Objectives

We propose this project to integrate hands-on learning experience on cutting-edge stepping-stone intrusion detection techniques into the cybersecurity curriculum. The primary purpose of this project is to expand the national cybersecurity workforce in both quality and quantity, specially to meet the future workforce demands of the U.S. federal government. Should this project be funded by NSA, and adopted by the CAE community and other peer institutions, it would have a great impact on producing more well-trained cybersecurity professionals for the national cybersecurity workforce. Just as GA Governor Nathan Deal stressed in an announcement to invest $50 million in funding to establish the Georgia Cyber Innovation and Training Center in Augusta, GA that “cybersecurity is especially important now that cybercrime is bigger than the global black market for marijuana, cocaine and heroin combined” [NDeal2017]. The Governor also mentioned that since cybercrime continues to grow, the protection of Georgia’s citizens, businesses and institutions in the digital realm is becoming significantly urgent and more necessary.

Cyberattacks and threats are increasingly faced by business, consumers, and all other users of the Internet along with more and more aspects of the national infrastructure depend upon the correct operation of computers, networks, and the Internet [MHill2001]. Some statistics from [IIS2017] show that up to 2015, the individuals using the Internet worldwide can be as high as more than 3 billion users, and the reported global data breaches in the number of internet incidents can reach 1.7 billion at 2015. More individuals and businesses are exposed to cyber threats than ever. We need more well-trained and qualified cybersecurity professionals to protect our nation against existing and potential devastating cyber-attacks. According to a report on Cyberseek [CSeek2017], the total number of employed cybersecurity workforce is 778,402 in the U.S., and the total number of cybersecurity job openings is 348,975 nationally in 2017. The cybersecurity supply/demand heat map [CSeek2017] shows that California, Texas, Georgia, New York, Florida, Illinois, Maryland, and Virginia are among the states having more than ten-thousand cybersecurity job openings. So, educating and training more qualified cybersecurity professionals is more urgent than ever. In this project, we take the approach to integrate the cutting-edge techniques of intrusion detection into our cybersecurity curriculum not only to educate our students to be cybersecurity experts to defend our digital resources, but also to make them be keen of offensive cyber skills. Therefore, the goals for 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 activities proposed in this project, the students will be able to: 1) understand the approaches to establish a connection chain to launch attacks through stepping-stones; 2) 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 the stepping-stone intrusion detection techniques, and solve real-world cybersecurity problems using the stepping-stone intrusion detection techniques[AMcGettrick2013].