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 server 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

[1] Seed. http://www.cis.syr.edu/~wedu/seed/, (accessed December 15, 2016).

[2] Deterlab. http://info.deterlab.net/, (accessed December 15, 2016).

[3] Edurange. http://edurange.org, (accessed December 15, 2016).

[4] Seattle. https://seattle.poly.edu/html/, (accessed December 15, 2016).

[5] Cyberpatriot. http://www.uscyberpatriot.org/Pages/default.aspx, (accessed December 15, 2016).

[6] Cyber grand challenge. https://www.cybergrandchallenge.com/, (accessed December 15, 2016).

[7] National Collegiate Cyber Defense Competition. http://www.nationalccdc.org/.

[8] J. Mirkovic and T. Benzel. Teaching Cybersecurity with DeterLab. *IEEE Security and Privacy Magazine*, 10(1), 2012.

[9] J. Mirkovic and P. A. H. Peterson. Class Capture-the-Flag Exercises. In *Proceedings of the USENIX Summit on Gaming, Games and Gamification in Security Education*, 2014.

[10] Richard Weiss, Michael E. Locasto, and Jens Mache. A reflective approach to assessing student performance in cybersecurity exercises. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, SIGCSE '16, pages 597–602, New York, NY, USA, 2016. ACM.

[11] Richard S. Weiss, F. Turbak, Jens Mache, Erik Nilsen, and Michael E. Locasto. Finding the balance between guidance and independence in cybersecurity exercises. In *Proceedings of USENIX Security: Advances in Security Education Workshop (ASE)*, 2016.

[12] Daniel Manson, Portia Pusey, Mark J. Hufe, James Jones, Daniel Likarish, Jason Pittman, and David H. Tobey. The cybersecurity competition federation. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, pages 109–112, 2015.

[13] J. Mirkovic, A. Tabor, S. Woo, and P. Pusey. Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015. *USENIX Summit on Gaming, Games and Gamification in Security Education*, 2015.

[14] Diana L Burley an dDavid H. Tobey, P Pusey, and M Leary. Mapping Report: Centers of Academic Excellence (CAE) Knowledge Units (KUs) to the National Initiative for Cybersecurity Education (NICE) Knowledge, Skills, and Abilities (KSAs). Technical report.

[15] L R O'Neal, T J Conway, D H Tobey, F L Greitzer, L C Dalton, and P Pusey. SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Behavioral Interview Guidelines by Job Roles. Technical report PNNL-24139.

[16] O'Brien C., Tobey D. H., and Pusey P. Learning and playing: Integrating competition experiences into formal curriculum. *Community College Cyber Summit, Center for Systems Security and Information Assurance*, 2015.

[17] D H Tobey and P Pusey. Cyber defense competition design: A vignette-based method to improve cybersecurity talent management. Conference presentation presented at the Community College Cyber Summit, Center for Systems Security and Information Assurance.

[18] D H Tobey and P Pusey. A practice-based pedagogy for cybersecurity education research. Community College Cyber Summit, Center for Systems Security and Information Assurance.

[19] David H. Tobey, P Pusey, and Diana L Burley. Engaging Learners in Cybersecurity Careers: Lessons from the Launch of the National Cyber League. *ACM Inroads*, 5(1):53–56, March 2014.

[20] Campbell D. J. Task Complexity: A Review and Analysis. *Academy Of Management Review*, 13(1):40–52, 1988.

[21] R Gandhi, D H Tobey, P Pusey, and R Reiter-Palmon. Buffer Overflow Concept Inventory: Pilot Study. Technical Report. UNO-VW-0227020015.

[22] Dirk Ifenthaler. Relational, structural, and semantic analysis of graphical representations and concept maps. *Educational Technology Research and Development*, 58(1):81–97, 2010.

[23] Dirk Ifenthaler, Iskandaria Masduki, and Norbert M. Seel. The mystery of cognitive structure and how we can detect it: tracking the development of cognitive structures over time. *Instructional Science*, 39(1):41–61, 2011.

[24] Sven Fuchs, Angela Carpenter, Meredith Carroll, and Kelly Hale. *A Hierarchical Adaptation Framework for Adaptive Training Systems*, pages 413–421. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[25] Gary Klein and Holly C. Baxter. Cognitive Transformation Theory: Contrasting Cognitive and Behavioral Learning. 2009.

[26] Karen Cooper. Go with the flow: engagement factors for learning in second life. In Robert M. McGraw, Eric S. Imsand, and Michael J. Chinni, editors, *SpringSim*, page 39. SCS/ACM, 2010.

[27] B. S Bloom. Learning for mastery. *University of California press*, 1968.

[28] J. H. Stiehm. US Army War College: Military education in a democracy. *Temple University Press*, 2010.

[29] Travis Mandel and Jens Mache. Practical error correction for resource-constrained wireless networks: Unlocking the full power of the crc. In *Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems*, SenSys '13, pages 3:1–3:14, New York, NY, USA, 2013. ACM.

[30] Travis Mandel and Jens Mache. Developing a short undergraduate introduction to online machine learning. *J. Comput. Sci. Coll.*, 32(1):144–150, October 2016.

[31] E. Kline, M. Beaumont-Gay, J. Mirkovic, and P. Reiher. RAD: Reflector Attack Defense Using Message Authentication Codes. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2009.

[32] A. Viswanathan, A. Hussain, J. Wroclawski, S. Schwab, and J. Mirkovic. A Semantic Framework for Data Analysis in Networked Systems. In *Proceedings of the Networked System Design and Implementation (NSDI)*, 2011.

[33] V. Sharma, G. Bartlett, and J. Mirkovic. *Critter: Content-Rich Traffic Trace Repository*. Workshop on Information Sharing and Collaborative Security (WISCS), 2014.

[34] Richard Weiss, Jens Mache, Vincent Nestler, Ronald Dodge, and Brian Hay. Teaching Cybersecurity Through Interactive Exercises in a Virtual Environment. *J. Comput. Sci. Coll.*, 28(1):159–161, October 2011.

[35] Richard Weiss, Michael Locasto, Jens Mache, and Vincent Nestler. Teaching cybersecurity through games: A cloud-based approach. *J. Comput. Sci. Coll.*, 29(1):113–115, October 2013.

[36] Richard Weiss, Jens Mache, and Michael Locasto. Edurange: Hands-on cybersecurity exercises in the cloud. *J. Comput. Sci. Coll.*, 30(1):178–180, October 2014.

[37] Richard Weiss, Vincent Nestler, Michael E. Locasto, Jens Mache, and Brian Hay. Hands-on cybersecurity exercises and the rave virtual environment (abstract only). In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, SIGCSE '13, pages 759–759, New York, NY, USA, 2013. ACM.

[38] Richard Weiss, Jens Mache, Michael E. Locasto, and Vincent Nestler. Hands-on cybersecurity exercises in the edurange framework (abstract only). In *Proceedings of the 45th ACM Technical Symposium on Computer Science Education*, SIGCSE '14, pages 746–746, New York, NY, USA, 2014. ACM.

[39] Teaching security with interactive exercises, October 2012. Annual Computer Security Conference.

[40] Evan Damon, Julian Dale, Evaristo Laron, Jens Mache, Nathan Land, and Richard Weiss. Hands-on denial of service lab exercises using slowloris and rudy. In *Proceedings of the 2012 Information Security Curriculum Development Conference*, InfoSecCD '12, pages 21–29, New York, NY, USA, 2012. ACM.

[41] Richard Weiss, Michael E. Locasto, Jens Mache, Blair Taylor, and Elizabeth Hawthorne. Teaching security using hands-on exercises (abstract only). In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, SIGCSE '13, pages 754–754, New York, NY, USA, 2013. ACM.

[42] Richard Weiss, Michael E. Locasto, Jens Mache, Elizabeth Hawthorne, and Justin Cappos. Teaching security using hands-on exercises (abstract only). In *Proceedings of the 45th ACM Technical Symposium on Computer Science Education*, SIGCSE '14, pages 736–736, New York, NY, USA, 2014. ACM.

[43] Richard S. Weiss, Stefan Boesen, James F. Sullivan, Michael E. Locasto, Jens Mache, and Erik Nilsen. Teaching cybersecurity analysis skills in the cloud. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, SIGCSE '15, pages 332–337, New York, NY, USA, 2015. ACM.

[44] Stefan Boesen, Richard Weiss, James Sullivan, Michael E. Locasto, Jens Mache, and Erik Nilsen. Edurange: Meeting the pedagogical challenges of student participation in cybertraining environments. In *7th Workshop on Cyber Security Experimentation and Test (CSET 14)*, San Diego, CA, August 2014. USENIX Association.

[45] E. Damon, K. Ganz, C. Humbeutel, M. Crabill, and J. Mache. A comparative analysis of hands-on firewall configuration exercises for the undergraduate classroom. In *Proceedings of the 12th International Conference on Wireless Networks (ICWN)*, 2013.

[46] E. Damon, J. Mache, R. Weiss, K. Ganz, C. Humbeutel, and M. Crabill. Cyber security education: the merits of firewall exercises. In *Emerging Trends in ICT Security*, chapter 31. Springer, 2013.

[47] T. Fendt and J. Mache. Teaching cybersecurity to wide audiences with table-top games. In *Proceedings of the 2014 International Conference on Security and Management (SAM)*, 2014.

[48] A. Kirkland and J. Mache. Tlearnfire: A firewall learning tool for undergraduate cybersecurity courses. In *Proceedings of the 2014 International Conference on Security and Management (SAM)*, 2014.