

EXPERIENCES WITH DEVELOPING A COMPUTER SECURITY INFORMATION ASSURANCE CURRICULUM*

*Thomas Bacon and Rahul Tikekar
Department of Computer Science
Southern Oregon University
Ashland, OR 97520
bacont@sou.edu, tikekarr@sou.edu*

ABSTRACT

Attacks on the computing infrastructure have gained prominence as the world harnessed the business transaction capability of the Internet in the last few years. Denial of service attacks and viruses cripple systems, making them unavailable to users and often destroying data. Information theft allows the thief to assume false identities, steal trade secrets and classified information, and perform transactions with accounts owned by others. There is a shortage of skilled computer security professionals capable of reducing vulnerabilities in computing systems.

This paper describes the process of creating a computer security and information assurance (CSIA) curriculum Bachelors degree. The process begins with determining goals, followed by developing a plan of action and ends with determining a curriculum consisting of new computer science and interdisciplinary synthesis courses.

INTRODUCTION

Increasing awareness of our nation's computer system vulnerability brought strong support for the national Cyber Security Research and Development Act [1] to fund development of computer security educational programs through the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST). In the recent past, firms focused

* Copyright © 2003 by the Consortium for Computing in Small Colleges. Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the CCSC copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Consortium for Computing in Small Colleges. To copy otherwise, or to republish, requires a fee and/or specific permission.

more on improving the bottom line and expanding infrastructure than investing in computer security [2], producing a strong need for computer security professionals.

Oregon has a large number of firms developing computer security solutions but few educational opportunities. Intel, Swan Networks, Tripwire and others are involved in R&D and implementation of innovative systems and products. Public-private consortiums, including the Oregon Regional Alliance for Information and Network Security [10] (RAINS) and Oregon Security Institute [7] (OSI), foster development of the local computer security industry. Oregon's only existing university level computer security program in 2001 was a masters program at Oregon State University [13]. More computer security graduates are needed to fill roles in business, leading edge research firms and local government.

SOU is a 5000 student liberal arts university serving a rural population 300 miles from the nearest large city. The Computer Science Department offers three undergraduate tracks and a masters degree. The department grew in size and stature during the late 90's (from 19 graduates in 1997 to 47 in 2002) but is currently experiencing a decline in students. A major department goal is to enhance its reputation and ability to recruit nationally in order to expand the pool of potential students.

SOU offers four tracks in the undergraduate program [8]: Computer Programming and Software; Computer Science and Multimedia; Computer Information Science and the newly approved Computer Security and Information Assurance track discussed in this paper. Each track requires a 6-class core with a varying number of electives.

There are a number of Masters and PhD programs in CSIA offered nationally, but it is difficult to find computer security programs for undergraduates. Undergraduate CS programs typically cover a breadth of topics and rarely focus in depth on security issues.

Research online, in journals and computer magazines confirmed the need for computer security professionals and the dearth of applied education for undergraduate students. Despite reduced funding, the SOU faculty decided to develop an undergraduate CSIA program with the goals of increasing enrollment and maintaining the strength of the department.

To answer these needs, the Computer Science department decided to develop an undergraduate CSIA program, working in "Internet time." SOU focuses more on teaching than research and prior experience developing an e-Commerce curriculum [3] facilitated rapid development of seven new classes and augmentation of existing core classes. Three faculty members began research into development of the program in mid 2002.

This paper begins with Section 2 discussing the general issues faced developing a new curriculum. Section 3 summarizes the requirements for an NSA Center of Academic Excellence. Section 4 defines the structure, content and process of developing the new curriculum. Section 5 concludes the paper, exploring the status of the program and work remaining.

CURRICULUM DEVELOPMENT CONSIDERATIONS

Developing a curriculum in any discipline requires funding and an analysis of the skills needed by professionals in the workforce. The curriculum requires approval by the university and must meet guidelines for accreditation and certification. Due to the rapidly changing nature of CSIA, it is also important to ensure that faculty has the knowledge and skills needed to teach theoretical and applied implementations. The needs of the students require analysis and innovative teaching methods created to fulfill these needs. Ultimately, the goals of the curriculum development must be clearly defined. The section discusses the goals and the major considerations developing the new curriculum.

Defining Our Goals

We defined our goals before proceeding further:

1. Add a CSIA track to our existing computer science undergraduate degree as soon as possible by creating and obtaining university approval for a CSIA curriculum.
2. Develop courses for the new track.
3. Obtain public and private funding to support faculty and computer security lab development.
4. Differentiate our curriculum from existing CSIA programs by focusing on our strengths in teaching and applied technology.
5. Differentiate our curriculum by creating an undergraduate degree program.
6. Differentiate our curriculum by including computer forensics and wireless security courses.
7. Obtain NSA certification as a Center of Academic Excellence (CAE).
8. Increase enrollment in CS by advertising our new program and recruiting in regional high schools and community colleges.
9. Collaborate with other departments, industry, government and other Oregon University System (OUS) schools to develop research and Capstone opportunities.

It was a challenge to develop a four-year undergraduate program providing the necessary experience and knowledge. The curriculum is broad-based with only a few topical classes; it mainly focuses on general security concepts. In order to complete the CSIA track in 4 years, no CS classes are elective and specific courses fulfill some university general requirements. [TB1]

Skills Needed by Computer Security Professionals

Information Assurance (IA) is a broad topic, spanning many areas in computer science, criminology and business management. It requires conceptual understanding of broad basic and advanced CS topics as well as detailed implementation knowledge of specific protocols, methods, algorithms and systems. Legal issues, equipment management, information policy and

personnel administration are key topics not covered in a traditional CS curriculum. To the best of our knowledge there were no peer institutions with undergraduate programs we could use as a model, so we relied largely on our real-world experience and professional certification requirements to define topics needed in the curriculum.

Certified Information Systems Security Professional (CISSP) certification is highly respected by CSIA professionals in private and public industry. The CISSP covers ten subject areas [16]: Access Control Systems and Methodology; Application and Systems Development; Business Continuity Planning; Cryptography; Law, Investigations and Ethics; Operations Security; Physical Security; Security Architecture and Models; Security Management Practices; Telecommunications, Network and Internet Security. CISSP certification verifies an individual has substantial skills in the CSIA discipline.

The National Security Telecommunications and Information Systems Security Committee (NSTISS), recently renamed the Committee on National Systems Security (CNSS), certifies curriculum compliance with Document 4011[4]. This certification covers seven areas: Automated Information Systems; Communications Basics; Security Basics; NSTISS Basics; System Operating Environment; NSTISS Planning and Management; NSTISS Policies and Procedures. Certification verifies the institution teaches the necessary skills to implement computer security in non-classified government settings.

Computer forensics and the study of legal and ethical aspects of computer security are rarely included in CSIA programs. SOU has a highly respected Criminology department and the proliferation of computer crime has brought a need for professionals with knowledge of these topics. Testing methodology, operational procedures and policy are missing from most programs.

The team used Document 4011 as the main guideline for the curriculum and built on strengths in policy and procedures, criminology and applied industry experience. One faculty member's strong interest in wireless communication security added another topic for consideration.

Funding

Declining budgets makes obtaining funding a top priority. A \$50,000 grant in mid 2002 from Oregon's Engineering Technology Industry Council [11] provided initial funding. CISCO contributed two routers, one 802.11 compliant wireless access points and wireless access cards as our first industry donation. The department also pursued an NSF grant for curriculum development and private grants to enhance library resources.

The NSA CAE designation is a prerequisite for substantial NSF SFS Scholarship grants [6] and the CCLI [12] program.

The Students

SOU students typically progress to industry and business rather than research and development. An initiative by the Extended Campus Program to create an online Criminology undergraduate degree is expanding the pool of students, reducing geographical and time constraints.

Faculty Experience in Csia

Six of eight faculty members were hired in the last five years; two last year have many years in industry. Faculty experience covers a broad range of topics including low-level network implementations, enterprise e-commerce and data systems with complex middleware connectivity, security risk analysis, security policy and operational procedures. Individual faculty cover the spectrum of security topics with the applied focus that government, industry and students need.

Curriculum Approval

The department budget has a component that rewards increasing enrollments in the major that can offset the declining university budget. The current President strongly supports creation of Academic Centers of Excellence. With the goal of obtaining approval as an NSA CAE and the likelihood of increasing enrollment, the belief was that it would not be a substantial hurdle to obtain curriculum approval in this climate.

DEFINITION OF AN NSA CENTER OF ACADEMIC EXCELLENCE

In order to obtain NSA certification as a Center of Academic Excellence, an educational institution must prove that it has the capability to deliver excellence in information assurance (IA) education. Points are awarded for each of ten criteria; the institution must receive a minimum number of points for each category and 200 points total. The measurements as defined by the CAE website [15] are:

1. The academic program is tied to NSTISSI Standards [4] (25 points required, 45 possible).
2. The academic program demonstrates IS is not treated as a separate discipline, but as a multidisciplinary science with the body of IS knowledge incorporated into various disciplines (20 points required, 30 possible).
3. The academic program demonstrates how the university encourages the practice of IA, not merely that IA is taught (10 points required, 30 possible).
4. The academic program encourages research in IA (15 points required, 35 possible).
5. The IA curriculum reaches beyond the normal geographic borders of the University (10 points required, 35 possible).

6. It is clearly demonstrated that the faculty is active in IA practice and research, and contributes to IA literature (15 points required, 35 possible).
7. The university library and reference systems/materials and/or the IA Center maintain state-of-the-art resources (15 points required, 30 possible).
8. The academic program has declared concentrations or certificates in IA (5 points required, 65 possible).
9. The university has a declared center for IA education or a center for IA research from which IA curriculum is emerging. The center may be departmental, school or university-based (25 points required, 50 possible).
10. The university IA faculty consists of more than one individual (10 points required, 35 possible).

Nstiss Document 4011

Document 4011 (titled "National Training Standard") defines competencies needed by computer security professionals to work in non-classified government areas. Competencies organize into seven major areas providing either Awareness or Performance knowledge. The Awareness Level creates an understanding of systems, information and security principles, requirements and policies. The Performance Level provides the skills necessary to implement information security procedures and practices. Document 4011 consists of a three-tier hierarchy: the seven major areas, each consisting of component areas, each of which has specific competencies. We will call these tiers the areas, components and competencies.

Each of the seven areas has a historical and current methodology component as well as detailed exploration of area-specific components.

The five Awareness Level areas build computer security general knowledge:

- Communications covers communication transmission concepts and features of various communication mediums.
- Automated Information Systems covers the basics of hardware, software, memory, media and network systems.
- The Basics of the NSTISS area covers general security concepts and national policy including legal elements, concepts of trust, risk management, system life cycle management, threats, vulnerabilities and countermeasures. Personnel roles and modes of operation and facets of the NSTISS are also covered.
- Security Basics teaches the characteristics of information and security measures to protect the information. Information Security (INFOSEC) and Operations Security (OPSEC) are the components of this area.
 - o INFOSEC covers the basics of security for information systems and networks including security risk analysis, policy, information and security status, storage and

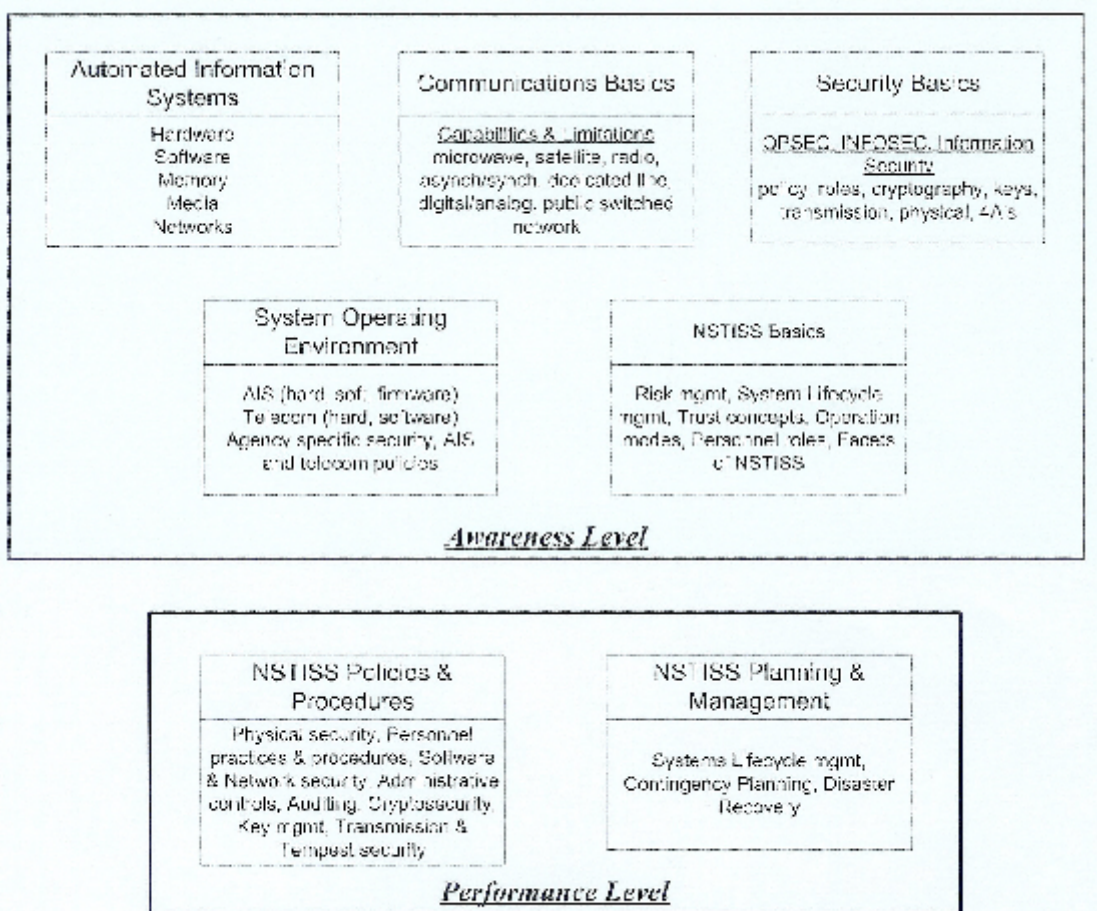


Figure 1. NSTISS National Training Standard subject areas

transmission, cryptography, encryption, keys, access, authentication and audit are included.

- o OPSEC focuses on identifying, controlling and protecting unclassified information associated with US national security programs and activities.
- The agency-specific System Operating Environment area covers telecommunications and AIS purchase and maintenance control points, system architectures and security policies for non-classified government entities.

The two Performance Level areas ensure competence in implementing security for unclassified government information:

- NSTISS Planning and Management focuses on practical methods to design security measures and program with generic security planning guidelines and documents.
- NSTISS Policies and Procedures cover NSTISS specific technological, policy and educational solutions as well as threats, vulnerability and controls in AIS and telecommunication systems.

DEFINING A CURRICULUM

The Curriculum Definition

Industry needs and certification requirements provided the framework for our curriculum; faculty experience, student needs and capabilities molded it. We chose to focus lab work and research on secure networking and hardware to provide a fit with much of Oregon's security industry.

Depth in computer science concepts forms the foundation upon which IA specialists may grow. We augmented six CS core classes with three existing elective classes (Data Structures, C & Unix, and Unix Administration) and three Math classes (Elementary Statistics, Calculus I and Discrete Structures) to provide a solid foundation from which we could train computer security students. We determined the need for additional classes by having each instructor map the coverage of his classes to the appropriate Document 4011 competencies.

Mapping the Existing Curriculum to Document 4011

The first step in designing the curriculum was to map existing classes into Document 4011.

Programming I, II and III (CIS 200, CS 257, and CS 258) cover many of the competencies in the Automated Information Systems (AIS) area, particularly in the hardware, software and memory components. These classes cover the system lifecycle component from the NSTISS Basics area and the passwords and backups competencies from the NSTISS Facets component. The System Lifecycle component of the NSTISS Planning and Management area includes various competencies introduced in these and other programming classes.

Systems Software and Architecture (CIS 326) covers all of the AIS area competencies thoroughly except for distributed vs. stand-alone systems. It also touches some software security competencies in the Policy and Procedures area.

Data Structures (CS 411/511) and a C & Unix (CS 367) class provide foundational programming experience that touches most of the AIS area components. Data Structures provides additional foundation in network and graph topologies as well as cryptographic basics such as hashing and minimum redundancy codes. C & Unix (CS 367) provides experience working in the Unix environment to augment the Windows experience gained in Programming I, II and III.

Networks I (CIS 336) covers layer 1, 2 and 3 of the OSI 7-layer model and Networks II (CIS 436/536) covers TCP/IP, substantially covering the Communications Basics area and the AIS Networks component. Both classes cover the traffic analysis competency in the Policy and Procedures area.

Many classes touch a few competencies while providing broad foundational knowledge. Unix Administration (CIS 450/550) covers AIS competencies, various encryption

competencies and the Auditing and Logging component. Databases I (CIS 360) covers many of the same competencies as the programming classes.

Gaps in the Curriculum

Core classes cover many Document 4011 competencies; the mapping process identified the missing pieces. Education about secure transmissions (encryption, cryptology, keys, etc.), secure programming methodology, security policy and procedures, threat/vulnerability identification and mitigating controls, ethical and legal aspects of IA were identified as missing from the existing curriculum. The seven new classes cover these subject areas in depth.

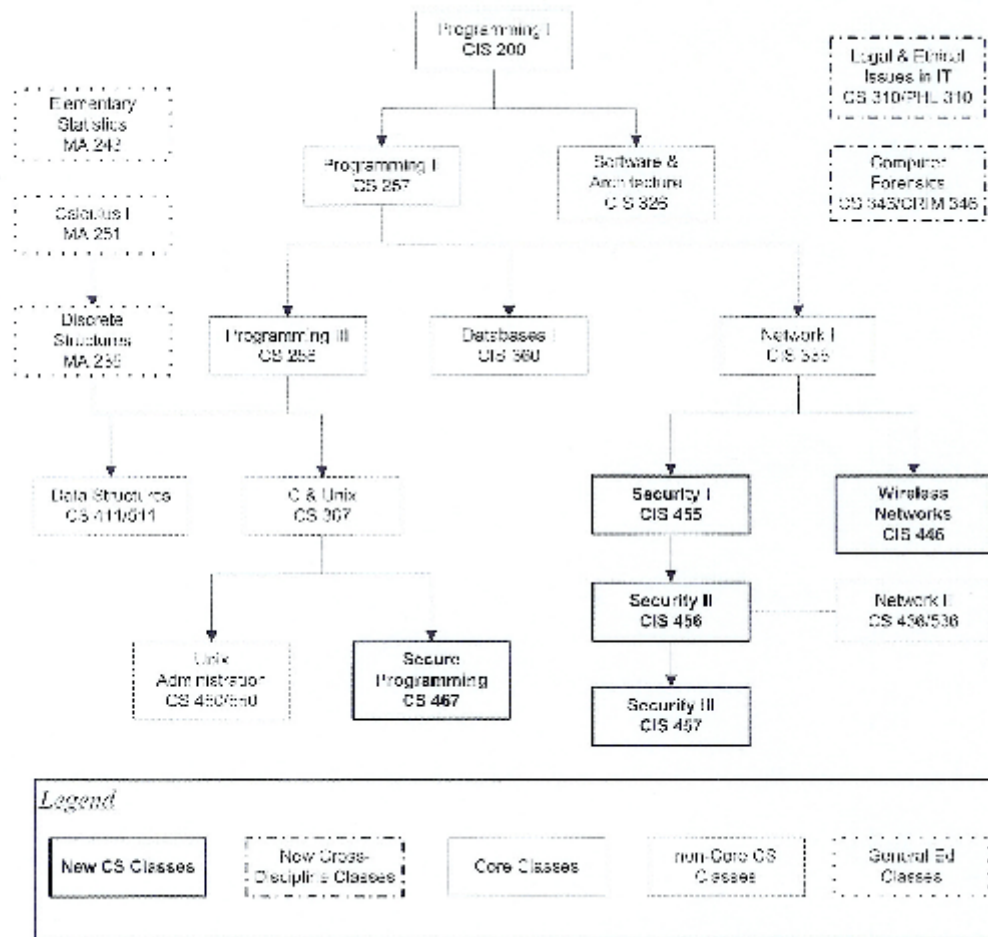


Figure 2. Undergraduate CSIA Curriculum

Seven New Classes

Five new CS classes fill most of this gap. Security I, II and III provide an overview of computer security. These classes cover threats and controls, policy and procedures, secure systems, network protection and encryption in depth. Secure Software covers how to minimize exploitable software vulnerabilities and Wireless Networks covers basics of wireless communication. Two new interdisciplinary classes, Computer Forensics and IT Legal & Ethical Issues, complete the new CSIA curriculum. These topical courses attract working students. This curriculum provides a solid foundation in computer security concepts with added depth in focus areas.

Security I (CIS 455) covers a substantial number of competencies in the Policy and Procedures, NSTISS Basics and AIS areas providing an overview of the broad computer security and information assurance field. It explores the security infrastructure along with organizational policies and procedures needed to create a secure environment. Cryptographic protocols, modes and algorithms are covered in depth. Students develop a security risk and assessment plan for a mock corporation and research a recent security breach. The university computer labs are sufficient to develop a program implementing a cryptographic algorithm.

Security II (CIS 456) teaches how to create a secure computing infrastructure, including workstations, servers and a secure LAN. VPNs, perimeter protection and intrusion detection are explored along with data assurance monitoring. Researching a recent major LAN security breach, designing a secure LAN and installing and using intrusion detection and data assurance systems give computer security lab experience.

Security III (CIS 457) gives hands-on experience detecting and mitigating threats to the Internet. The course explores how crackers find a system and the various methods used to exploit vulnerabilities by examining methods and tools used both to attack and to defend systems. This class provides an overview of Unix and Windows operating systems. Tools implemented on wired and wireless systems in our computer security lab provide experience detecting and analyzing intrusions.

Wireless Networks (CIS 446) begins by exploring fundamentals of electromagnetic wave propagation. Study of information transmission techniques leads to exploration of implementations on specific networks (IrDA, Bluetooth), cellular systems (IS-95, GSM, GPRS) and satellite systems. Hands-on experience is gained implementing wireless networks and access points in our computer security lab. Sampling wireless signal strengths around the community and examining transmissions via oscilloscope provide more hands-on experience.

Secure Programming (CS 467/567) explores the major security aspects of developing secure programs. This material thoroughly covers the Software Security component in the NSTISS Policies and Procedures area. Topics include buffer overflows, access control, race conditions, randomness, input validation, and passwords. Students learn the importance of planning for security and some of the tradeoffs involved in dealing with security issues. Lab work can be done on any computer and is a substantial part of this class.

Computer Forensics (CS 346/CRIM 346) is an interdisciplinary course developed with the Criminology Department and offered to upper division students in either department. The

class provides the opportunity to train a broad base of students in investigative skills that are rarely, but critically, needed at times in our rural environment. A broad spectrum of topics covers the legal/criminal and computer aspects of forensics. Basics of computer systems, computer search and seizure rules and the liabilities and responsibilities of the investigator are covered using the latest tools and technologies. Lab work requires dedicated Mac and Intel personal computers to practice mock lock downs and diagnostics.

The Philosophy Department joined us in developing the interdisciplinary IT Legal and Ethical Issues course (CS 310/PHL 310). This course is a critical inquiry into the ethical, legal and societal implications of the products, activities and behaviors of digital technology with emphasis on US laws, legislation and technology. Digital works, copyright laws, software and business practice patents will be examined, as well as some significant court cases that raise fundamental Constitutional issues. Insight into legal and moral issues will allow the student to competently examine the aspects of intellectual property right protection. This course fulfills a general education requirement while covering many competencies in the NSTISS Basics area.

Evolution of the Curriculum

We delivered our first CSIA classes as special topics courses in the 2001-2002 academic year, prior to developing the CSIA program. As of Fall 2002, we have delivered each class at least once, with full enrollment in most.

During our first term, we determined two new courses lack the needed security depth. We are currently developing replacements for these courses. Wireless Networks teaches the concepts of wireless communication, but we need to cover the security aspects in greater depth. Adding a Wireless Security course for CSIA majors will extend the general knowledge learned in Wireless Networks and focus on security aspects of wireless communication.

There is a wide disparity in the needs and skills of the interdisciplinary Computer Forensics class; the students from each discipline lack the foundational skills of the other discipline. CS Computer Forensics will replace the interdisciplinary course for CSIA majors, assuming knowledge of computer concepts and focusing on legal aspects, diagnostic tools and techniques. The Criminology Department is planning to continue the Computer Forensics course for their majors. We will develop electronic versions of the Computer Forensics and Legal Aspects classes as part of an online undergraduate Criminology degree.

Implementation Challenges

We obtained university approval for and developed a curriculum of seven new courses (with two more on the way) in about six months. One faculty was full time on the project during the summer and fall, with part time support of several others. The development process continues with curriculum revisions, course development and lab creation.

New classes required more development time than a typical CS course. Lab exercises are more abstract than typical programming classes. IA is developing rapidly and changing constantly, requiring us to look beyond textbooks as our main source of material.

Implementation details change, but new concepts are introduced regularly also as hackers find even more clever ways to penetrate systems and developers find clever ways to defend systems.

CURRENT STATUS OF THE CSIA TRACK

About six months after initial planning began, the curriculum committee approved our program and we are successfully training tomorrow's computer security professionals. The students have been very receptive to the courses; they are some of our most anticipated offerings. We expect to have a large percentage of our new students pursue the CSIA degree. Good opportunities in computer security, particularly in Oregon, should ease transition to the working world.

We are actively pursuing funding to develop our curriculum and spread the computer security gospel via an outreach program to small and rural businesses and local government in our area. Our layered approach to security implementation should be cost-effective for these unique users. These efforts may have the welcome side effect of attracting students to our program and creating Capstone projects.

Universities are now creating undergraduate CSIA programs. Pennsylvania State House Resolution 409 claimed in 2002 that East Stroudsburg University of Pennsylvania [20] recently "established the first undergraduate degree program in computer security in the United States [14]." Towson University [18] has received an NSF grant to develop an undergraduate track in computer security.

Work Remains to Be Done

We spend a lot of our time developing research opportunities, traveling to meetings and submitting proposals for funding. We are pursuing an NSF grant for CSIA curriculum improvement and plan to pursue certification as an NSA CAE before Fall 2003. We are working with Oregon Regional Alliance for Information and Network Security (RAINS) [10] to develop the Oregon Trial Emergency System Test (O-Test), a public-private partnership developing a statewide interoperable information network, a communication system and testing platform for secure disaster management. These efforts are beginning to bear fruit despite our distance from Portland where they are situated.

A lab network isolated from the university IT, yet having the capability to connect to O-Test is necessary to simulate real-world experiences. Minimal equipment requirements include a small bank of PCs and routers to provide isolation. Wireless network experiments require a Tempest shield to isolate them from the operational wireless network. Forensic experiments and demonstrations require dedicated computers that can't be used for general CS class work. The lab requires regular reconfiguration to support a variety of experiments. Instructors have developed these experiments and the laboratory as the standard computer science lab fully occupies our student lab aide.

Collaborative efforts with O-Test and RAINS, in particular by becoming a test node on the O-Test system when it comes online in early 2003, are facilitating Capstone project development, always a challenge. This requires substantial travel as most of Oregon's security industry is located in Portland, 300 miles away. We will continue developing Capstone and internship opportunities by collaborations with and outreach to business.

We need to develop, expand and update our varied faculty experience. We hope to fill a new position with an industry person with current fulltime security experience; security experience has become one of the criteria for filling replacement positions. We need to plan for the rapidly approaching day when our CSIA program faculty lead retires to his farm.

We need to further augment our existing classes with security concepts by adding access control to Database I (CIS 360) and exploring the Java security model in depth in Programming III (CS 258). Much work remains to be done, but the program is approved, accepted and active.

REFERENCES

1. US House posting on Cyber Security Act:
<http://www.house.gov/science/press/107pr/107-155b.htm>
2. Applied Computer Security Associates invited essay program:
<http://www.acsac.org/invited-essay/essays/2001-schell.html>
3. Tikekar, Rahul and Wilson, Daniel, "Implementing an e-Commerce Program in a CIS Curriculum", *The Journal of Computing in Small Colleges*, Vol 16, Number 2, pp. 9-20
4. National Security Telecommunications and Information Systems Security Standards (NSTISS): <http://www.nstissc.gov>
5. NSTISS Document 4011: <http://www.nstissc.gov/Assets/pdf/4011.pdf>
6. Scholarship for Service program: <http://www.ehr.nsf.gov/ehr/du/programs/sfs/>
7. Oregon Security Institute homepage: <http://www.oregonsecurityinstitute.org>
8. Southern Oregon University Computer Science homepage:
<http://www.sou.edu/cs/#degree>
9. Southern Oregon University CSIA homepage: <http://www.sou.edu/cs/csia>
10. Oregon Regional Alliance for Information Security homepage:
<http://www.oregonrains.org/>
11. Oregon Engineering Technology Industry Council (ETIC) homepage:
<http://www.oregonetic.org/>
12. NSF CCLI program: <http://www.ehr.nsf.gov/EHR/DUE/programs/ccli/default.asp>

13. Oregon State University Information Security Lab: <http://islab.oregonstate.edu/>
14. Pennsylvania State House Resolution No. 409, 2002 Session:
<http://www.legis.state.pa.us/WU01/L1/B1/BT/2001/0/HR0409P3222.HTM>
15. National Security Administration, Centers of Academic Excellence Measurement
Criteria: <http://www.nsa.gov/isso/programs/coeiae/measure.htm>
16. CISSP Certification Exam Overview: <http://www.isc2.org/cgi/content.cgi?category=19>
17. SANS Institute: <http://www.sans.org>
18. Towson University,
http://www.towson.edu/math/about_the_faculty/research_grant.html
19. Portland State University Computer Science Department:
<http://www.cs.pdx.edu/website/index.php>
20. East Stroudsburg University of Pennsylvania Computer Security Program:
<http://www.esu.edu/cpsc/security/csecwebpage.htm>