Integrating Cybersecurity Concepts Across Undergraduate Computer Science and Information Systems Curriculum

Dr. Uma Kannan

Dr. Uma Kannan is Assistant Professor of Computer Information Systems in the College of Business Administration at Alabama State University, where she has taught since 2017. She received her Ph.D. degree in Cybersecurity from Auburn University in 2017. She specialized in Cybersecurity, particularly on the prediction and modelling of insidious cyber-attack patterns on host network layers. She also actively involved in core computing courses teaching and project development since 1992 in universities and companies.

Dr. Rajendran Swamidurai, Alabama State University

Dr. Rajendran Swamidurai is an Professor of Computer Science at Alabama State University. He received his BE in 1992 and ME in 1998 from the University of Madras, and PhD in Computer Science and Software Engineering from Auburn University in 2009. He is an IEEE senior Member and ASEE Member.

Integrating Cybersecurity Concepts Across Undergraduate Computer Science and Information System Curriculum

Abstract
The global Cybersecurity skill gap in 2020 is about 3.1 million and the Cybersecurity staff shortage is about 69%. Universities are waking up to the need for developing skills in Cybersecurity. Though many Universities offer a master's degree in Cybersecurity, it is impractical to fill this huge demand for Cybersecurity through only graduate degree holders. After careful analysis, it has become evident that there is a gap in the curriculum as it relates to training for Cybersecurity concepts in foundational computing courses for students. To be more specific, there is relatively less focus on the infusion of Cybersecurity concepts in undergraduate computing courses and its impact on classroom practices. This paper serves to address this gap by providing an experience in infusing, teaching, and assessing Cybersecurity modules in various undergraduate computing courses that immerse students in real-world Cybersecurity practices through active learning.

1. Introduction

Today, cyber networks (cyberspace and the Internet) are as much a part of the American homeland as our cities, farmlands, mountains, and coastlines. Because they are where we do almost all our day-to-day activities such as shopping, banking, working, playing, learning, to connect with family members, etc., [1]. Cybernetworks are a critical infrastructure for commerce and communications [2] and they are the backbone of our 21st century economy [1]. Cyber networks are also the major nerve center of our national security [1]. Disruptions in networks and lapses in security affect our lives in ways that range from the inconvenient to the life-threatening [2,3].

Cyberspace is vulnerable to an ever-evolving range of threats from criminals as well as nation-state actors. The purpose of cyberattacks span the spectrum of criminal activity, such as identity theft, data theft, espionage, and disruption of critical functions [1]. Attacks can be small-scale, aimed at stealing personal information from unsuspecting citizens' home computers, or large-scale, like the one that took down the CIA (Central Intelligence Agency) website several hours in early February 2012 [2] and Danish shipping company Maersk in 2017, which disrupted their operations for two weeks and cost the company $300 million [4,5]. Cyberattack is a growing threat. In March 2013 Senate hearing, the nation's top intelligence officials warned that "Down the road, the cyberthreat will be the number one threat to the country," eclipsing terrorism [2,3]. The McAfee 2020 report [4] indicates that the monetary loss from cybercrime is $945 billion and the cost of global crime since 2018 is $1 trillion which is a more than 50% increase in the last two years [4,5].

Confidential information about users is collected, processed, and stored in cyberspace by institutions using the Internet as a transport mechanism. According to Massachusetts state officials, nearly one in five residents had personal or financial information stolen in data breaches in 2013 [6]. In 2015, the Office of Personnel Management was hacked, and 21.5 million individual's SF-86 data plus 5.6 million individual's fingerprint records were leaked [7]. Similarly, 147 million Americans' data were exposed in the 2017 Equifax hack [5]. USA Today

reports indicate that about 43% of companies and 47% of adult Americans have been exposed to one or more security breaches [8]. The UNODC (United Nations Office on Drugs and Crime) estimates that the cost of global identity theft is $1 billion per year and the cost of identity theft in the US was $780 million per year. Other kinds of losses by banks in the United States are estimated in the range of somewhere between $300 million and $500 million a year [9].

The 2020 (ISC)² (Association for inspiring a safe and secure cyber world) Cybersecurity Workforce Study [10] estimates that the global cybersecurity workforce needs to grow 41% in the U.S., and 89% worldwide to effectively defend organizations' critical assets. Despite COVID-19 and economic pressures, organizations' plans to increase cybersecurity staffing over the next 12 months remain consistent with previous years [10]. The $(ISC)^2$ report also indicates that 49% of their survey respondents expect their organizations to hire more cybersecurity professionals within the next year [10]. Despite a huge demand for cyber security personnel the industry is facing great challenges to hire sufficient, qualified security personnel and retain them. The global cybersecurity skill gap in 2020 is about 3.1 million [10]. Due to this cybersecurity staff shortage 69% of the ISACA (Information Systems Audit and Control Association) 2020 survey [11] respondents say their cybersecurity teams are understaffed and 56% of the $(ISC)^2$ [10] survey respondents accept their institution is at risk. According to various reports, about 40% of junior-level and over 50% senior and manager level security jobs are vacant and Cyber Security job postings took 8% longer to fill than other IT job postings overall. In a lot of cases, even the people who should know how to do this job and know how to run these systems do not even exist. [12]

One of the challenges faced in addressing cyber workforce issues is the well documented shortage of STEMC (Science, Technology, Engineering, Mathematics, and Computing) graduates with technical proficiency [11]. While STEMC careers in academia and industry are increasingly requiring technical skills for dealing with cybersecurity and information assurance, undergraduate courses in computing, including those offered at Alabama State University, fall short of providing key training to students in cybersecurity that integrate both theory and practice. Equipping students with such skills greatly improves their employability. The U.S. Bureau of Labor Statistics' (BLS's) Occupational Outlook Handbook [13] highlights our claim. This report projects that the employment growth from 2012 to 2022 for information security analysts will be 37%, much faster than the average for all jobs of 11%. The report states that "Demand for information security analysts is expected to be very high as these analysts will be needed to come up with innovative solutions to prevent hackers from stealing critical information or creating havoc on computer networks." Additionally, the (ISC)² Foundation's 2020 Global Information Security Workforce study [10] points out that 3.1 million more cybersecurity professionals will be needed to accommodate the predicted global shortfall.

Industry do not want compliance officers or cybersecurity policy planners, but they want Cybersecurity graduates with technical skills such as secure system design, defense tools creation, and finding and solving software and hardware vulnerabilities [11,16]. The Cybersecurity industry looks the following essential skills from the Cybersecurity graduates: 1) Fundamental knowledge on wide variety of computing courses, such as computer architectures, cryptography, networking, secure coding, secure system development, penetration testing, incidence response, tool development, operating systems internals (such as Linux), and low-level

programming [17-21] and how and the organization's information system operates [22-24], 2) soft skills such as team-work, problem-solving, and communication [25-28], and 3) hands-on training on cyber ranges [29]. Cyber range is an interactive simulated representation of an organization's cyber infrastructure that includes their local networks, systems, tools, and applications that provide a safe and legal environment for learning and testing Cybersecurity operations [30].

To address this serious problem, Alabama State University with the support of Auburn University employed a unique technique called infusing Cybersecurity concepts in various undergraduate computer science and computer information systems courses. Though many Universities offer a master's degree in Cybersecurity, it is impractical to fill this huge demand for Cybersecurity through only graduate degree holders. The following statistics [10] vindicate our decision. In 2020, the IT service industry employed 41% cybersecurity professionals with bachelors' degree. Moreover, this survey also indicates that the employers are planning to fill the 32% of the cybersecurity gap with new university graduates. But ISACA survey indicates that current Cybersecurity curricula is mostly theoretical with very little hands-on training [14] and in a NIST (The National Institute of Standards and Technology) survey 80% of the hiring managers indicate that the current four-year degree is not adequately prepares students for Cybersecurity jobs [15]. We have taken a step in departing from the traditional curricula by orienting undergraduate courses to Cybersecurity practices. This paper presents our two years' experience in adapting and integrating security concepts across the undergraduate computer science and computer information systems curriculum. Our security course modules walked students through producing working solutions by having them perform a series of hands-on exercises developed specifically to apply cutting-edge industry techniques with each course module. We strongly believe that equipping students with such skills greatly improves their employability.

2. Infusing Security Concepts in Existing UG Computing Courses

Universities are waking up to the need for developing skills in Cybersecurity. Several universities now have graduate level courses focused on Cybersecurity. There are evidences of Cybersecurity concepts being integrated in undergraduate computing courses, they are the United States Air Force Academy [31,32] and the NSF-funded projects such as Security Knitting Kit (SecKnitKit) project (Tennessee Technological University) [33], Security Injections project (Towson University) [34], SEED project (Syracuse University) [35,36], and EDURange project (Evergreen State College and Lewis and Clark College) [37]. In addition to Tennessee Tech, the SecKnitKit materials were also disseminated in additional 9 Universities: University of Wyoming, James Madison University, Murray State University, College of St. Scholastica, Fairmont State University, Middle Tennessee State University, University of Central Arkansas, University of North Carolina at Wilmington and University of North Texas [33].

Practical Cybersecurity involves a wide range of subject areas, therefore, the Cybersecurity curricula must concentrate on infusing security concepts in wide variety of computing courses, such as computer architectures, cryptography, networking, secure coding, operating systems, low-level programming, computer literacy, computer programming, web development, database and software engineering [17-21,32-34].

The initial set of courses in which we planned to integrate cybersecurity concepts are chosen using two criteria: suitability of material for pedagogical integration of cybersecurity concepts and impact on all computing and STEM majors. Instructors may eventually choose to expand the integration of methods to other computing courses. The initial set of courses includes: Data Communications and Networks/Computer Networks, Operating Systems, Software Engineering, and Information Security. We used a two-stage process to integrate cybersecurity concepts into computing courses. The first part focused on theoretical and conceptual ideas behind the methods under discussion and the second part had hands-on experimentation.

- ***Computer Networks:*** From Spring 2019 to Spring 2021, we reworked CSC315 Data Communication and Networking, and CIS310 Networking Fundamentals (for computer information systems majors) courses. A firm understanding of Network/Operating System fundamentals is essential to being able to secure a network or attack one. The purpose of these courses is to emphasize covering the fundamental concepts needed to understand computer attacks and defenses from a network perspective. In CSC315 and CIS310 we have introduced many new fundamental topics required for the network and cyber security including 1) Linux, 2) PowerShell, 3) Network Protocols and Standards, 4) network commands widely used in network and cyber security, and 5) network security hands-on experiments using GNS3 (Graphical Network Simulator-3), Wireshark, and Cisco packet tracer.
- ***Operating Systems:*** In spring 2020 and again in spring 2021, we resigned the CSC414 Introduction to Operating Systems (for computer science majors) course by infusing the following security concepts which explains to the students how to protect the operating system from threats. The topics include, 1) command line usage (Linux and DOS), 2) common administrative functions using Microsoft PowerShell, 3) system security, 4) system and network threats, 5) how to use cryptography as a security tools, 6) how to implement security defenses such as Security Policy, Vulnerability Assessment, Intrusion Detection, Virus Protection, Auditing, Accounting, and Logging, and 7) how to harden an operating system (Linux or Windows), 8) firewalling, and 9) hands-on experiments using operating system tools used for security.
- ***Information Security*****:** In Fall 2019 and Fall 2020 we reworked the CIS341/CSC341 Information Security course with an emphasize to infuse those aspects of information technology that are directly relevant to network and application layers security and to provide students the opportunity to obtain Security+ certification and/or Certified Ethical Hacker (CEH) certification. This modified course will leverage topics typically found in Security+ and CEH certification such as scanning networks, denial-of-service attacks, SQL injection, cryptography, penetration testing, threat management, identity management, security risk identification and mitigation, and network access control.

3. Results

From spring 2019 to spring 2021 semesters, Alabama State University faculty developed Cybersecurity modules to infuse into the existing undergraduate computer science and computer information systems courses. After the beta test between spring 2019 to Fall 2020, these Cybersecurity modules went through various updates – some based on student feedback and some due to the change in Cybersecurity industry needs. These modules were evaluated for their effectiveness through pre- and post-tests. In addition, students in all offered classes were asked to

complete a survey pertaining to their coursework, confidence in using Cybersecurity modules in their classes, and strategies they use to learn in their math classes.

3.1. Student Knowledge

Students in each class completed pre- and post-tests to examine changes over the duration of the module implementation. In each class, there were students that failed to complete the pre, post, or both tests. Overall, scores on the pre-tests averaged just 61.82% while averaging 82.96% on the post-tests. The paired t-test result is shown in figure 1. The two-tailed P value for the 95% confidence interval less than 0.0001, by conventional criteria, this difference is extremely statistically significant.

P value and statistical significance:
The two-tailed P value is less than 0.0001
By conventional criteria, this difference is extremely statistically significant.

Confidence interval:
The mean of Test1 minus Test2 equals -21.138
95% confidence interval of this difference: From -27.618 to -14.658
Intermediate values used in calculations:
t = 6.5320
df = 57
standard error of difference = 3.236

Data Summary:

Group	Mean	SD	SEM	N
Test1	61.819	23.626	3.102	58
Test2	82.957	14.708	1.931	58

Figure-1: t-Test Results for Student Knowledge

3.2. Student Academic Efficacy, Motivation and Learning Strategies in Computing Courses

Finally, students were asked to respond to survey items pertaining to their level of academic efficacy, motivation and goals in learning computer science, and strategies that they use and prefer to learn Cybersecurity.

- Academic Efficacy: Students were asked to respond to five items related to their academic efficacy as it pertains to the computing class in which they were enrolled. Overall, students reported a great deal of confidence in their academic abilities with the average for each term above 4 (on a 5-point scale). Students believed that they would learn if they tried, worked hard, and did not give up. They also believed that they could master the skills and figure out the most difficult class work.
- Goals in Computing: While all goals were important to them, students believed that getting a good grade was most important. They also wanted to meet requirements for their degree, improve their ability to communicate math ideas to others, learn new ways of thinking and specific procedures for solving real-world computing problems.
- Preferred Learning Environments: When asked to indicate their perceptions of statements describing different learning environments, students reported the greatest agreement with "the instructor explains the solutions to problems" and "the assignments are similar to the examples considered in class." Students also indicated situations in which they compared their computing knowledge to other students, studied their notes, explained ideas to

others, worked in small groups, and got frequent feedback on their computational thinking. They were less supportive of having the class critique their solutions, exams that prove their skills and group presentations.

- General Learning Strategies Used by Students: In general, students reported using a variety of strategies in their computing classes and not giving up when they get stuck. They most frequently reported finding their own ways of thinking and understanding and reviewing their work for mistakes or misconceptions. They also reported checking their understanding of what a problem is asking, studying on their own and using their intuition about what an answer should be.
- Motivation to learn Cybersecurity - Task Value: Students reported high levels of task value, indicating their belief in the importance and utility of course content in their computing classes. Their understanding of Cybersecurity is extremely important to them and their motivation to learn Cybersecurity is strong.
- Learning Strategy – Critical Thinking: In terms of learning Cybersecurity, students reported many strategies that require critical thinking. They reported developing their own ideas based on course content and evaluating the evidence before accepting a theory or conclusion. They also reported questioning what they read or hear in class and thinking or possible alternatives.
- Learning Strategy – Self-Regulation: Students reported using many effective self-regulation strategies in their computing classes. In particular, they pay careful attention to concepts that they find confusing and focus on studying and reviewing these, so they learn them.
- Learning Strategy – Time and Study Environment Management: Another positive strategy reported by students related to the management of their time and study environment. They reported attending class regularly, finding a place to study and keeping up with the weekly readings and assignments.

The reliability of these scales was generally supportive, with internal consistency estimates ranging from .491 to .926, with a median of .867. Perceptions were also very positive as overall scale means exceeded the scale midpoints. A more detailed summary of items from these scales are shown in Table 1.

TABLE I. STUDENT ACADEMIC EFFICACY, MOTIVATION AND LEARNING

Measurement Scale	**Items**	**Reliability**	**Mean (SD)**
Academic Efficacy[a]	5	.864	4.16 (.8)
Goals in *Computing*[b]	10	.920	4.26 (1.13)
Preferred Learning Situations[c]	11	.869	5.42 (1.56)
Learning Strategies used in class (general)[d]	15	.890	5.35 (1.43)
MSLQ- Motivation - Task Value[e]	6	.909	5.71 (1.21)
MSLQ – Critical Thinking[e]	5	.888	5.05 (1.46)
MSLQ – Self-Regulation[e]	11	.821	5.049 (1.45)
MSLQ – Time and Student Environment Management[e]	8	.491	4.87 (1.61)
a=5-point scale (1=Strongly Disagree…5=Strongly Agree) b=7-point scale (1=Not at all important …7=Extremely important) c=7-point scale (1=Strongly Disagree…7=Strongly Agree) d=7-point scale (1=Very Seldom…7=Very Often) e=7-point scale (1=Not True of Me…7=Very True of Me)			

4. Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant Number 1818722.

5. Conclusions

We have created about 30 one-week Cybersecurity modules and infused them into four existing core undergraduate computing courses over a period of three years. The modules were taught using examples that were worked through interactively during class. The students then worked on assignments that incorporated the new Cybersecurity instructional concepts. We have evaluated the Cybersecurity modules effectiveness through pre- and post-tests, and surveys. The paired-samples t-test results show that matched pre-post student knowledge is statistically significant. Regarding confidence in using Cybersecurity modules in class, we had significantly positive results. Students' perception was very positive as overall scale means exceeded the scale midpoints. We feel the courses were a success but indicated there was room for improvement.

References

1. Jeh C. Johnson, Let's pass cybersecurity legislation, http://thehill.com/opinion/op-ed/217151-lets-pass-cybersecurity-legislation
2. Cyber Security and Network Reliability, https://www.fcc.gov/encyclopedia/cyber-security-and-network-reliability
3. Cyber Security Primer, http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm
4. Zhanna Malekos Smith and Eugenia Lostri, "The Hidden Costs of Cybercrime," McAfee Report 2020
5. Tonya Riley, "The Cybersecurity 202," The Washington Post, Dec. 7, 2020, https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/
6. Kyle Alspach, Local cybersecurity startups grow into IPO contenders, September 11, 2014, http://www.bostonglobe.com/business/2014/09/11/amid-expanding-hacking-threat-local-cybersecurity-startups-grow-into-ipo-contenders/6diHyy7YhZOqEAbQXOw4MI/story.html
7. https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/
8. 2 stores, 100M hacks. Where's cybersecurity? Our view, The Editorial Board, 7:42 p.m. EDT September 14, 2014, http://www.usatoday.com/story/opinion/2014/09/14/home-depot-target-data-breach-credit-card-editorials-debates/15642867/?utm_source=feedblitz&utm_medium=FeedBlitzRss&utm_campaign=news-opinion
9. The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies and McAfee, July 2013
10. Cybersecurity Professionals Stand Up to a Pandemic, (ISC)2 Cybersecurity Workforce Study, 2020
11. State of Cybersecurity 2020, https://www.isaca.org/go/state-of-cybersecurity-2020.
12. (ISC)² 2015 Global Information Security Workforce Study
13. The U.S. Bureau of Labor Statistics's (BLS's) Occupational Outlook Handbook, http://www.bls.gov
14. Preparing Cybersecurity Professionals to Make an Impact Today and in the Future, ISACA Headquarters, August 1, 2017, Agency Docket Number – 170627596-7596-01, Docket Number – 2017 - 14553
15. National Initiative for Cybersecurity Education, "Workshop on Cybersecurity Workforce Development: Notes from Panel Discussions," August 2, 2017, https://www.nist.gov/sites/default/files/documents/2017/09/28/chicago_workshop_summary_notes.pdf.
16. Franklin S. Reeder and Katrina Timlin, Recruiting and Retaining Cybersecurity Ninjas (Washington, DC: CSIS, October 2016), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/161011_Reeder_CyberSecurityNinjas_Web.pdf.

17. George I. Seffers, “National Security Agency Program Fills Critical Cyber Skills Gaps,” Signal Magazine, June 1, 2014, https://www. afcea.org/content/national-security-agency-program-fills-critical-cyber-skills-gaps
18. Chris Krebs, “Why So Many Top Hackers Hail from Russia,” Krebs on Security, June 22, 2017, https://krebsonsecurity.com/2017/06/why-so-many-top-hackers-hail-from-russia/
19. Intelligence and National Security Alliance, Cyber Intelligence: Preparing Today’s Talent for Tomorrow’s Threats (Arlington, VA: September 2015), https://www.insaonline.org/wp-content/uploads/2017/04/INSA_Cyber_Intel_PrepTalent.pdf
20. Workforce Intelligence Network for Southeast Michigan, Cybersecurity Skills Gap Analysis (Michigan: July 2017), https://winintelligence.org/wp-content/uploads/2017/07/ FINAL-Cybersecurity-Skills-Gap-2017-Web-1.pdf
21. Laura Lee, “Circadence responses to NIST RFI on Cybersecurity workforce education or training,” August 2, 2017, https://www.nist.gov/sites/default/files/documents/2017/08/02/circadence.pdf
22. Evans and Reeder, A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Nov 2010, Center for strategic & International Studies
23. Martin C. Libicki, David Senty, and Julia Pollak, H4ackers Wanted: An Examination of the Cybersecurity Labor Market (RAND, 2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf
24. Homeland Security Advisory Council, CyberSkills Task Force Report (Washington, DC: Fall 2012), https://www.dhs.gov/sites/default/files/publications/HSAC%20Cy- berSkills%20Report%20-%20Final_0_0.pdf
25. John Costanzo, Bridging the Cybersecurity Talent Gap in Hampton Roads (Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance, July 2017), http://securitybehavior.com/hrcyber/doc/HRCyber%20Mid-Project%20Report. Pdf
26. Ray Lapena, “Survey Says: Soft Skills Highly Valued by Security Team,” Tripwire, October 17, 2017, https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/
27. Arthur Conklin, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development – Request for Information Response,” August 3, 2017, https:// www.nist.gov/sites/default/files/documents/2017/08/03/university_of_houston_center_for_information_security_research_and_ed- ucation.pdf
28. Sara Castellanos, “Cybersecurity Requires ‘Insatiable’ Problem-Solving Skills; Technical Skills Can Be Taught,” Wall Street Journal, May 24, 2018, https://blogs.wsj.com/cio/2018/05/24/cybersecurity-requires-insatiable-problem-solving-skills-technical-skills-can-be-taught/
29. https://www.csis.org/analysis/cybersecurity-workforce-gap
30. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf
31. Cynthia E. Irvine, Shiu-Kai Chin, and Deborah Frincke. 1998. Integrating Security into the Curriculum. Computer 31, 12 (December 1998), 25–30. DOI: https://doi.org/10.1109/2.735847
32. Gregory White, “Security across the curriculum: using computer security to teach computer science principles,” January 1996, USAF Academy, CO.
33. Ambareen Siraj, Blair Taylor, Siddarth Kaza and Sheikh Ghafoor, "Integrating Security in the Computer Science Curriculum," ACM Inroads 2015 June, Vol. 6, No. 2
34. Ambareen Siraj, Blair Taylor, Siddarth Kaza and Sheikh Ghafoor, "Integrating Security in the Computer Science Curriculum," ACM Inroads 2015 June, Vol. 6, No. 2
35. Wenliang Du and Ronghua Wang, "SEED: A Suite of Instructional Laboratories for Computer Security Education,” (Extended Version) In The ACM Journal on Educational Resources in Computing (JERIC), Volume 8, Issue 1, March 2008.
36. Du, W. “The SEED Project: Providing Hands-on Lab Exercises for Computer Security Education.” IEEE Security and Privacy Magazine, September/October, 2011.
37. Stefan Boesen, Richard Weiss, James Sullivan, Michael E. Locasto, Jens Mache, and Erik Nilsen. 2014. EDURange: meeting the pedagogical challenges of student participation in cybertraining environments. In Proceedings of the 7th USENIX conference on Cyber Security Experimentation and Test (CSET'14). USENIX Association, USA, 9.