Pace University
DigitalCommons@Pace

Cornerstone 3 Reports : Interdisciplinary Informatics

The Thinkfinity Center for Innovative Teaching, Technology and Research

5-1-2012

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

Follow this and additional works at: http://digitalcommons.pace.edu/cornerstone3

Part of the Computer Engineering Commons

Recommended Citation
Chen, Li-Chiou and Cotoranu, Andreea, "Enhancing the Interdisciplinary Curriculum in Cybersecurity by Engaging High-Impact Educational Practices" (2012). *Cornerstone 3 Reports : Interdisciplinary Informatics.* Paper 76.
http://digitalcommons.pace.edu/cornerstone3/76

This Report is brought to you for free and open access by the The Thinkfinity Center for Innovative Teaching, Technology and Research at DigitalCommons@Pace. It has been accepted for inclusion in Cornerstone 3 Reports : Interdisciplinary Informatics by an authorized administrator of DigitalCommons@Pace. For more information, please contact rracelis@pace.edu.

Mid-Project Progress 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

June 1, 2012

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 **Northeast Collegiate Cyber Defense Competition (NECCDC)**, a regional event that is one of the most popular and highly-regarded cyber competitions. The 2012 competition was organized by Northeastern University and hosted by EMC. The event took place outside of Boston (Franklin, MA) in early March (March 9-11, 2012).

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

During the three days of competition time (nearly 20 hours), the student team simulated a group of new employees brought in to secure, manage, and maintain 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 they also 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 (9) included: Ariana Abramson (CS/Freshman/PLV), Christopher Carvalho (IT/Junior/PLV), Marc Kowtko (IT/Sophomore/PLV), Marcus Hernandez (IT/Senior/PLV), Allison Llewelyn (CS/Junior/PLV), Patrick Prescott (IT/Freshman/PLV), Max Wagner (CS/Senior/PLV), David Wallach (IS/Freshman/PLV), Christopher 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.

A meeting was held after the competition to debrief on the experience. Students provided feedback and made recommendations for improvements in preparing for future competitions.

Progress: This activity was completed. An online questionnaire was administered in late May 2012 to all students who trained for, and participated in, the 2011 and 2012 NECCDC exercises. The purpose of the questionnaire is to determine the 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. The results of the questionnaire will be analyzed in Summer 2012.

A review of the topics tested in the competition, how these topics fit into our current undergraduate cybersecurity curriculum, faculty observations, and student comments will be summarized in a report highlighting curriculum recommendations. The report will be forwarded to the Seidenberg faculty for discussion in Fall 2012/Spring 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. Students used these items in preparation for the 2012 NECCDC. The collection of items will be revised and finessed in Summer 2012.

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 will host a set of talks tailored to first and second-year Pace students to discuss career opportunities with the federal government as well as security clearance requirements for employment in Fall 2012.

Impact on Students:

As of June 1, 2012, there were only nine students directly impacted by the activities related to this project.

Impact on Faculty:

As of June 1, 2012, there was no impact on faculty (it excludes the PIs of this project).

Next Steps:

- Assess the impact of the project activities on students. Data collected via the online questionnaire will be analyzed to determine the 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. (Summer 2012)

- Offer talks to first and second-year Pace students to discuss career opportunities with the federal government, as well as security clearance requirements for employment.(Fall 2012)

- Evaluate Pace's Cybersecurity formal curriculum and co-curricular activities (Fall 2012)

- Disseminate project results at internal/external academic conferences.(Spring 2013)