An undergraduate business information security course and laboratory
Michael Russell Grimaila;Kim, Inkoo
Journal of Information Systems Education; 2002; 13, 3; Research Library
pg. 189

An Undergraduate Business Information Security Course and Laboratory

Michael Russell Grimaila
Inkoo Kim
Department of Information and Operations Management
Texas A&M University
College Station, Texas 77802, USA
mgrimaila@cgsb.tamu.edu kim-i@masters-lab.tamu.edu

ABSTRACT

In an environment of growing security threats, it is essential to raise the awareness and capabilities of business students entering the workforce to mitigate threats to the enterprise. In this paper, the authors present their experience in the design, implementation, and teaching of a foundation undergraduate business information security course with laboratory components using security tools. The authors identify key resources consulted in the development of the curriculum and discuss various teaching methods and their effectiveness in offering the course for the first time.

Keywords: Information security management education, information system security pedagogy.

1. INTRODUCTION

Information Security (InfoSec) is a unique field of study in that it is rapidly changing; it requires knowledge in diverse subject areas including engineering, ethics, law, management, policy, and social sciences; and it can be impacted (both positively and negatively) by the actions of everyone in the enterprise. A key question is how to deliver effective InfoSec education to undergraduate business students. The purpose of this paper is to document our efforts to address this question through the development of a new undergraduate InfoSec course.

2. MOTIVATION

Corporate responsibility dictates the need to protect the enterprise against harm from competitors, criminals, hackers and other security threats (CSI/FBI, 2002). As a result, there is an increasing demand for InfoSec professionals. Texas A&M University (TAMU) has placed a high priority on the development of Information Assurance and Security (IAS) curriculum and research programs across all departments within the university to address this critical need. There are two primary thrusts of the educational component of this program: 1) to develop undergraduate and graduate foundation courses in IAS, and 2) to develop specialization courses in each of the departments to facilitate the creation of an interdisciplinary IAS certificate at the Master's and Ph.D. level. The course development discussed in this paper addresses the first element through the development of a foundation undergraduate IAS course targeted towards MIS undergraduate students.

3. COURSE DESIGN PHILOSOPHY AND CONTENT

The diversity of knowledge that is required to effectively practice business information security is enormous. It requires that the practitioner be well versed in a number of different technical, social, and political skills (Irvine, 1998). Since InfoSec technology is rapidly evolving, it is essential that the individual not only be grounded in the basics of the technology, but also be capable of continually learning about new developments in the field, which can occur daily. Further, one must also appreciate the importance of security policy development, implementation, and awareness in the overall success of a security program (Miller, 1997). Finally, there are political ramifications when implementing security programs. Students must be aware of these political issues in order to be successful when dealing with management, other organizational units, and end users.

The authors recognize it is not possible to teach students everything they need to know about InfoSec in a single semester course. However, we believe that we can provide a foundation course that provides basic knowledge and

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

experiences and fosters the ability of the individual student to continue to grow and develop their InfoSec skill set.

3.1 Target Audience

When developing a curriculum, it is essential to consider the existing skill sets and needs of the target audience. Ideally, all InfoSec practitioners should be familiar with: 1) research, development, and application of technical principles (know how to make); 2) application of industry accepted techniques and practices (know how to use); and 3) non-technical aspects such as policy development, resource allocation, and risk assessment and management (know how to manage). While engineers focus on the first element and system administrators on the second, an effective business InfoSec manager should be more familiar with the third element. Barnett (Barnett, 1996) identifies the need for different InfoSec education and training based upon the particular role an individual plays. He describes two categories of security related jobs: One that deals with pragmatic and operational issues (operational computer security), and the other that provides technical solutions through research and development (computer security technology). Based upon this categorization, our students more properly belong to the first group, although the division is not absolute. Barnett also identifies the benefit of providing dedicated courses for non-technical majors in InfoSec.

3.2 Reference Materials

The authors consulted a wide variety of sources during the development of this course. In this section, we will discuss only the most relevant reference materials that guided our curriculum development.

In 1992, the International Information Security Foundation (I^2SF) formed a committee to develop and promulgate generally accepted system security principles (I^2SF, 2002). The committee produced a summary document known as the Generally Accepted System Security Principles (GASSP) that identified a core set of "best practice" InfoSec principles that were collected from practicing InfoSec professionals. The GASSP further divided the principles hierarchically from high-level Pervasive Principles (PPs), through mid-level Broad Functional Principles (BFPs), to low-level Detailed Principles (DPs). We drew upon the PPs and BFPs as a set of core principles to highlight in the course.

The International Information System Security Certification Consortium, Inc. $(ISC)^2$ was formed, in part, to standardize and maintain a Common Body of Knowledge (CBK) of security information relevant to Information Security professionals ($(ISC)^2$, 2002). The CBK drew upon the GASSP results and enumerated 10 domains that are essential knowledge for IS professionals working to obtain their Certified Information Systems Security Professional (CISSP) certification. The 10 domains represented in the CBK were deemed essential learning focus areas for the course. Each of the domains was further expanded using multiple sources of information including the textbook, other reference books, and websites.

The National Institute of Standards and Technology (NIST) Computer Security Division (CDS) maintains the Computer Security Resource Center (CSRC) website that contains a wide selection of IT specific documents (NIST, 2002). We gained deeper insight into the issues surrounding InfoSec by reading the "800" series of documents, all of which relate to different aspects of IT security. We incorporated elements from a number of documents including the "Risk Management Guide", "Security Self Assessment Guide", and "IT Security Training Requirements" into the lecture and coursework.

The Systems Administration, Networking, and Security (SANS) Institute provides a number of InfoSec resources via their web site (SANS, 2002). One of the more beneficial resources we utilized during the course development was the SANS reading room which contains more than 1000 publications, all written by practicing InfoSec professionals. We made use of the information in these papers in two distinct ways. First, we found a number of real world examples of dealing with security issues in the corporate environment and used them to construct mini-case studies. Second, some papers provided insight into current security assessment tools and techniques and were used as a basis for the development of the laboratory exercises. SANS also maintains a top twenty security vulnerability list, a forum for InfoSec related discussions, and a security incident mailing list. Students were required to subscribe to the security incident email list to gain an appreciation for the dynamic nature of InfoSec incidents.

Finally, we identified documented failures in information security programs in the corporate environment (Kessler, 2001). While developing our course, we highlighted these problem areas to the students so they would not fall victim to these pitfalls. While there are a wide variety of information security topics, review of the references helped us to identify the most important topics to be covered in our course and prepared us to select a suitable textbook.

3.3 Textbook

It is essential to select a textbook that provides students a solid foundation on the topics being studied. We reviewed over twenty textbooks in the InfoSec area, but did not find a single one that incorporated all of the elements we desired. As a result, we selected a textbook that presented a concise, non-technical overview of the InfoSec process (Pipkin, 2000). The book was relatively easy to read and presented numerous real-world stories to illustrate the key issues of InfoSec. Additional books were identified as supplementary material for the course and placed on reserve in the library (Greenstein, 2002; Tipton, 2002). Table 1 shows a summarized list of weekly lecture topics with a cross-reference to the related textbook chapters, the I^2SF GASSP PPs and BFPs, and the $(ISC)^2$ CBK domains.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

3.4 Admission Requirements

One unique aspect of our course is that students wishing to take the class were required to complete an application form which requested basic background information, asked essay questions about the student's desire to take the course, and required students to execute a knowledge of laws affidavit which stated that the student had read and understood the Federal, State, and local laws relating to information system security. We felt strongly that if the students were exposed to the tools and methodologies that "hackers" employ, they should be fully aware of the legal consequences of using this knowledge outside of the laboratory.

Table 1. Summarized Weekly Lecture Topics

WK	Topic	Chapter	References
1	Introduction, Motivation, and Ethics	Prologue	PP 3; BFP 14; CBK 9
2	Networking Basics and Infrastructure Elements	N.A.	BFP 12; CBK 2
3	Resource Inventory and Threat Assessment	1,2,3,4	BFP 4,12; CBK 3
4	Risk Assessment, Risk Management, and Loss Analysis	3,6	PP 5,8,9; BFP 4, 5, 11; CBK 3
5	Security Policy Development and Awareness, Politics	6,7	PP 2,4,9; BFP 1,2,5; CBK 3
6	Identification, Access, and Authentication	8,9,10	BFP 5,9; CBK 1,10
7	Cryptography, PKI, SSL, Virtual Private Networks	8,10	BFP 5; CBK 2,5
8	Authorization, Availability, and Accuracy	11,12,13	BFP 6,7; CBK 1,8
9	Confidentiality, Accountability, and Administration	14,15,16	PP 1; BFP 5,6,7, 8; CBK 3,5
10	Intrusion Methods, Intruder Types, and Intrusion Detection Methods	17,18, 19,20	PP 7; CBK 7
11	Incident Response Plan, Determination, Notification, and Containment	21,22,23, 24,25	PP 7; BFP 10; CBK 8,9
12	Disaster Recovery Planning, Business Continuity Planning	7,12,16,26	BFP 5,10; CBK 8
13	Incident Recovery, Incident Evaluation, Legal Considerations	26,29,31	PP 7; BFP 10,13; CBK 8,9
14	Project Presentations	N.A.	N.A.

3.5 Lectures

The lecture was designed to make use of various interactive learning techniques. Particular attention was placed on making the lectures interesting by linking the topics to current, real world situations. A small portion at the beginning of the class time was dedicated to reviewing current InfoSec related news items. Students gain a much better appreciation for the importance of the InfoSec area when they see how often real world security incidents occur (Yurcik - Approaches, 2001).

Role-playing exercises proved to be effective in maintaining class interest. For example, when learning the details of network communications that occurs when accessing a web site, students were assigned different roles to play in the network protocol stack of the interacting computers including the client web browser, the router, the DNS server, and the web server. Students were required to verbally represent the sequence of communications to illustrate the overall process. Once students understood the overall process, a discussion then ensued about how one could subvert the process. In another example, the class was divided into two groups. The first group represented the high-level policy makers within an organization and the second group represented the information system end users. Each group was given a short period of time privately to make suggestions on the implementation of a number of different security policies from their perspective. After ten minutes, each group shared their suggestions with the whole class and a discussion ensued to see if the class could reach consensus on what should be the specific policy for the organization. This exercise provided insight into the struggle in developing policy that meets the goals of both the corporate security objectives and the end user community.

Case studies were incorporated whenever possible, to breathe life into otherwise unexciting topics. Consider the difficulties encountered in retrofitting security solutions in the corporate environment. Simply discussing the issues does not necessarily lead to a student developing intuition into the key issues. In contrast, through the study of real-world examples where businesses succeeded and/or failed in incorporating security programs and the resulting impact, students are more likely to retain the "lessons learned." Further, case studies are very effective in developing group learning, speaking, and critical thinking skills, all of which are desirable qualities of an InfoSec professional.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Providing students with the opportunity to interface with practicing InfoSec professionals is an important way to provide linkage between the curriculum and the corporate world. Throughout the semester, guest speakers from industry were invited to come speak to the class to provide students insight into the InfoSec professional. Students were also encouraged to attend InfoSec related forums whenever possible. For example, in April of 2002 the Center for the Management of Information Systems at TAMU sponsored a Business Information Security Forum and invited professionals from a number of companies including Texas Instruments, JC Penny, Dell, Price Waterhouse Coopers, and Deloitte & Touche to discuss their views, in an open forum setting, on the topic of Information Security. The forum provided an excellent environment for companies to share "war stories" and provided students with a better understanding of the issues surrounding information security in the corporate environment.

3.6 Final Project

The final project was designed as a vehicle for students to experience the dynamics of group learning in the corporate environment. The goal of the project was for students to develop a deeper understanding of a specific InfoSec technology area, create a presentation targeted for upper management, and to make recommendations about incorporating the technology. At the beginning of the semester, students were asked to form into groups of three and were given the task of selecting a new InfoSec technology to investigate. Each group had to conduct preliminary research and write a brief one-page proposal to the instructor about the topic they selected. Yurcik describes this "Project Approach" (Yurcik - Approaches, 2001). Upon approval, each group was required to write a report and produce a brief presentation at the end of the semester on their topic. Students were restricted on the number of slides and the amount of technical detail used in their presentation to simulate the interaction between mid-level and upper management. The use of a group project highlighted the dynamics of group learning, scheduling, resource allocation, and conflict resolution in the corporate environment. Further, students had to "sell" their security solution to the instructor, who played the role of a member of upper management who viewed security as a resource drain with no tangible value. The ability to communicate effectively is a very important attribute for any aspiring InfoSec professional to possess.

4. LABORATORY DESIGN PHILOSOPHY AND CONTENT

In order for students to learn the skills required to protect their corporate information assets, they need to gain a deeper understanding of the strengths and weaknesses of information system technologies. For this reason, we chose to incorporate a security laboratory experience into the course design.

4.1 Different Approaches

We identified two different approaches one can take when developing security exercises in a sandbox environment. The first approach is described by Hill (Hill, 2000) and Welch (Welch, 2002), and incorporates attack-defense exercises involving two opposing groups: the attackers (black hats) and the defenders (white hats). In Hill's approach, students are assigned to one of the two groups at the beginning of the semester. As the semester progresses, the two groups engage in cyber combat with each other outside of class time while they learn about attack and defense strategies during class. In contrast, Welch's approach assigns all students to be white hats and recruits black hats from external organizations. A majority of the semester is allocated for students to learn how to set up, administer, and defend a network. During this time, students learn about effective defenses by perpetrating attacks on their own systems. Finally, the semester culminated when the external attackers are allowed to attempt to compromise the student systems during a one week time period.

The second approach is limited in scope, and is best described as "penetration testing" exercises. In this approach, the students learn about attack and defense strategies through a sequence of examples that illustrate the strengths and weaknesses of operating systems, services, and tools. In this approach, there is no static assignment of attacker or defender, as students play both roles in different exercises each week. This style represents more of a "know your enemy" approach. Many IT security consultants offer this type of education to corporate IT employees.

4.2 Our Approach

We selected the penetration testing approach as the most effective means to deliver the material to our students. Undergraduate business students entering our class do not have the background necessary to facilitate a meaningful attack-defense exercise within the allocated time. As a result, we designed the laboratory as a "guided tour" of security technologies.

We had four primary criteria in designing the laboratory: 1) provide a set of core experiences, 2) make it easy to understand and complete, 3) focus on business information systems and their security issues, and 4) keep the environment tightly controlled. First, we wanted to give students a core set of experiences. We achieved this by guiding students through the steps involved in a typical attack and defense scenario. Students explored the tools and techniques used to conduct network reconnaissance, port scanning, vulnerability scanning, system integrity checking and intrusion detection. Our belief is that once students realize how easy it is to penetrate a network, they will forever support and promote the cause of information security, even if they choose a non-security IT career path. Second, we wanted to make it easy for the students

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

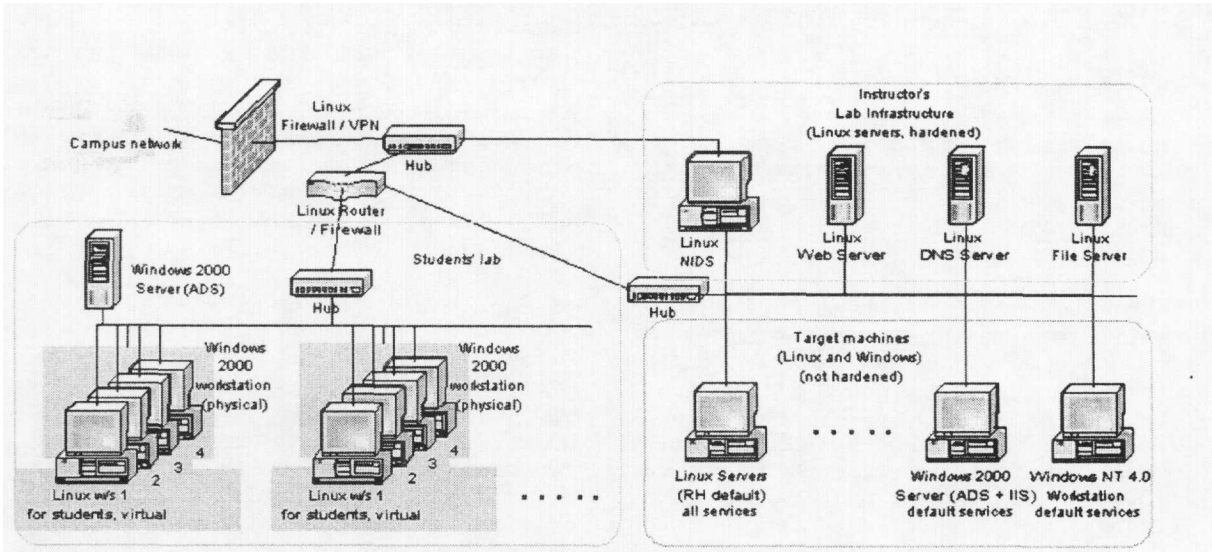

Figure 1 – Security Laboratory Architecture

to achieve the desired result by selecting visual tools to the extent possible, making the lab exercises modular, and keeping the exercises short. Third, we used the Linux operating system, a UNIX clone, as a vehicle for learning because it provides an easy way to implement a wide range of business information services including web servers, mail servers, database servers, name servers, compilers, etc. We believe strongly that knowledge of UNIX is essential for any aspiring security professional. Finally, we used various techniques to ensure that the laboratory was immune to accidental disruption from student activities, and could easily restored to the original configuration at the start of future semesters.

4.3 Security Laboratory Architecture

The laboratory network consists of two different sub-networks as shown in Figure 1. The security laboratory was designed to be both physically and logically isolated from the campus network by the creation of a "network sandbox" (Bishop, 1996; Hill, 2001; Yurcik - Approaches, 2001; Welch, 2002). The "sandbox" environment ensured that any malicious content or activities studied in the laboratory did not adversely affect the campus production network. For example, to prevent attacks like "port scanning" going out of the sandbox, we blocked all outgoing traffic. However, during some limited exercises we allowed only outgoing http requests to provide access to Internet information resources.

4.3.1 Student Subnet

The student subnet consists of a network of fourteen personal computers configured as Windows 2000 Professional workstations and one Windows 2000 Active Directory® server. The student subnet is interconnected using a hub to provide the capability for students to "sniff" network traffic during laboratory exercises. Each of the student workstations contains a 1.7GHZ Intel Pentium IV processor, 512 MB of main system RAM, a CD-R/W drive, and two 40GB hard disks: One hard disk is reserved for the OS and related applications and the other is reserved exclusively for student disk space.

4.3.2 Infrastructure Subnet

The infrastructure subnet contains both the systems required to support the student laboratory and the systems targeted during attack exercises. The infrastructure subnet was physically inaccessible to the students, in order to strengthen their experience in reconnaissance and network mapping of unknown networks. The support systems were all configured as RedHat Linux 7.2 servers and hardened in accordance with industry accepted best security practices. These servers implemented a variety of network functions including a Domain Name Server (DNS), a mail (SMTP) server, an Apache web server, a log server, a print server, an intrusion detection system (IDS), and a "workbench" server. We also set up ten target systems in this subnet, each loaded with stock installations of various operating systems. All of the systems in this subnet were acquired from University surplus at no cost to our department.

4.4 Laboratory Exercises

The laboratory exercises were designed to reinforce the key concepts developed in the classroom. Each of the exercises was designed to take no more than sixty minutes to complete and was tested by the authors and selected students in the semester preceding the first offering of the class. The exercises give the students hands on experience in the configuration, operation, monitoring, and analysis of various security tools and technologies. The laboratory also required students to develop troubleshooting skills. For example, when a new command was introduced to change the behavior of the network interface card, some students incorrectly typed the command causing their system to lose network connectivity. Students had to apply their knowledge of the environment and the tools that they had learned to determine why their network connection was non-responsive. Table 2 shows a listing of the laboratory topics and tools studied.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

4.5 Operational Issues

All of the infrastructure and target machines were installed, configured and maintained by the instructor and a graduate student. Access to the student laboratory was only permitted during class and designated lab hours. All network traffic was logged to insure the integrity of the laboratory.

One problem we encountered in implementing the lab had to do with the limited number of student workstations in the laboratory. Since we had four times as many students as we had workstations, we had to schedule four different lab sections. We could have partitioned the hard disks physically into four separate Linux installations on a disk, but previous experience indicated that a simple mistake by one student could render all installations unusable. Fortunately, a product called VMWare Workstation (www.vmware.com) provided a perfect solution. VMWare is an operating system emulator that allows a user to create a number of virtual systems on their system. Each of the virtual systems appears and operates as if it were an actual independent physical system. All of the information required to run the virtual machine is stored in a few files on the host computer disk and can be easily removed at the end of the semester.

Table 2. Laboratory Topics

Lab	Topic	Category
1	Operating System Installation, Configuration, and Administration	Operating Systems
2	Exploring the Network Infrastructure	Network Reconnaissance
3	Nessus: System Vulnerability Scanning	Vulnerability Assessment
4	UNIX Network and File System Basics	Operating Systems and Network Basics
5	Understanding Authorization and Permissions	File System Protection
6	Using PGP for Secure Email	Cryptography
7	PKI: Certificates for Secure e-Commerce Transactions	Business Information Security
8	Tripwire: Validating System Integrity	Monitoring File System Integrity
9	Windows Domain Vulnerabilities	Exploits
10	SNORT: Intrusion Detection Basics	Real-time Intrusion Detection
11	NMAP: Network Reconnaissance Tools	Port scanning
12	Ethereal: Sniffing Network Traffic	Network Sniffing
13	Jack The Ripper: Password Capture and Cracking	Network Sniffing and Cryptography
14	System Compromise Competition	All

5. CONCLUSIONS

Overall, the first offering of the course was a great success. The lecture techniques discussed above proved to be very effective at maintaining student interest in class. During the semester, there were a number of high profile information security incidents published in the popular media that spawned lengthy discussions in class. Students appreciated the relevance of class when they realized that they could have prevented many of these incidents with the knowledge they gained in the class. The role-playing exercises were valuable because they allowed students to be placed in a variety of situations and to appreciate the view of an issue from various perspectives. Students were especially divided in their discussions about privacy in the business enterprise. The case studies also resulted in a number of lively discussions. Specifically, one ethics case study that highlighted the conflict between an employee's responsibility and the potential loss of their employment status resulted in a highly divided class opinion (Boyer, 2000). One area that needs improvement in the course is the presentation of risk management in the corporate environment. Although students recognized the value of the process, they felt that the formalization of the process was tedious.

The laboratory was also very successful. Since we designed the lab more as a guided tour, no student had difficulty in completing the lab in the allotted time. We initially provided GUI screen shots as part of our instruction, but students soon got used to the text form instructions and command line interfaces. Since most of the students in the class had never used security tools before, they were very excited when they discovered that the network sniffing tool Ethereal revealed usernames and passwords during FTP and TELNET sessions and when Nessus displayed a long list of vulnerabilities present on one of the target system. Some students were so captivated by the experience that they began to further explore security tools on their own time, which was one of the goals of the class. We did experience a problem due to the late delivery of the laboratory equipment. As a result, we were only able to offer half of the lab exercises planned for the semester. One difficulty we anticipated was that of students having problems understanding UNIX syntax and using a command line interface. We were able to offset some of the problem by providing condensed command "cheat sheets".

At the end of the semester, all of the students were surveyed about their perceptions of the course. Students

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

uniformly indicated they enjoyed the class and believed that it filled a void in their education. A majority of students indicated that they wanted more time in the laboratory, an issue that has been resolved. As a result of the overwhelming positive responses from the students, the department decided to expand the course by adding additional undergraduate sections. Additionally, a graduate version of the course will be offered that and we plan to offer an attack-defense exercise in conjunction with our school's Computer Science department.

6. REFERENCES

Barnett, S. [1996]. "Computer Security Training and Education: A Needs Analysis", In Proceedings of the IEEE Symposium on Security and Privacy, pages 26 - 27, Los Alamitos, CA, May. IEEE Computer Society Press.

Bishop, M. and Heberlein, L. T. [1996], "An Isolated Network for Research," *19th National Information Systems Security Conference*, Baltimore, MD, October 22-25, pp. 349-360.

Boyer, K. W. [2000], "Pornography on the Dean's PC: An Ethics and Computing Case Study", *Journal of Information Systems Education*, Summer-Fall 2000, pp. 121-126.

Computer Security Institute and Federal Bureau of Investigation. [2002], 2002 CSI/FBI Computer Crime and Security Survey. Computer Security Issues & Trends, Vol. VIII, No. 1, Spring.

Greenstein, Marilyn and Miklos Vasarhelyi [2002], "Electronic Commerce - Security, Risk Management, and Control", McGraw-Hill Irwin, New York, NY. ISBN 0-07-241081-7

Hill, J. M. D., Carver, C. A., Humphries, J. W., Pooch, and U. W. [2001], "Using an Isolated Network Laboratory to Teach Advanced Networks and Security", In Proceedings of 32nd SIGCSE Technical Symposium on Computer Science Education, February 21 - 25.

International Information Security Foundation (I^2SF) [2002], Generally Accepted System Security Principles (GASSP), available as of May 19, at http://web.mit.edu/security/www/gassp1.html

International Information System Security Certification Consortium, Inc. $(ISC)^2$ [2002]. Common Body of Knowledge (CBK), available as of May 19, 2002, at http://www.isc2.org/cgi-bin/content.cgi?category=8

Irvine, C. E., Chin, S. K., and Frincke, D. [1998], "Integrating Security into the Curriculum," in *IEEE Computer,* December, pp. 25-30.

Kessler, G. C. [2001], "Nontechnical Hurdles to Implementing Effective Security Policies", *IEEE IT Professional,* March / April, pp. 49-52.

Miller, K. W. [1997], "Computer Security and Human Values Interact", *IEEE Frontiers in Education Conference,* Session F4C, pp. 1025-1029.

National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Center [2002], available as of May 19, at http://csrc.nist.gov

Pipkin, D. L. [2000], Information Security: Protecting the Global Enterprise, ISBN 0-13-017323-1, Prentice Hall, Upper Saddle River, New Jersey.

SANS (System Administration, Networking and Security) Institute [2002], available as of May 19, at **http://www.sans.org/**

Tipton, Harold and Micki Krause [2000], "Information Security Management Handbook", Auerbach, Boca Raton, FL., ISBN 0-8493-9829-0

Welch, D., Ragsdale, D., and Schepens, W. [2002], "Training for Information Assurance ", *IEEE Computer*, Vol. 35, No.4, pp. 30-37.

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

Yurcik, W., B. Smith, D. Doss [2001], "Ethical Hacking: The Security Justification", In Proceedings of the Ethics of Electronic Information in the 21st Century Symposium (EEI21), October 18-21, University of Memphis, Memphis TN, USA.

AUTHOR BIOGRAPHIES

Michael Russell Grimaila, SANS GSEC, B.S., M.S., Ph.D., is a Visiting Assistant Professor of MIS at Texas A&M University. He has over 17 years of experience in the management of computer systems and their security. He is a member of the IEEE and the Computer Security Institute. His research interests include Critical Infrastructure Protection, Risk Assessment and Management, and Computer Forensic Investigations.

Inkoo Kim, B.S., M.S., is a Masters Candidate (MIS) at Texas A&M University. His interests are network security in corporate information system and industrial systems.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

Copyright ©2002 by the Information Systems & Computing Academic Professionals, Inc. (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to the Editor-in-Chief, Journal of Information Systems Education, editor@jise.org.

ISSN 1055-3096