Wednesday, November 1st

10:15 AM - CCERP

Towards Assessing Cybersecurity Posture of Manufacturing Companies: Review and Recommendations

John Del Vecchio , Yair Levy, Ling Wang, Ajoy Kumar

With the continued changes in the way businesses work, cyber-attack targets are in a constant state of flux between organizations, individuals, as well as various aspects of the supply chain of interconnected goods and services. As one of the 16 critical infrastructure sectors, the manufacturing sector is known for complex integrated Information Systems (ISs) that are incorporated heavily into production operations. Many of these ISs are procured and supported by third parties, also referred to as interconnected entities in the supply chain. Disruptions to manufacturing companies would not only have significant financial losses but would also have economic and safety impacts on society. The vulnerabilities of interconnected companies created inherited exploitations in other interconnected companies. Cybersecurity practices need to be further enhanced to understand supply chain cybersecurity posture and manage the risks from lower-tier interconnected entities up to the top-level dependent organization. This paper will provide an overview of the Theory of Cybersecurity Footprint to emphasize the relationship among interconnected entities and the cybersecurity effects one organization can have on another regardless of size. This paper provides a literature review on the manufacturing industry with a recommendation for future developmental research using the Delphi method with a panel of experts to develop an index to measure cybersecurity posture based on interconnected entities from lower tiers and establish index weights specifically for the manufacturing industry.

10:35 AM - CCERP

Quantum Computing: Computing of the Future Made Reality

Janelle Mathis

Quantum computing is an emerging new area focused on technology consisting of quantum theory aspects such as electrons, sub-atomic particles, and other materials engineered using quantum mechanics. Through quantum mechanics, these computers can solve problems that classical computers deem too complex. Today the closest computing technology compared to quantum computers are supercomputers, but similarly to classical computers, supercomputers also have faults. With supercomputers, when a problem is deemed too complex, it is due to the classical machinery components within the computer, thus causing a halt in solving the task or problem. In contrast, these problems could be solved with a quantum computer due to the advancements in engineered materials based on quantum mechanics. Apart from the hardware that enables a quantum computer to function more intelligently, the software developed for these computers can also show tremendous improvements in certain aspects, such as cryptography. This research examines quantum computing from its origins and details how the computer runs, its faults and limitations, ways to protect from quantum computing attacks, and demonstrates what programming a quantum computer would entail.

10:55 AM - CCERP

RFID Key Fobs in Vehicles: Unmasking Vulnerabilities & Strengthening Security

Devon Magda, Bryson R. Payne

In modern vehicles, radio frequency identification (RFID) key fobs, a form of remote keyless entry (RKE), play a pivotal role in vehicular security and functionality. The goal of this research is to implement and demonstrate radio-based cyberphysical attacks against identified

vulnerabilities associated with RFID key fobs and provide insights on how to fortify security precautions against such attacks. Furthermore, this research reviews and acknowledges pre-existing security features that have been implemented to prevent the recurrence of these vulnerabilities. An additional goal of this research is to discover the security disparity between RFID tags and readers from vehicles manufactured in the early 2000s and vehicles from the mid-2010s or later.

11:15 AM - CCERP

The Impact of Individual Techno-characteristics on Information Privacy Concerns in the Diffusion of Mobile Contact Tracing

Jiesen Lin, Dapeng Liu, Lemuria Carter

In the wake of the global health crisis, mobile contact tracing applications have emerged as important tools in managing disease spread. However, their effectiveness heavily relies on mass adoption, significantly influenced by the public's information privacy concerns. To date, systematic examination of how these privacy concerns relate to the innovation adopter categories in mobile contact tracing remains sparse. Furthermore, the influence of individual techno-characteristics on these concerns is to be explored. This research seeks to fill these gaps. Drawing on the diffusion of innovation theory, we examine the impact of the key techno-characteristics—adopter category, propensity for identification misrepresentation, and exposure to media reports of privacy invasion incidents - on information privacy concerns in the diffusion of mobile contact tracing applications. We aim to investigate how these factors in culmination shape privacy concerns. Our findings offer insights to devise more effective strategies for managing privacy concerns. This research expands the current academic discourse around technology adoption and privacy and has practical implications for the design and rollout of mobile contact tracing applications.

11:35 AM - CCERP

Exploring Information Privacy Concerns During the COVID-19 Pandemic: A Juxtaposition of Three Models

Dapeng Liu, Lemuria Carter, Jiesen Lin

Government agencies across the globe utilize mobile applications to interact with constituents. In response to the global pandemic, several nations have employed contact tracing services to manage the spread of COVID-19. Extent literature includes various models that explore information privacy. Several researchers have highlighted the need to compare the effectiveness of diverse information privacy models. To fill this gap, we explore the impact of information privacy concerns on citizens' willingness to download a federal contact tracing app. In particular, we compare three types of prevalent information privacy concerns: global information privacy concerns (GIPC), concern for information privacy (CFIP), and internet users' information privacy concerns (IUIPC). The results of an online survey administered to 209 citizens reveal that in all models trusting beliefs increase adoption intentions while risk decreases them. However, IUIPC is the only privacy construct that significantly reduces trusting beliefs.

1:40 PM - CISSE

Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students

Lowri Williams, Eirini Anthi, Yulia Cherdantseva, Amir Javed

This paper investigates the use of gamification and game-based learning in the field of cybersecurity education. Due to their technical complexity and lack of coherence, traditional pedagogical methods, such as lectures, may fail to engage and inspire students

especially from non-cyber backgrounds. To address this issue, we devised two distinct cybersecurity frameworks/games based on traditional Capture The Flag (CTF) competitions; an open-ended CTF event and a story-based CTF. Such games have demonstrated potential across multiple disciplines, including computer science, physics, mathematics, and engineering, as well as across multiple levels of study including undergraduate and postgraduate students. The positive feedback and significant increase in the interest to pursue a postgraduate course in cybersecurity, especially among non-cybersecurity students, attest to the success of this gamification strategy. As such, this paper provides valuable insights for enhancing the attractiveness and efficacy of cybersecurity education, thereby encouraging a broader spectrum of non-technical and non-cybersecurity students to pursue this crucial field.

2:00 PM - CISSE

What Is Interesting and Relevant About Cybersecurity?: NLP Analysis of a Survey of CS Students

Cheryl Resch, Jinnie Shin, Christina Gardner-McCune

Cyber attacks are a common feature of current news and many of them are the result of easy to avoid vulnerabilities in software. It is imperative that students graduating from an undergraduate Computer Science (CS) curriculum understand the consequences of vulnerable code. When developing lessons and assignments, it would be useful to have a sense of students' attitude toward cybersecurity and appreciation of the need to write secure code. This paper describes an analysis of the results of a survey of students in core CS courses at our large public university, in which students answer free response questions about what they find interesting and relevant about cybersecurity. The survey was conducted in Fall 2022 and repeated in Spring 2023 after cybersecurity interventions were introduced into several core CS courses. We performed a Natural Language Processing (NLP) analysis of the free response answers to determine the overarching themes in the responses. We found that the most prevalent topics students are interested in are cryptography and penetration testing, and did not change over the two semesters. In answer to the question about the relevance of studying cybersecurity, we found that as students progress through the curriculum, what students find relevant moves from protecting their personal data to its importance in job duties and writing secure programs. When developing lessons and assignments, it may be helpful to introduce cryptography or penetration testing to engage students. Also, students should be taught early and often about the relevance of cybersecurity in their future job duties.

2:20 PM - CISSE

Impact of a Cybersecurity Work-Related Course on Students' Career Thoughts and Attitudes: A PISCES Course Evaluation

Marcia Combs, Randall Joyce, Cain Bynum

This article proposes a research study conducted at Murray State University Cybersecurity and Network Management program to investigate the impact of work-related experiential learning on college students' career thoughts and attitudes within the context of cybersecurity career development. The Cybersecurity and Network Management program introduced the CNM 518 course based on the Public Infrastructure Security Cyber Education System (PISCES) project that offers practical, hands-on experiences. The proposed research project slated for Spring 2024, aims to assess how this work-related experiential learning influences students' career thoughts and attitudes, using the Career Thoughts Inventory as a measurement tool. This research project emphasizes the importance of reflective learning within CNM 518 and aims to contribute empirical evidence on the impact of work-related experiential learning on students' career thoughts and how such learning experiences positively

influence the career decision-making processes and, subsequently, the broader field of cybersecurity education.

2:40 PM - CISSE

Assessing Common Software Vulnerabilities in Undergraduate Computer Science Assignments

Andrew Sanders, Gursimran Singh Walia, Andrew Allen

As the demand for secure coding education grows, there is a need for improvements in how secure coding is taught and in preparing students to develop more secure software. As time in a Computer Science classroom is finite, educational efforts should be placed on targeting the most common types of vulnerabilities to better prepare students to avoid common security pitfalls in coding. Existing research in this area mainly focuses on developing vulnerability detection tools rather than analyzing the types of commonly produced vulnerabilities by students. Limited research exists in determining common student-produced vulnerabilities, and the available studies differ from the types of vulnerabilities that are researched in vulnerability detection literature. Our research works to further establish the types of vulnerabilities produced by students by using a static analysis tool on assignment code submissions in an undergraduate Programming II (CS2) course. We present our findings on what types of vulnerabilities are commonly produced by students and contrast them with what is commonly researched in the literature. We find there is little overlap between the vulnerability types reported by our study and other studies in the research area. This research has potential implications for secure coding education in a Computer Science curriculum. Further work should be done to establish the contexts in which specific vulnerability types are more likely to be produced and how to best teach students to avoid producing these vulnerabilities.

3:15 PM - CISSE

The Design and Development of Hands-on Activities for Digital Forensics Education

Xinli Wang, Vijay Bhuse, Sara Sutton

It has been widely admitted by researchers and educators that hands-on activities are a core component in digital forensics education to help students gain practical skills that are needed in real-world forensic investigations. However, it is not clear in existing works about what kinds of hands-on activities are recommended to be integrated into a digital forensics course and how to design and develop them. In our teaching practice, hands-on activities for a digital forensics course are designed in three categories: 1) activities that assist students in learning how to use common digital forensics tools; 2) activities that help students gain in-depth understanding of the basic concepts and fundamental knowledge that are presented in class lectures; 3) activities that promote students the development of mindsets and data analytical skills that are needed for a digital forensic investigator. Various formats are employed to develop these hands-on exercises in different categories. The educational objectives and student learning outcomes map well to the CAE-CD (Centers of Academic Excellence - Cyber Defense) outcomes by completing their forensic knowledge units. In this paper, we share our idea and experience to design and implement such hands-on assignments in each category for meeting specific educational objectives. Sample exercises are briefly described to explain our idea in each category. Open source tools and data sets are introduced for references. Experiences, lessons, and sample feedback from students are discussed. Our results will provide a point of reference for those who teach digital forensics courses at a college or university, or are developing a digital forensic curriculum.

3:35 PM - CISSE

Develop and Disseminate Hands-on Lab Materials of Privacy Concepts and Technologies to Educators

Na Li, Lin Li, Mengjun Xie, Bugrahan Yalvac

In the era of digitalization, massive amount of data has been generated from people's online activities or use of portable/wearable devices. The data often carries rich information about people. Therefore, privacy technologies are needed, from data generation to usage and from transmission to storage, to protect people's sensitive information. Although the research community is making great progress in addressing advanced privacy protection technologies, very few educational materials have been developed to incorporate the latest research results and engage students in learning privacy technologies, especially for younger generations. In this paper, we present our newly designed educational materials on privacy technologies, which can be used for training high quality cybersecurity professionals to meet the ever-increasing demand. The developed learning modules not only incorporate the latest research results in privacy technologies but also include effective hand-on lab activities. To help other institutions effectively teach privacy technologies, we organized a faculty training workshop in summer 2022. Twenty-nine faculty from twenty institutions nationwide participated in the training. Survey results show that the participants gained a better understanding of privacy issues and demonstrated strong interest in teaching privacy technologies after attending the workshop.

3:55 PM - CISSE

Creating a Practical Education in Space Cybersecurity Through Antenna Design and Implementation

Clark Duncan, Randall Joyce, Spencer Bugg, Jason Marquardt, Marcia Combs

With the increasing concerns over cybersecurity and space systems preparing the next generation of cybersecurity professionals is critical. In this research, undergraduate and graduate students were exposed to cybersecurity and space systems through practical antenna design and implementation in hopes of capturing pirate communication signals while in the Western Kentucky area. Students designed and built turnstile and helical antennas that focused on the 255 MHz and 318 MHz frequencies that interfaced with software-defined radios. With these systems, students were able to capture a limited range of low earth orbiting (LEO) satellite communications while ascertaining an understanding of satellite communication fundamentals. Overall, students were able to gain an understanding of antenna design, the importance of radio frequency, and satellite communications.

4:15 PM - CISSE

Immersive Learning: Understanding the Psychology of Crime Using Virtual Reality

Denise Ferebee, Jerome Blakemore, Zina Parker, Marcus Kelly, Michael Zhou, Tyana White, Farheen Dahani, Jiya Webster

Teaching cybersecurity professionals has changed from applying puzzle-based learning scenarios, general tabletops, and general gamification to an immersive learning environment. In today's teaching environment, there are known methods to teach cybersecurity tool techniques. However, beyond the technical aspect, cybersecurity professional need to understand the psychology of crime. These teaching and learning needs have become more prevalent in criminal justice,

education, and computer science degree programs and aspects of job professions because learners need to understand and be able to recognize why crimes are committed. Thus, opening another major area of research in cybersecurity. Teaching someone what it means to protect systems, networks, and programs from digital attacks is difficult. Each person needs some frame of reference. Through their personal frame of reference, they discern and consume the information and find a basis for its purpose. This is known as the learning process and each individual journey is different. The learning process is affected by personal experience. Thus, creating a climate for misunderstanding through applying personal experiences to a situation that may have had a different personal or professional interaction. Because of misunderstandings and unconscious bias that occur in this type of learning structure, the misunderstandings and unconscious bias have the potentiality of being propagated into professional career interactions and investigations. Thus, this project will present a learning platform/framework to explore cybersecurity methods, discern interactions, explore the psychology of why a crime is committed through a collaborative virtual reality (VR) immersive environment.

Thursday, November 2nd

3:15 PM - CISSE

Assessing the Effectiveness and Security Implications of AI Code Generators

Maryam Taeb, Hongmei Chi, Shonda Bernadin

Students, especially those outside the field of cybersecurity, are increasingly turning to Large Language Model (LLM)-based generative AI tools for coding assistance. These AI code generators provide valuable support to developers by generating code based on provided input and instructions. However, the quality and accuracy of the generated code can vary, depending on factors such as task complexity, the clarity of instructions, and the model's familiarity with the programming language. Additionally, these generated codes may inadvertently utilize vulnerable built-in functions, potentially leading to source code vulnerabilities and exploits. This research undertakes an in-depth analysis and comparison of code generation, code completion, and security suggestions offered by prominent AI models, including OpenAI CodeX, CodeBert, and ChatGPT. The research aims to evaluate the effectiveness and security aspects of these tools in terms of their code generation, code completion capabilities, and their ability to enhance security. This analysis serves as a valuable resource for developers, enabling them to proactively avoid introducing security vulnerabilities in their projects. By doing so, developers can significantly reduce the need for extensive revisions and resource allocation, whether in the short or long term.

3:35 PM - CISSE

Evaluation of AI Models to Update Cybersecurity Curriculum

Chizoba Ubah, Paige Zaleppa, Blair Taylor, Siddharth Kaza

This study explores the performance of several Large Language Models (LLMs) across different facets of Cybersecurity Modules. Using prompt engineering, this work evaluates publicly available LLMs for their ability to assess the suitability of secure coding topics based on learning outcomes, categorize these topics following OWASP standards, and generate up-to-date examples for curriculum use. The findings would highlight the transformative role that LLMs would play for future advancements in Cybersecurity education.

3:55 PM - CISSE

An Analysis of Prerequisites for Artificial Intelligence / Machine Learning-Assisted Malware Analysis Learning Modules

Portia Pusey, Mahmoud Abdelsalam, Maanak Gupta, Sudip Mittal

This paper presents the findings of action research conducted to evaluate new modules created to teach learners how to apply machine learning (ML) and artificial intelligence (AI) techniques to malware data sets. The trend in the data suggest that learners with cybersecurity competencies may be better prepared to complete the AI/ML modules' exercises than learners with AI/ML competencies. We describe the challenge of identifying prerequisites that could be used to determine learner readiness, report our findings, and conclude with the implications for instructional design and teaching practice.

Friday, November 3rd

9:25 AM - CISSE

An Exploration of Factors Influencing Oversharing on Facebook Groups

Marc Dupuis, Breanna Powell, Margaret Lanphere, Manuel Duarte, Billy Hao

Social media usage is extremely prevalent and so is the oversharing of personal information online. This paper aims to examine the factors that influence information disclosure on Facebook and how participation in groups may affect sharing behaviors. Groups can provide a more intimate and supportive environment, which may lead to excessive information sharing. An online survey was conducted on Amazon's Mechanical Turk platform with 373 accepted responses from self-reported Facebook users. The data was analyzed to determine which demographic and personality factors are correlated with oversharing behaviors on user profiles and within Facebook groups. This work has implications for understanding how individuals seek support online and what information they feel comfortable disclosing. Oversharing may increase user feelings of social support but also may make users vulnerable to cyberbullying and social engineering attacks.

9:45 PM - CISSE

Addressing the Need for Interculturality in Cybersecurity Education

Stephanie Swartz, Deveeshree Nayak

This paper addresses the need for incorporating global virtual team (GVT) projects into cybersecurity education curricula in an effort to develop students' understanding of different cultures and hone their abilities to work across multiple time zones, communicate using digital communication platforms as well as improve their virtual project and time management skills. An example of a GVTs project, Virtual Business Professional, is presented in order to illustrate how collaborative online international learning (COIL) can be embedded into IT-related coursework. It is the authors' intention to encourage instructors and administrators at institutions of higher learning to support and carry out transdisciplinary GVT projects in order to best prepare graduates for the challenges of the 21st century global workplace.

9:45 PM - CISSE

Transforming Cyber Education thru Open to All Accessible Pathways

Sin Ming Loo, Elizabeth Khan, Eleanor Taylor, Char Sample

Boise State University's (BSU) Cyber Operations and Resilience CORe program was intentionally designed so that any student, especially non-traditional and non-technical students, with an interest in cybersecurity could have an education and training pathway to enter

the cyber workforce. The CORe curriculum focuses on teaching students how to design, apply, and improve cybersecurity through the interaction of people, processes, and technology. CORe is a stackable curriculum with elective credit hours and options for various academic and industry certificates and certifications that enable students to customize their unique career pathway. The CORe program guides students to think about the system being managed, the risks presented, and the dynamic intersection of system elements when considering how to incorporate resilience frameworks in achieving a resilient system. By developing systems thinking, the students gain an understanding of the interdependencies interacting with the operational system. The CORe program encourages students to integrate cybersecurity knowledge with models and frameworks found in other academic disciplines through a unifying systems approach. CORe is designed around the realities of today's broad cyber landscape: that breaches will occur in any system over time and proactive design of resilience into systems to detect, respond, and recover in a timely and orderly manner is critical. Students are taught to think holistically about cybersecurity focusing on all system elements. CORe is not a traditional cybersecurity degree. CORe is distinguished by the non-traditional engineering, computer science approach to cybersecurity education with the singular focus on infusing resilience operations and transdisciplinary systems thinking principles throughout the curriculum.