

2021

From the Editors

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

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/jcerp>



Part of the [Information Security Commons](#), [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

Recommended Citation

Whitman, Michael E.; Mattord, Herbert J.; and Shahriar, Hossain (2021) "From the Editors," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2021 : No. 1 , Article 1.

Available at: <https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss1/1>

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

From the Editors

Abstract

A commentary from the editors, with an overview of the articles contained in this issue of the Journal.

Keywords

editorial

FROM THE EDITORS:

Welcome to the Spring 2021 edition of the Journal of Cybersecurity Education, Research, and Practice.

It seems like yesterday that the JCERP editorial board discussed the idea of starting a security-related journal. At the time there weren't many venues for security pedagogy and the scholarship of learning on information security, so we began the Information Security Education Journal (ISEJ). We ran with that title for two years, until 2016 the publisher began having difficulties. By that time, we discovered our university had a license for Digital Commons, a publishing platform that supports both conference-style publications and traditional journal-style publications. We quickly realized that we could create a true open-access Journal that was free to both authors and readers alike, allowing cutting-edge research in security pedagogy and practice to be disseminated to interested faculty quickly and freely. Thus, the Journal of Cybersecurity Education, Research, and Practice began.

Since then, we've had years of plentiful articles and years without many submissions, a veritable feast and famine. Last year was particularly challenging for everyone with the COVID pandemic changing the way a lot of organizations looked at employee work and at security. The need to protect employee's work created a new paradigm when nearly 100% of the workforce moved to work from home, for those fortunate enough to be able to do so. Here in academia, we weathered the storm better than most. At KSU most of our security degree programs (and there are many) were at least partially online (hybrid), with the BS-Cybersecurity and the brand-new MS-Cybersecurity being 100% online. So as some lost their jobs, and others had to work from home, many decided it was time to pursue a new career.

On the research front, with many scholars unable to travel to conferences, it seems that some research slowed. Some conferences (like the KSU Conference on Cybersecurity Education, Research and Practice) went online, to share fewer papers with generally larger audiences. CCERP was free last year – a last-minute decision designed to try to bolster the number of papers presented (only seven papers accepted). Thus, we appeal to you to consider submitting a paper to the CCERP this year and follow up on your well-written papers by submitting them to the Journal immediately thereafter. If we don't get a significant increase in submissions, the conference may be postponed or canceled outright.

We also 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 that number down, closer to 2-3 per year, but with so few reliable reviewers, it's becoming more and more difficult. We tend to get 15-20 submissions per year, accepting 8-10, giving us an overall 50% +/- accept rate. We would love to have you join us as a reviewer.

In This Issue

The papers published in Volume 2021, Issue 1 are:

1. In "Observations, Evaluations, and Recommendations for DETERLab from an Educational Perspective" by Ahmed Ibrahim (University of Pittsburgh) and Vitaly Ford (Arcadia University), the authors discuss DETERLab as "a cluster environment that provides a set of virtual machines that can be used by researchers and teachers to run cybersecurity experiments and competitions, and where it is possible to deploy different network configurations to research attack and defense mechanisms in the cyber world." The authors share "an analysis of experiments that have a step-by-step guide, sample solution, grading criteria, network diagram,

and teacher manual.”

2. In “Contingency Planning Amidst a Pandemic”, author Natalie C. Belford (University of West Florida) states “Proper prior planning prevents pitifully poor performance: The purpose of this research is to address mitigation approaches - disaster recovery, contingency planning, and business continuity planning - and their benefits as they relate to university operations during a worldwide pandemic predicated by the novel coronavirus (COVID-19). The most relevant approach pertaining to the University’s needs and its response to the coronavirus pandemic will be determined and evaluated in detail.”
3. In “Developing an AI-Powered Chatbot to Support the Administration of Middle and High School Cybersecurity Camps” authors Jonathan He (Princess Anne High School, Virginia Beach) and Chun Sheng Xin (Old Dominion University) assert “throughout the Internet, many chatbots have been deployed by various organizations to answer questions asked by customers. In recent years, we have been running cybersecurity summer camps for youth.” The authors “believe that a chatbot can be more useful than a Q&A agent and it can be further developed to become an advanced virtual assistant for both teachers and students. As for future work, we are interested in expanding the chatbot for general questions in the cybersecurity area so that the chatbot can provide standardized answers to more knowledge-related questions about cybersecurity.”
4. In “Secure Coding in Five Steps” authors Mini Zeng (Jacksonville University) and Feng Zhu (the University of Alabama in Huntsville) describe how “software vulnerabilities have become a severe cybersecurity issue. There are numerous resources of industry best practices available, but it is still challenging to effectively teach secure coding practices. The resources are not designed for classroom usage because the amount of information is overwhelming for students. There are efforts in academia to introduce secure coding components into the computer science curriculum, but a big gap between industry best practices and workforce skills still exist. Unlike many existing efforts, we focus on both the big picture of secure coding and hands-on projects. To achieve these two goals, we present five learning steps that we have been revising over the last four years. Our evaluation shows that the approach reduces complexity and encourages students to use secure coding practice in their future projects.”

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