Teaching strong security habits through cybersecurity competitions

Team: Rock Stevens, Virinchi Srinivas, Raveesh Mayya, Aditya Acharya, Noam Auslander
Contact: rstevens@cs.umd.edu, raveesh@rhsmith.umd.edu, noamaus@gmail.com, adiarya1a1@gmail.com, virinchimnm@gmail.com

Overview
According to the United States Computer Emergency Readiness Team, the number of reported cybersecurity incidents and vulnerabilities have steadily increased this past decade. Identifying the dire need for improvements in security training and awareness, federal efforts such as the National Initiative for Cybersecurity Education (NICE) exist to accelerate the learning and cyber awareness skills development of the American public. Other programs exist such as capture-the-flag (CTF) competitions which “gamify” security and evaluate competitors’ skills in core competencies essential to offensive and defensive cybersecurity. We propose blending these two approaches to develop methodologies for effectively communicating the impact of strong security habits through cybersecurity CTF competitions. By participating in these competitions, we believe competitors will learn full-spectrum cybersecurity skills and make themselves a more difficult target for hackers. CTFs inherently provide a scoring mechanism for evaluating competitors’ skills; by experimenting with various instructional techniques, we aim to understand which methods yield the highest CTF scores and understanding. Our projected audience is undergraduate and graduate college students, with the belief that instilling sound cyber practices before entering the workforce will build future capacity for the security of our nation. Offering this training to participants for free, we believe we will have a large captive audience willing to learn essential business skills.

Intellectual Merit
The digital arms race between attackers and defenders has been ongoing for over 30 years with no end in sight. The ability for miscreants to reuse old attack tools and methodologies against victims supports the fact that current security awareness training is largely ineffective. Research that will illuminate proven ways to teach strong security habits and understanding will improve the public’s cybersecurity posture and help eliminate the root cause of rudimentary cyber attacks and malware campaigns. Existing cybersecurity competitions are not focused on teaching but simply evaluating. We aim to remedy this problem by leveraging decades worth of first principles from psychology and educational instruction to better connect with our participants.

Broader Impact
Teaching strong security practices through cybersecurity competitions as part of a STEM+C educational program will have wide-reaching impacts throughout our nation. Cultivating a future workforce that is security-savvy will provide businesses with employees that understand threats and are resistant to common attacks like phishing and installing malware. From this same group of security-savvy citizens, the nation will reap the benefits of pioneering new defensive techniques that will ensure America’s continued prosperity in the face of the ever-increasing sophistication of our adversaries.