COMPUTER SECURITY AND IMPACT ON COMPUTER SCIENCE EDUCATION

T. Andrew Yang
Computer Science Department
Indiana University of Pennsylvania
Indiana, Pennsylvania 15705
TEL: 724-357-7995
Email address: yang@grove.iup.edu

ABSTRACT

The integration of computer security into existing Computer Science undergraduate education is an urgent and complicated task. With the increasing risk of computer intrusion, computer crimes and information wars, Computer Science educators bear the responsibility of cultivating a new generation of graduates who are aware of computer security related issues and are equipped with proper knowledge and skills to solve the problems. The task of integrating computer security into existing Computer Science programs, however, is complicated due to the fact that most faculty members lack the specialty knowledge in this field. This paper begins with a survey of the computer security field by examining the sequence of actions that the US government has taken since 1987 to counter the computer security issues, followed by an assessment of needs for practitioners in the field. A comprehensive approach of integrating computer security into an existing degree program is then proposed. The paper concludes with observations upon what should be taught and how computer security could be integrated into undergraduate education.

1. INTRODUCTION

Protection of information has been a major challenge since the beginning of the computer age. Given the widespread adoption of computer technology for business operations, the problem of information protection has become more urgent than ever. Computer files, databases, networking and the Internet-based applications all have gradually become part of the most critical assets of an organization. When these assets are attacked, damaged or threatened, data integrity becomes an issue and the proper operation of the business may be interrupted.

The problem of protecting data and information on computers has become even more critical and challenging since the widespread adoption of the Internet and the Web. The Internet has made computers across the globe interconnected. Despite the convenience of data sharing

© 2001 by the Consortium for Computing in Small Colleges

and information exchange, the Internet has also become the major highway for computer viruses to travel on. Instead of infecting one computer at a time by spreading the virus via floppy diskettes, the attackers/hackers use the Internet as the transmission channel to spread their attacking agents. Whether the spreading mechanism was a computer virus or a worm, thousands of computers could be affected within a short period of time.

The famous 'Denial of Service' (DOS)[1] attack on some of the popular e-commerce sites in 1999, for instance, had caught national attentions to the vulnerability of the Internet. Ironically, this vulnerability was part of the protocols that govern how the computers on the Internet communicate. When computers communicate more frequently with other computers over the Internet, they become increasingly vulnerable to hostile intruders who may take advantage of the very protocols, which were intended for the establishment and authentication of communication, to tie up our resources and to disable our servers. Since these attacks occur before parties are authenticated to each other, we cannot rely on enforcement of the appropriate access control policy to protect us. Instead we must build our defenses, as much as possible, into the protocols themselves (Meadows 1999).

The rest of the paper starts with examining the sequence of actions that the US government has taken since 1987, which were related to computer security. The needs of computer security curriculum in the Computer Science undergraduate education are then surveyed, followed by the current practice in computer security certification. By examining the certification requirements set by the certification bodies, I hope to identify common themes that would provide useful insights into the design of computer security curriculum. Questions regarding what and how we should teach computer security in a Computer Science undergraduate program are then asked and answered. A comprehensive approach to integrate computer security into an existing Computer Science program is then examined, which is followed by discussions upon proposed workshops, revision of courses, design of new courses, and addition of a new track in computer security into an existing degree program.

2. A LESSON OF HISTORY

The importance of computer security is best explained by examining the sequence of actions that the US government has taken during the past decade trying to address the issue. Before assessing the needs of integrating computer security into higher education, let us first take a brief look at some of the major computer-security-related documentations that have had great impact upon the US legislation and governmental structure.

The primary purpose of the *Computer Security Act of 1987*[2] was to "assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to

[1] DOS (Denial of Services): For details of the attack and counter tools, see http://www.cert.org/current/current_activity.html.

[2] Public Law 100-235 (H.R. 145) January 8, 1988.

assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate."

As stated in the *Joint Security Commission's 1994 Report* (see Joint Security Commission 1994), "the security of information systems and networks is the major security challenge of this decade and possibly the next century ... there is insufficient awareness of the grave risks we face in this arena."

In the *Executive Order 13010* (see Federal Register 1996), the President of the US ordered the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP), which consists of members from 10 executive branch departments and agencies. An Infrastructure Protection Task Force (IPTF) was also established with the Department of Justice, chaired by the Federal Bureau of Investigation, to undertake the interim coordinating mission. The Commission submitted its report, Critical Foundations, to the White House in October, 1997[3]. Among the recommendations made by the Commission include: a broad program of awareness and education; infrastructure protection through industry cooperation and information sharing; reconsideration of laws related to infrastructure protection; a revised program of research and development; a national organization structure.

The Critical Infrastructure Assurance Office (CIAO), the National Information Protection Center (NIPC), and the Information Sharing and Analysis Center (ISAC) were established in May 1998 as part of the *Presidential Decision Directive 63 (PDD 63).* PDD 63 officially expanded the US national policy to include the cyberworld (Schwartau 1999).

In the *Secretary of Defense's 1998 Annual Report to the President and the Congress*[4], a new center named Information Operations Technology Center (IOTC) was mentioned as the agency that was established to coordinate interagency information operations. Information operations (IO) were defined in the same report as "actions taken across the entire conflict spectrum to affect adversary information and information systems while protecting one's own information and information systems. Information warfare is conducted during crisis or conflict to achieve specific objectives over an adversary." Also defined in the same report, "Information assurance protects and defends information and information systems by ensuring their availability, integrity, authenticity, and confidentiality."

On 11 May 1999, NSA (National Security Agency) issued a press release designating seven universities[5] as the first Centers of Excellence in Information Assurance under the Centers

[3] See http://www.ciao.gov/PCCIP/report_index.html

[4] http://www.dtic.mil/execsec/adr98/chap8.html#top

[5] James Madison University, George Mason University, Idaho State University, Iowa State University, Purdue University, University of California at Davis, and University of Idaho.

of Excellence Program. As stated in the press release[6], "NSA's establishment of this program was spurred by the growing demand for professionals with Information Assurance expertise in various disciplines. The Centers for Academic Excellence may become focal points for recruiting and may create a climate to encourage independent research in Information Assurance."

3. ASSESSMENT OF NEEDS

While government agencies, major corporations and research institutions are examining the complex issues of protecting the Internet infrastructure against intrusions, CyberTerrorism, and even information warfare (Campen 1996; Minihan 1998), what and how should we as Computer Science educators prepare our students to operate, professionally, in such an insecure environment? I believe that it would take more than engineering and/or technology to cope with the crisis of computer security. In order to cope with the security issues, the revision of Computer Science curriculum cannot focus only on technical aspects of the discipline, but must also on broader, more comprehensive, and possibly "non-technical" aspects.

Here are some questions that educators in computing-related disciplines should address before starting to revise their curriculum to include computer security:

- How would we prepare our students so they would be security literate?"

- Given the fast advancement of computer technology, how would a faculty member become security aware and capable when teaching the new tools and techniques?

- In addition to technical solutions of computer security (such as firewalls, encryption, access controls, audit trails, training, benchmarking, interoperability, et al), should and how would the curriculum cover non-technical aspects such as social, cultural, political, legal, economic, and organizational issues? (Pattak 1999)

- Should computer security be integrated throughout the curriculum, or should special courses and/or tracks be created to address the needs?

- Should alternative curriculum delivery mechanisms be used? Examples include Web-based delivery, continuing education courses, corporate training, distance education, et al.

Before trying to answer the above questions, let us first look at a report on the 1998 NCISSE Conference, which was published in the November issue of the Electronic Journal of the U.S. Information Agency as a response of higher education to information security and warfare (Reynolds 1998). The following items mentioned in the report were particularly relevant to curricula in the higher education institutions: i) Educational institutions are encouraged to increase programs with concentrations in information security and include security courses in core curricula of all college graduates. ii) The inclusions of curricula that address the ethical and cultural issues that arise in modern information systems are especially important. iii) Since many ethical and cultural values are formed early in life, institutions of

[6] See http://www.nsa.gov/isso/programs/nietp/newspg1.htm

higher education are encouraged to develop information security curricula for and in collaboration with secondary education. iv) Educational institutions were encouraged to solicit guidance from accreditation organizations for appropriate placement of information security within their curricula. v) Higher education was encouraged to provide continuing educational programs for information security professionals who are already working in the field. vi) Information security educators are urged to develop and share practical laboratory exercises in information security, design computer games that express appropriate values for a responsible and information literate work force, develop a place to share instructional materials, and write more textbooks, especially on practical issues. vii) Specialists in legal education were called upon to help U.S. lawyers understand information security.

Based upon the report, I have made the following observations.

Observation #1: Involvement of higher education in computer security is urgently needed in training both college students and on-the-job professionals, in order to meet the challenges of protecting the information infrastructure.

Observation #2: It is important to address the ethical and cultural issues in the computer security curriculum.

4. PROFESSIONAL CERTIFICATION IN COMPUTER SECURITY

Certification programs in computer security have been provided by government agencies, professional organizations, and private corporations. By examining the certification requirements set by these certification bodies, I hope to identify common themes, which will provide useful insights into the design of computer security curriculum. The identified certification programs include the Certified Information Systems Auditor (CISA) program, the Certified Information Systems Security Professional (CISSP) program, the SNAP program, and the SAGE program. Details of these programs are discussed in the rest of this section.

The Certified Information Systems Auditor (CISA(r)) program was established in 1978 by the Information Systems Audit and Control Association (ISACA). The CISA certification focuses on five domain areas[7]: Information Systems Audit Standards and Practices and Information Systems Security and Control Practices (8%); Information Systems Organization and Management (15%); Information Systems Process (22%); Information Systems Integrity, Confidentiality, and Availability (29%); and Information Systems Development, Acquisition, and Maintenance (26%).

The Certified Information Systems Security Professional (CISSP) program was created by the International Information Systems Security Certification Consortium (ISC)2, which is supported by Computer Security Institute (CSI), Information Systems Security Association (ISSA), Canadian Information Processing Society (CIPS), and other industry presences (Power 1997). CISSP certification requires the participants to pass the CISSP exam, which

[7] See http://www.isaca.org/cert3.htm#examdescription

consists of questions covering 10 test domains[8]: Access Control Systems & Methodology; Computer Operations Security; Cryptography; Application & Systems Development; Business Continuity & Disaster Recovery Planning; Telecommunications & Network Security; Security Architecture & Models; Physical Security; Security Management Practices; Law, Investigations & Ethics.

The *SNAP*[9] program administered by GIAC[10] of the SANS[11] Institute is designed to serve the people who are or will be responsible for managing and protecting important information systems and networks. The GIAC program consists of a LevelOne Module covering the basics of information security followed by advanced and targeted LevelTwo Subject Area Modules. The LevelOne module consists of 18 elements[12]: Information Assurance Foundations; IP Concepts; IP Behavior; Internet Threat; Computer Security Policies: The Good, The Bad and The Ugly; Antiviral Tools on Desktops; Host Based Perimeter Protection; Windows NT Password Cracking; Unix Password Management; Introduction To PGP; Introduction To Cryptography 1; Introduction To Cryptography 2; Windows NT System Administration; Unix System Administration; Backups For Windows NT; Backups For Unix; Basic Windows NT Security/Auditing; Basic Linux Security/Auditing.

In 1999, after years of debate, *SAGE*[13] eventually took the first step in tackling certification for system administrators. As proposed in the latest update[14], "An overall certification program will need to have a core track with probably three levels of difficulties or progressions. ... There may also be specialty modules: security, networks, databases, et al."

The *Department of Defense* has issued a mandate that all system administrators will require "level 1" certification. The certification is required by 12-31-1999 for those working on classified systems and 12-31-2000 for those working on non-classified systems[15].

5. SO, WHAT SHOULD WE TEACH OUR STUDENTS?

[8] See http://www.isc2.org/examover.html

[9] SNAP: System and Network Assurance Program

[10] GIAC: Global Incident Analysis Center

[11] SANS: System Administration, Networking, and Security

[12] see http://www.sans.org/giactc.htm

[13] SAGE: The System Administrators Guild, a special technical group of the USENIX Association.

[14] see http://www.usenix.org/sage/cert/latest.html

[15] See http://www.usenix.org/sage/cert/latest.html

As pointed out by Powanda (1999), the basics of computer security education include: i) Understand and comply with security policy and laws; ii) Recognize potential security problems in their environment; iii) Know how to be proactive in preventing security problems; iv) React appropriately to an occurrence of a security problem; v) Know where to find additional help or information; vi) Make informed decisions on security matters; vii) Speak the "language".

The goal of a computer security program in the Computer Science education is to develop the student into a well-rounded professional who is capable of understanding, recognizing, and preventing security problems. When a problem occurs, he/she should be capable of getting necessary resources to find a solution. In addition, the computer security professional must be well versed when it comes to explaining security issues, problems, or the impact to others, such as the supervisor or co-workers.

In addition, the students graduating from the Computer Science programs must possess the following abilities: assessments of protection tools and methodologies, information on trends in disruption of information and information infrastructure, education and training on the employment of protection tools and methodologies, and the ability to educate co-workers regarding computer security.

Observation #3: A majority of computer security curriculum involves extension of traditional Computer Science curriculum, such as networking, programming, databases, et al.

Observation #4: Computer security education is more than just providing training on technical topics. It should contain components that address business and managerial aspects of computer security, such as law, investigations, ethics, physical security, and business continuity & disaster recovery.

Observation #5: Similar to other computer professions, the abilities of the students to recognize and analyze a problem and get a "handle" of it is critical for being successful in the profession of computer security.

6. A COMPREHENSIVE APPROACH

In this section, I try to answer the question of how computer security would be integrated into undergraduate education, by first examining the knowledge acquisition and transfer process in higher education institutions. The faculty plays a central role in this acquisition and transfer process. A faculty member enhances his/her professional knowledge by participating in professional conferences and seminars, collaborating with major research institutions and centers, engaging in curricular revision activities, conducting theoretical/applied research, developing and offering topical workshops, and interacting with students via classroom teaching and research activities. The knowledge and experience acquired through theses activities are then transferred to students via regular classes or workshops, as well as via publications. This acquire/transfer process is particularly characteristic in a field such as computer security, which is new to most faculty members.

To facilitate effective faculty training for newer knowledge and skills in computer security, the institution where the faculty member works must play an active supporting role, especially at the initial stage. Institutional support may include travel and/or training fund, reduced teaching load, summer research grant for professional development and/or research, support for publications and grant writing, and recognition of faculty accomplishments.

Collaboration with major research universities and research centers is an important factor in faculty professional development. Centers specializing in computer security research and training have been set up in both governmental and academic institutions. Among them are Center for High Assurance Computer Systems of the Naval Research Laboratory, Computer Security Technology Center of Lawrence Livermore National Laboratory (U.S. Department of Energy), Cyberspace Policy Institute at George Washington University, the CERT Coordination Center of the Software Engineering Institute (at Carnegie Mellon University), et al.

With the convenience of accessing information over the Web, a wide variety of resources are also available from Web sites. A list of Web sites hosting information related to computer security has been compiled and is available from my Web site[16].

Observation #6: Similar to integrating any new major technology into the Computer Science education, the integration of computer security into the undergraduate programs requires strong support from the Administration.

Observation #7: The process of integrating computer security into a program is a continuous process and involves the faculty's involvement in multiple activities, including research, professional development, curricular design, and teaching.

7. WORKSHOPS, COURSE REVISION, NEW COURSES, & A NEW TRACK

In this section, results of integrating computer security into our existing program are discussed. As stated in the previous section, the revision is a continuous process. What is presented here serves as tentative outcome from applying the comprehensive approach to answer the challenges.

- Proposed Workshops

As part of professional development as well as service to the local businesses and community, I propose the faculty to offer workshops related to computer security, by especially integrating security issues into existing technologies and specific areas in Computer Science. Sample workshops include Encryption and Cryptography, Dealing with CyberTerrorism, XML & Privacy, Building Security into Systems, Hostile Applets and the Java Security Model, Network Monitoring, Database Security, MFC & Security, Securing Your OS, and Securing Large Transaction Processing Systems, et al.

[16] See http://www.co103.iup.edu/ResourcesComputerSecurity.htm

The content of a workshop can later be incorporated into a regular course. Through the preparation and offering of workshops, faculty in Computer Science engage in learning computer security in their respective areas of specialty.

- Revision of Existing Courses[17]

Some existing courses will need to be revised to incorporate a computer security component. In a database course, for example, in addition to discussion of data modeling, SQL, et al, a major topic of the course should cover security issues in the usage and development of databases, and discuss the security features of existing database technologies.

The primary objective of this type of revision is to emphasize to the students the fact that computer security is a prevailing issue in Computer Science education, and a computer professional should take the issue into serious consideration when using or developing computer systems.

In addition to *CO441 Database Management Systems*, the following courses have also been identified as candidates for revision:

- *CO105 Fundamentals of Computer Science*

Suggested enhancement: Introduction to the importance of computer security, ethics of computer usage and legal implications of misuse. Introduction to computer viruses and awareness.

- *CO 201 Internet and Multimedia*

Suggested enhancement: Discussion of security of scripting languages (Anupam, 1998) and the security issues of Java applets, cookies, ActiveX, et al (Levine 1997)

- *CO 205 Programming Languages for Secondary Education*

Suggested enhancement: Discussion of security concerns and safe Internet access in a school setting

- *CO304 Internet Programming using Java*

Suggested enhancement: Discussion of the Java security package[18] (Levine 1997)

- *CO3*[19] *Software Engineering Concepts*

Suggested enhancement: Introduction of topics related to the development of secure software systems, such as the systems security engineering capability maturity model (Hefner 1997) and cryptographic verification (Devanbu 1997).

- New Courses

[17] See http://www.iup.edu/schedu/catalog/courses/co.htmlx

[18] See Java Security Architecture at http://java.sun.com/products/jdk/

[19] See http://www.iup.edu/schedu/catalog/courses/co.htmlx

For areas that are highly related to computer security, I propose new courses to cover computer security in these significant areas, which include Data Communications, Operating Systems, Networking, and Web-based System Development. In addition, courses that are not traditionally offered in Computer Science programs need to be created to cover the fundamental, and sometimes non-technical, aspects of computer security. These courses include Introduction to Computer Security, Ethics, Laws and Organizational Factors, Cryptography and Encryption, and CyberTerrorism and Counter Measures.

A new course titled *Information Security Lab* is proposed to provide hands-on experience for students to gain first-hand experience in hacking and defending computer systems.

Courses	Prerequisites
CO117 Introduction to Computer Security: Issues and Methodologies	CO110 Problem Solving & Structured Programming
CO207 Ethics, Laws and Organizational Factors	CO117
CO217 Information Security Lab	CO117
CO307 CyberTerrorism and Counter Measures	CO217
CO317 Cryptography and Encryption	CO310 Data Structures
CO417 Security of Operating Systems	CO432 Intro. to Operating Systems CO317
CO427 Secure Networking	CO345 Data Communications CO317
CO437 Security of Web-based System Development	CO415 Internet Architecture and Programming CO317

Table 1: Proposed New Courses in Computer Security

The courses are listed in Table 1, along with their respective prerequisites. For a listing of the exiting courses in our programs and their catalog descriptions, please see our Web site.19 We in the Computer Science Dept. are currently in the process of designing these new courses. The following paragraphs provide sketches of the major topics in each of the courses.

- *CO117 Introduction to Computer Security: Issues and Methodologies*

Issues: Why Computer Security Training Needs to be Comprehensive? One person's action can affect an entire organization; Recovering from computer virus infection is expensive; Break-in on one computer compromises a network; Poorly configured firewall can enable compromise of organizational information resources and reputation; Illegal user actions can incur liability to an organization; Laws and directives mandate relevant security training; Computer Security Act of 1987 (Powanda 1999).

Basic Units in Computer Security: Security Basics, Physical Security, Personnel Security, Technical Security, Operations Security, Network and Information Sharing, Special Applications Security, Review of Controls and Risk Management, Incident Handling, Continuity of Business Operations, Acquisition Management; Technological versus Non-Technical Aspects of Computer Security: an Overall Methodology (Pattak 1999)

- *CO207 Ethics, Laws and Organizational Factors*

Continued from CO107, this course deals with more advanced and specific topics of ethics, laws and organizational structures related to computer security.

- *CO217 Information Security Lab*

A closed lab for faculty and students to experiment with computer security theories and applications. Students may be divided into groups trying to intrude the other groups' system while protecting its own computer. The emphasis of this course is first hand experience on hacking/defending and information assurance.

- *CO307 CyberTerrorism and Counter Measures*

An intermediate level computer security course focusing on the discussions and studying of CyberTerrorism, the mechanisms adopted to launch such attacks, counter attacks that have been developed by the government agencies, legislation and resources that have been allocated for the development of these counter measures, and the link between CyberTerrorism and infowars.

- *CO317 Cryptography and Encryption*

Studying the technology of encoding and/or encrypting information so it can only be read by authorized individuals, private and public cryptography, certificates, digital signature, et al.

- *CO417 Security of Operating Systems*

The study of operating systems from perspectives of computer security, how to design a secure operating system, how to use an operating system in a secure manner, discussion of the existing mechanisms used by various operating systems to prevent intrusions.

- *CO427 Secure Networking*

Focused study of network security, discussion of security concerns on a network, the types of attacks that may be launched against a network, vulnerability of network protocols, denial-of-service attacks, studying of existing secure network servers, discussion of network protection measures such as firewalls, intrusion detection software, secure servers, network monitoring, authentication, encryption and access control methods

- *CO437 Security of Web-based System Development*

Discussion of security problems of scripting languages (Anupam & Mayer, 1998); New development of cryptographic protocols in Java development environment (Nikander & Karila, 1998); Design and implementation of a secure, intrusion-tolerant system (Wu, 1999); Major Issues of Web Security (McKee, 1999)

- Adding a New Track in the Existing Program

With the new computer security courses in place, I propose to add a new track in our undergraduate programs. Figure 1 shows the pre-requisites chart for the new track. The new track shares, with the other tracks in our programs, the lower level core courses such as co110 (Problem Solving and Structured Programming), co210 (Object-Oriented Programming and GUI), and co310 (Data Structures). It also shares some upper level core courses such as co432 (Introduction to Operating Systems) and co415 (Internet Architecture and Programming) with one of the tracks.

It is not feasible to require students majoring in this new track to take all the security related courses to fulfill the major requirements. Alternative scheduling is being investigated such that a student may choose one of the alternatives and complete the major requirements. Two of the alternatives are presented below.

Alternative 1:
freshmen year: co105, co110

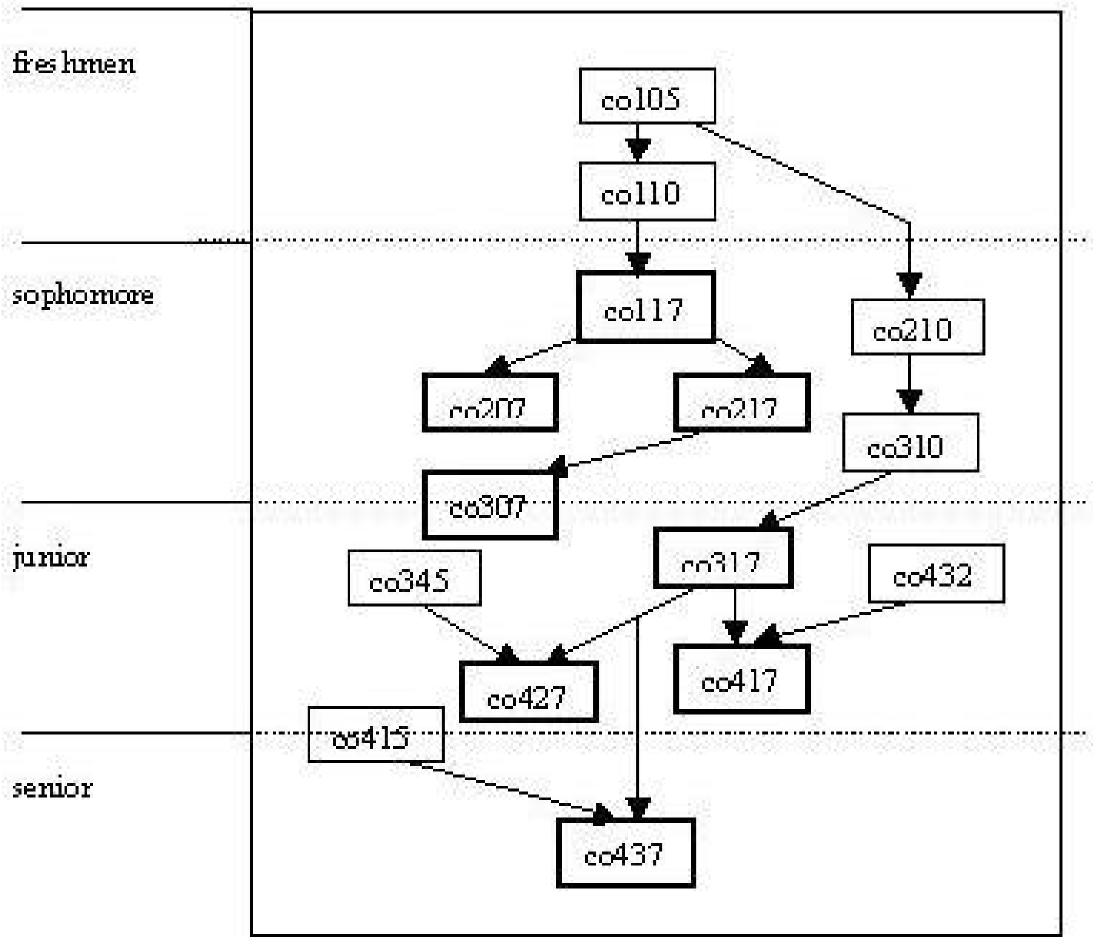

Figure 1: Pre-requisite Chart for the Computer Security Track

sophomore year:	co117, co210, co310, and one of co207 and co217
junior year:	co317, co432
senior year:	co415, co437

<u>Alternative 2:</u>

freshmen year:	co105, co110
sophomore year:	co117, co210, co310, co217
junior year:	co307, co317, co345
senior year:	co427

Depending on the area(s) in which a student is interested, he/she may pick either alternative 1, focusing on secure operating system and Web-based development, or alternative 2, focusing on CyberTerrorism and secure networking. Other combinations are certainly possible.

8. SUMMARY

The integration of computer security into the existing Computer Science undergraduate education is an urgent and complicated task. With the increasing risk of computer intrusions, computer crimes and information wars, Computer Science educators bear the responsibility of cultivating a new generation of graduates who are aware of computer security related issues and are equipped with proper knowledge and skills to solve the problems. The task of integrating computer security into the Computer Science programs, however, is complicated by the fact that most faculty members lack the specialty of the field. In addition, the fast advancement of computer technology, especially in the Internet and Web related fields, makes the updating of professional knowledge and skills a constant requirement.

In this paper, a comprehensive approach of integrating computer security into an existing degree program was proposed. Related issues and procedures were examined. It was realized that the integration of a new field such as computer security would have major impact on the overall curriculum and degree programs. A comprehensive knowledge acquisition and transferring process was proposed to enable successful integration. Strong and innovative institutional support will play a major role in determining the success of the integration.

Throughout the paper, observations that I made with respect to what should be taught and how computer security could be integrated into the undergraduate education were discussed. New courses and a new track on computer security were proposed as part of the integration.

9. REFERENCE

Anupam, V. & A. Mayer 1998: Security of Web Browser Scripting Languages: Vulnerabilities, Attacks, and Remedies, Proceedings of the 7th USENIX Security Symposium, USENIX.

Campen, A.D. et al (Ed.) 1996, CyberWar: Security, Strategy and Conflict in the Information Age, AFCEA International Press.

Federal Register 1996, Executive Order 13010 - Critical Infrastructure Protection, Federal Register Vol. 61, No. 138, July 17, 1996.

Hefner, Rick 1997: Lessons learned with the systems security engineering capability maturity model, Proceedings of the 1997 international conference on Software engineering.

Joint Security Commission 1994, Redefining Security: A Report to the Secretary of Defense and the Director of Center Intelligence[20].

Levine, D.E. 1997, What's Brewing with Java And ActiveX?, Information Security Magazine, December 1997.

McKee, B. 1999: A comprehensive view of Web security, Computer Security Alert, Computer Security Institute, March 1999.

Meadows, C. 1999: A Formal Framework and Evaluation Method for Network Denial of Service, Proceedings of the 1999 IEEE Computer Security Foundations Workshop, IEEE.

Minihan, K.A. 1998: Defending The Nation Against Cyber Attack: Information Assurance in the Global Environment, Electronic Journal of the U.S. Information Agency (USIA), Volume 3, Number 4, November 1998.

Nikander, P. & A. Karila 1998, A Java Beans Component Architecture for Cryptographic Protocols, Proceedings of the I7th USENIX Security Symposium, USENIX.

Pattak, P.B. 1999: Non-technical Factors Influencing IT Security, 12th Annual FISSEA (Federal Information Systems Security Educators' Association) Conference[21], NIST (National Institute of Standards and Technology).

Powanda, J. 1999: Assembling a Curriculum for Various Security Disciplines, 12th Annual FISSEA Conference, NIST.

Power, R. 1997: Should You Take the CISSP Exam?, Computer Security Alert, Computer Security Institute, March 1997.

Reynolds, C.W. 1998: The Response of Higher Education to Information Warfare, Electronic Journal of the U.S. Information Agency (USIA), Volume 3, Number 4, November 1998.

Schwartau, W. 1999, Infrastructure Is Us, Information Security Magazine, June 1999[22].

Wu, T. et al, 1999: Building Intrusion Tolerant Applications, Proceedings of the USENIX Security Symposium, USENIX.

[20] See http://fas.org/sgp/library/jsc/

[21] http://csrc.nist.gov/organizations/fissea/99Fissea.html

[22] See http://www.infosecuritymag.com/jun99/Infrastruc.htm