Overview

To support the goal of addressing expansion of the national cybersecurity workforce in terms of both quantity and quality, and meet the future workforce demands of the U.S. Federal Government, we propose to integrate hands-on learning experience on cutting-edge stepping-stone intrusion detection techniques into the cybersecurity curriculum. The goals of this project are to: 1) make students competitive by educating them with knowledge, skills, and abilities in the field of cybersecurity, and 2) train students to be successfully adaptive to the change in this dynamic cybersecurity field quickly and efficiently. Upon completion of the training on the proposed content modules and hands-on labs, students will be able to demonstrate the knowledge and skills to 1) understand the approaches to establish a connection chain to launch attacks through stepping-stones; 2) be able to design codes to collect and analyze network traffic; 3) detect and mitigate stepping-stone cyberattacks using various tools and techniques; 4) identify unauthorized, illicit, and anomalous users’ behavior based solely on network traffic; 5) know the trend of stepping-stone intrusion detection techniques, and solve real-world cybersecurity problems by using stepping-stone intrusion detection techniques.

We are facing lots of challenges to integrate cutting-edge stepping-stone intrusion detection techniques into the cybersecurity curriculum. Since there are tons of cutting-edge stepping-stone intrusion techniques developed in the last two decades, the first challenge would be which techniques should be selected to train students. The cutting-edge stepping stone intrusion detection techniques not only provide students with the knowledge to protect their own computer systems, but also equip them with rich ethical hacking skills. The second challenge would be “Should cybersecurity programs teach ethical hacking to their students?” The third challenge is what labs should be included into the curriculum, and how to test these labs.

To meet the challenges and expand the national cybersecurity workforce, we propose an innovative approach to integrate the cutting-edge stepping-stone intrusion detection techniques suitable to undergraduate students into the cybersecurity curriculum. We will carefully and comprehensively survey and review all such techniques developed in the last two decades. In this project, we plan to develop five content modules and ten hands-on lab exercises to enhance students’ engagement and improve their hands-on learning experience in cybersecurity.

The proposed project will greatly benefit the cyber community and CAE institutions. Our course modules and hands-on labs will be shared with the CAE community and other peer institutions in the U.S. through the dissemination approaches proposed in Section 2.6. The outcomes of this project will provide needed resources to help prepare new cybersecurity professionals for our nation’s governmental and private sectors, and military bases. We will also integrate the hands-on labs into our existing NetLab+ server and newly built cybersecurity center (supported by TSYS company) at Columbus State University (CSU). The expanded NETLAB+ server at CSU will benefit the cyber community, students from other institutions by providing them opportunities to get hands-on cybersecurity experience.

By organizing seminars and/or workshops to train cybersecurity professionals with directions from the NSA Regional Resource Center, our modules and hands-on labs will have a huge impact on our local industries, military bases, as well as the nation’s governmental sectors that are in urgent need of qualified cybersecurity professionals. The CAE institutions adopting our modules and hands-on labs for their cybersecurity curricula will make students well-trained in the field of intrusion detection systems and add valuable assets to their cybersecurity program. The hands-on labs designed from cutting-edge research in cybersecurity can help the students at the CAE institutions to engage in cybersecurity research activities at their early stages, resulting in much better trained and equipped cyber experts, and having great advantages over their peer students.