University of Houston

Systems Security Specialization Specification

Contents

Prepared by: Ed Crowley, Crowleye@Yahoo.com

Jan 04

1.0 **The Vision**

The Security Program began with a vision of what our graduates would be able to do after graduation. Like all College of Technology graduates, these students are expected to bring skills that add specific values to an organization. Security students are expected to: "Add value by providing information assurance."

The National Security Telecommunications and Information Systems Security Committee (NSTISSC)[1] defines information assurance as:

> Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Specific skills, these students bring to an organization include prudent business risk analysis and policy methodologies as well as knowledge of appropriate, cost effective, technical and administrative countermeasures.

Based upon this vision, program goals were articulated. Specific goals were that students would be able to: analyze, develop, implement, and maintain, appropriate organizational information systems services. Services include information integrity, confidentiality, availability, authentication and non-repudiation.

An appropriate Institutional Program Goal, for a College of Technology, is to "Teach basic skills with an emphasis on a professional path." Successful teaching requires the embrace of a unique security education attribute. That attribute is that "Students Learn Information Security by Doing It". In contrast to some other disciplines, knowing what to do (and why) does not necessarily enhance an organization's security posture.

Consequently, to achieve our vision, it is necessary that our students be able to do IA. As a result, the course specifications list both required knowledges and skills. Knowledges can be tested with conventional academic written and oral methodologies whereas skill must be demonstrated.

---

[1] *Now known as the Committee on National Security Systems (CNSS).*

As security is a broad multidisciplinary field, it is important that the program have a specific focus. InfoSec programs tend to have one of three general types of focus: managerial, technical, or balanced. Emphasis in a managerial program is on people, planning, policy, programs and projects. In contrast, emphasis in a technical program is on the design, installation, testing, and maintenance of security controls and equipment. As one would expect, balanced programs, typically found in community colleges, seek a balance between managerial and technical emphasis.

The UH program emphasizes security as a systemic process that includes policy, administrative, and technical components. In a curriculum matrix, it would lie closest to the managerial focus. The program however distinguishes itself in two technical dimensions. One, it is designed for people that have a technical background. And two, it provides a significant amount of laboratory technical experience. Our philosophy is that a security practitioner or manager that has built and run tools, like protocol analyzers and intrusion detection systems, will be a more effective professional than one lacking that experience. The program distinguishes itself from balanced programs by the depth of managerial coverage.

A survey of recent literature found that our students would likely pursue one of three career paths.

1.1 **Potential Career Paths**

Practitioner	Manages Enterprise Security
Managers/Planners	Responsible for enterprise operations e.g. CIO
Auditor/Investigator	Audit/investigate computing systems

Table 1.0

Research further showed that each career path required a specific set of Knowledges and Skills. As shown on the following table, each potential career path is supported by a core of related competencies.

Practitioner	Manager/Planner	Auditor/Investigator
Risk management	Risk management	Forensics
Ethics and Law	Ethics and Law	Law and evidence
Computing Tech	Software engineering	Privacy
Personnel Man	Personnel Man	Psychology
Design and test	Design and test	Multinational norms
Telecom and networking	Access control	Access control
	Intellectual property	
	Purchasing and acquisitions	

Table 1.1

1.2 Security Specialization

This graduate level specialization consists of four, three credit hour courses. Prior to enrolling in the specialization, students are expected to have either earned a technical undergraduate degree or to have gained equivalent experience working with information systems security.

Specialization development was based upon current security offerings, existing security standards, and input from local professional, governmental, and private organizations. Future goals include packaging the four courses as a certificate and submitting the curriculum to the NSA for 4011 certification.

Principles, the gateway class, may also be taken by advanced undergraduates. Principles serves as a prerequisite for the other three security classes.

2.0 Principles of Information System Security

This course covers the basic principles of information systems security. Included are specific, administrative and technical, security controls. It also includes the methodologies that organizations utilize to create and achieve security goals. In addition to information systems security legal and regulatory aspects, emphasis is placed on management issues and solutions. Specific control measures include system access controls, telecommunications network security, encryption, and physical security.

Class activities are augmented with laboratory activities that provide students the opportunity to apply the principles. Laboratory activities focus on four areas: Operating Systems, Telecommunications, Cryptography, and Security Management.

Table 2.1

Principles of Information Systems Security, Knowledges

Knowledges	
Management Practices Risk Management and Assessment Security planning Security policies Personnel security Security personnel Data classification and storage Risk Management Security education, training and awareness program Change/configuration management Assessment strategies	Physical Security Site selection and security Guards Keys and locks Doors, walls and gates Intrusion detection systems Fire detection and suppression systems Biometrics CCTV
Architecture and Models Security models Information systems evaluation criteria System certification and accreditation Security architectures	Cryptography Cryptosystems Ciphers and encryption algorithms Asymmetric key systems Symmetric key systems Hybrid key systems Message authentication/message digests Public key infrastructure Key management Digital signatures Alternative cryptosystems Security protocols

Access Control Systems Access control fundamentals Access control types Access control attacks	Telecommunications and Networking Network types (LAN/WAN) OSI reference model TCP/IP protocol suite Telecomm security management Telecommunications threats and attacks Remote access protocols
Application Development Systems development life cycles Database development and management Systems controls Distributed applications Object oriented concepts Knowledge based systems Application and systems attacks and vulnerabilities Malicious code	Incident response Auditing Monitoring
Operations Security Operations concepts Threats and countermeasures	Business Continuity Planning/Disaster Recovery Contingency planning Business continuity planning Disaster recovery planning Data backup and recovery methods Crisis management
Law, Investigations, & Ethics Law categories and types Computer crimes Computer crime investigations Computer ethics Computer forensics procedures	

Table 2.2

Principles of Information Systems Security, Skills

Skills	
Management Policy Policy Generation	Cryptography PGP Install/configure/operate Asymmetric Key Pair Generation Document Encryption Hashing Steganography S-Tools JPHS
Operating System Secure Install Baseline Patch Install/configure/operate Antivirus Spyware scanner Personal Firewall	Telecommunications Personal Firewall Firewall Log Analysis Install/Configure/operate Port Scanner Packet Analyzer

3.0 *Secure Enterprise Computing:*

Incident Response and Computer Forensics

Incident Response and Computer Forensics deal with detective aspects of computer security. Primary incident response goals include answers to the questions: What happened? And who is responsible? Other goals include the gathering and preserving of evidence in a manner congruent with court presentation. Specific procedures required to appropriately respond to a security incident are also presented.

This course focuses on the detection, isolation and response to security incidents. Security incidents may involve crimes using computers as the object of a crime or they may involve computer misuse. Both the preservation of evidence and the successful return of the computer system to routine operation are emphasized.

Class activities are augmented with laboratory activities. Laboratory activities concentrate on four areas: hard drive and network forensics, document integrity (hashing), password auditing (cracking), and system integrity.

Table 3.1

Incident Response and Computer Forensics, Knowledges

Knowledges	
Incident Response Incident Response Process Developing an Incident Response Team	Intrusion Detection Introduction
Basic Forensics Methodology HD Forensics System Forensics Network Forensics Internet Forensics	Cryptanalysis
Security Policy and the Law Privacy Law Evidence Rules Cyberspace Law	Access Control Radius Password Cracking
Computer Systems Audit and Assessment	Malicious Software
	System Integrity

Table 3.2

Incident Response and Computer Forensics, Skills

Skills	
HD Forensics • Linux DD Network Forensics • Ethereal Network Scans	Access Control • Password Cracking • L0pht Crack • John the Ripper
Cryptography • Integrity (MD5-SUM) Editors (Win-Hex)	Systems Integrity • Tripwire

4.0 Information Systems Security

Applied Cryptography and Intrusion Detection

This class covers the cryptographic services required to securely send confidential information across the Internet. It also covers related cryptographic services that provide integrity, authentication, and nonrepudiation. General topics include Network Defense and Countermeasures. Specific technical topics include: public key infrastructure, digital signatures, certificates, virtual private networks (VPNs), and Intrusion Detection.

Intrusion detection systems either provide an organization assurance that their network infrastructure has not been compromised or a means to detect and limit the security compromise.

Class activities are augmented with laboratory activities that provide the students the opportunity to apply the principles. Laboratory activities focus on five areas: Public Key Infrastructure, Proxy Servers, Intrusion Detection Systems, building a bastion host, and Remote Access.

Table 4.1

Applied Cryptography and Intrusion Detection, Skills

Knowledges	
Symmetric Ciphers DES AES	Intrusion Detection System Components Process Preventive Measures Logging Intrusion Signature Analysis Identifying Suspicious Events Developing IDS Filter Rules
Cryptographic Applications Hashes Digital signatures Key exchange Protocols Cryptographic Protocols	Virtual Private Networks Tunneling Protocols IPSec/IKE Secure Shell (SSH) Layer 2 Tunneling Protocols
Communications Concepts TCP/IP	Web Security TLS/SSL

Perimeter Devices Firewalls Bastion Hosts Proxy Servers Rules and Restrictions	

Table 4.1

Applied Cryptography and Intrusion Detection, Skills

Skills
Certificate Server Installation Managing Certificates
IPTables Identifying an Nmap Scan
IDS Installation • SNORT • Capture packets with Snort • Configure a SNORT rule set • Use IDScenter as a Snort Front End Perform Network Signature Analysis Differentiate between normal and abnormal signatures
Set up a Remote Access Server Configure a VPN Server Establish a VPN Connection Activate IPSec and Specifying a Policy Configuring L2TP
Build a Bastion host

5.0: *Information Systems Security:*

Risk Analysis and Management

This course examines the enterprise strategic security analysis and planning process. This process begins with an examination of an enterprises goals and how security adds value. It proceeds through vulnerability, threat, and risk analysis. Issues related to risk response and policy generation are also covered. Specific issues include an enterprise's ethical and legal environment.

Students are introduced to several threat, vulnerability, and risk analyses methodologies. Formal methodologies enable an enterprise to demonstrate that its informational assets are secured in a prudent and cost effective manner.

Students utilize the NSA's IAM to perform an INFOSEC Assessment. Students also learn to analyze and construct appropriate security policies and procedures. Related subjects include security planning, security process models, as well as continuity planning and disaster recovery planning.

Class activities are augmented with projects that provide students the opportunity to apply risk management principles. Projects focus on three areas: creating a policy handbook, planning a security assessment, and creating an organization disaster recovery plan.

Table 5.1

Information Systems Security Risk Analysis and Management, Knowledges

Knowledges	
Strategic Risk Analysis and Management Methodologies including: Vulnerability Analysis Threat Analysis Risk Analysis	Formal Risk Analysis Process FRAP OCTAVE IAM
Risk Assessment Methodologies Frap OCTAVE NSA's IAM	Contemporary issues in computer security regulations and laws, including: Contract law Intellectual and other property law Criminal law Constitutional law Liability law Regulatory law

Differentiate between quantitative and qualitative assessment methodologies.	Principal ethical issues with relationship to legal standards.
Current Information Systems Security legal and regulatory environment.	Distinguish the legal issues in an information architecture that can be analyzed by a computer security professional from those that require an attorney.

Table 5.1

Information Systems Security Risk Analysis and Management, Skills

Skills
Create a contingency and disaster recovery plan.
For a particular industry, research the current legal and regulatory environment.
Create a security auditing and monitoring plan for an enterprise.
Create a policy handbook.
Perform a service learning activity such as creating an INFOSEC Assessment

References

[1] Bishop, M., "Teaching Computer Security," SEC 1993: 65-74.

[2] Bishop, M., "Computer Security Education: Training, Scholarship, and Research," IEEE Computer 35 (4) Privacy and Security Supplement pp. 30-32 (Apr. 2002).

[3] Bishop, M., "What Do We Mean By 'Computer Security Education'?," Proceedings of the 22nd National Information Systems Security Conference p. 604 (Oct. 1999).

[4] Bishop, M., "Academia and Education in Information Security: Four Years Later," Fourth National Colloquium on Information System Security Education (May 2000).

[5] D. L. Brinkley and Schell, R. R., Concepts and Terminology for Computer Security, in Information Security: An Integrated Collection of Essays, ed. Abrams and Jajodia and Podell, IEEE Computer Society Press, Los Alamitos, CA, 1995, pp. 40-97.

[6] Chin, S.-K., Irvine, C. E., and Frinke, D., "An Information Security Education Initiative for Engineering and Computer Science," Technical Report NPSCS-97-003 ,Naval Postgraduate School, Monterey, CA, December 1997.

[7] Dark, M., and Davis, J., "Report on Information Assurance Curriculum Development", June 2002.

[8] Davis, J. and Dark, M., "Defining a curriculum framework in Information Assurance and Security", 2003 ASEE Annual Conference, Nashville, TN, June 2003.

[9] Davis, J., "Building an IA Program: A Few First Steps," NCISSE Boot Camp, June 2002.

[10] Fundaburk, A. (in review) Assessing the Need for Teaching Information Security in an Office Information Systems Curriculum. Information Technology, Learning, and Performance Journal.

[11] Irvine, C.E., Warren, D. F., and Clark, P. C. The NPS CISR Graduate Program in INFOSEC: Six Years of Experience. In Proceedings of the 20thNational InformationSystems Security Conference, pp. 22-30, Baltimore, MD, October 1997.

[12] Laswell, B., Simmel, D., and Behrens, S. "Information Assurance Curriculum and Certification: State of the Practice," CMU/SEI-99-TR-021, Software Engineering Institute, Carnegie Mellon, Pittsburg, PA, Sept. 1999.

[13] Maconachy, V., Schou, C., Ragsdale, D., and Welch. D., "A Model for Information Assurance: an Integrated Approach," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, (West Point, NY), 2001.

[14] NSTISSI, "No. 4011 - National Training Standard for Information Systems Security (INFOSEC) Professionals," 1994.

[15] Spaford, E., "Teaching the Big Picture of InfoSec," National Colloquium For Informationsystems Security Education (NCISSE), VA. 1998.

[16] Vaughn R., "Ware to Start?," National Colloquium For Informationsystems Security Education (NCISSE), 2001.

[17] Vaughn R., Henning R., and Fox K., "An Empirical Study of Industrial Security - Engineering Practices," Journal of Systems and Software, vol. 61, no. 3, pp. 225-232, June 2002.

[18] Wilson, Mark, ed. Information Technology Security Training Requirements: A Role- and Performance-Based Model, NIST Special Publication 800-16, National Institute of Standards and Technology, U.S. Department of Commerce, 1998.

[19] Yasinsac, A. Information Security Curricula in Computer Science Departments: Theory and Practice. Manuscript, 2001.

[20] Yurcik, W. and Doss, D., "Different Approaches in the Teaching of Information Systems Security," Information Systems Education Conference (ISECON), Cincinnati, OH, 2001.