Editorial

The current challenges brought by the cybersecurity crisis compels higher education to reflect upon its practice on pedagogy, student engagement, and connection with broader intellectual domains. There are three timely challenges. First, how to build and update a cybersecurity lab environment economically, which enables students to practice wide-range of security concepts and experiments. Unlike traditional computer science courses, the cybersecurity curriculum presents unique technical and administrative challenges in setting up a learning environment. Students need to be exposed to a near-real simulation environment to practice network security. Traditional network simulation tools such as Cisco Packet Tracer weren't designed for security education. Such tools offer very little room for security-related training. Secondly, how to engage contemporary prospective students and stimulate their interest in cybersecurity. For the generation who grew up with social media and online games, the real hacking work might appear less visually exciting than the one presented in sci-fi films. The amount of technical preparation and limitation of network infrastructure have also alienated potential cybersecurity enthusiasts among high-school students. Lastly, cybersecurity is no longer merely a branch of computer science. Proliferation of zero-days vulnerabilities and malwares have shown the limitation of many theoretical assumptions in computer science. It is crucially important for cybersecurity research to look upon other domains of knowledge to obtain insights and metaphors.

This issue of the **Information Security Education Journal** collects three articles, each addressing one of the above issues. In his "**First Laboratory Experience for Cyber Engineering and Cybersecurity Students**", Fong K. Mak presents a novel, open source virtual lab environment which allows students to gain hands-on experience to support their understanding of networking technologies with security concerns in using network components and software applications. The platform is very useful for small liberal art colleges with budget restrictions and limited network infrastructure. The proposed virtual labs have been used in Gannon University and well received by students and instructors. In his article, "**A Virtual and On-site Hackathon to Recruit High School Students within Cybersecurity Major**", Yunkai Liu proposes to use hackathon events to attract high school students to cybersecurity subjects. Traditional hackathon events are oriented for programming and software development. Yunkai discusses various ways to adapt a hackathon to cybersecurity subjects such as ethical hacking. The focus of the proposal in his article is on web application security. At the end, the author also shares experience on how to use cybersecurity hackathon to help small liberal art colleges recruit students. Our last article, "**Mind, Unity and Software Security - Analysis of Functional Unity in Cases of Data-only Attack"**, is contributed by Ziyuan Meng. The author suggests that there is an inherent connection and structural similarities between the human mind and computer programs. The author argues that 18th century German philosopher Immanuel Kant's theory on how mind functions can provide crucial insights on the how a secure program functions. The author includes two case studies from the recent data-only attacks to examine these conditions.

We hope that this collection of articles will stimulate readers of this special issue to broaden their scopes of research and to make wider scholarly connections to their colleagues in this field. We thank all the authors, who contributed to these special issues, as well as the reviewers who devoted their time and energy for the review process.

Editors