Revitalizing Cyber Security Education and Research through Competitions

Cyber Security field is adversarial – human defenders and attackers are constantly engaged in a battle of wits, trying to outsmart each other. Problems and defenses evolve at a fast pace due to this dynamics. Yet the way we teach cyber security, and the way we conduct research in this field, mimic education and teaching in other, non-adversarial computer science fields, where problems evolve at a much slower pace.

In education, teachers impart knowledge to students through lectures and textbooks. Some may engage students in practical exercises that demonstrate concepts learned in class. In both cases students learn required materials, and some key skills, but do not get the mastery that comes from independent evaluation of offense and defense options, in adversarial setting. In research, the teams that create defense prototypes are also the ones to perform their evaluation, usually testing straightforward attack scenarios but not the challenging ones. Competing research teams must wait after the original solution is published (which may take time) and after its code is released (which may be never) to evaluate it, uncover potential problems and propose improvements. This makes security research advance at a slow pace, making it uncompetitive against much faster evolving attacks.

Intellectual Merit: We propose to revitalize cyber security education and research by introducing competitive aspects into their current lifecycles. In education, we propose to create, deploy and evangelize light-weight, online and diverse Class Capture-The-Flag (CCTF) exercises. These will pit teams of students taking a security class against each other on the DeterLab testbed. Competitions will be light-weight, requiring modest preparation and engagement. Students will engage in competitions remotely, at any time convenient for both teams, which will enable wide participation. Our competitions will be diverse, covering a broad range of security topics, such as infrastructure threats and defenses (routing, DNS), denial-of-service, botnet detection and infiltration, etc. Competitions will occur multiple times during a semester and will involve students from different institutions, alternating between an attacker and a defender role. Repeated exposure will enable students to continuously improve their cyber security skills, learn from their mistakes and acquire real mastery of the material. To address ethical concerns about teaching students offensive technologies, we will develop online materials on ethical offense, and will require each participant to view the materials and pass the related quiz before engaging in competitions. We will further create educational modules that cover topics related to each CCTF exercise, to facilitate participation by underprivileged and minority institutions that may not regularly teach a security class.

We propose to revitalize cyber security research by creating the Security Challenge portal, where researchers can challenge others to break their research prototypes experimentally or by design analysis. We will seed this portal with several challenges of our own. We will further develop the Grand Challenge portal, hosting grand challenges in several security sub-fields. We will seed this portal by organizing virtual workshops with experts in selected sub-fields to create the initial grand challenges. Both security challenges and grand challenges will introduce competitive aspects into security research.

Broader Impact: Our activities have a potential for tremendous impact on security education and research world-wide. Courses that participate in CCTFs will result in better student learning and engagement, which should over time translate into a larger and more skilled security workforce. Especially, the education modules we will develop to accompany the CCTFs have potential to increase the size of the security workforce, because they will reach student audiences that would not otherwise receive security education. Researchers that engage in security challenges will benefit from having more sound solutions and stronger publications than they would otherwise. Grand challenges will engage multiple teams competing towards the common goal, galvanizing research on that specific class of problems. Further, through teamwork and involvement of multiple research groups in common environment and on common goals, security challenges and grand challenges will organically promote better security metrics, experiment methodologies and code and data sharing. This will improve the quality of security research, and the science of security experimentation.

We will engage in extensive outreach activities to specific target groups that PIs are closely involved with, to promote the products of this research. PI Mirkovic will advertise to current and future DeterLab users, consisting of researchers and educators. PI Pike will perform outreach to institutions involved in CyberWatch West and other underrepresented groups. Jointly the PIs will also advertise the materials developed in this project to a wide community of researchers and educators at conferences and professional meetings.