4-1-2013

Enhancing the Interdisciplinary Curriculum in Cybersecurity by Engaging High-Impact Educational Practices

Li-Chiou Chen
Seidenberg School of CSIS, Pace University

Andreea Cotoranu
Seidenberg School of CSIS, Pace University

Final Project Report

Enhancing the Interdisciplinary Curriculum in Cybersecurity by Engaging High-Impact Educational Practices

Cornerstone: III. Interdisciplinary Informatics

Principal Investigators:
Li-Chiou Chen, Seidenberg School of CSIS
Andreea Cotoranu, Seidenberg School of CSIS

April 15, 2013

Project Objectives

The project aims at 1) enhancing the active learning experiences of Pace University undergraduate students interested in studying cybersecurity, and 2) performing a needs assessment and evaluation of the current undergraduate cybersecurity curriculum at the University.

Proposed Activity I: Participate in Regional or National Cybersecurity Competitions
Outcome: This activity will contribute to increasing student awareness of cybersecurity topics, and to stimulating interest in pursuing studies and careers in this field.

A team of nine students participated in the **2012 Northeast Collegiate Cyber Defense Competition (NECCDC)**, a popular and highly-regarded cyber competition funded by both the federal government and the private sector. The 2012 competition was organized by Northeastern University and hosted by EMC. The three day event (March 9-11, 2012) took place outside of Boston, in Franklin, MA.

The student team trained for six consecutive weeks prior to the event. Each student selected a set of systems/services to investigate. Questions and problems were provided for practice purposes. A virtual network infrastructure, emulating the competition network, was set up in the Security Laboratory (G321) on the Pleasantville campus so that students could experiment in a network environment similar to the competition environment. There were one-hour weekly sessions to discuss progress on independent student research, address questions, and provide direction for next steps. Some network administration work was completed during these one-hour meetings. However, in order to prepare for the event, the students had to invest numerous hours in individual and/or small group work, outside these weekly meetings.

During the three days of competition time (nearly 20 hours), the student team simulated a group of new employees brought in to secure, maintain and manage the small business network of World Wide Financial, a fictitious company. The students had to respond to routine business tasks while defending against a live Red Team that attacked their systems. In addition, the team had to maintain a set of critical services (e.g. email server, e-commerce site, etc.). This was hardly an easy exercise, but the students found it to be a unique learning experience.

Participating cyberwarriors included: A. Abramson (CS/Freshman/PLV), C. Carvalho (IT/Junior/PLV), M. Kowtko (IT/Sophomore/PLV), M. Hernandez (IT/Senior/PLV), A. Llewelyn (CS/Junior/PLV), P. Prescott (IT/Freshman/PLV), M. Wagner (CS/Senior/PLV), D. Wallach (IS/Freshman/PLV), C. White (IT/Junior/PLV).

In addition to the cybersecurity exercise, the students had the opportunity to network with cybersecurity practitioners from companies like EMC, RSA (the security division of EMC), the Space and Naval Warfare Systems Command (SPAWAR), the Federal Bureau of Investigation (FBI), the United States Army Intelligence and Security Command (INSCOM) as well as with students and faculty from participating institutions.

Participating institutions included: Alfred State College, Champlain College, Harvard, Northeastern, Pace, Rochester Institute of Technology, Stevens Institute of Technology, University of Buffalo, University of Maine, UMass Boston, University of New Hampshire, and Worcester Polytechnic Institute.

Progress: This activity is finalized. A meeting was held after the competition to debrief on the experience. Students provided feedback and made recommendations for improvement in future competitions.

An online questionnaire was administered to all 14 students who participated in the 2011 and 2012 NECCDC exercises. All participants were undergraduates. The purpose of the questionnaire was to determine students' perceptions relative to their experience with the NECCDC exercise, and how it has shaped their knowledge, skill, and motivation to pursue a course of study, and a career as cybersecurity professionals.

Ten students answered the questionnaire. The results are summarized below, and the findings support the hypothesis that competitions have a high impact on the students' perception relative to pursuing an education/career in cybersecurity, and expanding their knowledge of the domain.

- The ten respondents were from the following majors: computer science (5), information technology (3), information systems (1), and criminal justice (1). Nine were male and one was a female. The distribution by year of study is as follows: first year (1), junior (4), and senior (5).

- Out of the ten respondents, only one did not take a college course with a cybersecurity component. However, the majority took one, two or three courses from the undergraduate "Security Track": Overview of Information Security (8), Network and Internet Security (7) and Computer Forensics (7).

- All ten respondents participated in activities/programs with a cybersecurity component: competitions (9), federal scholarship programs (7), internships (5), guest speaker series (5), independent projects (4), professional organizations membership (4), conferences (4), and independent research (3).

- In addition to participating in the NECCDC, three also participated in the 2011 Cyber Security Awareness Week Competition (CSAW) at NYU-Poly.

- Six respondents devoted over 15 hours to prepare for the NECCDC, while three devoted between 5 hours and 15 hours. Only one respondent devoted less than 5 hours to preparing for the exercise.

- In regard to the NECCDC:
    - All ten respondents "Strongly Agreed" and "Agreed" that the exercise *"introduced [them] to new concepts, tools, and techniques that strengthened [their] expertise"* and that it *"motivated [them] to take cybersecurity courses."*
    - Nine of the ten respondents "Strongly Agreed" and "Agreed" that the exercise *"enhanced [their] ability to work in a team to accomplish a common goal,"* and *"motivated [them] to pursue a career as a cybersecurity professional."*
    - Eight of the ten respondents *"Strongly Agreed" and "Agreed" that the exercise "allowed [them] to apply concepts, tools and techniques acquired through coursework or independent projects, to a real works situation."*
    - Eight of the ten respondents expressed an "*interest in participating in similar exercises in the future;"* two were neutral.
    - Only four respondents agreed that the exercise *"enhanced [their] ability to communicate in a business-like environment, both verbally and in writing,"* while five were neutral and one disagreed with the statement.

- In regard to the impact of curricular and co-curricular activities on students:
    - Respondents conveyed that the following had the *highest impact on motivating them to pursue a career in cybersecurity*: internships (7.8/10), competitions (7.7/10), and faculty mentorship/advising (6.9/10). The following were considered to have a slightly *lower impact* (6.7/10): independent projects, independent research, and guest speaker talks. In contrast to co-curricular activities, coursework was ranked as the lowest motivator (6.1/10).
    - Respondents further conveyed that internships (8.3/10) and competitions (8.1/10) had the *highest impact on enhancing their cybersecurity knowledge*. A *lower impact* (7/10) was recorded for independent research and independent projects. In contrast to co-curricular activities, coursework was deemed to have a lower impact (6.8/10).

A review of the topics tested in the competition, how these topics fit into our current undergraduate cybersecurity curriculum, faculty observations, and student comments have been summarized and curriculum recommendations were highlighted. The report will be shared with the IT and CS curriculum committees for discussion.

The recommendations will be discussed in the same context as the 2013 Knowledge Unit requirements for Center of Academic Excellence in Information Assurance/Cyber Defense designation. The designation is supported by the National Security Agency and the Department of Homeland Security. The cybersecurity curriculum will be aligned with these knowledge units starting with Fall 2013.

Proposed Activity II: Design Virtual Lab Exercises
Outcome: This activity will contribute to expanding students' theoretical and practical knowledge, and to enhancing their ability to analyze and solve cybersecurity problems.

Progress: A set of practice questions/problems on various networking and system administration topics has been developed in Spring 2012. The students completed these problems in preparation for the 2012 NECCDC. The practice questions/problems are currently available to interested students by request, and it is our intent to make them available online by Fall 2013. In addition, the students acquired skills and knowledge needed in their respective cybersecurity classes and practiced their skills on a Linux virtual machine (available in http://csis.pace.edu/~lchen/sweet/) and a CISCO router simulator.

Proposed Activity III: Careers with the Federal Government
Outcome: This activity will contribute to increasing student awareness of career prospects with the federal government, and of federal employment requirements.

Progress: The nine students who participated in the 2012 NECCDC had the opportunity to network with representatives from federal agencies including the Space and Naval Warfare Systems Command (SPAWAR), the Federal Bureau of Investigation (FBI), and the United States Army Intelligence and Security Command (INSCOM).

For a broader impact, we discussed career opportunities with the federal government and security clearance requirements for employment at the Computer Club, and various classes, including CIT251 Computer Security Overview, CIT352 Internet and Network Security, CIT354 Computer Forensics, and in CIS 101 Introduction to Computing (which includes a module in cybersecurity awareness). We also expanded the outreach to prospective students attending special interest tours; this audience included high-school and transfer students interested in computing, criminal justice, or both. We estimate that the total number of students impacted by this activity is about 100.

Impact on Students

There were approximately 110 students directly impacted by the activities related to this project; these include participants in the NECCDC exercise and attendees on various talks touching on careers with the federal government and requirements for security clearance. However, we expect that the lessons learned at the curricular and teaching/mentoring level will impact all undergraduate students studying cybersecurity at Pace University.

Impact on Faculty

The impact of the project is limited to Pace/Seidenberg faculty, particularly those teaching cybersecurity courses, and those involved with the cybersecurity scholarship programs. Based on the project activities, the PIs learned about various aspects that could improve the School's cybersecurity curriculum. First, the activities provided students with excellent opportunities to apply the skills and knowledge acquired in the classroom to solving problems "hands-on." Those who participated in the project activities shared their experience with their fellow classmates and thus stimulated

discussion and raised interest in the subject matter. Second, the PIs had the opportunity to examine the content of the cybersecurity courses. A better integration of practical experience with the course content is being reviewed in an effort to provide recommendations for developing new cybersecurity courses.

Conclusion

The project met its objectives through the proposed activities. The project furthers the Thinkfinity cornerstone, interdisciplinary informatics, though its emphasis on cybersecurity education; cybersecurity is an interdisciplinary domain.

Elements of the project will continue to be supported through current and future grants. For example, we were awarded a capacity building grant from the National Science Foundation in 2012 which will allow us to continue our focus on high-impact educational practices such as independent research and independent projects at the undergraduate level, as well as to reach out to prospective transfer students from partner colleges.

In addition, other current and future awards from the National Science Foundation and the Department of Defense will allow the PIs to focus on enhancing the experience of students studying cybersecurity through high-impact educational practices, including but not limited to faculty mentoring and advising, internships, competitions, guest speakers and conference participation.