligence (AI) into cybersecurity is revolutionizing the approach to addressing increasingly complex cyber threats. As the demand for expertise in both AI and cybersecurity grows, Historically Black Colleges and Universities (HBCUs) have a unique opportunity to develop programs that equip students to meet these evolving challenges. This paper presents a strategic roadmap for the development of AI in Cybersecurity programs at HBCUs, highlighting interdisciplinary collaboration, hands-on learning, adversarial defense, explainability, ethical leadership, and diversity. Drawing on a comprehensive review of existing literature, this roadmap provides a flexible framework that can adapt to rapid technological advancements and the dynamic needs of the industry. By implementing this roadmap, HBCUs can create programs that not only provide students with the necessary technical skills but also cultivate the leadership, ethical understanding, and adversarial defense strategies required to shape the future landscape of cybersecurity.

November 13th at 2:15 PM - Virtual

AI-Cybersecurity Education Through Designing AI-based Cyberharassment Detection Lab

Ebuka Okpala, Nishant Vishwamitra, Keyan Guo, Song Liao, Long Cheng, Hongxin Hu, Xiaohong Yuan, Jeannette Wade, Sajad Khorsandroo

Cyberharassment is a critical, socially relevant cybersecurity problem because of the adverse effects it can have on targeted groups or individuals. While progress has been made in understanding cyberharassment, its detection, attacks on artificial intelligence (AI) based cyberharassment systems, and the social problems in cyberharassment detectors, little has been done in designing experiential learning educational materials that engage students in this emerging social cybersecurity in the era of AI. Experiential learning opportunities are usually provided through capstone projects and engineering design courses in STEM programs such as computer science. While capstone projects are an excellent example of experiential learning, given the interdisciplinary nature of this emerging social cybersecurity problem, it can be challenging to use them to engage non-computing students without prior knowledge of AI. Because of this, we were motivated to develop a hands-on lab platform that provided experiential learning experiences to non-computing students with little or no background knowledge in AI and discussed the lessons learned in developing this lab. In this lab used by social science students in institution A across two semesters (spring and fall) in 2022, students are given a detailed lab manual and are to complete a set of well-detailed tasks. Through this process, students learn AI concepts and the application of AI for

cyberharassment detection. Using pre-and post-surveys, we asked students to rate their knowledge or skills in AI and their understanding of the concepts learned. The results revealed that the students moderately understood the concepts of AI and cyberharassment.

November 13th at 2:50 PM - Virtual

Using AI Assistants in the Creation of an Academic Program of Study (PoS) in CyberAI

Paige Zaleppa, Siddharth Kaza, Blair Taylor

Artificial Intelligence (AI) is playing an increasingly vital role in cybersecurity. As AI becomes more prevalent, cybersecurity professionals need AI skills, and academic institutions need to provide students with the opportunities to gain them. To meet this demand, the NSA National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, in collaboration with the National Science Foundation (NSF), launched an initiative to outline the AI content cybersecurity academic programs need to teach their students. The initiative aims to build knowledge units (KUs) and recommend a Program of Study (PoS) in Cybersecurity and Artificial Intelligence (Cyber AI). This paper outlines the development of an AI assistant that was used to collaborate on the KU creation process for the CyberAI PoS. We will discuss the methodology behind the integration of the AI assistant, evaluate its contributions, and explore future directions for using AI assistants to develop curricular guidelines for academic programs.

Session 3: Privacy and Persuasion in Cybersecurity

November 14th at 10:15 AM

Efficient Machine Learning for Malware Detection

Thomas Koch, Tamirat Abegaz, Hyungbae Park

As the landscape of cyber threats continues to expand, malware detection has become increasingly crucial for maintaining robust cybersecurity. While standard malware detection techniques such as signature-based methods are very effective and widespread, they face certain challenges with zeroday and novel malware. The emergence of artificial intelligence in recent years has led to the development of alternative approaches to this issue, specifically through machine learning techniques. This research aims to analyze the effectiveness and viability of one such machine learning approach; the use of a Convolutional Neural Network (CNN) model for the classification of benign and malicious Windows executable binaries. To accomplish this, we gathered a substantial dataset of both benign and malicious Windows binaries and converted them into grayscale images to train several CNN models with slightly varying architecture for the classification task. Following the training of the models, they were evaluated on an unseen test dataset to compare label predictions against each other, as well as Windows Defender. This approach aims to achieve a definitive metric for determining the effectiveness of this type of malware detection for Windows-based antivirus applications. What we found is that certain CNN models are not only able to perform on par with Windows Defender, but in some cases even

outperform them. In conclusion, our study demonstrated that utilizing CNN models with grayscale image conversion of Windows binaries is an effective and efficient approach to malware detection.

November 14th at 10:35 AM

Teaching Secure Supply Chain Risk: Experiment in an 'Introduction to Cybersecurity' Course

Terry Downing-Harris, Siddharth Kaza, Blair Taylor, Yeong-Tae Song

The software supply chain and the security of software applications purchased through the Commercial-Off-The-Shelf (COTS) is becoming the focus of government and industry. Higher educational institutions can help by teaching secure supply chain risk management (SCRM), which can help secure COTS software applications. This work presents the results of an experiment that integrated secure SCRM into the software engineering curriculum at Towson University (a diverse, comprehensive institution with a large computer science program). This integration focuses primarily on using the US National Institute of Standards and Technology (NIST) standards to secure COTS software applications effectively. With a focus on undergraduate education, learning modules used in this integration are designed to be injected into almost any course in software engineering curriculum. The overall goal is to provide a model that can be replicated by all universities for integrating secure SCRM into the software engineering curriculum.

November 14th at 11:15 AM - Virtual

Persuasion and Phishing: Analysing the Interplay of Persuasion Tactics in Cyber Threats

Kalam Khadka

This study extends the research of Ferreira and Teles (2019), who synthesized works by Cialdini (2007), Gragg (2003), and Stajano and Wilson (2011) to propose a unique list of persuasion principles in social engineering. While Ferreira and Teles focused on email subject lines, this research analyzed entire email contents to identify principles of human persuasion in phishing emails. This study also examined the goals and targets of phishing emails, providing a novel contribution to the field. Applying these findings to the ontological model by Mouton et al. (2014) reveals that when social engineers use email for phishing, individuals are the primary targets. The goals are typically unauthorized access, followed by financial gain and service disruption, with Distraction as the most commonly used compliance principle. This research highlights the importance of understanding human persuasion in technology-mediated interactions to develop methods for detecting and preventing phishing emails before they reach users. Despite previous identification of luring elements in phishing emails, empirical findings have been inconsistent. For example, Akbar (2014) found 'authority' and 'scarcity' most common, while Ferreira et al. (2015) identified 'liking' and 'similarity.' In this study, 'Distraction' was most frequently used, followed by 'Deception,' 'Integrity,' and 'Authority.' This paper offers additional insights into phishing email tactics and suggests future solutions should leverage socio-technical principles. Future work will apply this methodology to

other social engineering techniques beyond phishing emails, using the ontological model to further inform the research community.

November 14th at 11:35 AM - Virtual

Reframing Cyber Security for the Next Generation of Digital Activists

Elizabeth A. Quaglia, Joseph Reddington

This paper presents a novel short course on cyber security designed for secondary school students in the UK. Our approach uniquely frames cyber security within the context of social activism and change-making, aiming to broaden participation and break down entry barriers in the field. The course contextualizes standard cyber security concepts such as information management, privacy, threat modeling, and cryptography within scenarios relevant to young activists.

We developed comprehensive lesson plans, interactive activities, and tools like “Change Cards” to facilitate engagement. The course was tested in two educational settings, leading to insights about content delivery and student engagement. Key outcomes include a teacher's guide and professionally designed resources that have been downloaded by over 1,000 teachers worldwide.

Feedback from students and teachers has been overwhelmingly positive, highlighting the course's relevance to daily life and its effectiveness in improving understanding of security concepts. This project contributes to the field by offering an innovative approach to cyber security education that resonates with young people's desire for social change, potentially fostering a new generation of diverse cyber security advocates and professionals.

Session 4: Cybersecurity Applications in Professional and Occupational Settings

November 14th at 10:15 AM

What Does An OT Security Professional Need To Know?

Sean McBride, Glenn Merrell

Industrial Cybersecurity is an emerging interdisciplinary field of study and practice. This paper presents the results of research and collaboration to create a data-supported and consensus-based curricular guidance document describing the knowledge needed of professionals in the field.

November 14th at 10:35 AM

Virtual Gamification in a PBS-based SETA Program

Krista Stacey, Jeff Landry

The severity of the insider threat has been emphasized in Information security literature. Self-efficacy and Protection motivation are factors that can increase an insider's compliance. Self-efficacy can be addressed by implementing a Security education training and awareness (SETA) program, but the programs do not usually address increasing Protection motivation. This paper approaches SETA programs from an educational perspective by implementing Positive behavior

support (PBS) pedagogy in order to increase one's sense of belonging and Protection motivation. As a PBS- friendly methodology, gamification, is considered as a basis for implementing training scenarios that increases Self-efficacy and Protection motivation. In addition, immersion provided by virtualization of the scenarios further increases both Protection motivation and Self-efficacy. Defense of this pedagogy and methodology is presented as a nomological model to be tested in future studies.

November 14th at 10:55 AM - Hybrid

Positioning Cybersecurity as a Pillar of Safety in Occupational Therapy

Heather Bednarz, Jane Blanken-Webb

The rapid digitalization of society has transformed occupational therapy practice, introducing both opportunities and challenges. As occupational therapists increasingly rely on electronic documentation, telehealth, and assistive technologies, cybersecurity is emerging as a critical concern. This position paper argues that occupational therapy is a vital domain for the integration of cybersecurity education, emphasizing the need to safeguard sensitive patient information, enhance digital literacy, and address the unique vulnerabilities faced by occupational therapy clients. The paper outlines the key intersections of occupational therapy and cybersecurity education, highlighting the impact of cyber threats on healthcare, the importance of digital literacy, and the role of occupational therapy in educating and protecting vulnerable populations. Recommendations are provided for integrating cybersecurity education into occupational therapy curricula to better prepare practitioners for the evolving digital landscape. By integrating cyber safety principles into occupational therapy education, the field can fulfill its mission of enhancing individuals' participation in meaningful activities by equipping practitioners with the skills necessary to protect patient data, manage digital risks, and ensure safe, effective care in a technology-driven world.

November 14th at 11:35 AM - Virtual

Educating the Next Generation of Ethical AI Practitioners

Noah Kenney, Annie Antón

Artificial intelligence (AI) technologies are rapidly advancing, increasing concerns about data privacy harms in AI models. To this end, we examine how ethical AI can be incorporated into computer science curricula. This paper describes the design process for the first ‘AI Privacy Engineering' course, to the best of our knowledge, taught in the United States. The course is designed for both undergraduate and graduate students at the Georgia Institute of Technology. Throughout this course, students examine ethical implications of AI system design, development, deployment, and utilization. Recognizing that data privacy represents only one possible form of harm, the course blends theoretical and conceptual lectures with hands-on projects that require students to address ethical issues, including bias, fairness, and accountability in AI systems. Herein, we discuss the course design process, including selecting the appropriate body of knowledge, establishing learning objectives, creating assignments, and considering pedagogical methodologies we employed. We explain the empirical methods used to inform our design,

including a systematic review of courses teaching AI development at over 40 universities. Additionally, we introduce a structured curriculum that can be used to effectively teach ethical and safe AI, and we propose how these topics may be incorporated more broadly into computer science courses. Finally, we discuss the early successes of the course, and the challenges faced while teaching it, particularly in maintaining relevance despite fast-paced changes in the field of AI, an evolving legislative landscape, accessing computational systems to run AI models, and varying levels of student preparedness.

Session 5: Innovations in Cybersecurity Labs and Practical Applications

November 14th at 1:15 PM

Multidisciplinary Quantum Cybersecurity Research for the Undergraduate Laboratory

Brian Callahan, Keenan Schilp, Quinn Colognato, Emily Goldman, Shoshana Sugerman, Aanya Mehta, Angela Imanuel, Kaitlin Kaii, Hannah Rose

Quantum computing has a critical need to be integrated into the undergraduate classroom to meet the needs of cybersecurity education in the 21st Century and to prepare a robust quantum workforce. A cybersecurity laboratory that specializes in undergraduate research explored a pair of quantum security projects in order to develop the foundations of a rich pedagogy to realize these needs: one on cracking pseudo-RSA, and one on understanding the limitations of quantum machine learning in aiding LLM development and refinement. This paper explores why this integration is necessary, explicates the research projects undertaken by these undergraduate researchers, and discusses their contributions to applied quantum security. Our contribution is to provide a template for how to quickly and effectively establish a multidisciplinary quantum security pedagogy for undergraduate students, provide example projects that can be adapted to student interests and abilities, and demonstrate how to enroll students from a wide variety of disciplines, increasing diversity and resiliency in quantum cybersecurity and cybersecurity broadly.

November 14th at 1:35 PM

Cybersecurity Threats and Mitigation Strategies in AI Applications

M. Sajjad Bhuiyan, Joon S. Park

The integration of artificial intelligence (AI) into daily life and critical infrastructure has elevated the importance of addressing cybersecurity concerns within AI applications. While AI systems offer numerous benefits, such as enhanced efficiency, automation, and decision-making, they also introduce novel vulnerabilities and threats. Ensuring the security and reliability of these systems is crucial. This paper investigates key cybersecurity challenges associated with AI, including data privacy, integrity, adversarial attacks, and the ethical implications of AI in security. Additionally, it examines the role of Shapley Additive explainable AI in promoting transparency, allowing for greater interpretability of AI models and insights into decision making processes.

November 14th at 1:55 PM

An Improved Phase Coding Audio Steganography Algorithm

Guang Yang

As AI technology continues to advance, voice cloning is becoming increasingly easy. Recently, cases of fraud involving audio forgery using AI technology have emerged, making it particularly important to covertly embed information and verify the authenticity and integrity of audio. Digital Audio Watermarking has thus become a crucial tool in this context. This study proposes an improved Phase Coding audio steganography algorithm that dynamically segments the audio signal and embeds information into the phase components of the mid-frequency range. This approach not only enhances the algorithm's resistance to steganalysis but also simplifies the computational process, ensuring the authenticity and integrity of audio both efficiently and securely.

November 14th at 2:15 PM - Virtual

A Cyber Bridge Experiment

Mary Ann Hoppa

This paper describes the design, implementation and first delivery of a no-cost, no-credit, multi-week virtual bootcamp called Cyber Bridge. The motivation underlying Cyber Bridge is to cast a wider recruitment net by easing the transition of students – especially those from non-technical academic preparations – into cybersecurity studies, particularly at the graduate level. It provides background insights regarding the inception and evolution of the Cyber Bridge project, experimental methodologies and observations, and findings based on analysis of collected metrics and feedback. Results support the view that a Cyber Bridge is a reasonable approach to: increasing students' comfort level regarding virtual learning environments; introducing and reviewing some cybersecurity foundations; connecting students to additional resources to improve upcoming academic experiences; and moderating their confidence by recognizing knowledge gap areas they may need to review or remediate. Future direction ideas and recommendations are shared that align with a longer-term vision to mobilize this capability to empower more underrepresented, underserved individuals to succeed as cybersecurity professionals and researchers.

November 14th at 2:35 PM - Virtual

Practical Teaching of Digital Forensic Analysis Using Group Dynamics Techniques: Think like a hacker and think like a investigator

Ivo Rosa

Cybersecurity is one of the most dynamic and challenging fields today, with digital threats constantly evolving. Digital forensic analysis is a sub-area of forensic science applied to the specific case of digital media and components, with the aim of reporting, explaining and justifying a series of events that take place in a digital context. As a sub-family of the forensic sciences, digital forensic analysis has a set of very specific methods, techniques and procedures to ensure that they are not questionable or that the evidence is invalidated. To prepare future information security professionals, it is essential to provide hands-on education that goes beyond theory and offers practical opportunities for

applying knowledge. This article reports on an innovative technical-practical experience in teaching digital forensics applied to cybersecurity. The methodology involves the creation of challenging attack scenarios, forensic image analysis, and the promotion of collaboration among students. This article reports on the methodology and results of the technique developed for teaching the subject of digital forensic analysis used in the university course held at ISTEC - Instituto Superior de Tecnologias Avançadas in Portugal (Lisbon). By adopting this approach, students gain valuable practical skills and prepare themselves to face real-world cyber threats.

Session 6: Privacy and Persuasion & AI and Cybersecurity Education

November 14th at 1:35 PM - Virtual

Enhancing AI-Centered Social Cybersecurity Education through Learning Platform Design

Nishant Vishwamitra, Ebuka Okpala, Song Liao, Keyan Guo, Sandeep Shah, Hongxin Hu, Xiaohong Yuan, Long Cheng

Artificial Intelligence (AI) technologies have become increasingly pervasive in our daily lives. Recent breakthroughs such as large language models (LLMs) are being increasingly used globally to enhance their work methods and boost productivity. However, the advent of these technologies has also brought forth new challenges in the critical area of social cybersecurity. While AI has broadened new frontiers in addressing social issues, such as cyberharassment and cyberbullying, it has also worsened existing social issues such as the generation of hateful content, bias, and demographic prejudices. Although the interplay between AI and social cybersecurity has gained much attention from the research community, very few educational materials have been designed to engage students by integrating AI and socially relevant cybersecurity through an interdisciplinary approach. In this paper, we present our newly designed open-learning platform, which can be used to meet the ever-increasing demand for advanced training in the intersection of AI and social cybersecurity. The designed platform, which consists of hands-on labs and education materials, incorporates the latest research results in AI-based social cybersecurity, such as cyberharassment detection, AI bias and prejudice, and adversarial attacks on AIpowered systems, are implemented using Jupyter Notebook, an open-source interactive computing platform for effective hands-on learning. Through a user study of 201 students from two universities, we demonstrate that students have a better understanding of AI-based social cybersecurity issues and mitigation after doing the labs, and they are enthusiastic about learning to use AI algorithms in addressing social cybersecurity challenges for social good.

November 14th at 1:55 PM - Virtual

Building a Cybersecurity and AI Integrated Learning Pathway for Criminal Justice Professionals

Yan Bai, Juan Li

With support from the National Science Foundation, we have developed scenario-based security curriculum and online showcase labs with interactive simulations and case studies across three progressive courses, revolutionizing cybersecurity education for Criminal Justice (CJ) professionals. By incorporating

artificial intelligence into the curriculum, this project enhances CJ professionals' capabilities. Our goal is to develop a skilled workforce of CJ professionals with cybersecurity and privacy knowledge, addressing the critical need for such cybersecurity expertise in CJ. Literature review, focus group survey results, course framework tailored for CJ professionals, example course modules, and implementation results are presented.

November 15th at 9:15 AM

A Zero Trust Module for Cybersecurity Education

Xinli Wang, Vijay Bhuse, Yuan Cheng

Zero Trust (ZT) is a conceptual and architectural framework for cybersecurity teams to design networks into secure micro-perimeters and strengthen data security with dynamic and context-aware policies by systematically integrating state-of-the-art technology, risk management, and threat intelligence. Both theoretical analysis and industrial practice have shown that ZT can ensure that organizations are not victims of known attacks or fail to discover a breach for a long time. ZT has recently gained momentum in industry to defend against lateral movement of malicious actors in today's borderless networks. The United States 2021 President Executive Order requires the federal government must adopt security best practice and advance toward a Zero Trust Architecture (ZTA). However, it is not a trivial task to implement a ZTA due to its novelty and complexity. We need to understand what ZT or ZTA is to take full advantage of it. Therefore, there is a need to introduce the fundamental concepts, principles, and architectures of ZT in cybersecurity courses at a college to better prepare our new cybersecurity professionals for their careers.

In the last few years, we have developed a module and used it to introduce ZT in cybersecurity courses at senior undergraduate and graduate levels. Students' feedback is positive. This module includes an introduction to ZT and its principles, design issues in the traditional model of perimeter-based network security, zero trust architectures, security benefits of ZT, technical challenges to implement a ZTA, and the main threats to ZT networks. This article provides an overview of this module. We will also share the experience and lessons we have learned in our teaching practice. Our work will provide a good reference for those who teach cybersecurity courses at a college or university, or are developing a cybersecurity curriculum. It will also help busy professors develop or revise a zero trust module for their cybersecurity courses.