Education
Scholarship for Service: New Mexico Tech's Undergraduate Program

Lorie M. Liebrock • New Mexico Institute of Mining and Technology

The Scholarship For Service program educates and prepares students for leadership roles in government positions in information assurance. SFS gives me the opportunity to support some of the best students at the New Mexico Institute of Mining and Technology and to work closely with them in their education, professional development, and research. For an overview of this National Science Foundation-funded program, see “Education: Scholarship For Service” in the September 2006 IEEE Distributed Systems Online (pdf). That column describes the national program and our program at NMT, including student requirements and the benefits for agencies and students. Here, I focus on the education of NMT’s undergraduate SFS students.

Required courses

Undergraduate SFS students must take at least two information assurance courses, typically Introduction to Information Assurance and Protection and Information Assurance. For some students, these requirements overlap technical-degree requirements. For students in less closely related degree programs, these are additional requirements that count toward the required two years’ experience in information assurance. Typically, students are in the SFS program for two years, and they take at least two more information-assurance-related courses.

Introduction to Information Assurance and Protection

This sophomore-level course gives a broad overview of the issues related to information assurance. The catalog course description is


The course outcomes are an understanding of the breadth of issues and concerns in information security and assurance, as well as practical experience

- evaluating system security,
- developing security policy,
- evaluating security technology, and
- protecting systems from attack.

I occasionally teach this course. My students must find a client (customer). Only the student and I know the client’s identity, and we strictly protect it by using pseudonyms for in-class discussions. So, the students’ first test is to get a client who will allow them access to perform the required analysis. The first time I taught the course, I thought that students would have trouble getting access to client systems. However, I learned that this was to be the first service that the students provided their clients—a little social engineering education.
After the clients signed the agreements—in most cases, without even verifying the course’s legitimacy—I contacted them to discuss social engineering and the associated risks to their organization. Most clients hadn’t even considered that they were taking a student’s word that the project was legitimate; they were ready to give the students access to their systems. Such access would let an attacker collect valuable intelligence or do substantial damage; such intelligence is the reason for protecting client identity.

Most weeks, the students do some assignment related to analyzing their client’s security vulnerabilities. Exercises begin with a standard survey—for example, the Computer Security Institute’s “Computer Crime and Security Survey”—which the student completes with the client. This survey forms a basis for the student and client to understand each other’s computer security terminology and perspective. In particular, discussing the survey helps the student understand the client’s security needs.

The second assignment begins the analysis of security vulnerabilities. This focuses on analyzing access controls and site security at the client’s local facility. This is preliminary in considering information assurance issues, but it’s important—being able to walk up to a machine and start typing gives an attacker an immense advantage. In this analysis, students walk through the client’s facility and determine how easy it is to access computers, in terms of both physical restrictions such as locked doors and computer access controls such as passwords.

Other assignments include

- analyzing network mapping,
- analyzing the client’s firewalls,
- developing a security baseline,
- installing and using public key encryption,
- analyzing the client’s use of cryptographic systems,
- analyzing the client’s application security,
- analyzing the client’s disaster recovery plan, and
- analyzing the state’s security and privacy laws.

For each analysis project, the students perform an analysis based on the client’s security needs and then make recommendations to the client for improving how these security needs are met.

When students analyze the client’s application security, they determine what applications are installed, who can access them, and which ones are highly used. For a specific high-priority application, the students determine whether the application has known vulnerabilities, whether those vulnerabilities are patched, and what processes the client follows to keep patches for vulnerabilities up to date. The students perform a risk analysis with their clients, educating the clients about the typical attacks the application might face and recommending policy and process improvements as needed on the basis of the organizational goals. This gives students practical experience analyzing vulnerabilities, attacks, and application patches and instructing clients in the types of issues they should consider in their environment. In-class discussions compare and contrast the needs, policies, and procedures for clients with different goals and environments.

Many clients originally agreed to let students install and configure firewalls on their systems. For organizations that didn’t know the students, this was a huge risk that the client readily agreed to. So, not only did the students get clients, they got root privileges, too! Nonetheless, I modified the firewall project so that students installed and configured firewalls on their own machines, not the client’s systems. Students performed firewall analysis for the clients and provided recommendations on improving the software used, configuration, and firewall rules; this reduced the clients’ risk. In all projects, if the systems required extended privileges, I asked the clients to have the students work with a system administrator.
This course had a surprising outcome. Clients hired three students in my last class to do exactly the type of analysis and security improvement that I taught in class. In each case, the students went on to implement many of their recommended improvements. I found this to be an impressive outcome for a sophomore-level class.

**Information Assurance**

This senior-level course delves deeper into information assurance issues. The catalog course description is:


This course’s outcomes are that students will:

- understand computer attack taxonomies,
- be able to protect, detect, and respond to information security threats,
- identify different protection mechanisms,
- identify threats and risks to information and information systems,
- develop prevention mechanisms based on assessments,
- develop effective mitigation and detection strategies,
- develop in-depth defense mechanisms to protect information and information systems,
- develop strategies for vulnerability assessments and penetration testing, and
- understand current issues and difficulties in information assurance.

In this class, students learn in much more depth how to test and analyze firewalls, intrusion detection systems, and virus scanners. In each case, students learn about system weaknesses and compare different systems and approaches. In class projects, students develop attacks, defenses, or a vulnerability analysis that in some way extends the state of the art. After this course, some students have participated in red team exercises to test the security of government agencies and commercial entities.

**Additional courses**

We regularly teach other courses that focus on information assurance or computer security.

Internet Security and Applications is a computer security course. The course description is:


Cryptography and Applications, a focus area for some students, has this course description:

*Basic theory of encryption and decryption. The RSA algorithm and the public and private key system. Cryptography systems in use for Internet and business applications.*
Our other courses consider soft computing (where students often apply genetic algorithms and evolutionary computing to computer security problems), compiler writing (where students examine what's required to develop compilers that prevent buffer overflows and other vulnerabilities), and operating systems (where students examine current operating systems' security vulnerabilities and how to eliminate them). Overall, these courses and our security and assurance considerations (stemming from our Center of Academic Excellence in Information Assurance Education focus) provide students with a broad awareness of security and assurance. Furthermore, we periodically develop special-topics courses that we offer based on demand (for example, Digital Forensics).

NMT's undergraduate SFS program takes students well beyond the typical undergraduate education in terms of education, research, and intensive interaction with instructors and the rest of the SFS cohort (that is, the set of students, both undergraduate and graduate, in NMT’s SFS program). In addition to the time I work with the students, the students in the cohort collaborate for many courses, research projects, and extracurricular activities. In a future column, I hope to discuss these research projects, professional development, and developmental extracurricular activities. Intensive education, interaction, and collaboration prepares this talented group of students to participate in the rapidly changing information assurance arena and to face the challenges in civil service.

Lorie M. Liebrock is associate chair for undergraduate programs in the Computer Science Department, an assistant professor of computer science and information technology, and an adjunct professor of management for the New Mexico Institute of Mining and Technology. She's also the principal investigator for NMT’s Scholarship for Service Program. Contact her at liebrock@cs.nmt.edu.

Related Links

- DS Online's Web Systems Education Page
- "How to Develop a Career in Information Assurance and How to Advance in this Field," *Proc. ACSAC 05*
- "Tools for Information Assurance Arguments," *DARPA Information Survivability Conf. and Exposition* (DISCEX II 01)

Cite this article: Lorie M. Liebrock, "Scholarship for Service: New Mexico Tech’s Undergraduate Program," *IEEE Distributed Systems Online*, vol. 8, no. 3, 2007, art. no. 0703-o3002.