Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

Approaches for Integrating Trustworthy Computing in the Computing Curricula

Kassem Saleh, *CISSP, Senior Member, IEEE* and Imran Zualkernan, *American University of Sharjah*

Abstract – Trustworthiness and Education figure among the challenges and risks facing the constructive use of information technology. Security, reliability, survivability, predictability are among system attributes that are not receiving enough attention. Critical infrastructures are still vulnerable to attacks and accidental collapses. University curricula seem to be less responsive to trustworthiness needs of critical systems and infrastructures. In this paper, we propose two approaches for embedding trustworthy computing foundational topics within the knowledge areas of two computing-related disciplines, namely computer science and computer engineering. These additional topics are elicited from the information security common body of knowledge introduced by (ISC)^2, and from the main requirements for compliance to the ISO17799 information security management standard.

Index terms – Common body of knowledge, computing curricula, education, ISO17799, trustworthy computing.

I. INTRODUCTION

Two of the most pressing problems associated with risks to the constructive use of information technologies, as identified by Peter Neumann [1], are trustworthiness and education. According to Neumann, system and network security reliability, survivability, interoperability, and behavioral predictability are not receiving enough attention. The current computing-related curricula are not responsive to the trustworthiness concerns needed to be addressed in critical systems and infrastructures. In this paper, we contribute in addressing these two issues by proposing two approaches for the inclusion of the foundational background of trustworthiness requirements in two existing computing-related curricula, namely, the computer science and the computer engineering curricula [2, 3].

In our work, we adopt Microsoft's definition of trustworthiness. According to Microsoft [4], the four pillars of trustworthy computing are security, privacy (P), reliability (R), and business integrity (BI). Security addresses issues are generally divided into confidentiality (C), integrity (I), availability (AV), and accountability (AC). Privacy is related to the fair handling of information. Reliability is related to the dependability on the system to offer its services. Finally, business integrity is related to the responsiveness and ethical responsibility of the service provider. Other related definitions exist. According to the Software Engineering Institute, system survivability is related to the capability of the system to fulfill its mission in a timely manner in the presence of attacks, failures or accidents. Consequently, survivability is related to tolerance to both accidental harm (system safety), and malicious harm (system security) [5,6]. Cisco defines business resilience to involve strategies for business continuity by maintaining operations during and after a disruption and also improves the organization's overall ability to do its business [7]. The six components of a business resilience strategy include network, applications, communications and workforce resilience, in addition to security and network management.

Various information security educators have addressed the incorporation of information security knowledge in the computing curriculum. In what follows, we provide a brief overview of this work. Whitman and Mattord [8] propose five approaches to implementing information security curricula: 1) adding elements to existing courses, 2) adding elements to a capstone course or courses, 3) creating independent security courses, 4) offering minors or certificates in security, and 5) offering separate security degree programs. These different approaches are then offered according to four different scenarios. Irvine et al. [9] propose two approaches for integrating security in the computing curricula: 1) computer security as the focus of the curriculum and can be studied in depth, and 2) security as an important property to be addressed in all courses. White and Nordstrom [10] recommend the infusion of security across the curriculum. Petrova et al. [11] propose two approaches for embedding security in the curriculum: (1) offer seven security courses as part of an undergraduate specialization, and (2) offer an elective course in information security. Finally, McGinnis and Comstock [12] propose the inclusion of additional topics in four of the knowledge areas of the ACM/IEEE Computing Curricula 2001 [2].

Our work differs in many aspects from existing approaches. First, we address security as a part of trustworthiness, and we aim at integrating trustworthiness in two computing-related curricula of computer Science and computer engineering. Second, unlike [12], one of our proposed approaches is more comprehensive, and

The authors are with the School of Engineering at the American University of Sharjah, Box 26666, Sharjah, UAE
Email: ksaleh@aus.edu

ISBN 1-933510-96-7/$15.00 ©2007 CISSE

covers the trustworthiness elements in all the computing curricula knowledge area. Finally, unlike other works, we derive trustworthiness elements from two authoritative sources: the information security common body of knowledge [13], and the international standard for information systems security management [14]. One primary objective of these proposed changes is to produce graduates that are able to work effectively in organizations implementing and maintaining compliance to the ISO17799 international standard [14].

The rest of the paper is organized as follows. Section 2 provides a preliminary background on the various elements of our proposed approaches to incorporating trustworthiness in the computing curriculum. Section 3 describes our approach for integrating trustworthiness and proposes a way for its implementation. Section 4 provides two alternative curriculum deliveries. Finally, Section 5 concludes the paper.

II. BACKGROUND

In this section, we provide preliminary background on the elements of our proposed outcome-driven approaches for integrating trustworthiness in the curriculum. We first describe the main idea behind our approaches. Then we briefly introduce the information security common body of knowledge (ISBOK) [13] and the components of the international standard for information systems security, ISO 17799 [14]. Finally, we briefly describe the model ACM/IEEE body of knowledge for two computing curricula.

A. The Idea

The main idea behind our proposed approaches is to embed the foundational elements of trustworthy computing within the existing knowledge areas of the computer science and computer engineering disciplines, and to introduce a new knowledge area on information security whose elements are not covered in the existing areas. The foundational elements of trustworthy computing are elicited based on two sources; the information security common body of knowledge and the ISO 17799 security standard. The ultimate goal of our proposed integrative approach is to have graduates that will be able, within three years after graduation, to effectively participate in teams implementing and maintaining standard-compliant security programs in their respective organizations.

B. Information Security BOK

The Information Security Common Body of Knowledge (ISBOK) was defined by the International Information Systems Security Certification Consortium, or (ISC)² [13]. The ISBOK includes the basic knowledge elements an information security professional should possess. It consists of ten knowledge domains as briefly described in the following.

1. Security management practices: it includes the identification of assets and the development and maintenance of policies, standards, procedures and guidelines for managing the security of assets and developing a comprehensive security program. The use of risk management and mitigation techniques to identify threats, vulnerabilities, and appropriate controls is emphasized.
2. Security architecture and models: it includes the concepts and principles for securing systems, including networks, operating systems, database systems and software systems.
3. Access control systems and methodology: it includes the techniques and technologies used to identify, authenticate and authorize accesses to the assets of a system.
4. Physical security: includes the techniques, technologies and standards for the physical protection of assets and their perimeter and embedding infrastructures.
5. Operations security: includes the roles and responsibilities of security personnel in ensuring system security and reporting on the security status. Operational security also includes the various operational controls needed.
6. Cryptography: includes the methods, techniques and standards needed to ensure confidentiality, integrity, authenticity and non-repudiation.
7. Application development security: includes the concepts and environment needed to develop secure software.
8. Telecom, networks and internet security: it includes the security controls needed to provide confidentiality, authenticity, integrity and availability of transmitted messages over various networking devices and links.
9. Business continuity planning: includes the techniques and controls to ensure system availability and business recoverability when an incident or disaster occurs.
10. Law, investigation and ethics: includes the laws and regulations governing the use of computers, and the means for performing and concluding a successful computer crime investigation.

C. ISO 17799 Standard

The ISO 17799 standard [14] establishes the code of practice for information security management. It provides recommendations for initiating, implementing and maintaining information security within an organization. It can also be used as the basis for the development of an

effective security program. The standard emphasizes the following building blocks for information security.

1. Security policy: addresses the importance of developing and maintaining security policies.
2. Organizational security: addresses the importance of putting an organizational structure with clear roles and responsibilities, and reporting mechanisms to deal with security, both within the organization and when dealing with a third party.
3. Asset management: addresses the issues related to the classification and control of inventory for information system assets.
4. Human resources security: addresses the security controls and screening when hiring employees, user training and security awareness and responsibility programs.
5. Physical and environmental security: addresses the physical security aspects related to the perimeter and the assets.
6. Communications and operations management: addresses operational security issues related to the day-to-day procedures and responsibilities, media handling, system and capacity planning, monitoring and network management.
7. Access control: addresses the various mechanisms to control access to operating systems, networks and software, and defines the user access management rights and responsibilities.
8. Information systems acquisition, development and maintenance: addresses the elicitation of security requirements, and the development of secure software and systems applications using cryptographic controls and secure acquisition, development and maintenance processes and environments.
9. Information security incident management: deals with the reporting of security events and weaknesses, and the management of incidents and security improvements.
10. Business continuity management: addresses issues related to the development and maintenance of an effective business continuity plan including risk management.
11. Compliance: addresses the compliance with laws, regulations and standards, and the importance of maintaining these compliances. It also stresses the importance of auditing as a control for enforcing compliance.

It is clear that for an information security professional to be involved in the many aspects of the ISO 17799 standard requires the professional to be knowledgeable in the domains of the ISBOK.

D. Computing Curricula

The computing curricula (CC 2001) [2] includes twelve knowledge areas, each includes both core topics and optional topics. These areas are: algorithms and complexity (AL), architecture and organization (AR), discrete structures (DS), human-computer interaction (HCI), information management (IM), intelligent systems (IS), net-centric computing (NC), operating systems (OS), programming fundamentals (PF), programming languages (PL), software engineering (SE), and social and professional issues (SP).

The Joint Task Force on Computing Curricula from the IEEE Computer Society and the Association of Computing Machinery proposed the curriculum guidelines for computer engineering in 2004 [3]. This report divides the computer engineering knowledge areas into algorithms (ALG), computer architecture and organization (CAO), computer system engineering (CSE), circuits and signals (CSG), database systems (DBS), digital logic (DIG), digital signal processing (DSP), electronics (ELE), embedded systems (ESY), human-computer interaction (HCI), computer networks (NWK), operating systems (OPS), programming fundamentals (PRF), software engineering (SWE), VLSI design and fabrication (VLS) and social and professional issues (SPR). In addition, the Computer Engineering and the Computer Science curriculum include foundation courses in discrete structures (DS) and probability and statistics (PRS).

III. MODIFIED KNOWLEDGE AREAS

In this section, we list the topics that are added to the knowledge areas of the computer science and computer engineering curricula. The trustworthiness requirements that are addressed by each topic are also listed in an abbreviated form after the topic.

A. Trustworthy Computing in the CS Curriculum

To incorporate the knowledge needed in the ISBOK and to be able to be an effective participant in an ISO17799-compliant security program, we propose the following additional topics to the CSBOK shown in Table 1.

AL. Algorithms and Complexity
-Cryptographic algorithms and analysis (C, I, AC)
-Hashing algorithms (I, AC)
-Design and analysis of fault-tolerant, self-stabilizing, error-recoverable algorithms (AV,R)
-Forward and backward recovery algorithms (AV, R)
AR. Architecture and Organization
-Hardware redundancy and reliability concepts (AV, R)
-Design for Testability, Built-In Self-Test (AV, R)
-Self-diagnosis and self-repairing (AV, R)

DS. Discrete Structures -Number theory (C) -Discrete log and reducibility (C)
HC. Human-Computer Interaction -Secure user interface design (AV, R, BI) -Tradeoffs between security and usability (AV, R, BI)
IM. Information Management -Information classification (C, I) -Database security and access control (C, I) -Granularity, auditing and availability (AC, AV) -Replicated and distributed databases (AV) -Database backup, recovery and fault-tolerance (AV, R)
OS. Operating Systems -Trusted OS, layered security architecture (C, I, AV, AC) -Orange book, ITSEC & common criteria (C, I, AV,AC) -Hardening OS (C, I, AV, AC) -Security Models and access control models: MAC, DAC, RBAC, NDAC (C, I, AC, BI) -Computer and hardware forensics (AC, BI) -Accountability, auditing and monitoring (AC, BI)
PS: Probability and Statistics -Reliability estimation and modeling (R, I, A, BI)
PF. Programming Fundamentals -Secure coding techniques (C,I,AC,AV,R) -Code reviews and walkthrough for security (C,I,AC,AV,R,BI) -N-version programming, N-voting (AV,R)
PL. Programming Languages -Exception handling (AV,R) -Cryptographic API (C,I,AC)
IS. Intelligent Systems -Agents security (C, I, AV, P, BI)
NC. Net-centric Computing -Network resiliency, redundancy, reliability and error-recoverability (AV, R) -Communications and network security: email security, PGP. Firewalls, IDSs, IPSec, SSL, SSH, SET, wireless security, VPN (C, I, AV, AC) -Key management & public key infrastructures (C,I, AC) -Vulnerability assessment/penetration testing (C,I, AV,R) -Mobile agents, platforms and security (C, I, AV, AC, R) -Network forensics (AC) -Web services security (C, I, AC, AV, R)
SE. Software Engineering -Software reliability (AV, R) -Software Fault-tolerance, Design for security (AV, R) -Testing security, Misuse case (C, I, AC, AV, R) -Software security – requirements specifications, design, coding and testing (C, I, AC, AV, R, BI) -Software forensics (AC, BI) -Software vulnerabilities and risks: malware, Trojan horses, covert channels, buffer overflows and data validation attacks (C, I, AV, AC, R, BI)
SP. Social and Professional Issues -Law and ethics in information security (AC, BI) -Privacy laws and concerns (P, BI) -Forensics and evidences (AC) -Liability, due care and due diligence (AC, BI) -Roles & responsibilities of security personnel (AC,BI,P)

Table 1. Summary of topics on trustworthiness added to existing computer science knowledge areas.

In addition, we propose to include a new knowledge area on information security as follows in Table 2.

SC. Information Security Management -Security engineering life cycle models (C,I,AV,AC) -Security planning, security programs, security awareness (C, I, AV, AC, BI, P) -Contingency planning: IRP, BIA, DRP, BCP (C,I,AV,AC,R,BI) -Physical and infrastructure security (C, I, AV, AC) -Security standards (C, I, AV, AC) -Security procedures and policies (C, I, AV, AC) -Security risk management (C, I, AV, AC) -Personnel security (AC, BI, P) -Security tools (C, I, AV, AC)

Table 2. Proposed additional knowledge area on information security management.

B. Trustworthy Computing in the CE Curriculum

A number of topics in the CE curriculum [3] overlap with those in CS. These knowledge areas (algorithms, computer architecture and organization database systems, software engineering, human computer interaction, operating systems, discrete structures, probability and statistics) require addition of the same trustworthiness topics as the corresponding CS areas as outlined in Table 1. It should be noted that some knowledge areas have slightly different names. For example, the Database knowledge area in CE corresponds to the Information Management area in CS. In addition to these topics, we propose the following additional topics to the CEBOK shown in Table 3.

CSE. Computer Systems Engineering -Software/Hardware Integration Security Trade-offs (I, AV, AC, R) -Specification of Trustworthiness Requirements (P, R, BI, C, I, AV)
CSG. Circuits and Signals - Introduction to Shielding Technologies (C)
DSP. Digital and Signal Processing - Encryption Algorithms (C, I) - Biometric Application (P)
ELE. Electronics - Hardware Redundancy and Reliability (AV, R)
ESY. Embedded Systems -Communications and network security for RTOS (C, I, AV, AC)

-Security Models and access control models for RTOS (C, I, AC, BI)
NWK: Computer Networks -Network resiliency, redundancy, reliability and error-recoverability (AV, R) -Vulnerability assessment and penetration testing (C, I, AV,R) -Mobile agents, platforms & security (C, I, AV, AC, R) -Network security and forensics (C,I,AV,AC) -Web services security (C, I, AC, AV, R)
VLS: VLSI Design and Fabrication -Device Reliability (AV, R) -Design for testability and Built-in self-test (I, R) -Boundary scan principles (I, R) -Manufacturing test techniques and process reliability (R, I, BI) -IDDQ testing (R, I)

Table 3. Summary of topics on trustworthiness added to existing CE knowledge areas.

IV. ALTERNATIVE CURRICULUM DELIVERIES

After having decided on the additional knowledge topics within existing and new knowledge areas, we should be providing ways for delivering this new content to students. We propose two approaches to deliver these additional foundational elements of trustworthy computing.

In the first approach (Approach A), we propose to distribute these new elements on the existing supporting courses in the curriculum. For example, software security would be addressed in one of the software engineering courses in the curriculum. In this approach, an additional new core course on Information Security Management would be needed to cover the new knowledge area on Information Security.

In the second approach (Approach B), we propose to cluster together related topics in trustworthy computing in separate courses. These courses could be offered as part of a specialization area within the degree program or can be taken as computer elective courses towards the degree program. Hence, we propose the following three courses as shown below in Tables 4-6.

Each of the proposed alternative delivery has its own merits and demerits. The main merits of Approach A are that (1) additional trustworthiness foundations are taught along with the related knowledge area topics and it seems a natural flow of topics, and (2) all students will be exposed to these additional topics. However, the drawbacks of this approach are (1) 'information overloading'; It requires the course instructor to squeeze additional advanced topics in the already heavy material in each individual course, (2) the lack of textbooks that can be used, and (3) the collaboration and willingness of all instructors teaching the affected courses. On the other hand, the main merit of Approach B is that by bundling the three proposed additional (elective) courses in a specialization area, we are making trustworthy computing a clear and visible body of knowledge allowing students to add value to their computing degree. The demerit is that not all graduates will be exposed to the additional body of knowledge. However, interested students will still be able to take one or more of these courses as computer elective courses.

Trustworthy Security Management Course
-Security engineering life cycle models (C,I,AV,AC)
-Security planning, security programs, security awareness and training (C,I,AV,AC,BI,P)
-Contingency planning: incidence response planning (IRP), business impact analysis (BIA), disaster recovery planning (DRP), and business continuity planning (BCP) (C,I,AV,AC,R,BI)
-Physical and infrastructure security (C,I,AV,AC)
-Security standards (C,I,AV,AC)
-Security procedures and policies (C,I,AV,AC)
-Security risk management (C,I,AV,AC)
-Security tools (C,I,AV,AC)
-Law and ethics in information security (AC, BI)
-Privacy laws and concerns (P,BI)
-Forensics and computer crime investigation (AC)
-Liability, due care and due diligence (AC,BI)
-Personnel security, roles & responsibilities (AC,BI,P)

Table 4. Proposed common CS and CE course on Trustworthy System Management

Trustworthy Computer Systems Course
-Cryptographic algorithms and analysis (C, I, AC)
-Hashing algorithms (I, AC)
-Number theory (C)
-Discrete log and reducibility
- Reliability estimation and modeling (R, I, A, BI)
-Hardware redundancy & reliability concepts (AV, R)
-Design for Testability, Built-In Self-Test (AV, R)
-Self-diagnosis and self-repairing (AV, R)
-Network resiliency, redundancy, reliability and error-recoverability (AV, R)
-Communications and network security: email security, PGP. Firewalls, IDSs, IPSec, SSL, SSH, SET, wireless security, VPN (C, I, AV, AC)
-Public key infrastructures (C,I,AC)
-Vulnerability assessment & penetration testing (C,I,AV,R)
-Mobile agents, platforms & security (C, I, AV, AC, R)
-Network forensics (AC)
-Web services security (C, I, AC, AV, R)
-Trusted OS, layered security architecture (C,I,AV,AC)

-Orange book, ITSEC &common criteria (C,I,AV, AC) -Hardening OS (C, I, AV, AC) -Security Models and access control models: MAC, DAC, RBAC, NDAC (C, I, AC, BI) -Computer and hardware forensics (AC, BI) -Accountability, auditing and monitoring (AC, BI)

Table 5. Proposed common CS and CE course on Trustworthy Computer Systems

Trustworthy Computer Software Course
-Secure coding techniques (C, I, AC, AV, R) -Design and analysis of fault-tolerant, self-stabilizing, error-recoverable algorithms (AV, R) -Forward and backward recovery algorithms (AV, R) -Code reviews & walkthrough for security (C, I, AC, AV, R, BI) -N-version programming, N-voting (AV, R) -Cryptographic API (C, I, AC) -Software reliability and exception handling (AV, R) -Software Fault-tolerance, Design for security (AV, R) -Testing security, Misuse case (C, I, AC, AV, R) -Software security – requirements specifications, design, coding and testing (C,I,AC,AV,R,BI) -Software forensics (AC, BI) -Software vulnerabilities and risks: malware, Trojan horses, covert channels, buffer overflows and data validation attacks (C, I, AV, AC, R, BI) - Information classification (C, I) -Database security and access control (C, I) -Granularity, auditing and availability (AC, AV) -Replicated and distributed databases (AV) -Database backup, recovery & fault-tolerance (AV, R) -Secure user interface design (AV, R, BI) -Tradeoffs between security and usability (AV, R, BI) -Software agents security (C, I, AV, P, BI)

Table 6. Proposed CS course on Trustworthy Computer Software.

Trustworthy Computer Engineering Course
-Secure coding techniques (C, I, AC, AV, R) -Design and analysis of fault-tolerant, self-stabilizing, error-recoverable algorithms (AV, R) -Forward and backward recovery algorithms (AV, R) -Software reliability and exception handling (AV, R) -Software Fault-tolerance, Design for security (AV, R) - Information classification (C, I) -Database security and access control (C, I) -Granularity, auditing and availability (AC, AV) -Secure user interface design (AV, R, BI) -Tradeoffs between security and usability (AV,R, BI), Sw/Hw Integration Security Trade-offs (I, AV, AC,R) -Specification of Trustworthiness Requirements (P,R, BI,C,I,AV) - Introduction to Shielding Technologies (C) - Encryption Algorithms (C, I) - Biometric Application (P)

- Hardware Redundancy and Reliability (AV, R) - Device Reliability (AV, R) -Design for test (at the transistor level) (I, R) -Boundary scan principles (I, R) -Manufacturing test techniques & process reliability (R, I, BI) and -IDDQ testing (R, I)

Table 7. Proposed CE course on Trustworthy Computer Engineering.

Each of the proposed alternative delivery has its own merits and demerits. The main merits of Approach A are that (1) additional trustworthiness foundations are taught along with the related knowledge area topics and it seems a natural flow of topics, and (2) all students will be exposed to these additional topics. However, the drawbacks of this approach are (1) 'information overloading'; It requires the course instructor to squeeze additional advanced topics in the already heavy material in each individual course, (2) the lack of textbooks that can be used, and (3) the collaboration and willingness of all instructors teaching the affected courses. On the other hand, the main merit of Approach B is that by bundling the three proposed additional (elective) courses in a specialization area, we are making trustworthy computing a clear and visible body of knowledge allowing students to add value to their computing degree. The demerit is that not all graduates will be exposed to the additional body of knowledge. However, interested students will still be able to take one or more of these courses as computer elective courses.

In our school of engineering, we have adopted Approach B. We have introduced a minor and a specialization area in software engineering and security. In the security part, we have introduced three courses: computer security, software security and security management. These offerings are in their second year and they seem to be well-received by engineering students.

V. CONCLUSIONS

In this paper, we proposed additions to the knowledge area topics of computing-related curricula to address the important issues related to the trustworthiness of computer systems and infrastructures. These additions aim at meeting the requirements for the ISBOK and the information security code of practice standard elements. Students taking these topics will become effective participants in team developing or maintaining a standard-compliant security program. We then propose two approaches for delivering these additional topics: one relies on injecting these topics in their related courses, and the second relies on bundling together these additional topics in separate courses. Each of these approaches has its own merits and demerits. We think that the approach

to adapt depends on the available resources and the strategic plan of the department offering these courses.

VI. REFERENCES

[1] P. Neumann, "Inside risks: the big picture", Communications of the ACM, Vol. 47, No. 9, September 2004, pp. 112.

[2] ACM/IEEE Computing Curricula 2001, December 2001.

[3] ACM/IEEE Computer Engineering 2004: Curriculum Guidelines, December 2004.

[4] C. Mundie, P. deVries, P. Haynes, and M. Corwine, "Trustworthy computing", Microsoft White Paper, October 2002, 10 pages.

[5] D. Firesmith, "Common concepts underlying safety, security and survivability engineering", Carnegie Mellon University, Software Engineering Institute Technical Report CMU/SEI-2003-TN-033, December 2003, 61 pages.

[6] R. Linger, H. Lipson, J. McHugh, N. Mead, and C. Sledge, "Life-cycle models for survivable systems", Carnegie Mellon University, Software Engineering Institute Technical Report CMU/SEI-2002-TR-026, October 2002, 57 pages.

[7] G. Otteson, "Recipe for resilience", Packet, First Quarter 2005, Cisco Systems, pp. 35-39.

[8] M. Whitman and H. Mattord, "Designing and teaching information security curriculum", Proceedings of the 1st Annual Conference on Information Security Curriculum Development, pp. 1-7, 2004.

[9] C. Irvine, S. Chin and D. Frincke, "Integrating security into the curriculum", Computer, Vol. 31, No. 12, 1998, pp. 25-30.

[10] G. White and G. Nordstrom, "Security across the curriculum: using computer security to teach computer science principles", Proc. 19th National Information Systems Security Conference, NIST, Baltimore, MD., 1996, pp. 483-488.

[11] K. Petrova, P. Kaskenpalo, A. Philpott and J. Buchan, "Embedding information security curricula in existing programs", Proceedings of the 1st Annual Conference on Information Security Curriculum Development, pp. 20-29, 2004.

[12] D. McGinnis and K. Comstock, "The implication of information assurance and security crisis on computing model curricula", Information Systems Education Journal, Vol. 1, No. 9, September 2003.

[13] S. Hansche, J. Berti and C. Hare, Official (ISC)2 Guide to the CISSP Exam, Auerbach Publications, 2003.

[14] ISO/IEC 17799:2005. (2005). International Organization for Standardization (ISO), Code of Practice for Information Security Management, Switzerland.