Information Security Curriculum Creation: A Case Study

Bradley Bogolea
College of Engineering
The Pennsylvania State University
University Park, Pa 16802
bdb194@cse.psu.edu

Kay Wijekumar
School of Information Sc & Technology
The Pennsylvania State University
Monaca, Pa 15601
+1 724-773-3814
kxw190@psu.edu

ABSTRACT
Information Security is a critical part of the technology infrastructure. A survey of undergraduate degree programs in Computer Science, Information Technology, Management Information Science, and others show a lack of emphasis on security issues in their curriculum. The purpose of this paper is to present a case study on our approach to creating an undergraduate curriculum that will enhance existing degree programs in Computer Science and Information Technology to provide an increased awareness of Information Security concepts. Our rationale includes: research on existing Information Security programs, review of other Information Security curriculum development efforts, assessments and surveys of workforce needs in Information Technology pertaining to security, applying government directives, and the process of creating a curriculum to address the discovered gaps. Our approach is unique in its usage of surveys of Information Technology professionals, interviews with professionals, and a comprehensive survey of workforce needs in Information Security along with a review of other curriculum development efforts. From this case study, we will be able to suggest and define an Information Security curriculum that will best answer today's security challenges.

Categories and Subject Descriptors
K.3.2 [**Computer and Information Science Education**]: Computer Science education, Curriculum, Information Systems education.

General Terms
Management, Measurement, Documentation, Performance, Design, Experimentation, Security, Human Factors.

Keywords
Curriculum, Information Security, Information Assurance, Information Technology, Security, Infosec, Assessment, Surveys

1. INTRODUCTION
Computer Security is defined as the prevention of, or protection against, access to information by intruders and intentional but unauthorized destruction or distortion of that information [1]. Computers have become integral to businesses, governments, and agencies in their everyday activities. Many millions of dollars are lost when there is any disruption of computer availability. In recent months, malware such as MyDoom, NetSky, SoBig, Sasser and others have cost vast sums of work time and capital, caused disruptions in banking and power systems and even shutdown entire company networks and equipment. Therefore, computer security, which once was a secondary issue, is taking center stage in many companies and their Information Technology (IT) groups. How do we prepare Computer Science or IT majors for this new world? The purpose of this paper is to present a case study on our approach to creating an undergraduate curriculum that will enhance existing degree programs in Information Technology and Computer Science. We include our rationale, research on existing programs, surveys, reviews of existing curriculum development efforts, and plans for the curriculum.

InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA.

2. BACKGROUND INFORMATION
As technology and its uses and abuses expand at rapid rates, the need for information security professionals is rising at a demanding rate. More professionals are also slated to join the computer security industry to police and protect cyberspace [2]. This shortage could be remedied by increasing and developing security education as specialized collegiate degrees or enhancing existing degree programs with security related courses.

Users of cyberspace, especially computer security students and professionals, must take responsibility for the overall health and security of the cyberworld. Adequate education and training curriculum must be identified and implemented beginning in the halls of academia [2].

3. CURRICULUM REVIEW
Historically, courses in Information Security have been offered as special topics, as a small part of a curriculum, or as specialized programs designed just for security. We reviewed five university programs that have been recognized as Information Security leaders. These degree programs are designed to address the shortage of security professionals created by high-paced technology growth and the complexities of securing data and networks [3]. These programs were all Graduate Programs.

Graduate Programs Reviewed
Carnegie Mellon University [4]
Master of Science i*n Information Security Technology and Management*

James Madison University [5] Master of Science in *Computer Science Concentration in Information Security*
Purdue University [6] Master of Science *in Information Security*
Johns Hopkins University [7] Master of Science in *Security Informatics*
George Mason [8] Master of Science in *Information Security and Assurance*

In preparation for conducting our needs analysis and documenting the concepts that must be part of the curriculum, we started by identifying the major themes of the Graduate Programs. The following table by Ed Crowley, University of Houston, developed from the Report on Information Assurance by Melissa Dark and Jim Davis [10], coincides with our findings:

Graduate Programs Areas [9]

Management, Policy and Response	Security Policy Guidelines, Security awareness, Ethical decision making and high technology, Employment practices and policies, Operations security and production controls, E-mail and Internet use policies, Using social psychology to implement security policies, Auditing and assessing computer systems, Cyberspace law and computer forensics, Privacy in cyberspace, Protecting intellectual property, Security standards for products, Management responsibilities and liabilities, Developing security policies, Risk assessment and risk management, Incident Response and Recovery
Recovery Secure Computing Systems	Access control, Identification, Authentication, and Authorization, Design of Secure Systems, Evaluation, Databases and their applications, Software Development, Auditing, Operations Management
Network Security	Protocols, Network basics, Vulnerabilities, Attacks, Application layer services, Management, Monitoring, Auditing and Forensics, Infrastructure, Wireless and broadband, Filtering
Cryptography	Development, Fundamentals, Symmetric algorithms, Asymmetric algorithms, Cryptographic protocols, Hardware Implementations, Digital signatures, Public Key Infrastructure and Certificate Authorities, Implementation issues, Applications, Cryptanalysis, Steganography, Latest Developments

Initially, multiple undergraduate programs in Computer Science and Information Technology were reviewed. We found few programs that offered an emphasis/minor in Information Security.

Therefore, it was necessary to identify and turn to the visionary curriculum efforts that did focus on Information Security for our analysis.

We examined five of these curriculum development efforts within academia. This comparing and contrasting of findings of other curriculum developers, paired with our analysis, gives our study a unique perspective and more in-depth coverage of Information Security Curriculum needs.

The five published works completed case studies [11, 9, 12, 10, 13] analyzing development of curriculum within higher education. The analyses included a variety of findings ranging from defining curriculum needs to survey development.

Our goal is to compare the findings of these previously published works, analyze the data and integrate the discoveries into a more comprehensive curriculum recommendation.

Case A: Security Education within the IT Curriculum [11]:

Case A sought to implement a security component into their existing IT curriculum. The researchers administered a web-based survey seeking to gather information from individuals who attended an educator's conference at the Institute. They surveyed the need for more security content within IT Curriculum and their mechanics for creating it. Their response rate was rather poor and only received a 10% response. The respondents of the survey stated that security was a concern for all IT disciplines. However, the lack of respondent feedback and relevancy in certain survey questions create questionable conclusions.

Case B: Information System Security Curricula Development [9]

Case B surveyed current literature concerning Information Systems Security training and education. Then they created a four-course graduate level program specializing in Information Security Education. The curriculum was gleaned from government efforts by the National Security Telecommunications and Information Systems Security Committee (NSTISSC); National Training Standard for Information Systems Security Industry efforts (ISC2); the International Information Systems Security Certifications Consortium, Inc.; Information Systems Audit and Control Association (ISACA); in addition to other graduate academic efforts.

Case C: An Undergraduate Track in Computer Security [12]

Case C developed a high-quality computer security track that uses and builds upon already-established computer courses and allows students to finish degrees in four years without an additional course load. The targeted courses expose students to various vulnerabilities and security problems as well as hands-on security breaches.

Case D: Report on Information Assurance Curriculum Development [10]

Case D developed a framework for undergraduate and graduate programs in Information Security. The framework was established through discussion via workshops and working groups of education experts. The report resulted in an outline of

knowledge and skills required in a comprehensive Information Security Degree program.

Case E: Computer Security and Impact on Computer Science Education [13]

Case E addresses the immediate need for the integration of computer security education into undergraduate curriculum and the difficulty of this task. Through a survey of the computer security field, examination of US government efforts since 1987 to counter computer security issues and the implementation of a field needs assessment, the researcher proposes a comprehensive approach of integrating computer security into an existing degree program. The paper suggests Information Security topics that should be taught and how it can be assimilated into today's undergraduate programs.

4. SURVEY OF RECENT GRADUATES

We surveyed recent graduates from the Computer Science and Information Technology program to identify how many graduates had experienced security related issues in their job and how prepared they were to handle those situations. The survey was constructed by blending findings from existing needs assessment instruments and focal issues from the curriculum research. We believe these topics are mandated for IT program graduates with a security focus. Table 1 presents the themes identified for the survey of recent graduates.

Table 1:

Information Security Fundamentals
• Information Security challenges brought about by computers and the Internet.
• Basic Information Security terminology.
• Importance of protecting information assets.
• Information Security related issues, unauthorized or inappropriate access to information or systems, malicious hackers, cyberterrorism, viruses, etc.
Information Privacy
• Why privacy is a major concern to individuals, businesses, and government agencies.
• Strategies for protecting privacy.
Information Security Policies
• Why information security policies play a critical role in a secure framework.
• Explore writing Information Security policies, procedures, and standards.
Risk Management
• Define risk management and its importance.
• Explore risk analysis techniques to identify and quantify the threats.
• Importance of contingency and disaster recovery planning.
Access Controls
• Understand why access control is a critical part of Information Security.
• Identify three basic categories of controls as physical, technical or system, and data access.
Cryptography
• Understand why cryptography is a critical part of Information Security.
• Basic cryptography terminology.
• Explore how cryptography is used to provide integrity, confidentiality, and authentication.
Firewalls
• Understand the purpose for using firewalls.
• Hardware vs. software firewalls.
• Different firewall technologies such as packet filtering, proxying, and network address translation (NAT).
Intrusion Detection
• Understand why Intrusion Detection Systems (IDS) are a critical part of Information Security.
• Intrusion Detection terminology: intrusion, misuse, anomaly detection, etc.
E-commerce Security
• Understand the importance of e-commerce security to the business enterprise.
• Identify current threats facing organizations that conduct business online and how to mitigate these challenges.
Virtual Private Networks
• Understand Virtual Private Networks (VPNs) and their purpose.
Wireless Network Security
• Explore threats to wireless systems.
Incident Response
• Identify different types of incidents and response methods.
• Computer emergency response teams and incident handling.
Computer Forensics
• Understand why computer forensics is an essential part of Information Security.
• Basic forensic principles and methodology
• Forensic techniques, processes and procedures must be executed in accordance with legal and evidence standards.
Identity Theft
• Identity theft and identity fraud crimes are an increasing problem.
• How to reduce your chances of becoming a victim.

5. SURVEY OF IT PROFESSIONALS

The purpose of this survey is to gather information from Information Technology professionals about their needs for employees with security training and the areas of security that are of highest concern to their organizations. Table 2 presents the themes identified for the survey:

Table 2:

Information Security Fundamentals
• Information Security concepts: confidentiality, integrity, availability, authentication, auditing, etc.
• Information Security awareness.
• Threats, vulnerabilities, viruses and other malicious code.
• Legislation and industry standards.
Information Security Policies
• Information Security policies, procedures, and standards.
• Acceptable Use Policies (AUP).
• Compliance and enforcement.
Access Control
• Physical, technical, and administrative access control mechanisms.

• Biometric identification.
Risk Analysis
• Identify and quantify information security threats.
• Contingency planning and disaster recovery
Security Resources
• CERT, CIAC, SANS, and other resources.
Operating System security
• Common server threats, vulnerabilities, and control issues
• Password management, user accounts/privileges, antiviral solutions.
Authentication and Encryption
• Key encryptions and algorithms.
• Public Key Infrastructure (PKI).
• Digital signature and certificate authorities.
• SSL and secure web transactions.
Firewalls
• Firewall technologies such as packet filtering, proxying, and network address translation (NAT).
• Content filtering.
Network Auditing Tools and Penetration Testing
• Network vulnerability assessment tools and scanners.
E-Commerce Security
• Current threats facing organizations that conduct business online and how to mitigate these challenges.
Computer Forensics
• Detecting computer crime.
• Investigating computer crime.
• Identifying, collecting, processing, and preserving evidence.
• Processes and procedures must be executed in accordance with legal and evidence standards.
• Preventing computer crime.

6. SURVEY RESULTS

Surveys were conducted with Information Technology professionals and undergraduate students concerning the importance of Information Security issues.

6.1 Results of IT Professionals

78 Information Security professionals were surveyed at the InfoSecurity 2003 conference, New York City, 12-2003 [14]. All survey subjects were IT professionals holding upper management and high level technical positions.

Review of results revealed a strong consensus that the Information Security topics should be a focus in IT undergraduate study and those students must be aware of and have a basic understanding of these Information Security issues.

Respondents suggested more emphasis in curriculum focused on the studies of application security and physical security. It was also suggested that undergraduates should have the opportunity to join a professional organization such as the ISSA (Information Systems Security Association) to increase awareness as well as other professional opportunities [15]. Other major security resources suggested were the Open Web Application Security Project [16] and the ICAT Database [17].

At the InfoSecurity Conference, we also culled suggestions for future survey development from interviewees.

Table 3:

Title	**Number of Individuals**
President	8
Senior Manager	28
IT Director & Security	28
Marketing/Sales	14
Number of Employees	**Number of Organizations**
>5000	10
1000 – 4999	9
100 – 999	30
< 100	29

6.2 Results of IT Students

52 Information Technology students were surveyed. Initially, a small group of students was asked the survey questions orally. Using this method, we found a fairly unanimous consensus that the students lacked a concrete understanding of Information Security issues. Since we needed to confirm this with a larger pool, we decided to administer a written survey. This survey was then distributed to the students and once they completed it, it was collected. However, these results were inconclusive because the students were from the same pool and stated they had a detailed understanding of these concepts.

7. INTERVIEW RESULTS

Personal interviews were conducted with Information Technology professionals to gather their thoughts on the Information Security education process. Interviews are still being conducted. All interview subjects are IT professionals holding upper management and high level technical positions.

Listed below are the interview questions. These interviews were conducted via e-mail. Due to the open ended nature of these questions and different opinions about the Information Security Education process, it is difficult to document the results. These results will be presented at the *InfoSecCD Conference'04* or can be retrieved by contacting the authors.

Interview Questions
• What is the biggest problem within Information Security education?
• What is your opinion on the best method to stay atop of this dynamic industry (e.g. formalized education within academia, certifications, training, etc)?
• What skills are InfoSec professionals lacking and your thoughts on addressing this issue?
• What are some of the strengths of your InfoSec professionals?
• What other problems are you currently running into with InfoSec professionals (e.g. shortage of skilled individuals, scope of expertise, cost of skilled individuals, training, staying atop dynamic industry)?
• What methods are you using to increase InfoSec awareness

within your organization?

8. CURRICULUM DEVELOPMENT

The curriculum approach we plan to propose includes a new focus for the much-needed addition of courses for undergraduates who would like to learn more about security.

Our approach is a unique blend of recent publication findings by educators, surveys of IT professionals, interviews with professionals attending a major Information Security conference [14], graduate curriculum and IT undergraduate degree earner's contributions.

Through researching all these avenues, our recommendations present a comprehensive list of Information Security curriculum concepts.

In addition, the findings should complement what is required to meet industry standards and correlate with new government directives.

It is a must that our recommendations rise to accommodate such criteria. The Software Engineering Institute at Carnegie Mellon University in *Information Assurance Curriculum and Certification: State of the Practice* cites that strong and diverse skills are required by professionals in *the dynamic and increasingly hostile networked environment [18]*.

Government organizations have also come to the forefront to define directives to security curriculum development and standards. National Security Agency (NSA), the National Institute for Standards and Technology (NIST), The Committee on National Security Systems (CNSS) are all proponents making security education and training a goal and have set new standards.

NSA, through partnerships with academia and industry, has developed the National Information Assurance Education and Training Program (NIETP) for advocacy of improvements in Information Security through education, training and awareness.

The NIETP encourages and recognizes universities through the outreach program, Centers of Academic Excellence in Information Assurance Education, and sponsors the National Colloquium for Information Systems and Security Education [19].

The CNSS, under presidential directive, has developed national training standards for security. The committee sets national policy and oversees the protection of the nation's critical infrastructure including emergency preparedness.

The NIST creates guidance on computer security. The agency provides a learning continuum for security awareness, training, education and professional development [20].

We suggest curriculum developers utilize these government resources.

We believe our research is an effort to answer these standards for Information Security by blending the best studies and research.

The following Information Security curriculum concepts were tabulated after compiling our results from the surveys, results and suggestions from our interviews, comparing with other curriculum development efforts and suggested government directives. These concepts identified below must be covered in courses preparing computer professionals for the future. Table 4 shows a comprehensive list of the proposed curriculum concepts.

Table 4:

Information Security Fundamentals
• Information Security challenges brought about by computers and the Internet. • Basic Information Security terminology. • Importance of protecting information assets. • Information Security related issues, unauthorized or inappropriate access to information or systems, malicious hackers, cyberterrorism, viruses, physical security, etc. • Information Security concepts: confidentiality, integrity, availability, authentication, auditing, etc. • Increasing Information Security awareness. • Threats, vulnerabilities, viruses and other malicious code. • Legislation and industry standards.
Information Privacy
• Why privacy is a major concern to individuals, businesses, and government agencies. • Strategies for protecting privacy.
Security Resources
• CERT, CIAC, SANS, NIST, and other resources.
Information Security Policies
• Why information security policies play a critical role in a secure framework. • Explore writing Information Security policies, procedures, and standards. • Acceptable Use Policies (AUP). • Compliance and enforcement.
Risk Management
• Define risk management and its importance. • Explore risk analysis techniques to identify and quantify the threats. • Importance of contingency and disaster recovery planning.
Access Controls
• Understand why access control is a critical part of Information Security. • Identify three basic categories of controls (security) as physical, technical or system, and data access. • Biometric identification.
Cryptography
• Understand why cryptography is a critical part of Information Security. • Basic cryptography terminology. • Explore how cryptography is used to provide integrity, confidentiality, and authentication. • Key encryptions and algorithms. • Public Key Infrastructure (PKI). • Digital signature and certificate authorities. • SSL and secure web transactions.
Operating System security
• Common server threats, vulnerabilities, and control issues • Password management, user accounts/privileges, antiviral solutions.
E-Commerce Security
• Current threats facing organizations that conduct business online

and how to mitigate these challenges. • Web application security
Firewalls
• Understand the purpose for using firewalls. • Hardware vs. software firewalls. • Different firewall technologies such as packet filtering, proxying, and network address translation (NAT). • Content filtering.
Intrusion Detection
• Understand why Intrusion Detection Systems (IDS) are a critical part of Information Security. • Intrusion Detection terminology: intrusion, misuse, anomaly detection, etc.
Network Auditing Tools and Penetration Testing
• Network vulnerability assessment tools and scanners.
E-commerce Security
• Understand the importance of e-commerce security to the business enterprise. • Identify current threats facing organizations that conduct business online and how to mitigate these challenges. • Application Security.
Virtual Private Networks
• Understand Virtual Private Networks (VPNs) and their purpose.
Wireless Network Security
• Explore threats to wireless systems.
Incident Response
• Identify different types of incidents and response methods. • Computer emergency response teams and incident handling.
Computer Forensics
• Understand why computer forensics is an essential part of Information Security. • Basic forensic principles and methodology, processes and procedures must be executed in accordance with legal and evidence standards. • Detecting computer crime. • Investigating computer crime.

9. CONCLUSION

In this paper we presented a case study on our approach to creating an undergraduate curriculum that will enhance existing degree programs in Computer Science and Information Technology. The concepts identified must be covered in courses preparing computer professionals for the future. Our approach is unique in its usage of surveys of Information Technology professionals, interviews with professionals, and a comprehensive survey of workforce needs in Information Security along with a review of other curriculum development efforts. From this case study, we defined an Information Security curriculum that will best answer today's security challenges.

10. REFERENCES

[1] Ross, Seth. (1999) Unix System Security Tools. Computer Security a Practical Definition. Available on March 12, 2004 at http://www.albion.com/security/intro-4.html

[2] Khosla, Pradeep. (2003) Carnegie Mellon University Announces new degrees in Information Security to address needs of Government, Industry. Available on March 12, 2004http://www.ini.cmu.edu/academics/MSISTM/msistm_curricu.htm

[3] NSTSC (2003) National Strategy to Secure Cyberspace. A National Cyberspace Security Awareness and Training Program. p. 37 Available on March. 12, 2004 at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[4] Information Security (Master of Science in Information Security Technology and Management - MSISTM). 13 Jan 2003. Carnegie Mellon University. Available on March 12, 2004 at http://www.ini.cmu.edu/academics/MSISTM/index.htm

[5] Master of Science in Computer Science Concentration in Information Security. James Madison University. Available on March 12, 2004 at http://www.infosec.jmu.edu/website/overview.htm

[6] Infosec Graduate Program. Purdue University. Available on March 12, 2004 at http://www.cerias.purdue.edu/education/graduate_program/

[7] Master of Science in Security Informatics. Johns Hopkins University. Available on March 12, 2004 at http://www.jhuisi.jhu.edu/education/index.html

[8] Master of Science degree program in Information Security and Assurance. George Mason University. Available on March 12, 2004 at http://www.isse.gmu.edu/ms-isa/

[9] Crowley, Ed. "Information System Security Curricula Development." Proceeding of the 4th conference on information technology curriculum on Information technology education. Oct 2003. Available on March 12, 2004 at portal.acm.org/

[10] Dark, Melissa. Davis, Jim. "Report on Information Assurance Curriculum Development". The Center for Education and Research in Information Assurance and Security (CERIAS). Available on March. 12, 2004 at http://www.cerias.purdue.edu/education/post_secondary_education/undergrad_and_grad/curriculum_development/information_assurance/

[11] Border Ph.D., Charles. Holden, Ed. "Security Education within the IT Curriculum". Proceeding of the 4th conference on information technology curriculum on Information technology education. Oct 2003. Available on March 12, 2004 at portal.acm.org/

[12] Azadegan, S. Lavine, M. O'Leary, M. Wijesinha, A. Zimand, M. "An Undergraduate Track in Computer Security". ACM SIGCSE Bulletin, Proceedings of the 8th annual conference on Innovation and technology in computer science education, Volume 35 Issue 3. June 2003. Available on March 12, 2004 at portal.acm.org/

[13] Yang, Andrew. "Computer Security and Impact on Computer Science Education". The Journal of Computing in Small Colleges , Proceedings of the sixth annual CCSC northeastern conference on The journal of computing in small colleges, Volume 16 Issue 4. April 2001. Available on March 12, 2004 at portal.acm.org/

[14] Infosecurity Conference and Exhibition 2003. Available on March 12, 2004 at http://www.infosecurityevent.com/

[15] The Information Systems Security Association (ISSA)®. Available on March 12, 2004 at http://www.issa.org/

[16] The Open Web Application Security Project (OWASP). Available on March 12, 2004 at http://www.owasp.org/

[17] ICAT Metabase: A CVE Based Vulnerability Database. National Institute of Standards and Technology. Available on March 12, 2004 at http://icat.nist.gov/

[18] Information Assurance Curriculum and Certification: State of the Practice. Carnegie Mellon University. Available on March 12, 2004 at http://www.sei.cmu.edu/publications/documents/99.reports/99tr021/99tr021chap02.html

[19] National Information Assurance Education and Training Program (NIETP). National Security Agency (NSA). Available on March 12, 2004 at http://www.nsa.gov/ia/academia/acade00001.cfm

[20] Awareness, Training, and Education Computer Resource Center (CSRC). National Institute for Standards and Technology (NIST). Available on March 12, 2004 at http://csrc.nist.gov/ate/