Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

Development of a Security Education Program at a Minority Institution

Dr. Xiangdong Li, *NYC College of Technology, The City University of New York (CUNY)*, *IEEE*
Dr. Lin Leung, *Borough of Manhattan Community College*, *The City University of New York (CUNY)*

Abstract – We describe the development of an information security program which contains three security courses and a laboratory for the undergraduate students at New York City College of Technology, CUNY, one of the minority serving institution. We also explore collaboration with other minority serving institutions on information security education.

Index terms – Curriculum, Laboratory, Information Security, Education, Minority Institution.

I. Introduction

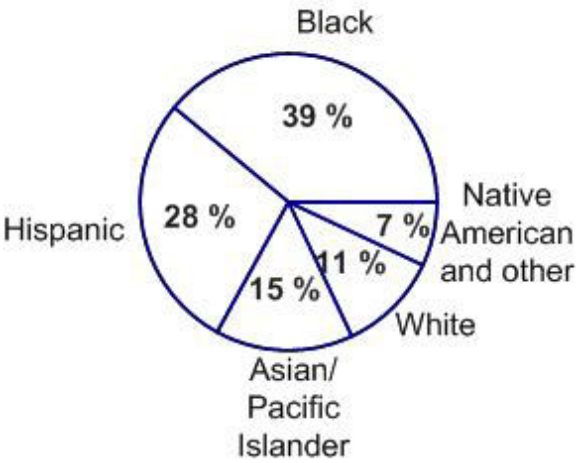
As the World's financial capital, New York City needs a large number of professionals in information security. Most students from the City University of New York (CUNY) will work in New York City area after they graduate. There are nineteen institutions in the CUNY system, sixteen of them are designated as Minority Serving Institutions by the U.S. Department of Education. The New York City College of Technology (City Tech) is designated as the only technical college in the CUNY system. We have developed an information security course module which contains three courses for a Bachelor of Technology (BTech) in the department of Computer Systems Technology at NYC College of Technology. This project is supported by the National Science Foundation (NSF) under Grant DUE-0417049 (Federal Cyber Services: Capacity Building). On another Grant, W911NF-05-1-0019 received from the Department of Defense (DoD), we are currently building a dedicated security laboratory, which is designed to support these newly developed courses at the City Tech and existing security courses for the students at the CUNY Graduate Center. This security program serves as a CUNY model for an experiment to provide hands-on experience for both associate and baccalaureate degree students at the City Tech and it also provides training programs for the faculty members in topics related to information security systems from different CUNY institutions.

Xiangdong Li: xli@citytech.cuny.edu
Lin Leung: lwleung_99@yahoo.com

II. Information Security Curriculum Development for Bachelor of Technology

A. Institution Background

NYC College of Technology is one of the most diversified colleges in the northeast, as reported by U.S. News and World Report; the College has been designated as a Minority Serving Institution (MSI). Currently, there are more than 12,400 undergraduate students; 50% are female:



Student Fact

63% are the first in their family to attend college
60% report household income less than $30,000
80% incoming freshmen receive need-based aid
65% continuing students receive need-based aid
48% work more than 20 hours per week
20% are single parents supporting at least one child

We have explored opportunities to collaborate with the national agencies, such as NSF and DoD, to assist Minority Serving Institutions in developing information security education for under-represented students and faculty.

B. Department Background

The Department of Computer Systems Technology (CST) at NYC College of Technology offers three curricula in addition to serving many other departments within the college.

• *Associate in Applied Science (AAS) in Computer Information System (CIB)*
• *Associate in Applied Science (AAS) in Microcomputer Business Systems (MBS)*
• *Bachelor of Technology (BTech) in Computer Systems*

A graduate from either of the AAS degree programs may enroll in the upper level program without the need supplement many pre-requisites. In addition, the department currently has articulation agreements with four CUNY community colleges for the existing computer related programs: Borough of Manhattan Community College, Kingsborough Community College, LaGuardia Community College and Queensborough Community College. Students from these colleges are able to make a seamless transfer to the upper division of the BTech program at NYC College of Technology. There are more than 1,120 enrollments in the Department of Computer Systems Technology as of Spring 2006, and of those, approximately 800 students are in the Baccalaureate program.

The department formerly provided six course modules for Bachelor of Technology program.

• *Client Server Technology*
• *Database*
• *Networks*
• *Object Oriented System Analysis and Design*
• *Programming Design*
• Web Design and Implementation

Each module contains three or four courses. The students need to complete at least three course modules in order to graduate with the Bachelor degree.

C. Security Curriculum

Information systems security is concerned with operations, which protect and defend information and systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. The White House recently published software security R&D strategy: The President's Science Advisor, the administration's most senior technology official, is calling for immediate government investment in software "reliability, availability, and serviceability." The formal document, the Report of the High End Computing Revitalization Task Force, is part of an extensive plan developed to reverse a lack of investment in high-end computing solutions.

We have addressed the need for education by establishing an undergraduate information security program, which contains three security courses and a security laboratory in the Computer Systems Technology Department at NYCCT. Our goal, in the broadest sense, is to assist in meeting national demand for a cadre of professionals with expertise in information systems security. These professionals will enter the work force better equipped to meet challenges facing our national information infrastructure. Furthermore, use of the laboratory is required to bolster our information security courses, and we intend to make this a model program among CUNY undergraduate institutions for information security systems.

A survey conducted among our students showed that they are highly interested in learning about information security technology courses, and would certainly apply to enroll, if the courses were available.

Originally, we planed to adapt the existing security courses given at Polytechnic University; however, due to the different student backgrounds in the case of these two institutions, a large part of the program provided at the Polytechnic was devoted to coding and algorithm. Most of these courses are designed for graduate level and are not suitable for students in the BTech program. We have developed a new information security curriculum based upon the background of our students. This curriculum contains three security courses described as below;

CS510: Computer Security (3 credits, 2 class hours and 2 lab hours)

This course is an introduction to security issues facing computer professionals today. Students will acquire the knowledge and skills on how to maintain the integrity, authenticity, availability and privacy of data. It covers

computer viruses, authentication models, certificates, group policy, cryptography, and access control. It also introduces the fundamental security issues of programming, database and web server. Other topics include how to monitor the system for suspicious activity and fend off attacks, keep spies and Spam out of e-mail, take control of security by encrypting data, design Active directory, blocking ports, and locking down the registry. It also covers basic security issues on UNIX/LINUX.

CS 610: Network Security Fundamentals (3 credits, 2 class hours, 2 lab hours)

This course is designed to provide a comprehensive overview of network security. It covers authentication methods along with common network attacks and how to safeguard against them. It also teaches communication security aspects important in the use of remote access, the Web, directory and file transfer, and wireless data. The roles of firewalls, routers, switches, and other network hardware in security are examined. Security considerations for transmission and storage media are discussed, as well as security considerations in Network Security Topologies, Intrusion Detection, and Network Operating System vulnerabilities. In the lab, students learn how hackers attack networks and how to defend them.

CS 710: Advanced Network Security: Design, Implementation, Integration and Management (3 credits, 2 class hours, 2 lab hours)

This is an advanced network security course and it provides a comprehensive look at advanced network security technologies applied in the real-world, as Firewalls, Virtual Private Networks (VPN), Intrusion Detection System (IDS), Network Intrusion Prevention Systems (IPS), Virtual Local Area Network (VLAN), and their uses with other network security components to secure a Local Area Network. It also includes Network Security Design, evolving security strategies, the evolution of identity and access management, and Policy and Risk management. The students will work on projects in the information security laboratory.

There is plenty of courseware in computer and network security that is available today. For example, the National Colloquium for Information Systems Security Education (NCISSE) facilitates the sharing of knowledge and resources through its web sites which currently contains course materials on Ethics in Computing, Risk Management and Malicious Logic. A more comprehensive resource is provided by the National Information Assurance Training and Education Center (NIATEC) at the University of Idaho, in the form of teaching and curriculum materials made available. The textbooks and reference books are listed in the Ref. [1-8].

The students who finish the A.A.S. of CIB or MBS programs are able to take the security module.

D. Schedule

CS510 is designed as the prerequisite for CS610 (the second course) and CS710 (third course) of the Module. The students are required to complete Operating System and Network Introduction courses in the AAS programs before taking CS510.

All the aforementioned security courses were approved by the College and University Council Committees in 2005. We have offered one section of Computer Security as an experimental course in Spring 2005. One section of CS510 was taught in Fall 2005. We are teaching one section of CS510 and one of CS610 in the current semester, Spring 2006. All these courses were well attended and received by the students. A Section of CS710 has been scheduled for Summer 2006, and two sections of CS510, and one course CS610 has been scheduled for Fall 2006.

III. INFORMATION SECURITY LABORATORY

Several universities, including Polytechnic University, Purdue University, UC Davis, George Mason University, James Madison University, University of Idaho, Iowa State University, and University of Milwaukee have excellent and highly successful computer security laboratory programs. However, in most of these cases, the focus is on research and graduate education. There is no information security laboratory among the CUNY institutions. Our goal is to develop a program that focuses on undergraduate (associate's and bachelor's level) education.

The development of the Laboratory included the purchase of computers, network devices, furniture, and security technology equipments. The security technology equipments included Firewall, Intrusion Detection (IDS), Virtual Private Network (VPN), wireless access and its security, Routers/Switches, Clean Access Manager, and Intrusion Prevention Systems (IPS).

Some of the student lab projects are chosen from the program partnered by SFS, NSA and the Computer Network Defense Research and Technology (CND R&T) (www.cndrt.org). These projects are described briefly below;

- Account Usage: This project will examine providing the capability to monitor and track abnormal user account activity such as account login while on vacation or non-duty hours.

- Data Transfer: This project will examine providing the capability to monitor and track abnormal user file transfer activities associated with copying and forwarding files to entities that are outside the user's enclave and are not normal recipients of such files.

- Fault Tolerant Architecture: This project will examine the current state of the art in techniques, methods and tools to design and develop dynamic fault tolerant network security architectures capable of withstanding attacks, failures and malicious applications.

- IP Hijacking: This project will examine the capability to detect that a TCP/IP session has been hijacked and to notify the administrator that such suspicious activity is occurring.

- OS Fingerprinting: This project will examine the capability to correctly identify the operating system of a network device based solely on available open source application fingerprint information.

- Printer Server Monitor: This project will examine providing the capability to monitor and track user print requests to identify abnormal printing activities.

- Process Isolation: This project will examine the current state of the art in techniques and methods for effectively creating an architecture that isolates the runtime environment for COTS software.

- Profile Response Research: This project will examine behavior and expected host responses generated due to external scanning activity.

- Security Dashboards: This project will examine the utility of, and make recommendations for improvements to, so called "security dashboards" that have been introduced as visualization tools to support risk and vulnerability management.

- Spyware: This project will examine the current state of the art in Spyware applications, how they are distributed, the threat they pose and the current capability to detect and remove them from a system. Also desired is an investigation to determine what a Spyware application may have already done on a system prior to its detection, what future Spyware applications may be capable of doing and what capabilities will be needed to prevent Spyware applications from being installed and executed on a system.

- Trusted Mobile Agents: Mobile agent software provides the ability to automate many network management functions.

- Designing a trusted network: Students will use advanced security technology: VPN, Firewall, IDS and IPS to design and secure a small business network.

The principal long-term goals of this laboratory are to:

- Establish an information systems security laboratory that becomes a CUNY model for an experimentation environment providing, hands-on experiences in topics related to information security for both associate and bachelors' degree levels. It can provide training programs for the faculty members and students from other CUNY institutions, and will serve to;

- Attract more students and encourage them to complete their associate degree in computer science or related majors to continue their bachelor degree at NYCCT. It also provides an opportunity for students and faculty from other disciplines who are interested in gaining knowledge on information security.

- Support students' and faculty research projects on information security among CUNY institutions.

- Enhance other course modules such as Network and Web Design in the Department.

- Enable students to engage in number of security projects which are designed for them in associate and bachelor's programs, such as:

Securing a web server

Analyzing a virus
Comparing operating system security
Detecting intrusions
Analysis, remediation, and improvement of security

In addition to these traditional projects students can also design and implement secure distributed applications based on client/server programming in TCP/IP and security protocols environment such as secure chat-room and attack/defend applications.

This laboratory equipment is supported by the Department of Defense as a one-year project. We have finished purchasing all of the furniture, computers, network devices, and security technology equipment.

IV. Faculty expertise development

There are a few programs providing training for faculty in IA. Purdue, Tulsa and Idaho are well established and highly qualified to address the need. Polytechnic University itself has hosted the Cisco Boot camp in IA for faculty, and plans to continue to hold one every semester. In fact, Cisco has been holding these boot camps across the country on an almost monthly basis.

Recently, we lead a consortium on information security education. Faculty members from three Minority Serving Institutions: NYC College of Technology, the City College of New York, and the Borough of Manhattan Community College all participated in this consortium. One or more information security courses are offered at each of these colleges. The consortium meets every month to discuss and share the experience on teaching, collaborative research works, writing papers, mentoring students and designing student research projects.

V. Student research and graduate education

Even high performing undergraduate students do not necessarily understand research methodologies. Their success is based upon having learned how to successfully complete courses. This clearly means they have learned how to study laid-out coursework and master well-known solution methods.

Many minority students have a limited chance to learn about research because in their institutions, research activity is usually limited. The students have received little training in how to think independently, invent new problems, and figure out ways to solve problems in relatively unconstrained situations. To stimulate their interest in a research career, students must be explicitly demonstrated the nature, value, and intrinsic rewards of research.

Currently, we are mentoring two minority students within the NYC Louis Stokes Alliance for Minority Participation (LSAMP) in Science, Mathematics, Engineering and technology program. Their research projects are executed in the security laboratory. We expect that many more minority students will join this program in the near future, and we are exploring various methods to enable support in their research.

The Graduate Center at the City University of New York also benefits from this program. We provide the hands-on practice for the high level graduate research projects.

VI. Challenge

Since many of our students have expressed interest in information security, we will encounter a shortage of qualified instructors. Therefore, we are limited in the number of course sections we can provide during each semester. First, we do not have enough faculty members who are able to teach the security courses. Security technology is a rapidly growing field. Several faculty members have shown their interest in teaching the introductory security course, but a training program is needed for them to gain the necessary hands-on experience, if they are to teach the subject. There are a few programs which provide training for faculty in security education. For example, Purdue, Tulsa and Idaho have well established and respected programs to address this need. However, due to budgetary constraints, our college could not afford to send faculty for the urgently needed outside training programs. Second, it is hard to recruit qualified adjunct instructors from such a dynamic field considering the salary our college provides. Given this situation, we need to set up a program to train our own instructors (full-time and adjunct) in order to provide more security course sections to our students.

Our goal is to establish a faculty information security training program among the CUNY colleges which includes laboratory components. First, we will design student laboratory projects and write laboratory manuals. Then we will organize training workshops and seminars on topics of security education for the various CUNY colleges. We already have the benefit of the consortium of the three CUNY senior and community colleges. We

anticipate this program can improve CUNY faculty expertise in information security education and reinforce their laboratory experience. We aim to build the laboratory at NYC College of Technology as a model of an undergraduate information-security laboratory for CUNY. As a result we will enhance our security education with a better laboratory environment.

VII. Reference

[1]. Ed. Bott and Carl Siechert, *Microsoft Windows Security for Windows XP and Windows 2000 INSIDE OUT,* Microsoft 2002
[2]. Conan Kezema and Stanley Reimer, *MCSE Guide to Designing Microsoft Windows 2000 Security*, Thomson 2002
[3]. Paul Campbell, Ben Calvert, Steven Boswell, *Security+ Guide to Network Security Fundamentals,* Cisco Learning Institute, Thomson, 2003
[4]. Paul Cretaro, *Lab Manual for Security+ Guide to Network Security Fundamentals,* Thomson, 2003
[5]. Greg Holden, *Guide to Firewalls and Network Security: Intrusion Detection and VPNs,* Thomson 2004
[6]. Shweta Bhasin, *Web Security Basics*, Premier Press 2003
[7]. Michael Palmer, *Guide To Operating Systems Security*, Thomson 2004
[8]. Eric Maiwald, *Fundamentals of Network Security*, McGraw Hill 2004.