Project Description

1 Introduction and Motivation

Student exposure to practical, hands-on exercises is critical for cybersecurity curricula. It helps students internalize concepts taught in class, learn to use cybersecurity tools for monitoring, diagnostics, forensics and defense, and learn critical and adversarial thinking. There are many public repositories of homework-type exercises in cybersecurity (e.g., SEED [1], DeterLab [2], EDURange [3], Seattle testbed [4]) and many instructors develop their own materials for the courses they teach. Further, there are many cybersecurity competitions (e.g., Cyber Patriot [5], Cyber Grand Challenge [6], CCDC [7]) that aim to enhance student learning through defense/offense games, and hone adversarial thinking and cybersecurity skills beyond those acquired in the classroom.

While there are multitude of opportunities for students to learn cybersecurity in a practical setting, there is a lack of tools to measure this learning and provide actionable feedback to students and instructors. Measuring learning as students go through a practical cybersecurity exercise and providing early intervention are important for the following reasons:

- **Complexity and dependence on prerequisites:** Cybersecurity brings together many branches of computer science, such as system administration, software engineering, algorithms, formal language theory, operating systems and networking. Cybersecurity builds on these, and it adds its own concepts and skills. Students who have gaps in their foundational knowledge and skills—call “foundations” for short in the rest of the proposal—may experience challenges in practical exercises, and underperform, in spite of having strong understanding of cybersecurity material. If the cause of the student’s poor performance is not detected and mitigated in time, the student may lose confidence and leave the cybersecurity field.

- **Hands-on learning:** Learning in practical exercises often occurs through student-computer interaction, with the instructor observing the final outcome (e.g., a report), perhaps after days or weeks of student work. By that time it is too late to intervene if the student has failed to complete some tasks, and there is little information about what went wrong, e.g., did the student fail to put enough time into the problem, did they lack some foundation, did they miss some key cybersecurity concept, etc.

- **Disadvantaged populations and minorities:** Like many other computer science fields, cybersecurity needs higher participation of disadvantaged populations and minorities. Such populations may have a wider gap in their foundations, but due to their minority status may also be less likely to ask for help of peers or the instructor. The instructor himself may fail to include and encourage minority students, due to unconscious bias. This combination can result in minority students being underserved. It is critical to develop automated methods of assessing and increasing learning, to retain these student populations in the cybersecurity field.

Automated assessment of student learning is a difficult challenge in general and particularly in cybersecurity. This is because moderately advanced cybersecurity exercises are open-ended and exploratory in nature. A student may complete the tasks in many different ways, some of which may be unanticipated by the instructor. It is relatively easy to assess the students who have achieved the final objectives, but it is hard to assess the sophistication of their path to the success. It is also very hard when students fail, to identify where and why their failed, due to the open-ended nature of the activities. In the latter case, it is important to provide useful and timely feedback to students and instructors.

2 Brief Summary of the Proposed Work

We propose to develop ACSLE—a framework for automated assessment of student learning in practical cybersecurity exercises. ACSLE will engage in constant and extensive monitoring of student interaction with the computer, it will be able to correlate these activities with desired learning outcomes. Based on the collected data and based on observation of different student activities on the same practical task, ACSLE will build a knowledge base of successful and unsuccessful paths. Using this knowledge, ACSLE will be able to: (1) identify paths that lead to failure and alert students and instructors in a timely manner, (2) suggest that contain helpful information (3) alert the instructor to provide hints to students who struggle with a task, (4) alert instructors to difficult tasks, where majority of students require help.

Our high-level goals are to:
• Identify students that struggle with a practical exercise early and investigate the cause of failure

• Provide rapid feedback to students, letting them know if they may be on the wrong track and provide useful guidance to bring them back to the track

• Provide assessment information to the instructor, as the exercise is taking place, on the individual and the aggregate student performance in the exercise.

**Intellectual Merit.** Learning practical cybersecurity skills is grossly understudied in literature, even though practical exercises are increasingly being added to curricula across the nation. Our work will uncover reasons that students underperform in these exercises, and it will help identify effective interventions. More generally, the reasons that cause students to underperform in practical exercises may be similar to the reasons that lead testbed users to abandon the testbed after initial registration. Thus our research may help network testbeds retain and better serve their users.

**Broader Impact.** Our activities have a potential for tremendous impact on security education and research worldwide. First, we will integrate ACSLE with our two platforms for cybersecurity exercises - DeterLab and EDURange. This will directly impact around 2,000 students annually that use these platforms to learn cybersecurity. Second, ACSLE will be highly portable to other platforms that, similarly to us, use Linux in practical cybersecurity exercises. Courses that adopt ACSLE will result in better student learning and engagement, which should over time translate into a larger and more skilled security workforce. Third, ACSLE will particularly help retain talent from disadvantaged and minority populations, as it will equip them to complete previously challenging, practical tasks.

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 Weiss and PI Mache will similarly advertise to the EDURange community and CyberWatch West. 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.
References


