

# THE DEVELOPMENT AND IMPLEMENTATION OF ONLINE UNDERGRADUATE AND GRADUATE SYSTEMS SECURITY COURSES: LESSONS LEARNED

G. EDWARD HARRIS

GEORGE KELLEY

*This article presents an example course template useful for the development and implementation of a systems security course intended to be delivered entirely over the Internet. The template is based on the authors' experience obtaining administrative approval and then teaching a set of graduate and undergraduate systems security courses entirely online. The undergraduate course was designed to serve a mix of MIS and Computer Science students. The graduate course was aimed at MBA and MSIS students. We provide specific suggestions for implementing the courses, as well as course structure, content coverage, and the selection of textbooks and hands-on learning activities. Additionally, we include links to supporting Internet resources. The instructor's effort was minimized, and the learner's experience was maximized. Lessons learned stress the importance of: (1) externally validated content that is supported by a full complement of student-centered learning tools, including hands-on practice activities, threaded discussion boards, and field-based mini-projects; (2) personalized attention and interactive feedback to the students from multiple sources, such as a bond-building welcome video featuring the instructor, self-expression welcome and exit surveys, and the facilitation of extensive peer-to-peer exchanges; and (3) supporting four communication channels simultaneously: student-to-content, student-to-instructor, student-to-student, and student-to-community.*

Rapid advances in telecommunications have made business dependent on non-stop interaction with massive digital data depositories provided by millions of globally networked computers. The intensity of the activity has spurred a surge in security-related legislation in the U.S. aimed at safeguarding the flow of digital content. Examples are the Health Insurance Portability and Accountability Act (HIPAA) (U.S. Department of Health & Human Services, 1996), the Sarbanes-Oxley Act (University of Cincinnati School of Law, 2002), the eGovernment Act (National Institute of Standards and Technology [NIST], 2002b), and the Fair and Accurate Credit Transactions Act (FACTA) (National Consumer Law Center, 2003). All have effective dates grouped in the same 2003-2006 time frame.

The consequences of these developments are far reaching. For one, security-related occupations have all vaulted to the very top of the

U.S. Department of Labor's list of the fastest growing occupations, as well as to the very top of its list of occupations projected to have the largest numerical increases in employment between 2002 and 2012 (U.S. Bureau of Labor Statistics, 2004). Computer and information systems managers, network systems and data communications analysts, and medical records and health information technicians are all projected to be in high demand for at least the next 10 years. In addition, the U.S. Cyber Security Research and Development Act (NIST,

*G. Edward Harris is Associate Professor, Department of Information Systems, Weber State University, Ogden, Utah.*

*George Kelley is Professor, Department of Information Systems, University of Massachusetts, Boston, Massachusetts.*

2002a) has recognized that “investment in computer and network security research and development must be significantly increased to: (A) improve vulnerability assessment and technological and systems solutions; and (B) expand and improve the pool of information security professionals, including researchers, in the United States workforce” (p. 1-2).

Clearly, colleges and universities are charged with enrolling and preparing a much larger number of information, network, and systems security professionals than ever before. To help develop the learning infrastructure needed to support growing enrollments in security courses, this article shares some of the experiences and techniques learned from the development and implementation of two introductory systems security courses taught entirely online as part of the regular course offerings of two universities. One was a graduate course aimed at MBA and MSIS students and the other an undergraduate course aimed at MIS and Computer Science students. Both courses sought to provide a good understanding of the basic theoretical principles, key concepts and terminology, and value metrics of information, network, and systems security as a discipline.

In the following sections, this article addresses the specifics regarding the teaching of the information systems security courses. First, the course methodology and content are validated by reference to literature precepts and to the content coverage of the established security certifications favored by employers. We then describe the course structure with a particular emphasis on the course components that proved important for the success of these online courses. Lastly, we describe the lessons learned.

#### COURSE APPROVAL AND CONTENT VALIDATION

To serve both the graduate and the undergraduate target audiences in a meaningful way and to expedite the course approval by the university administration, we

mapped the course content closely with the content covered by the industry-recognized security certifications favored by employers. See Table 1. We then included this content within the larger context of the literature precepts for the teaching of online courses.

The design framework for the online course was provided by the prior work of Carr-Chellman and Duchastel (2000) and Poole (2002) and included a strong experiential learning component (Conrad & Donaldson, 2004; DuCharme-Hansen & Dupin-Bryant, 2005; Neill, 2004).

Employers value certifications (Parker, 2005); therefore, students tend to be motivated to enroll and complete their studies with the prospect of being able to use their coursework to obtain greater credibility before potential employers. In addition, building security courses around nationally and internationally recognized security-related certifications increases the program’s visibility and credibility, thereby helping to attract and retain more students moving toward career paths tied to professional certification in information systems security, a major goal of the Cyber Security R&D Act (NIST, 2002a).

There are at least three well-known and established vendor-neutral security certifications. See Table 1 for links to them. Generally, each of the certifications in Table 1 seeks to serve a different audience, and, therefore, has different areas of emphasis. For example, the Certified Information Systems Security Professional (CISSP) certification targets advanced security professionals and consultants and, as such, is more applicable to MBA and MSIS students. The CISSP certification is designed around the 10 key knowledge domains within information security (Certified Information Systems Security Professional [CISSP], 2003). These are:

**Table 1. Vendor-neutral certifications**

Security Certification	Sponsor	Internet Link*
Security+	CompTIA	<a href="http://www.comptia.org/certification/security/">http://www.comptia.org/certification/security/</a>
SCNP and SCNA	SCP	<a href="http://www.securitycertified.net/certifications.htm">http://www.securitycertified.net/certifications.htm</a>
CISSP	(ISC)2	<a href="http://www.cissp.com/Exam/exam.html">http://www.cissp.com/Exam/exam.html</a>

\* Links as of December 5, 2005.

1. Security Management as a Profession
2. Security Architecture and Models
3. Business Continuity Planning and Disaster Recovery Planning
4. Privacy and Security: Law, Investigations, and Ethics
5. Physical Security and Access Control
6. Business Operations Security
7. Access Control Systems and Methodologies
8. Cryptography and Biometrics
9. Telecommunications, Network, and Internet Security
10. Software Application Development Security

In contrast, although the CompTIA Security+ and the SCP, SCNP and SCNA certificates shown in Table 1 tend to address the same general content areas, they are generally aimed more at entry- and mid-level systems security positions.

#### COURSE DESCRIPTION

One of the steps in preparing the systems security courses for university credit-granting approval was to write a course description for inclusion in the University catalog. The course approval process took approximately two years. After several iterations, the University approved the following course description:

*Systems Security (3).* An overview of information systems security concepts and theories, with applications. The course emphasizes the management of information security through the development of policies, procedures, logs, and audit metrics. It also identifies common security vulnerabilities; introduces the concept of risk; addresses methods for the analysis of legal, ethical, and privacy issues in information systems; and investigates emerging security technologies in areas such as smart cards, electronic digital signatures, and biometrics.

The course topic coverage capable of addressing this description is shown in Table 2.

#### COURSE TOPIC COVERAGE AND LEARNING OUTCOMES

The topic coverage in Table 2 is ordered according to the five security knowledge areas identified by the OEIS 12 - Information Systems Security course (Organizational Systems Research Association [OSRA], 2004):

1. Introduction, current concerns, and implications of IS security;
2. Risk and security management;
3. Countermeasures and audits;
4. Legal and ethical issues; and
5. Emerging security trends.

Additional topic detail and alternate knowledge areas can be obtained by referencing the OEIS Model Curriculum (OSRA, 2004) and the CISSP (CISSP, 2003) and CompTIA Security+ web sites ("CompTIA Security+," 2005). For example, the specific operational formulations of course outcomes for an introductory systems security course have been summarized as follows in OEIS 12, the information systems security course of the OEIS Model Curriculum (OSRA, 2004):

1. Understand and apply the concepts and theories underlying the administration of information systems security;
2. Examine and use current methodologies for information systems security design, implementation, and monitoring;
3. Undertake a review of information systems security approaches to securing the information assets of organizations; and
4. Consider and analyze the impact of information systems security on organizations and society.

#### COURSE SCHEDULE

We took great care in the preparation and organization of the online course schedule. As recognized in the literature, the online schedule is a study guide that serves as "perhaps the central element of an online course" (Carr-Chellman & Duchastel, 2000, p. 233). An online course plan

**Table 2. Weekly Course Schedule and Topic Coverage, Adapted from: OEIS 12 – Information Security Course (2004)**

Systems Security Knowledge Area	Week (Hours)	Topic Coverage
1.0 Introduction	Weeks 1-3 (9)	Definitions, history of IS security, current concerns, and implications of IS security. Overview of the history and concepts of information security. To include definitions, the field, context, and environment. Introduces intrusions, crimes, laws, and business concerns, and provides an awareness of information security software and hardware products.
2.0 Information Systems Security Management	Weeks 4-7 (9)	Key principles, management's role, standards, policies, procedures and risk management. Introduces the policy development process, and the concepts of standards-based policy development, implementation, and risk management, such as defense-in-depth and separation of duties.
3.0 Infrastructure Security	Weeks 8-10 (9)	Introduces threats, risks, and vulnerabilities. Defines classes of attacks and attackers and names approaches to hardware and software intrusion protection (IDSs and NIDSs). Describes various security logging and audit techniques, and ties the security infrastructure to information systems security management, standards, policies, and procedures.
4.0 Legal And Ethical Issues In A Global Context	Weeks 11 & 12 (5)	Cultural and legal issues related to the protection of computer data assets, information flow, copyright, and privacy. Differentiates security from safety, and intellectual property from fair use. Describes the moral and ethical implications of information systems security in a global setting.
5.0 Emerging Trends in IS Security	Weeks 12-14 (9)	Introduces emerging technologies in information security. Identifies the technologies, the issues in their implementation, and evaluates their value and limitations in an information security environment. Topics include e.g. biometrics, digital cash, wearable computers, wireless devices, and smart card technology.
Final Exam	Week 15 (3)	Final Examination

should serve a six-fold purpose beyond providing content: guidance, communication, building community, humanizing, evaluating, and assessment (DuCharme-Hansen & Dupin-Bryant, 2005).

A detailed schedule of topics and activities for the entire 13-15 week undergraduate and graduate online courses was prepared in advance of the beginning of the course. Each weekly module includes bullet-captioned learning objectives. Links for the discussion boards were largely collected in advance of the course from security topics in the daily news. A good number of multimedia media links, typically movie clips and rich interactive graphics, came from the online editions of the *Boston Globe* and *The New York Times*.

The entire weekly schedule of hands-on activities, discussion board forums, and reading

assignments was presented to the students from their first login at the start of the term. The students were given an instructor-paced, two-week rolling window to address the course content and activities. The anticipated time to complete each activity was roughly estimated so as to allow for a total of about 130 hours of effort. For example, reading assignments were estimated as requiring three minutes per page. One week of slack was planned into the schedule, in part to be able to address unanticipated topics mentioned as being of interest by students when responding to the Welcome Survey.

The detailed advance planning of the schedule of learning activities into parsed modules significantly increased the effectiveness of the course. It also helped make the course scalable, whether there were 10 undergraduate students or 40 graduate students in the course.

The detailed planning and reusable modules also made it easier to rebuild the course the next time it was taught. These strategies also greatly reduced the number of hours invested by the instructor for the daily course upkeep and, once set up, virtually eliminated the need for additional preparation.

In keeping with the student-centered model (Neill, 2004), much of the instructor's time and effort during the term was spent as a motivator, when providing individualized feedback to the students, and as a facilitator, when guiding the discussion boards and field projects. This is a significant shift away from the content- and instructor-centered emphasis of traditional in-person instruction.

#### SUGGESTED TEXTBOOKS AND SUPPORTING RESOURCES

Appendix A shows an annotated list of suggested security-related textbooks. The ISBN numbers and electronic bookstore links for the purchase of electronically searchable CD-ROM versions of both the undergraduate and graduate student's textbooks were noted in the syllabus side by side with the paper versions. However, all students seem to have preferred to purchase the actual paper-and-page-index textbook versions. The textbooks were available fairly inexpensively from online resellers like bookpool.com or amazon.com. This preference had been anticipated (Carr-Chellman & Duchastel, 2001) but came as a surprise to the authors. It was particularly surprising in the case of the undergraduate textbook given that the electronic version included some serviceable animations and interactive end-of-chapter self-graded quizzes.

Appendix B shows examples of some of the security-related Internet links used for the courses. The Internet links proved very useful as energizers and safe starting points for student participation in the online discussion boards because they provided a ready source of vetted content.

Support specialists must recognize the needs of the user and be able to assist in integrating new hardware and software into the work environment. This includes an understanding of

designing, developing, and providing training to a diverse set of users. Trainers and support consultants must be skilled in managing working relationships with customers, balancing resources against customer needs, accommodating multiple customer requirements, and establishing liaison communications with all users.

#### ONLINE COURSE COMPONENTS

Every effort was made to provide a student-centered online learning environment that would be effective in an online setting (Carr-Chellman & Duchastel, 2001; Conrad & Donaldson, 2004; DuCharme-Hansen & Dupin-Bryant, 2005).

The security courses were prepared for delivery entirely online with the support of the following components:

1. *Welcome Video*: A video streamed over the Internet was used to welcome the students to the class. In keeping with the need for online encouragement found in the literature (Carr-Chellman & Duchastel, 2000), the purpose of the welcome video was more to open a conversational channel of communication and caring and to provide an opportunity for the establishment of a humanizing bond between the instructor and the students as individuals than to convey information. The video consisted of a three- to six-minute overview of the course structure and content and an invitation for the students to learn and have fun in the process. It also contained some self-expressed personal and background information about the instructor. The welcome video was posted as part of the university's regular course listings in advance of the start of the enrollment period. As reflected in the survey, the welcome video was very important in helping students in their decision to sign up for the course.

2. *Welcome Survey*: A welcome survey was administered as one of the first student activities during the first week of the course.

The welcome survey served multiple purposes. As with the welcome video, one important purpose of the welcome survey was to provide a human dimension to the course and to help the instructor show a personal interest in, while developing some initial rapport with, the

students as individuals. A second intent was to provide an excuse to make the students explore and become comfortable with their online course shell. In addition, the welcome survey sought to establish what preparation and expectations the students had for the course. Finally, the welcome survey sought to engender a sense of belonging and participation in the larger online community of which the students were about to become members (DuCharme-Hansen & Dupin-Bryant, 2005). Table 3 lists some of the questions included in the welcome survey.

*3. Online Course Shells:* Prometheus was initially used for the undergraduate course and Blackboard for the graduate course. The undergraduate course was subsequently offered in WebCT Vista. As a backup, in the event of technical difficulties, the course schedule was also made available on a commercially hosted website. Online 24x7 access was available to the students.

All three course shells provided similar functionality in the way of a rich online learning environment. This functionality included form example links to the course syllabus and detailed schedule of assignments, shared areas for online discussions, support for Internet links leading to external content, and an electronic grade book.

Aside from these expected capabilities, the course shells served as an important means for initiating informal and private email communications among the students as peers. Email contact was available from the electronic roster to every other student in the class. WebCT's "Who's Online" feature, in particular,

made it easy to identify students currently online, who could then be contacted in real time by their peers.

The combination of mind-sharing enabled by the threaded discussion board interaction and off-channel email exchanges made for a much more frequent, and often richer and deeper, degree of peer-to-peer interaction than available in the classroom or hallway of a traditional in-person course.

*4. Detailed Syllabus and Schedule of Activities:* The syllabus and schedule of activities for the graduate course were prepared to emphasize the conceptual development of sound administrative security policies and procedures. The syllabus and schedule of activities for the undergraduate course placed greater emphasis on task-level implementation and technical detail.

The schedule of activities for both the graduate and undergraduate courses was very detailed. It included a synopsis of the reading assignments and lists of student tasks. The schedule of activities allowed the students to study largely at their own pace but within weekly rolling deadline windows specified in advance by the instructor (Carr-Chellman & Duchastel, 2000). This structured flexibility for the completion of activities within self-paced windows of completion was a course feature repeatedly noted as very helpful by the students in their exit surveys.

*5. Online Discussion Board:* The online discussion boards were open forums intended to encourage student self-expression and peer collaboration (Roby, 2005). They proved to be

**Table 3. Example Welcome Survey Questions**

1.	Is this the first online course you have taken? If not, what other courses have you taken online?
2.	Why are you taking this security course?
3.	In what ways do you anticipate this online course to be different from an in-class, in-person course? More effective? Less effective?
4.	How are you going to access this course online? Via a dial-up connection or a broadband connection?
5.	Do you anticipate being limited by the software, hardware, or connectivity available to you when accessing audio and video content, or attempting the hands-on practice activities?
6.	What are your prior coursework, background, and/or experience within the general areas of information, network, and systems security?
7.	What is your current employment situation? (work hours, workload, overall work satisfaction, next better job)
8.	What security-related issue or news story came to your attention in the last two weeks? Why? How many different people were affected?
9.	Are there topics or activities not included in the course schedule that you would like to see added? What are they?
10.	Do you have any questions or comments for your instructor? What are they?

one of the most important components of the graduate course. The questions and problem statements posted on the discussion board were mostly open-ended questions and were composed from the course content and reading assignments. Examples of topics posted on the Discussion Board are given in Appendix C.

The information contributed by the students was collected as a threaded collage by the online course shell software. The discussion board participants were told to read all previous replies before making their own unique contribution. The topics targeted at the undergraduate students were narrower in scope than those asked of graduate students. They were typically closely and narrowly tied to the reading assignments. Graduate students, on the other hand, were often asked to expand critically on the provided course materials with information from other sources and to take positions that required the application of concepts and values in the face of greater complexity and ambiguity.

One of the undergraduate courses, consisting of 15 students, had in excess of 1,900 postings during the term, or some 125 per student. The 37 graduate students made approximately 1,005 postings for an average of 27 per student. The graduate students were decidedly longer and more argumentative in their exposition and often drew content from external sources or from the poster's personal experience. The undergraduate students' postings tended to be repetitive of previous contributions, and a few undergraduate students had to be coaxed to contribute to the discussion boards. To encourage the more hesitant students, Kazmer (2004) has suggested: (1) pre-empting the repetition issue by not asking questions (because they tend to invite conforming answers), and, instead, posting more open-ended content and simply inviting some free-form commentary; (2) provide no content and, instead, ask the students to express in their own words what they have encountered in the week's readings and activities; (3) closing the board at the end of every week in favor of a fresh one; and (4) including a specifically designated peer help forum.

Overall, as DuCharme-Hansen & Dupin-Bryant (2005) found in their research, the value

of the discussion board was significant for both the graduate and undergraduate courses in terms of establishing a channel for open communication, sharing ideas, encouraging collaborative learning, and building a sense of belonging to the online community.

#### *6. Weekly Orientation and Reading*

*Assignments:* The instructor provided a weekly summary of learning objectives and activities mapped to the reading assignments, discussion topics, and hands-on activities for the week. An excerpt of the highlights was emailed to the students at the beginning of the week to help them plan their time and anticipate the more important points in advance of accessing the material.

The instructor's weekly orientation closed with a topic introduction and a set of questions that were directly linked to the discussion board thread topics pertaining to that week's reading assignments. The instructor's introduction to the reading assignments and the Internet and discussion board tie-ins served as an important means of encouraging online community interactions and the application of the information assimilated by the learners.

*7. Internet Resource Links:* Internet links were provided in the syllabus as general resource lists as well as interspersed with the instructor's weekly introduction to the material and the weekly schedule of activities and hands-on assignments.

The links expanded the online learning environment by providing a highly interactive environment for the students. They let the students explore particular areas of interest to them on their own. For example, in the category, "Recent Security-Related Legislation in the U.S.," the links provided accessible analyses of the eGovernment Act (NIST, 2002b), the 1996 Health Insurance Portability & Accountability Act (U.S. Department of Health & Human Services, 1996), and the Fair and Accurate Credit Transactions Act (National Consumer Law Center, 2003).

The links to the weekly topics were presented in the weekly course schedule but tied to the threaded online discussion board family of topic trees via a single click of the mouse. This cross-linking capability provided an important element of continuity between the course components, and

closely tied the conceptual acquisition of the material to its application in practice.

*8. Hands-on Mini-Projects:* The student's experiential learning was maximized by providing a set of some 35 hands-on mini-projects.

As elsewhere in the course, the students were given considerable flexibility in the selection of a subset of the individual hands-on activities out of the 30-odd hands-on activities provided. The hands-on mini-projects were accompanied by detailed and numbered step-by-step instructions to be executed on the student's own hardware. The hands-on activities were further adapted to the student's circumstances, abilities, and interests by letting the students select their hands-on activities from a variety of (roughly comparable) activity options and then have the students work on the hands-on activities they had selected on their own time. All the students had to do was submit a short templated report, including screenshots of the completed activities, by the instructor's deadline.

Both the graduate and undergraduate students were asked to complete and submit the hands-on activities. The hands-on mini-projects provided hands-on experiential learning (Neill, 2004) and proved very popular, particularly for the undergraduate students.

The hands-on activities typically called for downloading, installing, and investigating the functionality of a software application from the Internet to the student's computer. All the software needed for the completion of the hands-on activities was available for access or download from the Internet from plentiful third-party links. There was no need for the instructor to assume the burden of creating and maintaining their own online archive of laboratory resources.

Although the hands-on assignments were the same, certain students in the graduate course (mostly MBA students) generally had greater difficulty with the hands-on activities than any of the students in the undergraduate course. Examples of hands-on activities were to install the software needed to digitally sign and encrypt an email message using public and private keys, setting up and assigning users to groups to enforce access permissions to shared disk folders,

and adding a validated security certificate to a web browser.

Overall, the hands-on activities served to significantly increase the student's engagement and level of participation in the course, well above what would be possible in an in-person laboratory setting. They also helped sharpen the student's problem-solving abilities and sense of self-confidence in their ability to apply some of their knowledge (Conrad & Donaldson, 2004).

*9. Field Interview Project:* There is a need to foster student engagement in the student's physical social and employment community beyond simply lively interaction within the members of the online community themselves in a virtual online classroom (Berberet, 2002; Palloff & Pratt, 2004). To serve this need, undergraduate students were asked to go to a trade conference or expo in the locality in which they lived. Their assigned task was simply to sit in on a presentation or two by a security professional and/or visit informally with security industry vendors in their show booths. After the event, the undergraduate students were asked to write a one-page summary about their experience at the trade show. The instructor suggested several venues based on the student's physical zip code location. Graduate students, in turn, were asked to interview someone within a local company on a topic related to systems security from a list offered by the instructor or suggested by the students themselves. Graduate students were asked to complete their field assignment in small, self-selected groups of two to three students. To ensure full participation and a richer experience, all group members were required to attend the on-site field interviews. Example topics for the field project are shown in Appendix D.

*10. Term Paper Project:* Graduate students who opted not to participate in a field group interview project were required to write a 12-15 page double-spaced research term paper of about 3,000 words. Appendix D includes a list of suggested term paper topics. In the end, about 20% of the graduate students opted for the individual term paper over the field interview project. A set of example paper titles for the term project was provided to the students by the

instructor at the beginning of the course. Suggested topics were such that the students would have had to search the indexed literature for additional information beyond that provided in the text and in the reading assignments. Access to the online library literature databases (for example, EBSCO, Academic Source Premier, and Business Source Premier) was available to the students from within the online course shell.

*11. FAQ:* Answers to Frequently Asked Questions (FAQ) were made available to students in a dedicated area of the course shell. The purpose of the FAQ section was to reduce the number of email messages to the instructor on repetitive issues of common interest to all online students enrolled in the class. For example, a number of students showed an interest in the instructor's awareness of the student's login frequency and level of online activity and participation. The course shell was able to track this information using timed "access hits." Therefore, a common question from students for which an answer was provided in the FAQ was "What are access hits?"

*12. Online Examinations:* The midterms and final exams for the graduate course and the reading assessments for the undergraduate courses were conducted entirely online. The students were given a two-week long rolling window during which they submitted their exams. Graduate students were given open-ended questions with directions as to where to look for the answer in the textbook and elsewhere online. Undergraduate students were given a random subset of multiple choice questions drawn from a larger pool of questions tied closely to the course reading assignments. These randomized multiple-choice exams were timed and graded automatically by the online course shell. To encourage the undergraduate students to learn more by re-reading the pertinent sections of the book, incorrect answers were flagged with a reference to the page of the book where the student could find the correct answer. The undergraduate students were permitted to retake the multiple choice examinations for better grades at their convenience, as often as they cared to, within the two-week long completion window specified by the instructor. The online course

shell software was configured to make the quizzes available for several days, usually two weeks, before becoming unavailable again, on preset days and at preset times, without further instructor intervention. Despite reminders from the instructor, a good number of undergraduates waited until the last possible moment to submit their exams and reading assessment activities and, therefore, did not have the opportunity to re-submit their exams for better grades. The course shell's electronic grade book was used to keep the students informed of their progress within every graded activity in the course, with running point totals, including their scores on the online examinations.

*13. Synchronous Sessions:* Two online chat room sessions were scheduled the second time the undergraduate course was offered, and four were scheduled for the third offering. Students were asked to join an online chat room within the course shell at a certain day and time in the early evening of a weekday. The instructor sent a reminder the evening before the scheduled chat session.

The sessions were initiated based on feedback from a small, but vocal, group of students from the previous term. When asked in an exit survey to reveal what was important in an online course, one student replied "Meeting real time with the instructor in the virtual classroom to ask/answer questions and have a discussion." Students who responded similarly appeared to be motivated more by the novelty of the technology and natural curiosity. Because not every student could keep the appointments due to personal schedule conflicts, an alternate date and time for each of the two planned sessions was scheduled the third time the undergraduate course ran. The alternate sessions repeated the content of the primary sessions. Offering the duplicate sessions more than doubled the number of students who were able to join in the activity. On a related note, although the instructors provided their online handle for free Internet telephone access through skype.com in an effort to encourage real-time conversations with students using Internet telephony, none of the students took advantage of this opportunity.

Instead of relying on the text-only nature of chat sessions provided by the online course shell for synchronous sessions, in which the students are mostly relegated to becoming passive listeners in a virtual room, a richer real-time web-based environment may be necessary to enable a more interactive synchronous capability that would be of greater value and interest to the students. Providers, like *centra.com* and *webex.com*, offer a zero-install, fully interactive, take-over-my-station-over-the-Internet capability for a nominal fee.

*14. Exit Survey:* An exit survey was conducted to meet several purposes: to bring closure to the course in students' minds, to enable course participants to make suggestions for improvement in subsequent terms, and to provide a feedback channel for students to express their perceived sense of overall satisfaction with the course and the instructor. Both Likert scale and open-ended questions were asked. Examples of exit survey questions are listed in Table 4. Sample student responses are shown in Appendix E.

#### LESSONS LEARNED

Overall, the lessons learned from the author's experiences with the development and implementation of the undergraduate and graduate security courses described in this paper may be summarized as follows:

*Lesson 1.* Externally validated content made it easier to obtain approval for the courses, build them, and then share their content and structure

with the students in an interactive and participatory fashion.

The externally validated content helped to ensure that the content was representative of the expectations set by the vendor-neutral certifications shown in Table 1 and, therefore, also aligned with employer expectations. The tie-in to the related operational and implementation expectations of the OEIS Model Curriculum in Table 2 (OSRA, 2004) was also helpful. By extension, the university course approval committees were reassured by the external validation of the course content.

The courses were designed to foster experiential learning (Conrad & Donaldson, 2004; DuCharme-Hansen & Dupin-Bryant, 2005; Neill, 2004) and actively engage the online learner (Carr-Chellman & Duchastel; 2000; Palloff & Pratt, 2004; Poole, 2002). A welcome video, a set of welcome and exit surveys, hands-on mini-projects, a FAQ component, and an interactive online discussion board supported by occasional video and audio clips all helped enrich and support the externally validated course content. The hands-on assignments proved to be a means to ground and engage the students in the physical reality of their subject matter. It was substantially easier, cheaper, and less time-consuming to provide hands-on activities online than in an in-person setting with the instructor and the students present. There was no need for the instructor to schedule laboratory hours and maintain the related laboratory hardware or spend hours in a lab monitoring the students.

**Table 4. Example Exit Survey Questions**

1.	Compared to my other classes, this class was too easy/about the same/too hard.
2.	In what ways did you find this online course to be different from an in-class, in-person course? More effective? Less effective?
3.	Were you limited in this course by the software, hardware, or connectivity available to you?
4.	Would you recommend this course to a friend? Why or why not?
5.	Has this course improved your employment prospects? Why or why not?
6.	Name two things about this course that you liked.
7.	Name two things about this course that could be improved.
8.	Name two things about the instructor that you liked.
9.	Name two things about the instructor that could be improved.
10.	Do you have any questions or comments? What are they?

*Lesson 2.* A high degree of personal attention and interactive feedback proved very important to the online students and, therefore, for the overall success of the online security course. See Appendix E, Item 1.

Several devices used in combination served to increase the student's level of personal interaction and foster a sense of belonging and ownership within the online course learning community. For example, the 6 ½-minute welcome video was an effective way to initiate a personal bond with the students. Student feedback from the surveys verified that the video provided a means to associate a face with the instructor's name, thereby laying down a foundation of personal communication and human interaction between the instructor and the students. The welcome and exit surveys at the beginning and end of the course also served as important self-expression mechanisms for the students. They helped the students verbalize their needs and expectations while simultaneously taking individual ownership of their participation and success in the course. The discussion forum, once seeded by the threads posted by the instructor, invited a great degree of self-expression on the part of the undergraduate students and produced a feverish online virtual community for debating ideas on the part of the graduate students.

*Lesson 3.* At least four channels of communication are needed to support an online systems security course: student-to-content, student-to-instructor, student-to-student, and student-to-community. The first three have previously been recognized (Carr-Chellman & Duchastel, 2000). The four channels in combination define a distributed learning community, which is highly dependent on multi-channel communication for its success (Palloff & Pratt, 2004; Roby, 2005).

The first channel, the student-to-instructor channel, was evident from the large number of one-on-one personal email messages exchanged between the instructor and the online students. For example, in the case of the graduate course, over the 16-week duration of the semester, approximately 967 individual email messages were sent by the 37 students enrolled in the course. A good portion of these messages was

about term paper topics to be approved by the instructor and the field interview project. Some paper topics were scoped too broadly and were, therefore, too ambitious for the purposes of the course. These students were encouraged via email exchanges with the instructor to more narrowly define their topics. Certain students insisted on copying the instructor on every email message they sent their group on their field project. The email exchange average would likely have been higher if not for the 17 FAQ posted by the instructor in response of common questions. In subsequent courses, the instructor adopted the practice of sending a weekly email to the entire class. The weekly email outlined the coming week's activities and considerably decreased the student-to-instructor email volume.

The second channel, the student-to-student channel, was evident in the high number of discussion board student postings. As noted earlier, one course of 15 students had in excess of 1,900 postings during the term. Through the availability of the discussion board, students could ask and respond to questions among themselves, as encouraged in the literature (Roby, 2005). In addition, the online course shell permitted any student to email any other student or group of students in the course. With the instructor on the sidelines, the need for the instructor to support personal email exchanges to provide human contact was decreased.

The third channel, the student-to-community channel, serves to encourage student engagement in the daily functioning of the physical community in which they live and function. Its importance can be seen in the high percentage of students (about four-fifths) who opted to complete group term field projects that called for an on-site interview rather than a term paper. The field assignments gave students the opportunity to conduct field interviews and attend trade shows across the country in the communities in which they live and function. For example, one group of students wrote a paper entitled "HIPAA Privacy and Security Standards: A Brief Outline of the Development of Policies and Procedures at Lima Memorial Hospital" after interviewing personnel at their local hospital. Similarly, the undergraduate students in the exit survey

reported very favorable feedback on the value of the conference and expo field experience. Most of them had never before attended a professional trade show.

It appears that one of the challenges of the instructor in online courses is to learn how to minimize one-on-one student-to-instructor communications via email. Instead of contacting the instructor first, the students could be encouraged to use the FAQ, post their questions on the discussion board, or try contacting their study group peers via email. When initiating an exchange, the instructor should make every effort to post information in the way of a general announcement all can access in the announcements section of the online course shell, send an email in the format of a newsletter to the entire class on a weekly basis, and, as appropriate within the privacy context of the student's individual email query, answer these questions in an instructor's section of the course's FAQ area.

#### CONCLUSIONS

The literature validates many of the observations made when teaching the systems security courses described in this article. These observations included the need for richly interactive content and detailed advance preparation, flexibility in course delivery, structured time-management skills, the use of a variety of learning techniques and assessment strategies, generous support for interactive and multimedia content, and the building of strong student-to-instructor, student-to-student, and student-to-community engagement (Berberet, 2002; Palloff & Pratt, 2004).

Conrad and Donaldson (2004) and DuCharme-Hansen and Dupin-Bryant (2005) encourage the simultaneous use of multiple techniques when seeking to engage a learner in a well-designed online course. In the case of the design and implementation of the security course framework presented in this article, these techniques included establishing a sense of community early in the course; detailed assignment instructions; weekly work plans complemented by streaming multimedia content; extensive interaction and feedback in a learner

controlled environment; and ready access to a FAQ, chat rooms, discussion boards, and other forms of interactive assistance. As a result of the variegated approach and in accord with what has been observed by Carr-Chellman & Duchastel (2000) and Poole (2002), the four-channel interaction—(1) among the students as peers, (2) between the student and the course content, (3) between the student and the instructor, and (4) between the students and their home and employment community context—were all demonstrably better developed than in a traditional classroom.

#### REFERENCES

- Berberet, J. (2002). Nurturing an ethos of community engagement. *New Directions for Teaching & Learning*, 90, 91-101.
- Carr-Chellman, A., & Duchastel, P. (2000). The ideal online course. *British Journal of Educational Technology*, 31(3), 229-241. Reprinted in *Library Trends*, 2001, 50(1), 145-159.
- Certified Information Systems Security Professional. (2003). *(ISC)<sup>2</sup>'s certified information systems security professional: (ISC)<sup>2</sup> meets ISO Standard 17024:2003*. Retrieved December 26, 2005, from <https://www.isc2.org/cgi/content.cgi?category=97>
- CompTIA security+ certification. (2005). Retrieved December 26, 2005, from <http://www.comptia.org/certification/security/>
- Conrad, R. M., and Donaldson, J. A. (2004). *Engaging the online learner: Activities and resources for creative instruction*. Somerset, NJ: Jossey-Bass.
- DuCharme-Hansen, B. A., & Dupin-Bryant, P. A. (2005). Distance education plans: Course planning for online adult learners. *TechTrends: Linking Research & Practice to Improve Learning*, 49(2), 31-40.
- Kazmer, M. (2004, January). Online identity: Implications for course design. *Online Classroom*, 6-7.
- National Consumer Law Center. (2003). Analysis of the fair and accurate credit transactions act of 2003, Pub. L. No. 108-159 (2003). Retrieved December 26, 2005, from [http://www.consumerlaw.org/initiatives/facta/nclc\\_analysis.shtml](http://www.consumerlaw.org/initiatives/facta/nclc_analysis.shtml)
- National Institute of Standards and Technology. (2002a). *Cyber security research and development*

- act. U.S. public law 107-305. Retrieved December 26, 2005, from <http://csrc.nist.gov/policies/HR3394-final.pdf>
- National Institute of Standards and Technology. (2002b). *The federal information security management act. Title III of the e-government act, U.S. public law 107-347*. Retrieved December 26, 2005, from <http://csrc.nist.gov/policies/HR2458-final.pdf>
- Neill, J. (2004, December 11). *Experiential learning cycles: An overview of nine experiential learning cycle models*. Retrieved December 26, 2005, from <http://www.wilderdom.com/experiential/elc/ExperientialLearningCycle.htm>
- Organizational Systems Research Association. (2004). *Organizational & end-user information systems curriculum model for undergraduate education in information technology*. Retrieved December 26, 2005, from <http://www.osra.org/curriculum.pdf>
- Palloff, R. M., & Pratt, K. (2004). *Collaborating online: Learning together in community*. Somerset, NJ: Jossey-Bass.
- Parker, D. (2005, March 29). What value your security certification? *The Register*. Retrieved December 26, 2005, from [http://www.theregister.co.uk/2005/03/29/security\\_certification/](http://www.theregister.co.uk/2005/03/29/security_certification/)
- Poole, D. M. (2002). Student participation in a discussion-oriented online course: A case study. *Journal of Research on Computing in Education*, 33(2), 162-178.
- Roby, T. Y. (2005, March). 17 tips for successfully including peer collaboration in an online course. *Online Classroom*, 4-5.
- University of Cincinnati School of Law. (2002). *The Sarbanes-Oxley Act. U.S. public law 107-204*. Retrieved December 26, 2005, from <http://www.law.uc.edu/CCL/SOact/soact.pdf>
- U.S. Bureau of Labor Statistics. (2005). Occupational outlook handbook: Tomorrow's jobs table 1. Retrieved December 26, 2005, from <http://www.bls.gov/oco/ocotjt1.htm>
- U.S. Department of Health & Human Services. (1996). *The health insurance portability and accountability act. U.S. public law 104-191*. Retrieved December 26, 2005, from <http://aspe.hhs.gov/admnsimp/pl104191.htm>

#### ACKNOWLEDGEMENT

The authors would like to thank the reviewers for helpful feedback and Professor C. Steven Hunt for his tireless encouragement over the course of the last three years for the publication of this article.

**Appendix A. Suggested Security-related Textbooks and Readers**

1. Anderson, R. J. (2001). *Security engineering: A guide to building dependable distributed systems*. Somerset, NJ: John Wiley & Sons. 640 pages, ISBN 0-4713-8922-6. A friendly and peripatetic source for discussion board material.
2. Bishop, M. (2003). *Computer security: art and science*. Old Tappan, NJ: Pearson Addison-Wesley. 1,136 pages, ISBN 0-2014-4099-7. An alternative to Schneier. Intended for a fairly committed audience. Contains over 1,000 references.
3. Campbell, P., Calvert, B., & Boswell, S. (2003). *Security+ guide to network security fundamentals*. San Jose, CA: Cisco Learning Institute. 509 pages, ISBN 0-6191-2017-7. The value of this book lies mostly in its end-of-chapter hands-on activities. However, its companion Lab Manual (Cretaro, No. 4 below) functions very well independently of this parent book as a source of hands-on activities.
4. Cretaro, P. (2002). *Lab manual for security+ guide to network security fundamentals*. San Jose, CA: Cisco Learning Institute. 270 pages, ISBN: 0-6191-3104-7. A valuable and not overly technical source of hands-on activities for both undergraduate and graduate students.
5. Dhillon, G. (2006). *Principles of Information Systems Security: Texts and Cases*. Somerset, NJ: Wiley. 464 pages, ISBN 0-4714-5056-1. Addresses both the technical and human side of IS security by means of both formal and informal controls.
6. Fumy, W. & Sauerbrey, J. (Editors) (2006). *Enterprise security & IT security solutions: concepts, practical experiences, and technologies*. Somerset, NJ: John Wiley & Sons. 264 pages, ISBN 3-8957-8267-X. Maps standard concepts of security into practical applications within vertical industry sectors, such as e-health, e-government, the automotive industry, and financial services.
7. Gollmann, D. (2006). *Computer Security* (2<sup>nd</sup> ed.). Somerset, NJ: John Wiley & Sons. 386 pages, ISBN 0-4708-6293-9. Aimed at a more of a technical than business audience.
8. Krause, K., & Tipton, H. F. (Editors) (1999-2005). *Information security management handbook*. Five volume bundled set, hardcover, Volumes 1, 2, 3 and 4 (1999-2003), ISBN 0-8493-1068-7; Volume 5 (2004), ISBN 0-8493-1997-8. Volumes 1-4 are also available on a searchable CD-ROM, ISBN 0-8493-1234-5. There is also a 2005 CD-ROM edition, ISBN 0-8493-3947-2. New York, NY: Auerbach Publications. A collection of conceptual papers grouped by the CISSP test knowledge areas. Aimed at information security practitioners and advanced students. Not overly technical. An alternative to the SANS reading room.
9. LeVeque, V. (2006). *Information security: a strategic approach*. Somerset, NJ: Wiley-IEEE Computer Society Professional Series. 220 pages, ISBN 0-4717-3612-0. Describes how to incorporate information security into a general enterprise strategic planning framework.
10. Merkow, M., & Breithaupt, J. (2005). *Information security: principles and practices*. Upper Saddle River, NJ: Prentice Hall. 608 pages, ISBN 0-13-154729-1. The most recent textbook on the subject of information security. The chapters are organized according to the CISSP knowledge domain model.
11. Pfleeger, C. P., & Pfleeger, S. L. (2002). *Security in computing* (3rd. ed.). Upper Saddle River, NJ: Prentice Hall. 746 pages, ISBN 0-1303-5548-8. A computer-oriented view of security.
12. Pipkin, D. H. (2000). *Information security: protecting the global enterprise*. Upper Saddle River, NJ: Prentice Hall PTR. 364 pages, ISBN: 0-1301-7323-1. The chapters are short, and include illustrative case study vignettes and example interspersed applications.
13. Raval, V., & Fichadia, A. (2006). *Security and control of computer based systems*. Somerset, NJ: John Wiley & Sons. 528 pages, ISBN 0-4714-8579-9. Risk models, controls, and assurance in the networked environment.
14. Salomon, D. (2005). *Foundations of computer security*. New York, NY: Springer. 391 pages, ISBN 1-8462-8193-8. For advanced undergraduates.
15. Schneier, B. (2000, August). *Secrets & lies: digital security in a networked world*. Somerset, NJ: John Wiley & Sons. 432 pages, ISBN 0-4712-5311-1. A comprehensive textbook, if also often overly sententious and tiring. Offers a standard coverage, and strategies for the proper implementation of security systems.
16. Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise security architecture: A business-driven approach*. Manhasset, NY: CMP Books. 587 pages, ISBN 1-5782-0318-X. Describes the SABSA/Zachman security architecture matrix, with applications.
17. Trcek, D. (2005). *Managing information systems security and privacy*. New York, NY: Springer. 236 pages, ISBN 3-5402-8103-7. Combines technological, organizational, behavioral, and legal views into a "big picture" view of information systems security.
18. Whitman, M. E., & Mattord, H. J. (2004). *Management of information security*, ISBN 0-6192-1515-1, and (2002) *Principles of information security*, ISBN 0-6190-6318-1. Boston, MA: Thompson Course Technology. When used as a pair, a sound alternative to Pipkin.

**Appendix B. Suggested Security-related Internet Links\*****1. Multimedia Topical Security Coverage**

- a. The free online editions of *The New York Times* (<http://www.nyt.com/>) and *The Boston Globe* (<http://www.boston.com/news/globe/>) often offer multimedia video clips, audio-narrated photo spreads, and interactive graphics on information- and systems security-related articles as part of their daily news articles on international, government, daily living, and technology.
- b. The *SANS Security Reading Room* (<http://rr.sans.org/>) features over 1,300+ reports on sixty-two different information, network, and systems security topics.

**2. Security Certification-Related Resources**

- a. SCP Security Certifications: <http://www.securitycertified.net/>
- b. CISSP Certification: <http://www.cissp.com/>
- c. Linux Professional Institute Exams: <http://www.lpi.org/>
- d. CompTIA Security+ Cert: <http://www.comptia.org/certification/security/default.aspx>
- e. Cisco CCSP Cert: [http://www.cisco.com/en/US/learning/le3/le2/le37/le54/learning\\_certification\\_type\\_home.html](http://www.cisco.com/en/US/learning/le3/le2/le37/le54/learning_certification_type_home.html)

**3. Security Standards and Principles**

- a. GASSP/OECD Security Principles: [http://www.auerbach-publications.com/dynamic\\_data/2334\\_1221\\_gassp.pdf](http://www.auerbach-publications.com/dynamic_data/2334_1221_gassp.pdf)
- b. ISO/IEC 17799:2000 Security Standards: <http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf>
- c. The NIST Handbook Special Publication 800-12: <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>
- d. Universal Declaration of Human Rights, United Nations (1948): <http://www.un.org/Overview/rights.html>

**4. Security-Related Legislation in the U.S.**

- a. 2003 Fair and Accurate Credit Transactions Act (FACTA):  
[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108\\_cong\\_public\\_laws&docid=f:publ159.108.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf)
- b. 2002 eGovernment Act (FISMA): <http://csrc.nist.gov/policies/HR2458-final.pdf>
- c. 2002 Cyber Security R&D Act: <http://csrc.nist.gov/policies/HR3394-final.pdf>
- d. 2002 Homeland Security Act: <http://thomas.loc.gov/cgi-bin/query/z?c107:h.r.5005.enr>
- e. 2001 USA Patriot Act: <http://thomas.loc.gov/cgi-bin/query/D?c107:39:./temp/~c107svpdfx::>
- f. 1996 Health Insurance Portability & Accountability Act (HIPAA): <http://www.hhs.gov/ocr/hipaa/>
- g. 1986 Electronic Communications Privacy Act: <http://www.itpolicy.gsa.gov/itpolicy/5.pdf>
- h. 1974 Federal Privacy Act: <http://www.usdoj.gov/foia/privstat.htm>
- i. 1966 Freedom of Information Act: [http://www.usdoj.gov/oip/foia\\_updates/Vol\\_XVII\\_4/page2.htm](http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm)
- j. 1934 Communications Act: <http://fcc.gov/Reports/1934new.pdf>

\* Retrieved December 26, 2005.

**Appendix C. Example Discussion Board Topics**

<b>Systems Security Knowledge Area</b>	<b>Examples of Suggested Discussion Topic</b>
1.0 Introduction	<ol style="list-style-type: none"> <li>1. CIA: Confidentiality, Integrity, and Availability. Do you agree with the assertion in Anderson's Security Engineering (Ch. 24, p. 541) that "ten years ago, information security was about confidentiality, integrity and availability (CIA). In ten years, the list of priorities will be the other way around (AIC)." Why or why not?</li> <li>2. Security is often described as having "one way to get it right, many ways to get it wrong." What are some solutions to the "one way to get it right, many ways to get it wrong" problem?</li> <li>3. Secure, Safe, or Private? What distinctions does Anderson (Ch. 1, p. 10) draw between secrecy, confidentiality, and privacy? Why?</li> </ol>
2.0 Information Systems Security Management	<ol style="list-style-type: none"> <li>1. Watching The Watchman: Anderson (Ch. 23, p. 521) claims a recurring security weakness throughout the ages has been caused by a flawed answer to the question "who shall watch the watchman?" Give examples in which a security breach occurred because the safe-keepers didn't.</li> <li>2. What is HIPAA? When did it become effective? What additional security considerations are required by HIPAA for the protection of medical data and the securing of electronic medical transactions between physicians, patients, hospitals, insurance companies, and government agencies?</li> <li>3. Separation of Duties: Anderson (Ch. 9, p. 189) claims the Clark-Wilson security policy model "ducks the hardest question, namely: how do we control the risks from dishonest staff?" Anderson then proposes two kinds of separation of duty policies: dual control and functional separation. What do these terms mean? Give examples of how they could be used to good effect.</li> </ol>
3.0 Infrastructure Security	<ol style="list-style-type: none"> <li>1. eCommerce and Cryptographic Credit Card Protection: How are SSL (Secure Socket Layer), SET (Secure Electronic Transport), and PKI (Public Key Infrastructure) mechanisms used today to protect electronic credit card transactions on the Internet (eCommerce)? Do you have enough confidence in these mechanisms to use your Credit Card on the Internet? Why or why not?</li> <li>2. Fraud Rates vs. Insult Rates: In the context of security, what is meant by fraud rate? Insult Rate? Are the two always at odds with each other? Give examples.</li> <li>3. Certificates of Authority: VeriSign or Thawte? Two of the most popular issuers of Certificates of Authority (CAs) for secure web browser credit card and email exchange transactions are VeriSign (<a href="http://www.verisign.com">http://www.verisign.com</a>) and Thwate (<a href="http://www.thawte.com">http://www.thawte.com</a>). About how much do their Digital Certificates of Authority (DCA's) cost, and how does one go about procuring and installing DCA on a web server?</li> </ol>

**Appendix C. Example Discussion Board Topics (Continued)**

<b>Systems Security Knowledge Area</b>	<b>Examples of Suggested Discussion Topic</b>
4.0 Legal and Ethical Security Issues in a Global Context	<ol style="list-style-type: none"> <li data-bbox="686 312 1425 506">1. Carnivore Clipper. Anderson (Ch. 21, p. 470) tries to offer some assurance that telecommunications wiretaps can only be used with a court order, thus safeguarding constitutional provisions against unreasonable searches and seizures in the U.S. Other countries he points out are not as defensive about eavesdropping. Is he correct? And should the U.S. government be permitted to use information provided by international third parties not bound by U.S. constitutional protections?</li> <li data-bbox="686 512 1425 678">2. Data Protection in Asia and Latin America. Anderson (Ch. 21, pp. 475-479) presents the European and U.S. views of data protection security. Research the Internet and present the current position of several Asian and Latin American countries on data protection security. Are the positions of these countries more progressive or more regressive than those expounded by the U.S. and Europe?</li> <li data-bbox="686 684 1425 821">3. Security of Global Votes: Very soon transnational Global Votes on matters of all import large and small will not only be possible but expected by all peoples around the world. What are some mechanisms currently being proposed on the Internet to ensure the security of Global Votes?</li> <li data-bbox="686 827 1425 936">4. Biometrics Uses and Flaws: Anderson (Ch. 13, p. 261) discusses biometric authentication methods based on handwritten signatures, face recognition, hand geometry and DNA typing. Name the areas of application of each biometric authentication approach.</li> <li data-bbox="686 942 1425 1131">5. Smartcard Security, Three Grades of Toast: "Today's microprocessor-based smart card is more like a toaster, permanently programmed to provide three grades of toast, than like a computer, capable of accepting many applications from various sources while addressing multiple services." Is this limitation caused by political, technological, or security considerations? Identify and list global standards entities that are working to address the "toaster" limitation of smartcards.</li> </ol>

#### **Appendix D. Example Group Field Interview and Graduate Term Paper Topics**

##### **Example Field Interview Topics:**

1. Identity Theft: Prevention and Detection Safeguards at a Credit Card Processor
2. Security and Privacy of Corporate eMail: A Case Study.
3. Wireless and Remote Access Security: One Company's Perspective.
4. Choosing the Best Firewall: One Manager's Decision.
5. Security, Privacy, and the Law: An Attorney's Perspective.
6. Trust and Security of Online Transactions: The Importance of Certificate Brands.
7. An Example Password Security Scheme Implementation at a Small Company.
8. Outsourcing and Security: How My Company Contracted for Data Security

##### **Example Graduate Term Paper Topics:**

1. Security and Confidentiality of Online Sales Orders: An eTailer's Approach
2. Smart Wireless Inventory Tags: Security Capabilities and Limitations
3. Identity and Access Management: Practical Solutions
4. Sarbanes-Oxley: What It Means, and Why You Should Care
5. The Risks and Rewards of Instant Messaging in the Banking Sector
6. How Credit Card Transactions Are Kept Confidential and Secure: One eTailer's Policies and Procedures
7. Security Skills and HIPAA: Employer Expectations in the Medical Industry
8. The Ten Biggest Internet Security Vulnerabilities and What To Do About Them

#### **Appendix E. Sample Student Comments from the Exit Survey**

1. The importance of personal attention and timely feedback:
  - "The instructor was very helpful whenever I had any questions or doubts."
  - "Individual contact with the student."
  - "Very personable instructor."
  - "Instructor provided fast and detailed feedback on questions and assignments."
  - "I appreciated the contact had with me. The other class I took this semester was not as personal and with online courses, it is a very good thing to have regular contact with your instructors."
2. The level of detail and planning of the course structure:
  - "Instructor provided a well-organized and interesting class."
  - "I like the idea of having a set schedule, but still being able to pace myself in reading the material."
3. Discussion board, hands-on mini-projects, and field projects:
  - "The class discussions helped me learn, because they made me go over the material several times."
  - "I liked the hands-on assignments, course structure, and organization."
  - "The discussion board questions allowed me the opportunity to think in real world scenarios instead of just classroom use."
  - "The Field Term Project gave me an opportunity to meet people and learn things that I wouldn't have otherwise."

Material published as part of this journal, either on-line or in print, is copyrighted by the Organizational Systems Research Association. Permission to make digital or paper copy of part or all of these works for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage AND that copies 1) bear this notice in full and 2) give the full citation. It is permissible to abstract these works so long as credit is given. To copy in all other cases or to republish or to post on a server or to redistribute to lists requires specific permission and payment of a fee. Contact Donna Everett, [d.everett@moreheadstate.edu](mailto:d.everett@moreheadstate.edu) to request redistribution permission.