



ISSN: 1545-679X

Information Systems Education Journal

Volume 2, Number 3

<http://isedj.org/2/3/>

February 2, 2004

In this issue:

An Information System Security Course for the Undergraduate Information Systems Curriculum

Grace C. Steele

Morgan State University
Baltimore, MD 21251

Vojislav Stojkovic

Morgan State University
Baltimore, MD 21251

Jigish S. Zaveri

Morgan State University
Baltimore, MD 21251

Abstract: This paper presents the justification for a dedicated course called Information Systems Security (ISS) to be added as an elective course to the Undergraduate Information Systems (IS) Curriculum Model. The rationale and purpose for the development and implementation of such a course is provided. The IS'97 Model Curricula is used as the framework for discussion of the course and a suggestion is made for the proper placement of the course within the IS curriculum based on this model. A basic framework and design of the course is presented and instructional strategies and competency levels are discussed.

Keywords: IS curriculum model, IS security, course design

Recommended Citation: Steele, Stojkovic, and Zaveri (2004). An Information System Security Course for the Undergraduate Information Systems Curriculum. *Information Systems Education Journal*, 2 (3). <http://isedj.org/2/3/>. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2003*: §2422. ISSN: 1542-7382.)

This issue is on the Internet at <http://isedj.org/2/3/>

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: <http://isedj.org/> • Contact person: Don Colton (editor@isedj.org)

Editor
Don Colton
Brigham Young Univ Hawaii
Laie, Hawaii

The Information Systems Education Conference (ISECON) solicits and presents each year papers on topics of interest to IS Educators. Peer-reviewed papers are submitted to this journal.

2003 ISECON Papers Chair

William J. Tastle
Ithaca College
Ithaca, New York

Associate Papers Chair

Mark (Buzz) Hensel
Univ of Texas at Arlington
Arlington, Texas

Associate Papers Chair

Amjad A. Abdullat
West Texas A&M Univ
Canyon, Texas

EDSIG activities include the publication of ISEDJ, the organization and execution of the annual ISECON conference held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

© Copyright 2004 EDSIG. In the spirit of academic freedom, permission is granted to make and distribute unlimited copies of this issue in its PDF or printed form, so long as the entire document is presented, and it is not modified in any substantial way.

An Information System Security Course for the Undergraduate Information Systems Curriculum

Grace C. Steele
Vojislav Stojkovic
Computer Science Department, Morgan State University
Baltimore, MD 21251, USA

and

Jigish S. Zaveri
Department of Information Science and Systems
Morgan State University
Baltimore, MD 21251, USA

Abstract

This paper presents the justification for a dedicated course called Information Systems Security (ISS) to be added as an elective course to the Undergraduate Information Systems (IS) Curriculum Model. The rationale and purpose for the development and implementation of such a course is provided. The IS'97 Model Curricula is used as the framework for discussion of the course and a suggestion is made for the proper placement of the course within the IS curriculum based on this model. A basic framework and design of the course is presented and instructional strategies and competency levels are discussed.

Keywords: Information systems curriculum model, information systems security, course design

1. INTRODUCTION

The field of Information systems (IS) has seen dynamic growth, constantly evolving in response to the rapid advancements in technology. In response, the IS curriculum has undergone a number of significant changes in the past two decades. Every few years, IS professional bodies in conjunction with academia and industry engage in the redesign of the IS curricula in an effort to keep up with changes in technology and the environment. IS program directors and curriculum developers are forced to constantly update their programs to stay current with rapid developments of new technologies and to meet the needs of a changing society. A number of researchers have contended that there is a gap between what academia provides and what is required by industry

(Couger et al., 1995; Lee et al., 1995; Trauth et al., 1993).

One of the main objectives of the undergraduate curriculum in IS is to prepare graduates to understand the field, both as an academic discipline and as a profession within the context of a larger society (Davis et al., 1997; Lee, et al., 1995; Tucker et al., 1990; Trauth et al., 1993). Major goals of the IS undergraduate program are to provide a coherent and broad-based coverage of the discipline (Beane, 1995), and to provide sufficient exposure to the rich body of knowledge that underlies the field to allow students to appreciate the intellectual depth and abstract issues involved (Davis et al., 1997; Trauth, et al., 1993; Tucker et al., 1990). Therefore, the major goals of undergraduate programs in IS should be to focus

on meeting the needs of society, the student body and remaining current in terms of the body of knowledge.

A serious challenge facing many organizations today is the rapid changes in technology. A well developed IS curriculum should be designed in such a way as to reflect these changes in a timely manner. Therefore, a curriculum that is designed to provide individuals with the required knowledge, skills and abilities must also consider the need for frequent changes in technology and course content. These programs should provide students with a strong foundation on which to base lifelong learning and development. According to Lightfoot (1999), "it is the responsibility of the educational system, particularly at the undergraduate college-university level, to prepare future IT professionals for the dynamic environment of the 21st century." With these rapid advances in technology and globalization of the economy, IS security has become a major concern. This is due to threats from a variety of sources, both internal and external, that present new challenges to organizations. These sources range from a teenage hacker to domestic-international terrorist. This is why it is important that a dedicated course in information systems security (ISS) be included as an elective in the undergraduate IS curriculum.

2. THE NEED FOR SECURITY IN THE IS CURRICULUM

A number of reasons prevail that influence changes to the curriculum in higher education. Curriculum changes in higher education arise out of a response to changes in the areas of knowledge, in technology, in the general environment and in values (Posner et al., 2001; Beane, 1995). Knowledge fields play a significant role in structuring curricula and therefore curriculum changes will reflect the different values and practices of each specific field (McKeen et al, 1987; Fortune, et al., 1987). Curriculum is also shaped by changes in the production and application of academic knowledge. Shifts in emphasis on the different criteria used to evaluate the production and application of academic knowledge will also require the altering of the curriculum (McKeen et al, 1987; Fortune, et al., 1987).

Advances in new technologies have also brought about changes in the design of the curriculum. The "search for truth in the science fields" has been replaced by the need for efficiency due to new technologies (Posner, 2001). In addition, the new digital environment has brought about new values and attitudes. In today's job market doing is valued over knowing and productivity has taken precedence over understanding.

The design and development of new curriculum must take into account the needs of its major stakeholders: educators, businesses, students and the public (Lightfoot, 1999). New curriculum design and development is an essential constituent and fundamental condition for radical changes to practices in ISS. Lack of knowledge primarily arises from inappropriate education and deficient curriculum embodies far too many impractical topics presented in an inefficient manner (McKeen, et al 1987). Solutions to these problems should involve curriculum as well as new study techniques, internal policies and procedures and methods of instructions. The design of a new curriculum should include the industry's best practices (Beane, 1995).

The 1991 ACM undergraduate curricula in computing define information systems security as: "The ability of software and hardware systems to respond appropriately to and defend themselves against inappropriate and unanticipated requests; the ability of the computer installation to withstand catastrophic events. Examples include type-checking and other concepts in programming languages that provide protection against misuse of data and functions, data encryption, granting and revoking of privileges by database management system, features in user interface that minimize user errors, physical security measures at computer facilities, and security mechanisms at various levels in the systems" (Tucker et al., 1990). The growth of the Internet has spawned an increased awareness of and interest in security issues. Although security has been considered in the design of the basic Internet protocols, many applications have been and are being designed with minimal attention to issues of confidentiality, authentication, and privacy. As our daily activities become more dependent upon data networks, the importance of an understanding of such security issues will only increase.

Many organizations today operate in a wireless, mobile and virtual environment that necessitates a higher level of security. A survey conducted by Anderson & Schwager (2002) indicated that ISS issues have been gaining increasing attention and emphasis in the IS field from both industry and academia. In addition, a study conducted by Lee et al, (1995) found that "current IS curricula in many universities are not well aligned with business needs."

IS curriculum developers and researchers claim that IS curriculum need to be updated frequently in to remain effective (Davis et al., 1997; Couger et al., 1995). The main problem that many organizations currently face is the lack of appropriately trained personnel to deal with a growing number of security issues. While a large number and variety of security training courses are available, no formal and specific curriculum for identifying the type of training necessary to produce trained security personnel has been developed. The main reason for this is that while IS professionals, administrators and users in the field are placing more emphasis on security issues academia is lagging far behind. A study conducted to examine the skills and knowledge required by IS professionals found that "university curricula often lag in updating critical new technologies" (Lee et al, 1995; Trauth et al., 1993; Couger et al., 1995). In addition, Lee, et al., (1995) and Trauth et al., (1993) propose that IS graduates will need broader and in-depth education across different dimensions such as technology, business and human relationships. A recent online survey of IS faculty conducted by Anderson and Schwager (2002) found that there was a lack of coverage of IS security issues in the IS curriculum.

Information systems security today is an important issue at many academic and training institutions in the United States and many other parts of the globe. In the last five years information security has become an increasingly important area of study within many disciplines including Computer Science, Software Engineering and IS (Committee on National Security Systems, 1997). This is evidenced by the number of new programs that have emerged within a short period of time focused on this issue.

Although a number of academic institutions both in the US and abroad have implemented security programs within their curriculum this has not been done in the undergraduate IS curriculum. The US Committee on National Security Systems provides a list of fifty institutions that have been identified and declared Centers of Academic Excellence in Information Security (Assurance) Education (<http://www.nstissc.gov/>). The programs at these institutions range from certificate to masters and Ph.D. specializations in areas of information security. However, the major emphasis in education and training at these institutions is at the post-baccalaureate or graduate levels of education and not the undergraduate level (Committee on National Security Systems, 1997).

Couger et al., (1995) claim that, "students from most IS programs accept jobs in widely dispersed geographic regions, therefore, availability of curriculum models enables local academic units to maintain academic programs that are consistent with employment needs across the country." A major concern for academia relates to the lack of a comprehensive body of knowledge in ISS. In order to develop courses in information security and to define competencies and requirements for the 21st century workforce, a comprehensive body of knowledge must be identified and integrated into the current IS curriculum model. While curriculum developers in other countries have incorporated information security as a significant area of study within the undergraduate IS core body of knowledge, this has not been addressed adequately in the undergraduate IS curriculum in the US. The Australian computing Society (ACS) identifies ISS as one of the major areas of study in its core body of knowledge for IS professionals (Underwood, 1997). In addition, the 1991 ACM undergraduate curricula in computing include security as a core area of study and provide a comprehensive definition for this body of knowledge (Tucker et al., 1990).

A formally implemented dedicated information security course in the IS curriculum model could serve a variety of purposes. The main purpose is to respond to the heightened importance of security issues that stem from a number of changes in the IS environment. Some of the major issues and related changes that have arisen are:

- growth in demand for ISS professionals in many different areas of the economy
- demand for Certifications and Training in ISS
- more educational program arising out of a need for knowledgeable and skilled professionals in this specific field

These trends indicate a tremendous amount of growth and interest in the field and are very good reasons for ISS to be formally recognized as a major area for study and be included in the ACM/AIS/AITP model curriculum development process. As organizations experience phenomenal changes, the security environment in which these organizations operate will also experience dynamic change. A dedicated undergraduate course in information security is necessary to meet the needs of a rapidly changing IS field and to accommodate the growing demand for qualified individuals. The authors recommend that ISS be included as an elective within the IS Deployment and Management Practices presentation area in the IS'97 Curricula model at level 3 – for IS majors only.

3. KNOWLEDGE AND COMPETENCY LEVELS

Mission, Goals and Objectives of the Curriculum

The foundation of curriculum design and development arises from the goals and objectives set out by an educational system (Posner et al., 2001; McKeen et al., 2001). According to McKeen and Fortune (2001), "the purpose of curriculum is to provide the learner with skill in the processes of inquiry...while inquiry functions to control change and to advance the purposes of society." The institution must first establish the goals of its education system before it can begin to design a meaningful curriculum (Thapisa, 1999). Therefore the goals of the ISS course need to be specified.

Curriculum models should specify the attitudes, skills and the body of knowledge that is necessary to meet professional standards and the needs of employers (Davis et al., 1997). In the case of ISS curriculum, there is an urgent need for academia to introduce systematic change efforts that will address the needs of employers. Institutions of higher education are required to formulate a

mission, determine goals and develop strategy according to the needs of the labor market and the organization's own capabilities (Davis et al., 1997; Couger et al., 1995).

Although it is important to preserve core values and purposes, it may be necessary when designing new curriculum to change cultural or habitual operating practices, specific goals and strategies (Thapisa, 1999). The objectives for change in the design of a new curriculum for ISS should be to:

- Make education and training of ISS more practical by bringing education and work together by bridging the gap between training and work requirements
- Equip ISS professionals with marketable competences, knowledge and skills so that they become active, creative and comprehensive participants in the information economy
- Strengthen the relationship between education and employment by emphasizing the application of ISS and research skills in business and real work situations where students must have both technological and management skills.

Employers should be encouraged to take a more proactive role in influencing the education and training of ISS professionals. Occupational competencies and roles that are learnt in the ISS environment should be adaptable to management roles, responsibility for standards, creativity and flexibility to changing demands (Thapisa, 1999).

The debate in terms of what is more important to teach students: knowledge or skills, continues (Davis et al., 1997). Knowledge refers to the ability to apply information to efficient and effective action. Knowledge can be cultivated by acquisition and the successive application of information to action. It is more important however, to teach skills after developing the necessary attitudes to motivate students. Such reasoning should be the foundation for the development and transformation of the ISS curriculum.

Couger et al., (1995) claim that "competency levels help to distinguish the differences between the three main emphases of the IS curriculum." These distinctions in competencies are predicated on Bloom's taxonomy of learning competencies. Knowl-

edge and skills can be mastered in many ways, however; this course is designed for students beyond the junior level because it assumes a basic framework of knowledge, skills and abilities from which the student can progress. According to Bloom's taxonomy, most undergraduate level courses usually focus on the first two categories of learning, which are knowledge and comprehension (Krathwohl, 2002). Therefore, the course being proposed will not be suitable for sophomores or juniors because it assumes a previously acquired level of competency in the discipline. According to Bloom's taxonomy, students beyond the junior level should express higher level thinking skills (Krathwohl, 2002).

The course is designed as an elective to give senior IS students the ability to select an area of interest that the student may want to explore for personal fulfillment or may want to gain more in-depth knowledge and become familiar with the area in preparation for the workforce or for graduate school. One of the objectives of such a course would be to allow students to develop their application, analysis, synthesis and evaluation skills by working in-depth and intensely with a large number of different concepts. Therefore, it is expected that students who are IS majors will be expected to achieve the highest levels of competency in this course, which is the application level (4) according to IS'97 (Davis et al., 1997). The authors recommend that ISS be added as a significant sub-area to the IS curriculum at the application level (4) which should be the appropriate depth of knowledge and competency levels for this course. Students should be provided with meaningful assignments in order to facilitate the integration of previous discipline-specific knowledge with the goal of designing and developing effective security stances for the organization. The course is not designed with a focus on students whose minor is IS, however, if the course is taken by such a student, then the expected level of knowledge/competency will be at the literacy level (2). In addition, modifications to the course content and instructional strategies will be needed to render the course suitable to the IS minor.

4. DEVELOPMENT OF THE COURSE – INFORMATION SYSTEMS SECURITY

During the senior year the IS undergraduate should be invited to study information security as a dedicated elective course offering. The ISS course will be expected to tie together the concepts and exposures that have come in other more specific courses within the curriculum (Davis et al, 1997). Topics such as cryptography, risk assessment, management practices (disaster recovery, physical security, organizational issues, etc.), formal models of security, ethical computing and social issues need to be introduced and discussed. Texts such as Anderson (2001) and Whitman et al., (2003) would be excellent facilitators.

This course provides an introduction to the topic of security in the context of computer networks. It is intended for senior undergraduate students who have some understanding of computing issues, but do not have a background in security. The goal of the course is to provide students with a foundation allowing them to identify, analyze, and try to solve security-related problems in computer systems. The course covers fundamentals of number theory, authentication, and encryption technologies, as well as the practical problems that have to be solved in order to make those technologies workable in a networked environment, in particular in the wide-area Internet environment. This course will serve to again focus the student on database threats, operating systems, electronic commerce, networks and information development practices as previously discusses in other courses. However, during this class, focus can be better defined and explored in a more holistic fashion.

Statement of Needs

Information technology professionals are increasingly responsible for the incorporation of security services and mechanisms into overall IS under development and in operation. This responsibility is expected to increase as national and international guidelines and legislation are developed and enforced. The IS professional will need to be familiar with social, governmental and legal requirements in this area and be able to in-

corporate appropriate technologies into IS during the development phase with appropriate levels of security management created for ongoing usage of the systems.

This course will provide students with the necessary level of skills and knowledge in the areas of information security that they will need to function within an organization. At the completion of the course students should be able to complete the activities listed in the learning objectives and at the specified level of proficiency.

Goal Statement

Graduates of IS programs should be able to function in an entry-level position and should have a basis for continued career growth (Lee, et al., 1995). The main objectives for IS professionals are to support organizational needs and have a customer service orientation. At the completion of the course students will be able to use and develop the techniques, skills and tools necessary for ISS practice. Some specific goals of this course may include:

- learn about security in Microsoft/UNIX operating systems and programming environments
- learn how to attack a system, and to defend it by analyzing the system for vulnerabilities and ameliorating those problems
- understand the strengths, and weaknesses of cryptography as a tool of security
- learn how access to systems, resources, and data can be controlled
- learn the basics of writing security-related programs
- learn about security in networks
- understand how to coordinate hardware and software to provide data security against internal and external attacks
- model systems involved through use of formal models.

Target Student Population

This course is intended for senior undergraduate IS students who are in the last year of their program. It is recommended that this course be taken either in the first or second semester of the senior year. It is designed as an elective course for upper ranking students who have already gone through most of the core courses in the IS curriculum and are already comfortable with

the material in the major. This course should be taken by students who have an interest in the information security area or those students who want to get an idea of what this specific field entails. The course is designed as an elective to give senior IS students the ability to select an area of interest that the student may just want to explore for personal fulfillment or the student may want to gain more in-depth knowledge and become familiar with this area in preparation for the workforce or for graduate study.

Learning Objectives and Outcomes

Knowledge objectives: At the conclusion of the course, the student should have an understanding of:

- the role and importance of security policy
- network-related security threats and solutions
- principles of private- and public-key encryption
- principles of authentication
- Internet Protocol security architecture (IPSEC).

Application objectives: The project and homework portions of the course are intended to help students apply their understanding, for example by:

- analyzing security protocols for weaknesses
- designing and/or implementing an authentication protocol for a given set of constraints
- designing and/or implementing an encryption system

Therefore at the completion of this course students should be able to:

- Outline the technical basis of viruses and denial-of-service attacks
- Enumerate techniques to combat security attacks
- Discuss several different hacker approaches and motivations
- Apply the basic principles of ISS effectively
- Defend the need for protection and security
- Identify the IS professional's role in security and the tradeoffs involved

- Identify common security and control mechanisms and be able to apply these mechanisms effectively
- Summarize the features and limitations an operating system used to provide protection and security
- Explain the potential of distributed IS and the security problems such systems entail
- Compare/contrast the strengths and weaknesses of two or more currently popular operating system with regard to security
- Compare and contrast the security strengths and weaknesses of two or more currently popular operating system with respect to recovery management
- Provide examples of several computing applications that raise sensitive legal and ethical concerns
- Plan, design, develop and implement a simple security system

The skills developed here should give the student a strong foundation on which to build their understanding of information security issues and practices from a personal level through an organizational level to the collection, analysis and synthesis of external information. Learning outcomes should include the appreciation of the techniques for information security practices; an understanding of the basic concepts, policies and procedures involved in protecting the organization's information resources and the selection of appropriate security tools and techniques for the protection of the organization's information.

Prerequisites (KSAs)

The prerequisites for this course include all the required courses for the IS major provided in the IS'97 model curricula Presentation Areas and Courses by Educational Levels (Davis et al., 1997). Students are expected to have a solid grasp of the fundamentals of operating systems, computer networking, including a basic understanding of the operation of the protocols in the TCP/IP suite, especially IP. In addition, students are expected to have a level of mathematical maturity that includes basic algebra and the ability to learn and use new mathematical notations as specified by the IS'97 curriculum model (Davis et al., 1997). Some programming ability will be helpful for the implementation of algorithms. Students

should not be permitted to register for this course until all required courses toward the major has been completed up to the end of the junior year.

Course Content

Course Descriptions:

Course Name: Information Systems Security
Course Number: INSS XXX – Elective
This course introduces the basic principles of computer security, focusing on system elements. Among the topics covered are access control and integrity, system analysis, security in programming, and network security. An outline of the course content is provided in figure 1. The course may be divided into a number of learning units as indicated in figure 1.

Figure 1. Information Systems Security Course Outline

<p>1. Introduction</p> <ul style="list-style-type: none"> • Internet, Intranet -- Structure, growth, possibilities • Related subjects, overview of course • Definition of terms/concepts in computer network and internet security <ul style="list-style-type: none"> -basic security principles (privacy, confidentiality, integrity, availability, account-ability) -access control, firewalls, biometric devices <p>2. Threats, Risks and Vulnerabilities</p> <ul style="list-style-type: none"> • Viruses, worms (e.g. Trojan Horses) • Intrusion detection and types of attacks • Denial of service attacks • Security countermeasures <p>3. Data Security Policies/Administrative Security Procedural Control</p> <ul style="list-style-type: none"> • Institution, legislation, privacy, basic policies/protocols • Legal and ethical issues in information systems security <p>4. Security models</p> <ul style="list-style-type: none"> • Access matrix, multilevel, mandatory, discretionary models • Role-Based Access Control <p>5. Designing Secure Systems</p> <ul style="list-style-type: none"> • Secure system design methodology
--

- Evaluation/administration of secure systems
- 6. Effects of Hardware on Security**
- Modes of operation, protection rings, memory protection
- 7. Operating Systems Security**
- Unix, Windows XP, Linux
- Hardened operating systems
- Types of OS attacks
- 8. Network Security**
- SSL, Kerberos, VPNs, Wireless systems
- Dial-up vs. dedicated
- Public vs. private
- Traffic analysis
- 9. Database Security**
- Authorization systems in Oracle and similar database systems.
- 10. Programming Language Security**
- Programming Language security problems (e.g. buffer overflow, pointers, arrays, etc.)
- Java security
- 11. Cryptography**
- Symmetric and public key systems, PKI
- Strengths (complexity, secrecy, etc.)
- Encryption
- Key management
- 12. Distributed Systems Security**
- Security in .NET and Sun ONE, WebSphere and other application servers
- Security in XML and Web Services
- 13. Information Systems Security**
- Policies
- Roles and responsibilities
- Application dependent guidance

Catalog description: The course provides an overview of technical and behavioral aspects of information security with emphasis on networks, Internet and the design of secure systems. Prerequisite: general background on operating systems, architecture, databases and programming languages, as well as basic knowledge of object-oriented programming and design. Students will be introduced to principles, mechanisms, and implementations of com-

puter security; learn how attacks work, how to defend against them, and how to design systems to withstand them.

Instructional Strategies and Testing and Evaluation of Students

For effective learning in the digital world, novel instructional strategies need to be considered, implemented and evaluated.

Cooperative Learning – Simulation of Group Projects and Case Studies:

Aside from changes to the curriculum, the culture of learning also requires considerable transformation (Leidner et al., 1995). A number of important reasons to make changes to the way students learn may include:

- The need to exploit opportunities offered by ISS, which necessitates a drive for new competencies, skills and knowledge
- A drive for quality education, which is hands-on, more practical and work based. This relates to a deeper understanding of customer needs for first class education and training
- Competitive considerations that force the industry to respond to market forces
- The need to increase the availability of quality for use in decision making, policy formulation and development planning

Different types of learning environments require different types of instructional methods to provide meaningful learning experiences for students. The learning context can be critical to the learning experience. Kahn (2002:137) claims that the "learning environment plays a significant role in providing comprehensive learning to users." The learning environment acts as the conduit for the interaction between the user and specific software tool and contributes to the delivery of the learning experience. Khan (2002) cites a number of different learning environments that have been successful in enhancing student learning, including a simulation environment called 'MYCIN,' a discovery environment 'LOGO,' and a game environment 'WEST.' The most effective methods of instructions for this course would be simulation/group projects and case studies.

Simulation can be viewed as an interesting form of formal or informal instruction (Khan, 2002). One of the most basic advantages for using simulation in learning environ-

ments is because it provides "an opportunity to avoid abstraction" (Kahn, 2002:139). When simulation is used as a tool to examine complex systems and to facilitate a more thorough and meaningful comprehension of primary information and knowledge, it fosters the elimination of abstraction in the learning process. Students can adopt information but also gain a deeper understanding of the concepts by learning how to apply the information learned using simulation.

Most research tends to favor the simulation method of teaching over the lecture method when the primary goal is the retention of information and the economies of the respective methods are ignored (Eggen & Kauchak, 1988). Successful participation in simulations is viewed as requiring higher order critical thinking skills than those skills required to listen and take notes in a lecture (Krathwohl, 2002). Higher order thinking skills include analysis, synthesis and evaluation of information. All of these involve critical thinking skills such as analysis of elements, arguments, relevancy of issues, implications of information, and the drawing of logical conclusions. Learning becomes meaningful when students can make associations between concepts and ideas (Eggen and Kauchak, 1988). Simulation provides the ideal vehicle for this type of learning.

Simulation also promotes cooperative learning. Cooperative learning strategies have numerous benefits. Cooperative learning facilitates positive interdependence, individual accountability and face-to-face interaction. Research on students' behavior within cooperative learning groups shows that students who gain most from cooperative work are those who participate in elaborate explanations (Slavin, 1987). Effective learning occurs because students are "actively involved in organizing and finding relationships in the information they encounter rather than being the passive recipients of teacher-delivered bodies of knowledge" (Eggen and Kauchak, 1988).

Cooperative learning and simulation by association, enhances achievement in the classroom. Slavin (1990) reviewed 62 studies measuring academic achievement. Of those studies, 36 or 57% found significantly greater achievement in classes that utilized cooperative learning techniques such as

those promoted through simulations. Students learn from one another because of their discussions of the content of the class. During these discussions, inadequate reasoning will be exposed, and higher quality understanding will occur. If information is to be retained in the memory and related to information already learned, then the learner must engage in some sort of cognitive restructuring, or elaboration of the material (Slavin, 1990). One of the most effective means of elaboration is explaining information to someone else as in a simulation. Students would benefit from the experience if simulation and case studies were used as teaching tools for a course such as ISS.

For a course such as information security it would be advantageous for students to gain hands-on experience with the technology. However, since it is not practical for students to gain knowledge and skills in a real-world environment in a course such as information security, then the next best thing would be to use simulation as a teaching tool. Therefore, it is recommended that simulation, group projects and case studies be used as teaching instruments in a cooperative learning environment.

Table 1 presents recommended goal levels, methods of delivery and assessment for the course in ISS. While instructional methods include simulation and case studies, methods of evaluation and assessment include structured practice, homework, detailed exams, process performance using simulation and modeling tools and group research projects.

5. IMPLICATIONS FOR IS PROGRAMS AND FUTURE RESEARCH

Changes to and the development of new curriculum and the organization of instruction require investments of considerable resources into the process. An extricable bond must be established between teaching and learning infrastructure and curricula, between the technology infrastructure, the classroom and the teaching material (Thapisa, 1999). New and more effective methods of instruction such as simulation, case studies, projects and group work should be employed in this dynamic environment to produce better learning. Students should be involved in the development

Level	Goal	Methods of Delivery	Methods of Assessment
1	Awareness	Lecture, reading	Exam (fill-in-the-blanks, multiple choice, true-false, matching, etc)
2	Literacy	Lecture, reading	Structured practice, homework, detailed exam
3	Concept and use thereof	Lecture, reading, case study and well-structured projects	Structured practice, homework, case analysis, detailed exam, and project performance
4	Detailed understanding, application, skilled use	Lecture, reading and well-structured projects, ill-structured projects using simulation and modeling tools	Structured practice, homework, detailed exam, process performance using simulation and modeling tools, group research projects
5	Skilled use	Student-directed project, independent research	Research project

Table 1. Goal Levels, Methods of Delivery and Assessment

of programs and be active in their own learning. Students are more motivated when they are familiar with the goals of a subject matter, participate in the design and are responsible for acquiring resources (Davis, et al., 1997; Lee, et al., 1995). Faculty will also need to be retrained and new facilities and teaching resources will be needed.

6. CONCLUSIONS

Currently, there does not seem to be consensus about what ISS knowledge, skills and abilities should be included in the undergraduate IS curriculum and the proper placement for such information within the curriculum. In order to produce ISS professionals who are on the cutting edge of security issues and who can also understand the main concepts from a variety of disciplines, the official curriculum development body for IS undergraduate curriculum need to ensure that the IS curricula is updated regularly and reflects the rapidly increasing changes in the current environment.

IS curricula must be revised continually to meet the challenging needs of an information economy. In addition to constant revision of the security curriculum, academia needs to work with both government and industry to understand and prepare for a not too distant future when security may be the main and perhaps only competitive enabler of business success. This paper is an attempt to develop the basic outline for a dedicated elective undergraduate course in

information security which should be included as an important sub-area for study in the official IS curriculum models.

7. REFERENCES

Anderson, J. E., and P. B. Schwager, 2002. "Security in the Information Systems Curriculum: Identification and Status of Relevant Issues." *Journal of Computer Information Systems*, spring, pp. 16-24.

Anderson, R. 2001, *Security Engineering*. John Wiley and Sons, Inc., NY.

Beane, J. A., 1995. "Toward a Coherent Curriculum: 1995 Yearbook of the Association for Supervision and Curriculum Development." Alexandria, VA. Association for Supervision and Curriculum Development.

Committee on National Security Systems. 1997. "National Security Telecommunications and Information Systems Security Instruction," (NSTISSI 4009), Published by the Committee on National Security Systems, formerly National Security Telecommunications and Information Systems Security Committee, <http://www.nstissc.gov/>

Couger, J. D., G. B. Davis, D. G. Dologite, D. L. Feinstein, J. T. Gorgone, A. M. Jenkins, G. M. Kasper, J. Currie Little, H. E. Longenecker Jr., and J. S. Valacich, 1995. "IS'95: Guideline for Undergraduate IS Curriculum," *MIS Quarterly*, September pp. 341-359.

- Davis, G. B., J. T. Gorgone, J. D. Couger, D. L. Feinstein and H. E. Longenecker Jr., 1997. "IS'97 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems." Publication by the Association of Information Technology Professionals, 1997. <http://www.is2000.org/>
- Eggen, P. D., and D. P. Kauchak, 1988. *Strategies for Teachers: Teaching Content and Thinking Skills*. Prentice Hall, Englewood Cliffs, NJ.
- Fortune, J. C. and R. L. McKeen, 1987. "Curriculum Building: Start to Finish - Evaluation Instrument and the Management Information Systems." *Education*, 108(1), pp. 81-86.
- Khan, M.M., 2002. "Implementing an Intelligent Tutoring System for Adventure Learning." *The Electronic Library*, 20(2), pp. 134-142.
- Krathwohl, D., 2002. "A Revision of Bloom's Taxonomy: An Overview." *Theory into Practice*, 41(4), autumn, pp. 212-218.
- Lee, D., E. M. Trauth and D. W. Farwell, 1995. "Critical Skills and Knowledge Requirements of IS Professionals: A Joint Academic/industry Investigation." *MIS Quarterly*, September, pp. 313-339.
- Leidner, D. E., and S. L. Jarvenpaa, 1995. "The Use of Information Technology to Enhance Management School Education: A Theoretical View." *MIS Quarterly*, September, pp. 265-291.
- Lightfoot, J. M., 1999. "Fads versus Fundamentals: The Dilemma for Information Systems Curriculum Design." *Journal of Education for Business*, September/October, pp. 43-50.
- McKeen, R. L., and J. C. Fortune, 1987. "Curriculum Building: Start to Finish - Knowledge, Learning and the Design of Curriculum." *Education*, 108(2), pp. 220-227.
- Posner, G. J. and A. N. Rudnitsky, 2001. *Course Design: A Guide to Curriculum Development for Teachers*. Sixth edition, New York, Addison Wesley Longman, Inc.
- Slavin, R. E., 1987. *Cooperative Learning: Theory, Research and Practice*. Prentice Hall, Englewood Cliffs, NJ.
- Slavin, R. E., 1990. *Cooperative Learning: Student Teams*. National Education Association, Washington D.C.
- Thapisa, A., 1999. "Training for the Real Working World in an Information Economy." *Library Management*, 20(2), pp. 84-89.
- Trauth, E. M., D. W. Farwell and D. Lee, 1993. "The IS Expectation Gap: Industry Expectations versus Academic Preparation." *MIS Quarterly*, September, pp. 293-307.
- Tucker, A. B., B. H. Barnes, R. M. Aiken, K. Barker, K. B. Bruce, J. T. Cain, S. E. Conry, G. I. Engel, R. G. Epstein, D. K. Lidtke, M. C. Mulder, J. B. Rogers, E. H. Spafford, and A. J. Turner, 1990. "Computing Curricula 1991: Report of the ACM/IEEE-CS Joint Curriculum Task Force." <http://www.acm.org/education/curr91/homepage.html>
- Underwood, A., 1997, "The ACS Core Body of Knowledge for Information Technology Professionals." September, <http://www.acs.org.au/national/pospaper/bokpt1.htm>
- Whitman, M. E. and H. J. Mattord, 2003. *Principles of Information Security*. Thompson-Course Technology. Canada.



Grace C. Steele is an Instructor of Computer Science in the Computer Science Department, School of Computer, Mathematical and Natural Sciences, Morgan State University, Baltimore, Maryland. She is currently studying for the Ph.D. degree in the Department of Information Science and Systems, Earl Graves School of Business and Management at Morgan State University. Ms. Steele received the M.S. degree in Management Information Systems (1993) and B.S. degree in Accounting (1991) from the University of Baltimore. Ms. Steele's **research interests** include Information Systems Security, IS Curriculum Development, Issues in Mathematics and Science Education, Implementation of Technology into Higher Education, Bioinformatics (Modeling and Simulation), Knowledge Management, Human/user Interaction, Database and Multimedia Systems. Ms.

Steele has published in the IEEE Proceedings on Computational Systems in Bioinformatics and has presented at major Bioinformatics conferences. She has conducted workshops in C++ Programming and Simulation and Modeling (using Easel) at the Annual Mathematics and Science Education Conference in Baltimore, Maryland. Ms. Steele currently serves as a Coach for Morgan's ACM Programming Contest Teams.



Dr. Vojislav Stojkovic is an Associate Professor of Computer Science in the Computer Science Department, School of Computer, Mathematical and Natural Sciences, Morgan State University, Baltimore, Maryland, USA from 1989. He received his Ph.D. (1981) and M.S. (1977) degrees from University of Belgrade, Serbia, Yugoslavia. Dr. Stojkovic's primary research interests are Programming Languages and Compilers, Artificial Intelligence (Agents, Theorem Proving, and Expert Systems), Bioinformatics (Modeling and Simulation), Information Assurance, and Army Knowledge Management. Dr. Stojkovic has published more than 50 scientific, research, and professional papers in proceedings and journals. Dr. Stojkovic has served as a Coach of MSU's Programming Contest

Teams and as an Advisor of SACS (The Society for the Advancement in Computer Science).



Dr. Zaveri is an Associate Professor in the Department of Information Science and Systems, Earl Graves School of Business and Management at Morgan State University. He received the Ph.D. and M.S. degrees from University of Kentucky and the B.Tech. from Indian Institute of Technology. Dr. Zaveri's **research interests** encompass *Knowledge Management, Decision Support Systems, Artificial Intelligence, and others*. Dr. Zaveri has numerous **research publications** that have appeared in *Decision Science, IEEE Transactions on Systems, Man, and Cybernetics, and Decision Support Systems* and a **book chapter** in *Manufacturing Decision Support Systems (Chapman-Hall)*. He also has numerous **research presentations and articles** presented at major national and international conferences and has worked on numerous **projects** for

several agencies including *the National Transportation Center, and the National Security Agency*.