Enhancing Information Security Education with Lab Experiments and Collaboration in a Minority Technology Institution

Xiang-dong LI
Computer Systems Technology, New York City College of Technology, The City University of New York

Keywords: Information security education, Lab experiments, Minority technology institution.

Abstract. We present our experience on enhancing information security education with lab experiments and collaboration in a minority technical institution. We built an information security laboratory, which has supported security courses and several network courses for 10 years at New York City College of Technology (City Tech, CUNY). In addition, we have developed the collaboration with two national centers of Excellence in Information Assurance Education to enhance the student research capacity. The teaching method has been successfully implemented as a model for an experimentation environment providing hands-on experiences and research in topics related to information security.

Introduction

Today most of the universities or colleges offer the information security courses in their Associates in Applied Science (AAS) and Bachelor of Science (BS) programs. It is widely acknowledged by students and educators that the laboratory experiments or hands-on exercises can significantly advance learning at all levels of science education. There are many articles about implementing hands-on exercises in information security education [1-3]. However, the laboratory settings or the adoption should meet the individual educational environment of each institution.

New York City College of Technology at The City University of New York (City Tech, CUNY) is a broad-access Hispanic Serving Institution and has long been recognized as one of the most diverse university systems in the nation. City Tech is the only public technology institution designated in New York City area [4]. The Department of Computer Systems Technology (CST) is the largest department at City Tech, and currently has over 1,700 students in the program. Seventy percent of the students are minority population, which makes it the most diverse and the largest computing department of its kind in NYC metropolitan area. Since 2005, the CST department has been putting major effort into create security related courses to prepare students to meet national and industrial demands for a cadre of professionals with expertise in information systems security. These professionals will enter the work force better equipped to meet challenges facing the national information infrastructure.

Security Courses Development

The department has developed four security courses, they are:

<table>
<thead>
<tr>
<th>Course name</th>
<th>Credits</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>CST2410 Computing Security</td>
<td>3 credits, 2 class hours, 2 lab hours</td>
<td>AAS</td>
</tr>
<tr>
<td>CST3520 Computer Forensics</td>
<td>3 credits, 2 class hours, 2 lab hours</td>
<td>BS</td>
</tr>
<tr>
<td>CST3610 Network Security Fundamentals</td>
<td>3 credits, 2 class hours, 2 lab hours</td>
<td>BS</td>
</tr>
<tr>
<td>CST4710 Advanced Security Technology</td>
<td>3 credits, 2 class hours, 2 lab hours</td>
<td>BS</td>
</tr>
</tbody>
</table>

The course of Computing Security is also provided to high school students, as one of their advanced placement (AP) classes, through the Early College High-school Program (PTech). The courses of Computing Security and Network Security Fundamentals are also listed as elective courses for other
departments: the Computer Engineering Technology Department and the Electronic Engineering Technology Department. Today, we offer more than 26 security class sections each academic year with 24 students per section, which is the biggest number of security classes provided by an individual institution in New York area and its neighbors.

Security Laboratory Development

In 2006, we obtained an equipment grant of $150,000 from Department of Defense (DoD) and built a security information laboratory to support the information security courses and faculty/student research projects. This lab has been successfully implemented as a CUNY model for an experimentation environment providing hands-on experiences and research in topics related to information security; it benefits other CUNY’s institutions as well. We have helped CUNY community colleges to develop their security courses and lab settings. The security courses offered at City Tech with the DoD-supported laboratory have attracted a great number of students from high schools and community colleges to apply for or transfer to our Bachelor of Technology program, making the department as the largest computing department of its kind in NYC area.

This security lab has been used to support a large number of the security courses, network courses, and faculty/student research activities for the past ten years. During the past years, the security lab has been replenished with various pieces of new equipment through the author’s various National Science Foundation (NSF) student research and education grants, plus supplementary funding from the college for education equipment. Recently, we obtained another fund of $150,000 from DoD to upgrade the laboratory. The upgraded lab will strengthen the support for the research topics (will be mentioned in next section) and furthermore it allows us to include more advanced research topics. For example, we plan to include research on Secure Web Transaction, Application Threat Assessment, Server Security Testing, Vulnerability Management, Java Security, Authenticated Network Architecture, Covert Channels, Penetration Testing, and DNS Rebinding Attacks.

Students Research

The students conduct research activities on information security through their security courses and various national-, CUNY-, and college-wide student research programs. The department faculty members have served as mentors of student research in security for the NSF Scholarships in STEM (S-STEM) program, NSF Louis Stokes Alliances for Minority Participation (LS-AMP) program, NSF Research Experience for Undergraduates (REU) program (proposed for Summer 2017), CUNY Baccalaureate for Unique and Interdisciplinary Studies (CUNY BA) program, and college Honors Scholar program and Emerging Scholar Student Research Program. In recent years, several of the author’s NSF grants also supported student research activities in information security, including the awards of NSF DUE A Virtual Laboratory for Research and Education (with NYU-Poly, 2008-2010), NSF DUE Secure Web Development (with Pace University, 2009-2011), and NSF DUE Establishing the Information Assurance Student Pipeline Through Community College Outreach (with Pace University, 2012-2015). Each year, students give 3 or 4 presentations on their research projects at various research seminars, workshop or conferences.

Those research activities mainly focus on the computer system security, network security, and digital forensics. For example, the research projects cover the analysis of virus partners, detection of Trojan horse, installation and configuration of honey nets, security analysis on various encryption protocols and Trusted Platform Module (TPM), attacking analysis on wireless WEP, WPA and WPA2, detection on port scanning and enumeration, analysis on various level-2/3 or above attacks and their protections/detections/mitigation, analysis on cloud computing security, various advanced security technology research from industry, and advanced digital forensics technologies. The main part of the author’s research in information security focuses on the security analysis on the various
application protocols. The author has served as a mentor for many undergraduate, graduate and Ph.D. students in their security research projects.

Through enhancing students’ research involvement in the course work, in recent years we have seen that many of our graduates enter Master’s degree programs after they finish the Bachelor of Technology (BTech) at City Tech. We also see often that our students have been hired by federal or governmental agencies (e.g., FBI, CIA), financial industry (e.g., Goldman Sachs, Morgan Stanley), the IT industry (e.g., Google, IBM), pre-college education (as high-school teachers) and research fields (as faculty in colleges).

Collaboration

We have developed the collaborative relationship with two centers of academic excellence (CAE) in information security education by the National Security Agency (NSA). They are the Information Systems and Internet Security Laboratory (ISIS) at NYU-Polytechnic University [5] and the Security Program at Pace University [6]. Some of our student research topics are adopted from the mentioned two centers. However, their laboratory settings and research topics mainly focus on the research for Master’s and Ph.D. students and we modified them to meet the undergraduate (associate and bachelor’s) research and education at City Tech.

Each year, we collaborate with NYU-Polytechnic to organize and train our students as a team and participate in the national student Information Assurance Competitions (CSAW) held at NYU-Poly [7]. Recently City Tech students have proudly won one second prize, one third prize, and two finalist awards. They were the only minority students on the award lists when they competed against other students from some country’s top universities, including NYU, CMU, Yale, Columbia, Rensselaer Polytechnic Institute, Penn State, etc.

In 2009, the author collaborated with Pace University to develop the online course Secure Web Development Teaching Modules [8], which has been adopted by over 50 institutions in their security courses. The online course has been implemented in one of the security course and some of the research projects are developed based on the online course’s projects at City Tech.

In addition, we have hired 4 or 5 adjunct faculty in the security field from industry at City Tech to teach the security courses. Each year the department holds a meeting with our industry advisors to listen their opinions. Their security experience from industry can benefit our program and the students.

Summary

There are many available articles on the hands-on exercises in information security education; however, the lab settings and research topics should meet the educational environment of the individual institution. In this paper, we discuss our experience on developing and enhancing information security education with lab experiments and collaboration in a minority technical institution. The teaching method has been successfully implemented as a model for an experimentation environment providing hands-on experiences and research in topics related to information security. The security technology in industry varies fast, this requires us to update our educational and research topics often. The collaboration with centers of academic excellence in information security education and industry experts can benefit the educational and research topics at our minority technology institution.

References


