November 14, 2022

26th Colloquium - Pedagogy for Cybersecurity

The 2022 conference of the Colloquium on Information Systems Security Education (CISSE) celebrates its 26th year as the senior and premier conference on Cybersecurity Education. Participating in the Colloquium are representatives from education, industry, and government with an interest in conducting productive conversations, present new ideas, and improve the content and curricula for cybersecurity education.

The following are joint CISSE and CCERP papers (in alphabetical order) presented at the 26th Colloquium.

A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education

CCERP

Sherri Weitl-Harms, Adam Spanier, John Hastings, Matthew Rokusek

Gamification in education presents a number of benefits that can theoretically facilitate higher engagement and motivation among students when learning complex, technical concepts. As an innovative, high-potential educational tool, many educators and researchers are attempting to implement more effective gamification into undergraduate coursework. Cyber Security Operations (CSO) education is no exception. CSO education traditionally requires comprehension of complex concepts requiring a high level of technical and abstract thinking. By properly applying gamification to complex CSO concepts, engagement in students should see an increase. While an increase is expected, no comprehensive study of CSO gamification applications (GA) has yet been undertaken to fully synthesize the use and outcomes of existing implementations. To better understand and explore gamification in CSO education, a deeper analysis of current gamification applications is needed. This research outlines and conducts a methodical, comprehensive literature review using the Systematic Mapping Study process to identify implemented and evaluated GAs in undergraduate CSO education. This research serves as both a comprehensive repository and synthesis of existing GAs in cybersecurity, and as a starting point for further CSO GA research. With such are view, future studies can be undertaken to better understand CSO GAs. A total of 74 papers were discovered which evaluated GAs undergraduate CSO education, through literature published between 2007 and June 2022. Some publications discussed multiple GAs, resulting in a total of 80 undergraduate CSO GAs listing at https://bit.ly/3S260GS. The study outlines each GA identified and provides a short overview of each GA. It also provides a summary of engagement-level characteristics currently exhibited in existing CSO education GAs and discusses common themes and findings discovered in the course of the study.

Addressing the Cybersecurity Issues and Needs of Rural Pennsylvania Nonprofit Organizations

CISSE

Brian Gardner, Maryam Roshanaei, J. Andrew Landmesser, Jennifer Breese, Michael Bartolacci

The need for Cybersecurity competence has become a strategic area for all types of organizations today, be it large or small, for profit or nonprofit. This is an area of particular concern for smaller nonprofit organizations; and especially for ones in rural areas with limited budgets and manpower to address their Cybersecurity issues and needs. Cyber-attacks, such as ransomware attacks, distributed denial of service attacks (DDoS), and phishing attacks wreak havoc on the networks and systems necessary for supporting the populace via services provided by nonprofits. The problems associated with the various types of hacks, be it from outside nefarious individuals/groups or careless internal personnel, are particularly difficult for nonprofits in rural communities with limited resources for Cybersecurity infrastructure and limited staff proficient in Cybersecurity knowledge and skills. We have developed a Cybersecurity assessment process that can be used to ascertain key needs and weaknesses with respect to Cybersecurity for nonprofits in such rural communities in Pennsylvania. Beyond identifying these needs and weaknesses, this grant-sponsored work-in-progress research aims to also provide some guidance to rural nonprofits with "best practices" and related content that can be easily implemented despite their small budgets and staff.

An Empirical Study of Password Policy Compliance

CISSE

Robert C. Hall, Mary Ann Hoppa, Yen-Hung Hu

Abstract - Cybersecurity exploits that take advantage of weak passwords continue to succeed in virtually every industry. This motivates interest in empirically determining the extent to which websites that invite visitors to create new user accounts on them encourage or require users to engage in better password management practices, including strong passwords. This project examined a statistically significant sample of websites to assess how closely they voluntarily adhere to the National Institute of Standards and Technology's authoritative guidance on password policies. Over 100 representative websites were selected from industries that consistently report the most breaches in the Verizon Data Breach Investigation Report. Their respective user account creation processes were assessed via a scorecard approach based on observations collected when following standardized experimental procedures. Scorecard data then were aggregated and analyzed for trends. The research findings highlight potential vulnerabilities that persist in online account password creation practices, leaving many websites susceptible to brute force attacks due to cyber hygiene lapses. Recommendations to help remediate compliance gaps and as paths forward to build upon this work include refining the proposed scorecard, creating and using standardized user registration and profile manager plugins, widely adopting user-friendly password management tools, and enacting tougher legal consequences for website hosts when breaches occur.

Authentication Based on Periocular Biometrics and Skin Tone

CCERP

Kennedy Marsh, Clifton Wallace, Jeffrey Hernandez, Rodney Dejournett, Xiaohong Yuan, Kaushik Roy

Face images with masks have a major effect on the identification and authentication of people with masks covering key facial features such as noses and mouths. In this paper, we propose to use periocular region and skin tone for authenticating users with masked faces. We first extract the periocular region of faces with masks, then detect the skin tone for each face. We then train models using machine learning algorithms Random Forest, XGBoost, and Decision Trees using skin tone information and perform classification on two datasets. Experiment results show these models had good performance.

BEACON Labs: Designing Hands-on Lab Modules with Adversarial Thinking for Cybersecurity Education

CISSE

Jordan Whyte, Gaby G. Dagher and Sara Hagenah

Cybersecurity is an interdisciplinary field that is concerned with protecting digital assets from cyber-attacks aiming to illegally access sensitive information in order to tamper and disrupt systems and processes. Producing cybersecurity materials that are vertically-aligned is highly desired, given the shortage of cybersecurity educators and the dynamic and evolving nature of cybersecurity. More specifically, universities must do more to help fill the huge cybersecurity workforce shortage and address the lack of materials centered around adversarial thinking. In this paper, we propose a four-step process to turn a recent cybersecurity paper into a hands-on lab that utilizes game theory to promote adversarial thinking and show a case study where this process was used. The four-step process explains how papers are chosen, their research replicated, the production of lab materials, and complementary materials for students to work from. The case study demonstrates this process in practice and explains how game theory is incorporated into the lab.

Bringing the Industry Partner to the Cybersecurity Education Table as an Active Participant

CISSE

Randy Hinrichs, Viatcheslav Popovsky, Barbara Endicott-Popovsky

The University of Washington (UW) published their pedagogical model for Cybersecurity Education - the KBP Model. In 2005, the National Center for Academic Excellence in Cybersecurity certified the status of NCAE-CR based on the tight pairing to the KUs (Knowledge Units). The KBP model aided in maintaining the quality of the instruction. The original KBP model goals are reviewed here and the changes to those goals are explained. The model provided a solid public - private partnership engagement model. Industry professionals from the field taught the NIST / NICE KSAs and provided real-time experience, contributing to the curriculum's resiliency. We modified our competency assessment from the WOWI to the CYBERGenius.IQ, integrated industry-based CERT material for scalability, and created a certified student collaboratory to manage continuing education post-graduation and into the job.

Cyber-physical Shooting Gallery: Gamification to Address the IT-OT Gap in Cybersecurity Education

CISSE

Tiffany Fuhrmann, Taegan Williams, Michael Haney

While much has been written on the dire need for workers who understand both the IT and OT core concepts necessary to protect the cyber-physical systems of critical infrastructure, practical and specific recommendations for how to meet this need through education and workforce training are lacking. Many of the available programs for teaching cybersecurity of physical systems rely on virtual simulations and students may not encounter relevant physical equipment until they are in the workplace. [Lab Name]'s Cyber-physical Shooting Gallery is a critical missing piece toward a comprehensive system to develop the competent workforce the nation needs. Through a series of cyber-physical capture-the-flag challenges that integrate the Purdue ICS Model with the MITRE ATT&CK framework, the Cyber-physical Shooting Gallery provides an accessible educational model for cyber-physical security education and training.

CyberAlumni a Cybersecurity Collaboratory

CISSE

Alejandro Ayala, Barbara Endicott-Popovsky and Randy Hinrichs

CyberAlumni is a case study of a new model for using peer to peer digital networks to harden cybersecurity education. The CyberAlumni organization was founded in 2021 with the goals of pursuing continuing education and collaborations with academia, industry, and government to bridge the gap between curriculum and job placement. This model serves to accelerate the professional development and acquisition of top-level cybersecurity talent while recursively bolstering cybersecurity curriculum in the process. All goals were achieved within one year, leading to further investigation of applying this model at scale in conjunction with courses offered through NSA Centers of Academic Excellence.

Cybercrime in the Developing World

CCERP

David A. Ghelerter, John E. Wilson, Noah L. Welch, John-David Rusk

This paper attempts to discover the reasons behind the increase in cybercrime in developing nations over the past two decades. It discusses many examples and cases of projects to increase internet access in developing countries and how they enabled cybercrime. This paper examines how nations, where many cybercrimes occurred, did not have the necessary resources or neglected to react appropriately. The other primary focus is how cybercrimes are not viewed the same as other crimes in many of these countries and how this perception allows cybercriminals to do as they please with no stigma from their neighbors. It concludes that laws and law enforcement, fund distribution, and ethics of these developing countries need to change to reduce the amount of cybercrime.

Election Security and Technology Education

CISSE

Garry White

Democracy is based on education according to Socrates (470-390 B.C.) A lack of education leads to election problems. The 2020 presidential election has raised questions of election fraud and rigged software and the integrity of the results. Such questions can be resolved through election technology & security education. Education can put you in a position of knowledge if you find yourself in a discussion on voter fraud. The purpose of this paper is to propose a curriculum for different courses on election security and election technology to educate people. Individuals' trust of an election can be impacted by education which may over-riding propaganda, and fake news. Proposed curriculum also covers misleading election numbers from statistics and Benford's Law.

Framing Gamification in Undergraduate Cybersecurity Education

CISSE

Sherri Weitl-Harms, Adam Spanier, John Hastings, Matthew Rokusek

Gamification presents potential benefits in courses that traditionally require the comprehension of complex concepts and a high level of technical and abstract thinking. Courses in Cyber Security Operations (CSO) undergraduate education meet these criterion. This research evaluates organizational constructs that have been applied to gamification applications (GAs) in CSO education. It utilizes framing theory and frame-reflective discourse analysis to outline frames based on engagement levels and analyzes the current distribution of GAs. The following organizational constructs for GAs in data structures and algorithms education apply to CSO education: Enhanced Examination (EE), Visualization of Abstract Ideas (VAI), Social and Collaborative Engagement (SGE), Dynamic Gamification (DG), and Collaborative Gamification Development (CGD). Three additional frames are identified: Missions and Quests (MQ), Simulations (Sim) and Aspirational Learning (AL). MQ GAs have process-driven quests, stories, and/or descriptive scenarios to augment engagement. Sim GAs use environmental immersion to demonstrate real world problem solving while allowing freedom of movement. AL GAs use goal-based designs like Capture The Flag (CTF) missions to enhance engagement. Twenty-seven existing CSO GAs fit within the MQ frame as CSO education lends itself well to these types of experiences. Seventeen CSO GAs fall within the AL GA frame, many of these manifesting as CTF missions. Seventeen CSO GAs fit in the EE Frame due to their optimization in the analysis of learning progress. Nine Sim GAs were successfully deployed in CSO education, followed by 4 VAI, 3 SGE, and 3 DG GAs.

Improving Workplace and Societal Cybersecurity via Post-Secondary General Education

CISSE

Maeve Dion

Everyone has a role to play in cybersecurity and cyber risk management, but people without security backgrounds seldom understand - let alone accept or endorse - such roles. Public and private organizations face common challenges in facilitating more secure behaviors among employees. As part of their missions, most colleges and universities in the United States have general education programs that aim to instill certain competencies and characteristics in all graduates (for individual and greater good). This paper proposes that a cybersecurity general education course could help improve common workplace challenges in cybersecurity training and awareness, and that such a course could align with each institution’s general education goals to benefit not only graduates but also communities and society writ large.

Interactive Cyber-Physical System Hacking: Engaging Students Early Using Scalextric

CISSE

Jonathan White, Phil Legg, Alan Mills

Cyber Security as an education discipline covers a variety of topics that can be challenging and complex for students who are new to the subject domain. With this in mind, it is crucial that new students are motivated by understanding both the technical aspects of computing and networking, and the real-world implications of compromising these systems. In this paper we approach this task to create an engaging outreach experience, on the concept of cyber-physical systems, using a Scalextric racetrack. In the activity, students seek to compromise the underlying computer system that is linked to the track and updates the scoreboard system, in order to inflate their own score and to sabotage their opponent. Our investigation with this technique shows high levels of engagement whilst providing an excellent platform for teaching basic concepts of enumeration, brute forcing, and privilege escalation. It also provokes discussion on how this activity relates to real-world cases of cyber-physical systems security in the sports domain and beyond.

Interactive Program Visualization to Teach Stack Smashing: An Experience Report

CISSE

Harini Ramaprasad, Meera Sridhar, Erik Akeyson

This paper presents an experience report on using an interactive program visualization tool, SAVTool, and a complementary active-learning exercise to teach stack smashing, a key software security attack. The visualization tool and active-learning exercise work synergistically to guide the student through challenging, abstract concepts in the advanced cybersecurity area. SAVTool and the exercise are deployed within the software security module of an undergraduate cybersecurity course that introduces a broad range of security topics. A study is designed that collects and evaluates student perceptions on the user interface of SAVTool and the effectiveness of the two resources in improving student learning and engagement. The study finds that over 80% of responses to user interface questions, 66% of responses to student learning questions and 64% of responses to student engagement questions are positive, suggesting that the resources improve student learning and engagement in general. The study does not find discernible patterns of difference in responses from students of different ages and varying levels of prior experience with stack smashing attacks, program visualization tools and C programming.

Low-Cost CTF Platform for Industrial Control Systems Education

CISSE

Taegan Williams, Tiffany Fuhrmann, Michael Haney

In order to address the nationwide workforce shortage of skilled and educated cyber-informed engineers, we must develop low-cost and highly effective resources for industrial control systems education and training. College curricula in technology management, cybersecurity, and computer science aim to build students' computational and adversarial thinking abilities but are often done only through theory and abstracted concepts [1]. To better a student's understanding of industrial control system applications, post-secondary institutions can use gamification to increase student interest through an interactive, user-friendly, hands-on experience. [Lab Name] CTF can provide post-secondary institutions new opportunities for low-cost, guided exercises for the industrial control system (ICS) education to help students master adversarial thinking. Based on an extension to PicoCTF, [Lab Name] CTF is a platform for students to design, implement and evaluate exercises that test their understanding of core concepts in industrial control systems cybersecurity, answering the need for more interactive education methods. The main contributions of this paper are the improvement of the cybersecurity curriculum through extending the PicoCTF platform to promote the gamification of industrial control system concepts with consideration to the Purdue Reference Architecture.

Meeting the Challenges of Large Online Graduate Cybersecurity Classes in the Age of COVID

CISSE

Michael Whitman, Herbert Mattord

Designing curriculum and teaching delivery programs that can meet the needs of specialized groups of employers and students is challenging in the best of times. When extra criteria are added, such as making a degree program fully online when also limited with the number of fully qualified faculty due to constrained resources, flexibility is a requirement. This is a case study of one such program development project that saw the design and development of a Master-level program of study in Cybersecurity that was designed at one level of expected faculty resource availability that had to rapidly evolve in a new direction due to significant resource restrictions. Built on a model of maximizing the productivity of a few fully qualified faculty by leveraging less qualified but very capable part-time staff to meet the needs of online delivery of large sections of graduate instruction.

Microtransactions and Gambling in the Video Game Industry

CCERP

Christopher L. Antepenko, Samuel R. Rickey, Angel L. Hibbets, John-David Rusk

The beginning of the 21st century has had a drastic effect on the video game industry. The advent of almost universal Internet access, the release of inexpensive broadband-enabled consoles, and the availability of mobile gaming have led to game developers and publishers heavily relying on premium in-game currencies, exclusive paid items, and loot boxes to subsidize or even replace profits from traditional video game business models. By 2020, in-game purchases made up a market of $92.6B worldwide and, in the US, experienced growth of over 30%. In this highly lucrative market, the legal and ethical landscape is constantly bubbling with claims of unlicensed gambling, unfair pay-to-win mechanics, and extortion of minors. In the first part of this paper, we will explore the historical context of microtransactions from the first examples to modern ubiquity. In the second half of this paper, we will examine some relevant scandals and legal cases regarding the connection between microtransactions and gambling.

NIDS in Airgapped LANs - Does it Matter?

CCERP

Winston Messer

This paper presents an assessment of the methods and benefits of adding network intrusion detection systems (NIDS) to certain high-security air gapped isolated local area networks. The proposed network architecture was empirically tested via a series of simulated network attacks on a virtualized network. The results show an improvement of double the chances of an analyst receiving a specific, appropriately-severe alert when NIDS is implemented alongside host-based measures when compared to host-based measures alone. Further, the inclusion of NIDS increased the likelihood of the analyst receiving a high-severity alert in response to the simulated attack attempt by four times when compared to host-based measures alone. Despite a tendency to think that networks without cross-boundary traffic do not require boundary defense measures, such measures can significantly improve the efficiency of incident response operations on such networks.

Practical Labs for Teaching SDN Security

CISSE

Souvik Das, Kamil Sarac

The rapid adoption of Software Defined Networking (SDN) in the industry has exposed certain security risks today some of which are unique to its paradigm. Security issues around the use-cases that expose these risks are fundamentally aligned with the networking and cybersecurity concepts that are taught at the graduate level in academia. In this paper, we present a number of lab activities on SDN security that are inspired from practical use-cases in SDN deployments. The goal of this effort is to help students give a shape to their thought process about the practical security implications of SDN deployments and gain valuable practical domain knowledge in securing an environment with such deployments.

Secure Cloud-based IoT Water Quality Gathering for Analysis and Visualization

CCERP

Soin Abdoul Kassif Traore, Maria Valero, Amy Gruss

Water quality refers to measurable water characteristics, including chemical, biological, physical, and radiological characteristics usually relative to human needs. Dumping waste and untreated sewage are the reasons for water pollution and several diseases to the living hood. The quality of water can also have a significant impact on animals and plant ecosystems. Therefore, keeping track of water quality is a substantial national interest. Much research has been done for measuring water quality using sensors to prevent water pollution. In summary, those systems are built based on online and reagent-free water monitoring SCADA systems in wired networks. However, centralized servers, transmission protocols, and data access can present challenges and disadvantages for those systems. This paper proposes a secure Cloud-based IoT water quality gathering architecture for water quality analysis and visualization to address the limitations of the current systems. The proposed architecture will send, analyze and visualize water quality data in the Cloud by utilizing specialized sensors and IoT-based gateways to capture water measurements (Dioxygen concentration, and temperature, among others). Then, they communicate securely to the Cloud-based server through a high-speed wireless network. We evaluated the performance of the proposed framework on a process-oriented approach to success metrics for cyberinfrastructures. The experiments were conducted in a laboratory and focused on network security and resiliency, the IoT prototype performance in dropping real-time data transmission, and remote access. The results demonstrate higher data collection and transmission effectiveness with minimal data loss and low energy usage overtime. The accompanying cloud-based platform provided the flexibility needed for water quality monitoring and laboratory studies.

Security Mindset Fundamentals and Second Language Learning

CISSE

Amy Kuiken

Security mindsets can be said to engage elements of situational awareness and analytical, creative, and practical elements of adversarial thinking. Scholars have debated whether security mindsets are taught or fostered, but they have roundly acknowledged that greater development of security mindsets is needed. Here, the argument is made that implicit features of language itself can be drawn on in K12+ second language (L2) learning settings to foster the analytical, creative, practical and situational awareness capacities of learners. L2 lessons can also be adapted to familiarize students with security thinking and explicit topics. By exploiting these novel connections between language learning and security thinking, L2 learning contexts could become a security mindset training ground for millions of U.S. students.

Simulating Cybersecurity Risk Using Advanced Quantitative Risk Assessment Techniques: A Teaching Case Study

CISSE

Basil Hamdan

This paper; a scenario-based teaching case study, aims to introduce students in a Cybersecurity Risk Management course to advanced quantitative risk assessment techniques. The case study utilizes a fictitious company for which a risk assessment is underway. Assuming the role of a Cybersecurity Risk Team of the company, the students are tasked with determining the risk exposure the company faces from a threat scenario against one of its mission-critical information resources. Specifically, the students are required to (1) quantify the monetary losses that could result from a threat scenario, (2) compute the inherited risk exposure from the threat scenario (3) compute the residual risk given the implantation of certain security controls, and (4) compute returns on security controls. The case study holds the promise of enhancing the overall learning of the students and boosting their marketability as future cybersecurity professionals.

Social Media Platforms and Responsibility for Disinformation

CCERP

Matt T. Figlia, Brandon M. Henschen, Joseph T. Sims, John-David Rusk

Researchers are paying closer attention to the rise of disinformation on social media platforms and what responsibility, if any, the companies that control these platforms have for false information being spread on their websites. In this paper, we highlight the recent growth in concern regarding online disinformation, discuss other works regarding the use of social media as a tool for spreading disinformation, and discuss how coordinated disinformation campaigns on social media platforms are used to spread propaganda and lies about current political events. We also evaluate the reactions of social media platforms in combatting disinformation and the difficulty in policing it. Finally, we argue the point that governments should not have the power to regulate the content of social media platforms except in cases where said content is actively illegal or could be categorized as a type of speech that is not protected by the First Amendment.

Structure or Anarchy: A Bibliometric Analysis of Keywords in Cybersecurity Education Literature

CISSE

Jason Pittman, Helen Barker, Shaho Alaee

Bibliometric analysis is essential for understanding the growth, health, and trajectory of scientific disciplines. In effect, such analyses help researchers determine if a given field is well-structured or fragmented through anarchy. Prior work examined to what extent cybersecurity education research generated a follow-up study. The goal of the work was to uncover bibliometric features and characteristics linked to overall maturity of the field. The results suggested little, if any, research follow up or extension took place based on the dearth of interlinking between citations. This work continues the line of bibliometric description by investigating if cybersecurity education papers are not extended because of discoverability issues during literature reviews. To answer this question, this work explored structural bibliometric indicators in 163 journal and conference articles. Specifically, we extracted metadata keywords and paper content keywords as input to frequency analyses of the sample articles. The results revealed 12.4% of the sample contains metadata keywords. Further, 18.03% of the sample contained educated related keywords. Lastly, four of the top five sample papers by citation count do not contain keywords at all and papers with content only keywords exhibited more frequent citation than those with only metadata keywords. Based on these results, we offer observational conclusions as well as notions for future work.

Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range

CISSE

Phil Legg, Alan Mills, Ian Johnson

Computer Science as a subject is now appearing in more school curricula for GCSE and A level, with a growing demand for cyber security to be embedded within this teaching. Yet, teachers face challenges with limited time and resource for preparing practical materials to effectively convey the subject matter. We hosted a series of workshops designed to understand the challenges that teachers face in delivering cyber security education. We then worked with teachers to co-create practical learning resources that could be further developed as tailored lesson plans, as required for their students. In this paper, we report on the challenges highlighted by teachers, and we present a portable and isolated infrastructure for teaching the basics of offensive and defensive cyber security, as a co-created activity based on the teacher workshops. Whilst we present an example case study for red and blue team student engagement, we also reflect on the wide scope of topics and tools that students would be exposed to through this activity, and how this platform could then be generalised for further cyber security teaching.

Teaching Software Security to Novices With User Friendly Armitage

CISSE

Christopher Morales-Gonzalez, Matthew Harper and Xinwen Fu

With cybercrime increasing by 600% during theCOVID-19 pandemic, the demand for cybersecurity professionals has also risen significantly. There are roughly 700,000 unfilled cybersecurity positions that continue to affect businesses and have the potential to cause significant problems. Education for novice cybersecurity students suffers from teaching materials not being practical, modern, nor intuitive enough to inspire these students to pursue a career in the cybersecurity field. In this paper, we present our methodology and create a module for teaching the basics of software security using Armitage and Metasploit. We design our module and hands-on labs using a preconfigured Windows 10 VM, a Metasploitable VM and a Kali Linux VM with custom-made tools. Our methodology and module is validated through the results of a high school cybersecurity camp. The module is available at GitHub.

Techniques to Overcome Network Attacks (Sybil Attack, Jamming Attack, Timing Attack) in VANET

CISSE

Sinan Ameen Noman and Travis Atkison

VANET is a type of Ad hoc network that enables the communication between vehicles and roadside units. It provides a broad range of applications, such as blind crossing, accident avoidance, protection, interactive route planning, traffic situation monitoring in real-time, etc. These applications are required to be very secure to achieve a reliable service and provide safety for drivers. This paper sheds light on three different types of attacks (Sybil Attack, Jamming Attack, Timing Attack) that can critically affect the vehicular ad hoc network environment. Furthermore, we present techniques that can overcome these attack.

The Role of Education in Dispelling Myths and Misconceptions in Cybersecurity

CISSE

Eugene Spafford, Leigh Metcalf, Josiah Dykstra

In this session, the panelists will discuss their observations and experiences of cybersecurity myths across academia, industry, and government. They will draw on their decades of experience to discuss pitfalls they've encountered and examples of folk wisdom including: Is the user the weakest link? Is more security always better? Is cyber offense easier than defense? This will also touch on some of the biases humans bring to decision-making, and how those may negatively influence good security practices. These include the action and conformity biases. The panel will illuminate opportunities for education to help dispel prevalent and widespread myths that can be avoided or mitigated for the benefit of more effective cybersecurity. Portions of this presentation are drawn from personal experience and courses taught by the panelists, including a regular course offered at Purdue University as part of the graduate cybersecurity curriculum.

Towards Assessing Organizational Cybersecurity Risks via Remote Workers' Cyberslacking and Their Computer Security Posture

CCERP

Ariel Luna, Yair Levy, Gregory Simco, Wei Li

Cyberslacking is conducted by employees who are using their companies' equipment and network for personal purposes instead of performing their work duties during work hours. Cyberslacking has a significant adverse effect on overall employee productivity, however, recently, due to COVID-19 pandemic move to remote working also pose a cybersecurity risk to organizations networks and infrastructure. In this work-in-progress research study, we are developing, validating, and will empirically test taxonomy to assess an organization's remote workers' risk level of cybersecurity threats. This study includes a three-phased developmental approach in developing the Remote Worker Cyberslacking Security Risk Taxonomy. With feedback from cybersecurity Subject Matter Experts (SMEs) on the taxonomy and measures, we then plan to use the taxonomy to assess organizational remote workers' risk level of cybersecurity threats by using actual system indicators of productivity measures to estimate their cyberslacking along with assessing the computer security posture of the remote device being used to access organizational resources. Anticipated results from 125 anonymous employees will then be assessed on the proposed novel taxonomy where recommendation to the organizational cybersecurity leadership will be provided.

Towards the Development and Assessment of a Method for Educating Users into Choosing Complex, Memorable Passphrases

CCERP

Juan M. Madrid, Yair Levy, Laurie Dringus, Ling Wang

The currently most used method for authentication is the password because it is simple to implement, and computer users are very familiarized with it. However, passwords are vulnerable to attacks that can be mitigated by increasing the complexity of the chosen password, particularly in terms of length. One possible approach to accomplish this is through the usage of passphrases, which can be easier to remember than a standard password, thus reducing the loss of work time and productivity related to forgotten passwords. To achieve the required balance between complexity and memorability, the concept of passphrase categories can be used, i.e. more sensitive accounts or services should have more complex passphrases, and vice versa. This work-in-progress study proposes to develop and assess a method for educating users into creating complex, yet easy to remember passphrases, according to the category of account or service they want to protect. The work-in-progress study will be developed in three phases, including validation of the method by a panel of subject matter experts, a pilot test, and a main data collection and analysis phase.

Using Experts for Improving Project Cybersecurity Risk Scenarios

CCERP

Steven S. Presley, Jeffrey P. Landry, Jordan Shropshire, Phil Menard

This study implemented an expert panel to assess the content validity of hypothetical scenarios to be used in a survey of cybersecurity risk across project meta-phases. Six out of 10 experts solicited completed the expert panel exercise. Results indicate that although experts often disagreed with each other and on the expected mapping of scenario to project meta-phase, the experts generally found risk present in the scenarios and across all three project meta-phases, as hypothesized.

Virginia Cyber Navigator Internship Program (VA-CNIP): Service Learning in Local Election Security

CISSE

Angela Orebaugh, Jack Davidson, Deborah Johnson, Daniel Graham, Worthy Martin

A coalition of Virginia universities, in partnership with the Virginia Department of Elections (ELECT), launched the Virginia Cyber Navigator Internship Program (VA-CNIP) - an innovative educational program to develop future cybersecurity professionals to protect the election infrastructure. The program addresses the need for more skilled cybersecurity professionals, and those who are supporting public services such as elections. This paper provides an overview of the key components of the program: a full semester gateway course covering sociotechnical election topics, a two-day kickoff bootcamp to prepare students for their internship, an internship with an election office, and a one-day debrief and assessment at the end of the internship.

What You See Is Not What You Know: Deepfake Image Manipulation

CCERP

Cathryn Allen, Bryson R. Payne, Tamirat T. Abegaz, Chuck Robertson

Research indicates that deceitful videos tend to spread rapidly online and influence people's opinions and ideas. Because of this, video misinformation via deepfake video manipulation poses a significant online threat. This study aims to discover what factors can influence viewers' capability of distinguishing deepfake videos from genuine video footage. This work focuses on exploring deepfake videos' potential use for deception and misinformation by exploring people's ability to determine whether videos are deep fakes in a survey consisting of deepfake videos and original unedited videos. The participants viewed a set of four videos and were asked to judge whether the videos shown were deepfakes or originals. The survey varied the familiarity that the viewers had with the subjects of the videos. Also, the number of videos shown at one time was manipulated. This survey showed that familiarity with the subject(s) depicted in a deepfake video has a statistically significant impact on how well people can determine it is a deepfake. Notably, however, almost two-thirds of study participants (102 out of 154, or 66.23%) were unable to correctly identify a sequence of just four videos as either genuine or deepfake. The potential for deepfakes to confuse or misinform a majority of the public via social media should not be underestimated. This study provides insights into possible methods for countering disinformation and deception resulting from the misuse of deepfakes. Familiarity with the target individual depicted in a deepfake video contributed to viewers' accuracy in distinguishing a deepfake better than showing unaltered authentic source videos side-by-side with the deepfakes. Organizations, governments, and individuals seeking to contain or counter deepfake deception will need to consider two main factors in their operational planning: 1) a swift, near-real-time response to deepfake disinformation videos, and 2) creating more familiarity through additional, preferably live video footage of the target of the deepfake responding to and refuting the disinformation personally.