Journal of Cybersecurity Education, Research and Practice

Volume 2022 | Number 2 Article 1

2022

Editorial

Michael E. Whitman
Kennesaw State University, mwhitman@kennesaw.edu

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Hossain Shahriar
Kennesaw State University, hshahria@kennesaw.edu

Editorial

Abstract

Since 2016, it has been the mission of the Journal of Cybersecurity Education, Research, and Practice (JCERP) to be a premier outlet for high-quality information security and cybersecurity-related articles of interest to teaching faculty and students. This is the 13th edition of the (JCERP) and, as ever, we are seeking authors who produce high-quality research and practice-oriented articles focused on the development and delivery of information security and cybersecurity curriculum, innovation in applied scholarship, and industry best practices in information security and cybersecurity in the enterprise for double-blind review and publication. The journal invites submissions on Information Security, Cybersecurity, and related topics such as those found in this edition.

Keywords

Editorial

FROM THE EDITORS:

Since 2016, it has been the mission of the Journal of Cybersecurity Education, Research, and Practice (JCERP) to be a premier outlet for high-quality information security and cybersecurity-related articles of interest to teaching faculty and students. This is the 13th edition of the (JCERP) and, as ever, we are seeking authors who produce high-quality research and practice-oriented articles focused on the development and delivery of information security and cybersecurity curriculum, innovation in applied scholarship, and industry best practices in information security and cybersecurity in the enterprise for double-blind review and publication. The journal invites submissions on Information Security, Cybersecurity, and related topics such as those found in this edition.

We also continue to have the need for additional reviewers for the Journal. Currently, we have about 30 reviewers that have steadfastly stuck with us, reviewing 3-4 articles per year. We'd rather keep the reviewer assignments closer to 2-3 per year, but with so few reliable reviewers, it's becoming more and more difficult. We tend to get 20-30 submissions per year, accepting 10-15, giving us an overall 50% +/- accept rate. We would love to have you join us as a reviewer, so please reach out and volunteer.

Editorial

Will we ever fully recover from COVID?

For the past several years, we've heard the drum beat that there are hundreds of thousands of unfilled jobs in Cybersecurity. Not 3 years ago, our programs had a near 100% employment on graduation. In fact, we had issues with students starting work before graduation and struggling to finish their degree programs. Now the stats show that we are closer to 60-70% employment on graduation. What has changed? Was the impact of COVID-19 so severe that organization could no longer hire entry-level employees with little or no experience? Have organizations shifted their employment models such that remote workers exclude new college graduates? We wonder and try to help our students that graduate and then struggle to get that first, important, job in-field, to start their careers.

There is a similar challenge in Academia. Universities had virtually eliminated travel, which resulted in fewer venues to submit and publish articles as proceedings. While the travel budgets are slowly returning, at conferences like the Conference on Cybersecurity Education, Research, and Practice, submissions are still at an all-time low, with only 14 papers submitted and 11 accepted at the 2022 conference. We were extremely fortunate that the conference committee for the Colloquium for Information Systems Security Education reached out to us, to co-host a virtual CISSE alongside the virtual CCERP, last year. This generous offer essentially saved our conference, as we were poised to cancel. With the joint hosting, a few more submissions came in and we were able to host CCERP as a peer track with CISSE. Next year, KSU will host the event as a hybrid conference with CISSE, CCERP and one to two other conferences as a multi-venue event. We look forward to beginning the return to normality but have learned some valuable lessons regarding remote work and meetings. We hope our readers will consider submitting papers there as well. The call for papers should go out in April 2023.

In This Issue

For Volume 2022, Number 2 we are pleased to share the following scholarly articles:

1. **Alpha Phi-shing Fraternity: Phishing Assessment in a Higher Education Institution**
Marco Casagrande (University of Padua), Mauro Conti (University of Padua), Monica Fedeli (University of Padua), Eleonora Losiouk (University of Padua)

Abstract:
Phishing is a common social engineering attack aimed to steal personal information. Universities attract phishing attacks because: 1) they store employees' and students' sensitive data, 2) they save confidential documents, 3) their infrastructures often lack security. In this paper, we showcase a phishing assessment at the University of Redacted aimed to identify the people, and the features of such people, that are more susceptible to phishing attacks. We delivered phishing emails to 1.508 subjects in three separate batches, collecting a click rate equal to 30%, 11% and 13%, respectively. We considered several features (i.e., age, gender, role, working/studying field, email template) in univariate and multivariate analyses and found that students are more susceptible to phishing attacks than professors or technical/administrative staff, and that emails designed through a spear phishing approach receive a highest click rate. We believe this work provides the foundations for setting up an effective educational campaign to prevent phishing attacks not only at the University of Redacted, but in any other university.

2. **Toward a Student-Ready Cybersecurity Program: Findings from a Survey of STEM-Students**
Lora Pitman (Old Dominion University), Brian K. Payne (Old Dominion University), Tancy Vandecar-Burdin (Old Dominion University), Lenora Thorbjornsen (Old Dominion University)

Abstract:
As the number of available cybersecurity jobs continues to grow, colleges strive to offer to their cybersecurity students an environment which will make them sufficiently prepared to enter the workforce after graduation. This paper explores the academic and professional needs of STEM-students in various higher education institutions across Virginia and how cybersecurity programs can cater to these needs. It also seeks to propose an evidence-based approach for improving the existing cybersecurity programs so that they can become more inclusive and student-ready. A survey of 251 college students in four higher education institutions in Virginia showed that while there are common patterns observed across gender and race, there are still areas in which more should be done regarding some of these groups. In particular, some discrepancies are observed across gender when it comes to students' preparation with business fundamentals, the overall satisfaction of the received STEM education, and across race and ethnicity, when it comes to college advising, peer-mentoring, tutoring and faculty mentoring. The results from this study inform specific recommendations that will bring higher-education institutions and their cybersecurity program to a more student-ready level.

3. **Cybersecurity Continuity Risks: Lessons Learned from the COVID-19 Pandemic**
Tyler Fezzey (University of West Florida), John H. Batchelor (University of West Florida), Gerald F. Burch (University of West Florida), Randall Reid (University of West Florida)

Abstract:
The scope and breadth of the COVID-19 pandemic were unprecedented. This is especially true for business continuity and the related area of cybersecurity. Historically, business continuity

and cybersecurity are viewed and researched as separate fields. This paper synthesizes the two disciplines as one, thus pointing out the need to address both topics simultaneously. This study identifies blind spots experienced by businesses as they navigated through the difficult time of the pandemic by using data collected during the height of the COVID-19 pandemic. One major shortcoming was that most continuity and cybersecurity plans focused on single-axis threats. The COVID-19 pandemic resulted in multi-axes threats, pointing out the need for new business strategies moving forward. We performed multiple regression analysis and constructed a correlation matrix to capture significant relationships between percentage loss of revenue and levels of concern for different business activities moving forward. We assessed the most pervasive issues Florida small businesses faced in October 2020 and broke these down by the number of citations, the total number of impacts cited, and industry affectedness. Key security risks are identified and specific mitigation recommendations are given.

4. R**isk perceptions about personal Internet-of-Things: Research directions from a multi-panel Delphi study**
Paul M. Di Gangi (University of Alabama at Birmingham), Barbara A. Wech (University of Alabama-Birmingham), Jennifer D. Hamrick (University of Alabama at Birmingham), James L. Worrell (University of Alabama - Birmingham), Samuel H. Goh (University of Alabama at Birmingham)

Abstract:
Internet-of-Things (IoT) research has primarily focused on identifying IoT devices' organizational risks with little attention to consumer perceptions about IoT device risks. The purpose of this study is to understand consumer risk perceptions for personal IoT devices and translate these perceptions into guidance for future research directions. We conduct a sequential, mixed-methods study using multi-panel Delphi and thematic analysis techniques to understand consumer risk perceptions. The results identify four themes focused on data exposure and user experiences within IoT devices. Our thematic analysis also identified several emerging risks associated with the evolution of IoT device functionality and its potential positioning as a resource for malicious actors to conduct security attacks.

5. **The Impact of a GenCyber Camp on In-service Teachers' TPACK**
Kevin M. Thomas (Bellarmine University), Jessica Ivy (Bellarmine University), Kristin Cook (Bellarmine University), Robert R. Kelley (Bellarmine University)

Abstract:
The purpose of this study was to examine the impact of a GenCyber camp curriculum on teachers' technology, pedagogy, and content knowledge (TPACK). The camp was designed to engage participants in developing the knowledge and skills to incorporate GenCyber Cybersecurity First Principles and GenCyber Cybersecurity Concepts (GenCyber, 2019) into their curriculums. Participants (37 middle and high school teachers from a variety of disciplines) attended one of two weeklong camps held at a Midwestern liberal arts university. Using the TPACK Self-Reflection and TPACK Self-Assessment Surveys, pre- and post-camp data were collected from participants. Findings indicate that participants demonstrated an increase in all domains of the TPACK framework from pre- to post-survey. The greatest increase was in Technological Pedagogy Knowledge (TPK) (0.57), followed by Pedagogical Content Knowledge (PCK) (0.51), and Technological Pedagogical Content Knowledge (TPACK) (0.46). GenCyber participants also demonstrated an average increase in pre- and post-test scores in all areas on

the TPACK Self-Assessment Survey Results; however, individual results were mixed. The majority of participants (n=21), sixty percent, saw an increase in composite score from pre- to post, whereas 12 participants' (34%) scores decreased from pre- to post, and two (6%) stayed the same. Findings indicate the GenCyber Camp provided in-service teachers with the knowledge and skills necessary to incorporate GenCyber Principles and Cybersecurity Concepts into their curriculum. Recommendations for teacher professional development on cybersecurity are made.

6. **Reinventing Cybersecurity Internships During the COVID-19 Pandemic**
Lori L. Sussman (University of Southern Maine)

Abstract:
The Cybersecurity Ambassador Program provides professional skills training for emerging cybersecurity professionals remotely. The goal is to reach out to underrepresented populations who may use Federal Work-Study (FWS) or grant sponsored internships to participate. Cybersecurity Ambassadors (CAs) develop skills that will serve them well as cybersecurity workers prepared to do research, lead multidisciplinary, technical teams, and educate stakeholders and community members. CAP also reinforces leadership skills so that the next generation of cybersecurity professionals becomes a sustainable source of management talent for the program and profession. The remote curriculum innovatively builds non-technical professional skills (communications, teamwork, leadership) for cybersecurity research through student-led applied research and creating community-focused workshops. These student-produced workshops are in phishing, identity and privacy cyber safety, social media safety, and everyday home cyber safety. The CAs tailor the program to a particularly vulnerable population such as older adults, students, veterans, or similar people that make up most workshop participants. At this time, the data shows that this pedagogical approach to curriculum development, grounded in the Ground Truth Expertise Development Model (GTEDM), is a unique methodology. This curriculum teaches cybersecurity interns with key non-technical but critical KSAs for cybersecurity professional development has proved to be a factor in accelerated hiring for program participants.

7. **Lightweight Pairwise Key Distribution Scheme for IoTs**
Kanwalinderjit Kaur (California State University, Bakersfield)

Abstract:
Embedding a pairwise key distribution approach in IoT systems is challenging as IoT devices have limited resources, such as memory, processing power, and battery life. This paper presents a secure and lightweight approach that is applied to IoT devices that are divided into Voronoi clusters. This proposed algorithm comprises XOR and concatenation operations for interactive authentication between the server and the IoT devices. Predominantly, the authentication is carried out by the server. It is observed that the algorithm is resilient against man-in-the-middle attacks, forward secrecy, Denial of Service (DoS) attacks, and offers mutual authentication. It is also observed that the given scheme has low communication and computing overheads compared to some existing methods.

8. **Teaching by Practice: Shaping Secure Coding Mentalities through Cybersecurity CTFs**
   Jazmin Collins (Arcadia University), Vitaly Ford (Arcadia University)

   Abstract:
   The use of the Capture the Flag (CTF)-style competitions has grown popular in a variety of environments as a method to improve or reinforce cybersecurity techniques. However, while these competitions have shown promise in student engagement, enjoyment, and the teaching of essential workforce cybersecurity concepts, many of these CTF challenges have largely focused on cybersecurity as a general topic. Further, most in-school CTF challenges are designed with technical institutes in mind, prepping only experienced or upper-level students in cybersecurity studies for real-world challenges. Our paper aims to focus on the setting of a liberal arts institute, emphasizing secure coding as the focus of CTF-engaged learning for beginner to upper-level undergraduate students. We propose a survey system to evaluate the secure coding mentality of our students before and after taking these challenges, as well as an easily hosted, low-resource CTF platform that students can access either in or outside of the classroom. We have found this system to be moderately effective at framing and improving the secure coding mentalities of our students.

We hope you enjoy this issue, and as always, please consider submitting a manuscript of your own to JCERP.

Dr. Mike Whitman
Dr. Herb Mattord
Dr. Hossain Shahriar

KSU Institute for Cybersecurity Workforce Development