Cybersecurity Education using Open Source Software and Academic/Industry Partnerships

Aparicio Carranza, PhD[1] and Casimer DeCusatis, PhD[2]
[1]New York City College of Technology - CUNY, USA, acarranza@citytech.cuny.edu
[2]Marist College, USA, casimer.decusatis@marist.edu

Abstract* - *The growing number and variety of computer security threats has led to an increased interest in cybersecurity education, and the exploration of novel approaches to undergraduate courses in this field. We discuss a new approach for training nontraditional and under-represented students at The City University of New York. Learning objectives, class resources, and results of recent student information security projects will be presented. We also discuss opportunities for academic and industry partnership collaboration with the New York State Cloud Computing and Analytics Center at Marist College.

***Keywords* - Cybersecurity, Flipped Classroom, Cloud**

I. INTRODUCTION

With the growing importance of cloud computing, cybersecurity has received increasing attention. The rapid growth in this field has created a shortage of practitioners with an information security background, as emphasized by a recent National Science Foundation workshop on undergraduate education [1]. There have been several reports on the need to reform engineering and computer science education, as well as reports on the transformative power of early curriculum redesign efforts in this field [2, 3]. However, it is difficult to prepare students for careers in a field which is changing as quickly as cybersecurity.

In this paper, we discuss an approach to providing undergraduate training through an elective course in cybersecurity for computer engineering technology students. This approach uses a version of the flipped classroom approach based on open source software. The so-called flipped classroom is a pedagogical model in which the typical lecture and homework elements of a course are reversed [4]. The term is widely used to describe almost any class structure that provides students with resources (*such as text books or websites*) which are to be studied prior to regular class meetings. This approach attempts to replace traditional lecture periods with a working environment in which students ask questions to clarify their understanding of the class resources and interact with their peers in hands-on activities.

Instructors do not present a traditional stand-up lecture, rather they function more like coaches or advisors, encouraging students to pursue their individual interests. Students are encouraged to interact with the university's academic and industry partners to explore this work, which has also been presented at local technical workshops. This approach draws from educational concepts including active learning, student engagement, and hybrid course design.

In a traditional lecture, students often try to capture what is being said at the same instant the speaker makes a comment. In a flipped classroom, students control the rate at which they absorb and reflect upon new materials. This approach may be particularly effective for students with accessibility concerns, or for whom English is a second language. Devoting class time to conceptual understanding may give instructors a better chance to observe and correct student errors. Student roles change as well, as they become more active participants in their own learning experience. The flipped model gives students more opportunities to experiment, while placing more of the responsibility of learning on the student. Students and instructors may be uncomfortable in these new roles, or may not appreciate the value of hands-on exercises. On the other hand, when a flip is done well, it can shift the priorities of the class towards the achievement of deeper insight and understanding.

This program was recently piloted at the New York City College of Technology (City Tech), an open admission college which is part of the City University of New York (CUNY) system. Students enter with widely disparate levels of academic preparation, professional goals, and personal circumstances. Baccalaureate programs are experiencing rapid enrollment growth; at present, 33.7% of all students are enrolled in baccalaureate programs. Fall Semester 2013 student enrollment was 16,803, of whom 35% attended part-time. Approximately 31.5% of students self-identified as Black (non-Hispanic), 33.8% as Hispanic, 20 % as Asian/Pacific Islander, 11.3% as White, 0.6% as Native American, and 2.8% as "Other". Sixty-one percent (61%) reported a household income of less than $30,000. Eighty percent (80%) of incoming first-year students and 65% of returning students received need-based financial aid. Sixty-seven percent (67%) are the first in their families to attend college. The student body reported 138 different countries of origin; countries of origin of faculty also span the globe. Nineteen percent (19%) of students reported working 20 or more hours per week. The college is a federally designated Hispanic Serving Institution (HSI).

The primary goal for CUNY students concentrating on cybersecurity is to provide the background necessary to enable them to become successful information technology (IT) practitioners, including information security administrators, architects, and testers, within the context of a broader knowledge of computer engineering. We are particularly interested in local job opportunities in the nearby Wall Street financial district. Students are expected to achieve a basic understanding of cybersecurity principles and best practices, understand recent information security breaches, and gain hands-on experience with penetration testing environments.

The required textbook for the cybersecurity class is *Penetration Testing: A Hands-On Introduction to Hacking* by G. Weidman (2014) [5]. The course does not assume any prior knowledge of Windows, Linux, or computer networking, although an introductory programming course is prerequisite (such as C or C++). As a supplemental text, the course also uses *Applied Information Security, a Hands-on Guide to Information Security Software* by R. Boyle and J. Proudfoot (2014) [6]. The supplemental text is used primarily for teaching Windows security and command line management techniques. The course was offered for the first time in 2014, with an enrollment of 22 junior and senior students.

For the first two weeks of the course, students receive instruction on how to set up a VMWare virtual environment which is used for the rest of the course, including an introduction to Kali Linux, a Debian-based distribution that comes with a wide range of pre-installed security tools. In addition to lab assignments, students complete two case studies during the semester. Each case study is a short paper (typically 5 pages, though there is no upper limit) on a topic approved by the instructor which is of interest to the student. Some recent topics include the following:

Cryptographic validity in network security [7] – This project studies the prevention of man-in-the-middle attacks using cryptography. Simulations using Cryptographic Analysis Engine (CAE) compared different ciphers (simple, block, keyword, permutation, and Vigenere), and studied DES-based encryption methods.

Penetration testing with Kali Linux [8] - This project creates a virtual penetration testing environment using Kali Linux, and compares its performance of five different operating systems to perform penetration testing **(**Windows 7, Windows 8, Ubuntu 14.04, CentOS and Kali Linux 1.0.6.). Tools such as MetaSploit and Armitage are used to perform all exploits, Zenmap to access attacking information and Johnny to crack user passwords.

CloudStack vs OpenStack Comparison [9] – This project studies infrastructure as a service (IaaS) cloud computing security features of Apache CloudStack 4.4.0 and OpenStack (Icehouse release), two of the leading open source cloud middleware systems.

This program appears to be particularly well suited to engaging nontraditional and under-represented students because of its practical, hands-on focus and engagement with other academic and industry partners. The curriculum does not require extensive prerequisites, and can be deployed quickly at very low startup cost in an isolated, inherently secure student training environment. Further, students have an opportunity to interact with their peers at other colleges through our collaboration with the New York State Cloud Computing and Analytics Center at Marist College, which enables academic and industry partnerships related to cloud computing, cybersecurity, and software defined environments [10-12]. Undergraduate students from the CCAC have already contributed to OpenStack and other programs, and will shortly launch a multi-course series leading to a specialization in cybersecurity for computer science majors.

REFERENCES

[1] National Science Foundation Cybersecurity Workshop, George Washington University, Arlington, VA (February 24-25, 2014)

[2] A. Corno, "Evolution of the network engineer job role", Proc. 2014 Annual Meeting of the Association of Technology Management and Applied Engineering (ATMAE), St. Louis, MO (November 20-22, 2014) https://atmae.site-ym.com/?page=AnnualConference

[3] L.C. Wilcox and M.S. Wilcox, "A review and evaluation of engineering education in transition", IEEE Proc. 8th international conference on computer science and education (ICCSE), Sri Lanka (April 2013)

[4] J. Bishop and M. Verleger, "The flipped classroom: a survey of research", paper 6219, Proc. 120th annual ASEE annual conference and exposition, Atlanta, GA (June 23-26, 2013)

[5] G. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*, 2nd edition, No Starch Press, San Francisco, CA (2014)

[6] R. Boyd and J. Proudfoot, *Applied Information Security, a Hands-on Guide to Information Security Software* Prentice Hall, NY (2014)

[7] H. Carranza, A. Carranza "Cryptographic validity in network security", Proc. IEEE Mid-Hudson Section Workshop on Advanced Technology for Next Generation Computing, State University of New York, New Paltz (November 6, 2014)

[8] S. Zafar, A. Carranza, "Penetration testing using Kali Linux within VMware virtual networks", Proc. IEEE Mid-Hudson Section Workshop on Advanced Technology for Next Generation Computing, State University of New York, New Paltz (November 6, 2014)

[9] D. Piure, A. Florez, and A. Carranza, "Cloudstack and Openstack battle for network storage", Proc. IEEE Mid-Hudson Section Workshop on Advanced Technology for Next Generation Computing, State University of New York, New Paltz (November 6, 2014)

[10] C. J. Sher-DeCusatis and C. DeCusatis, "Developing a software defined networking curriculum through industry partnership", Proc. ASEE Annual Meeting, Hartford, CT (April 3-5, 2014)

[11] C. DeCusatis and P. Mueller, "Virtual firewall performance as a waypoint on a software defined network", Proc. IEEE 6th International Symposium on Cyberspace Safety and Security (CSS), part of the International Conference on High Performance Computing and Communications (HPCC), Paris, France (August 20-22, 2014)

[12] C. DeCusatis, R. Cannistra, and L. Hazard, "Managing multi-tenant services for software-defined cloud data center networks", Proc. 6th annual IEEE international conference on Adaptive Science & Technology (ICAST 2014), Covenant University, Nigeria (October 29-31, 2014)