Security in Computer Literacy- A Model for Design, Dissemination, and Assessment

Claude F. Turner
Department of Computer Science
Bowie State University
(301) 860-3965
cturner@bowiestate.edu

Blair Taylor
Department of Computer and Information Sciences
Towson University
(410) 704-4560
btaylor@towson.edu

Siddharth Kaza
Department of Computer and Information Sciences
Towson University
(410) 704-6310
skaza@towson.edu

ABSTRACT
While many colleges offer specialized security courses and tracks for students in computing majors, there are few offerings in information security for the non-computing majors. Information security is becoming increasingly critical in many fields, yet most computer literacy courses insufficiently address the security challenges faced by our graduates. This paper discusses the development and impact of a set of modules designed to integrate security into computer literacy across two universities and several community colleges in the state of Maryland. Results from our comparative analyses based on pre- and post- test analysis show significant improvements in post-test results.

Categories and Subject Descriptors
K3.2 [**Computers and Education**]: Computer and Information Science Education - *computer science education, curriculum, information systems education.*

General Terms: Security

Keywords: Security Education, Computer Science Curriculum, Information Security Curriculum Development.

1. INTRODUCTION
Computer literacy is offered as a required course by a variety of universities and colleges, where it aims to provide students with current knowledge and understanding of computers and their uses. For many college instructors, the computer literacy course is the bane of their teaching load – often the first course they teach and the first course they drop from their schedule. The disadvantages of teaching this course include: a new textbook every few years; lecture notes that quickly become obsolete; a variable, often ill-defined list of topics [4]; and large classes full of non-majors looking for an easy 'A'. Additionally, the class seems to afford few research or publishing opportunities; since 2000, less than a dozen papers have been written on computer literacy [4].

SIGCSE'11, March 9–12, 2011, Dallas, Texas, USA.

Epperson [4] provides an excellent history of computer literacy, starting with the coinage of the term in 1972, as well as its future direction. Shelly [11] informs us that the requirements that determine computer literacy evolve as technology changes. In recent years, to help people adapt to these rapid changes, become effective users quickly, and prepare for lifelong learning, there has begun a reexamination of the general structure of computer literacy. A National Research Council (NRC) report titled, *Being Fluent with Information Technology* [10], has proposed a variety of recommendations, including a new term that would replace computer literacy—*fluency with information technology* (FIT)—or as put more succinctly by Snyder, *fluency* [13]. FIT is described as "a package of skills, concepts, and capabilities wrapped into a project-oriented learning approach that ensures that the content is fully integrated" [13]. Other authors including Bartholomew [2], Hoffman & Blake [6] and Sloan & Halaris [12] have discussed this subject and have provided their recommendations on providing a breadth of IT knowledge to non-computing majors.

We believe that in addition to other important topics, non-computing majors need to be exposed to security topics. Information security has become increasingly critical to many other fields, business and health for example, and college graduates from all majors will encounter information security issues in their personal and professional lives. Even so, many books on literacy and fluency often have only a chapter or section on security, and lack the active learning component that would help students internalize the concepts.

To address this issue, we added the computer literacy course to the Security Injections project [8,14,18,19] currently underway at Towson University, Bowie State University, and several other community colleges in Maryland. The objective of the project is to integrate security throughout computing curricula using a minimally invasive thread based approach [14,18,19]. The project began with a focus on the core computer science classes, but the addition of the computer literacy course had many unforeseen advantages. With apologies to Dr. Seuss, "Maybe the Computer Literacy class...perhaps...means a little bit more!" Consider the following, which holds true at many institutions, including Towson and Bowie State University:

- The computer literacy class reaches more students than any other class in our department.
- The computer literacy class reaches students in computing majors, non-computing majors and students who have not yet decided on a major.

- The computer literacy class includes more female and minority students than any other class in our department.
- The computer literacy class allows some flexibility to add interesting and relevant topics.

This work reports on our efforts to integrate security into the computer literacy [1,3,7] course using modules that encourage active learning. We have developed, deployed, and assessed a set of three modules (called security injections) for computer literacy based on the general structure proposed by Taylor et al. [18]. The modules cover the topics of phishing, passwords and cryptography and are designed to provide students with the experiential learning in computer security. In this paper, we present and discuss the collaborative process involving two and four year institutions to design, disseminate, and assess the modules. We describe the general structure of the modules and provide a specific example. We also report on our experience in deploying modules and our assessment results.

2. PROJECT OVERVIEW

2.1 Security across the Curriculum

In fall 2006, we initiated a plan to integrate security throughout the computing curriculum. The goal was to complement our security track and introduce security principles to computing majors early and often. Early efforts targeted select sections of the core computing required courses, CS0 and CS1 [18]. Using a common set of learning objectives to link the materials across the classes, we created a set of security related laboratory modules that focused on the major secure coding issues of integer overflow, buffer overflow, and input validation. In 2008, the project expanded to include five additional courses: CS2, Computer Literacy, Database, Web Programming, and Networking; and to encompass five institutions: Towson, Bowie State, and three partnering community colleges: Anne Arundel Community College, the Community Colleges of Baltimore County, and Harford Community College.

2.2 The Model

Our collaborative approach to implementing curriculum change across varying institutions is based on a model with a set of well-defined goals and repeats a process of: develop materials, pilot across institutions, evaluate, revise, and disseminate [15]. Formal evaluation includes materials review from a technical expert in security, qualitative and quantitative feedback from experienced teachers at our partnering institutions, results from ongoing pilot programs, and quantitative results from security surveys and code checks. This model and assessment results for CS0, CS1, CS2 have been reported in previous publications [8,15,16].

2.3 Security Modules

Security modules were created with the objectives of *maximizing the learning experience* and *minimizing the burden on the instructor*. To increase the effectiveness of the module, we designed it with active learning in mind [9]. The "active" components include security related exercises and a security checklist, described below. Additionally, we formalized the module structure to promote critical thinking and reflection [17]. In contrast to the traditional computer laboratory exercise which is a loosely structured set of problems or exercises that inadequately address synthetic and analytical thinking [17, 18], the security lab modules in this project are patterned after the structured labs in physics and biology. Each module contains the following components:

- **Background** - The module begins with background information, including a concise description of the topic, the risk involved, and real-life examples that include links to articles describing actual occurrences of security vulnerabilities. The purpose of this section is to set the stage for the active learning process that follows.
- **Laboratory Assignments** – There are several hands-on lab exercises related to the specific security concept. Hands-on exercises that present meaningful concepts in an engaging manner increase motivation and enhance learning. Research shows that in a "learning by doing" environment, students learn more, retain the information longer, can apply learned material in more contexts, and the environment of the classroom is more enjoyable [9].
- **Security Checklists**. A key component to each module is the security checklist. A security checklist is a well-defined set of procedures for identifying potential security concerns. Checklists have many relevant applications, including aviation, software assurance, and have recently been shown to reduce errors in emergency rooms [5]. A well-developed checklist can reduce human error, serve as a reminder list, and help ensure consistency and completeness. Additionally, checklists can reinforce security principles and help students quantify and internalize important security principles. The checklists in our modules, initially designed to find potential vulnerabilities in software, proved to be readily adaptable for passwords, phishing, and cryptography.
- **Discussion questions** require students to reflect upon the process, the results, and the security implications of the new concept.

Minimally invasive. Finally, each module was designed towards ease of use by the instructor. Using feedback from faculty and students, each module has been streamlined and formatted to allow simple insertion within a lab or for stand-alone use. Estimated completion time for most modules is 20-30 minutes. We encourage instructors to use or adapt the modules to accommodate instructional needs. We also recommend that instructors allow students to work in pairs to encourage collaborative learning. The intention of each lab is that it can be completed without class instruction and with minimal help from the instructor.

3. Computer Literacy Modules

3.1 Module Design

Developing security modules for computer literacy is a challenging activity. Many of the students are freshmen and often lack the necessary prerequisites to understand computer security principles. In our case, this is further compounded by the fact that our modules are targeted to different communities of students, ranging from community colleges, minority serving institutions, to comprehensive universities. To address these

challenges, we designed the modules to be self-contained and targeted to a freshman audience. We also hold workshops at participating institutions to help train and prepare faculty who teach using the modules.

The topics for the modules were determined through discussions in workshops attended by faculty from all partner institutions. We found the computer literacy instructors, some of whom are graduate students and adjunct instructors, to be very receptive to our approach and full of ideas for future modules. We sought to identify essential issues in information security that were topical and cut across various communities of students. Although a variety of important topics were considered, phishing, passwords and cryptography emerged at the top of the list. A module that encompassed the basic definition of security—illustrating the challenge and significance of meeting the triangular concepts of confidentiality, integrity and availability (CIA), as well as the concept of risk analysis—was also deemed very important.

3.2 Using the Security Injection Modules in your Classroom

Currently, our project includes the following three modules for Computer Literacy: (1) Passwords, (2) Phishing, and (3) Cryptography. Modules are located at: http://triton.towson.edu/~cssecinj. A compressed form of the Phishing module is shown in Table 1. These modules are currently being used at Bowie State University, Towson University, Anne Arundel Community College, Community College of Baltimore County, and Harford Community College. The procedure for using the modules, described in the 'Faculty Access' section of the website is as follows:

1. Administer Security Survey
2. Introduce Security Injections in Class
3. Administer Security Survey after introducing Security Injections
4. Complete Faculty Survey.

4. ASSESSMENT DESIGN AND RESULTS

The primary goals for this project are: increasing students' general security awareness, improving students' knowledge on the content of specific security modules, increasing faculty security awareness, and increasing the number of security-skilled students. Each of these objectives is assessed using various instruments including surveys, qualitative inputs from faculty, and institutional data. In this paper, we present the student survey design and results on student awareness and learning from the use of modules in the computer literacy courses.

4.1 Pre and Post Surveys

Each class that used our modules was given a pre-survey at the beginning of the class and a post-survey at the end of the class. An independent evaluator has reviewed all assessment materials, including pre-surveys and post-surveys. The student surveys contain demographic questions (including questions on the interest in security), and two sets of multiple choice questions – one section targets general security awareness and the other focuses on specific knowledge gained through the modules (a list of sample questions is shown in Table 2). We used parts of this survey in CS0, CS1, and CS2 previously and it was well accepted by students [8].

Table 2. Sample survey questions

General Security Awareness
What are the possible consequences of insufficient computer security?
A set of related programs, usually located at a network gateway server, that protects the resources of a private network from other networks, is known as a …
Module specific
Who is it safe to tell your password to?
Phishing is …
The following are characteristics of suspicious email:
Encryption is a special technique employed only by agencies with highly sensitive data such as the FBI or CIA.
Consider the following email: (followed by an phishing email that the students had to identify)
Using letters from a memorable phrase is a recommended way to construct a password.(T or F)
Never give out personal information upon an email request (T or F)
Encrypting your personal files requires purchasing special software. (T or F)
The conversion of data into a ciphertext that cannot be easily understood by unauthorized people is known as …

Based on the pre and post survey, a set of two hypotheses were proposed to test student learning.

H1: The post-survey scores will be significantly higher than pre-survey scores.

H2: The post-survey scores in specific module topics will be significantly higher than pre-survey scores.

4.2 Basic Statistics and Demographics

A total of 384 survey responses from four institutions were received with 357 responses from sections that used the modules. After data cleaning, 300 valid survey responses were analyzed. Figure 1 presents the demographics of students who took the survey.

As can be seen, the classes had a fairly even distribution between gender and ethnicity. The classes also had a majority of freshman as was expected in a literacy course. Also as expected, the classes showed a skewed distribution among majors. A large majority of students were non-computing majors – this provides us with an opportunity to spread security concepts among students in other disciplines who are not exposed to security issues that they are almost certain to face in their professional and personal lives. In addition, the even spread in gender and ethnicity offers an excellent platform to introduce exciting computer science concepts and attract women and URMs to the field.

Table 1. An abbreviated version of the Phishing module (see complete module at http://triton.towson.edu/~cssecinj)

Phishing – "A scam to steal private information"

Summary - Phishing is a type of social engineering technique in which an attacker sends an e-mail or displays a Web announcement that falsely claims to be from a legitimate organization. The intention of the messenger is to trick the user into surrendering private information.

Description - A more specific definition is offered by the Anti-phishing Working Group (APWG): "Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials." The victim in a phishing attack is asked to respond to an e-mail or is directed to a Web site to update personal information, such as passwords, credit card numbers, Social Security numbers, bank account numbers, or other information for which the legitimate organization already has a record. However, the site is actually a fraudulent Web site designed to steal the user's information.

Risk - Phishing can and usually leads to online identity theft. By capturing a user's personal information, an attacker can gain access to the user's account on a legitimate Web site, and can engage in a number of activities resulting in substantial financial loss to the user, denial of access to e-mail, and other problems.

Example of occurrence - On the weekend of January 3, 2009, several users on the social network Web site, Twitter, became victims of a phishing attack. The users were deceived into giving away their passwords when they received an e-mail similar to one that they would receive from Twitter with a link that read, "hey, check out this funny blog about you…". The link redirects to a site masquerading as the real Twitter site. Any personal information entered by the user on the fake site is then captured by the attacker.

Anti-Phishing Training - Training users to identify a 'phish' is an important component in the fight against phishing. Training has taken two forms: the first is simply to provide anti-phishing information to users through e-mail and other media. The second is to give firsthand experience to users through games, simulated phish, cartoons, etc. Recent studies seem to indicate that the latter—giving firsthand experience to users—might be more effective. The game, Anti-Phishing Phil http://wombatsecurity.com/antiphishingphil, which teaches people how to identify suspicious Web site addresses while providing the experience of being captured by a phisher, is such an example. PhishGuru in the previous section is another example. It delivers cartoon-based, anti-phishing information after a user has been deceived by simulated phishing messages.

Anti-Phishing Technologies - Although user ability to identify phish is an important component in the battle against phishing, combining it with technology yields better results. One of the techniques used to automatically identify phish is **filtering**. The objective of filtering is to identify (or flag) phishing attempts in e-mail or on Web pages. Filters are usually integrated into browsers or e-mail software. When a Web address is encountered the software compares it with a so-called "blacklist" of known phishing Web sites. It then takes appropriate actions, which usually include informing the user. The blacklist is updated periodically (for example, every 30 minutes) as new phishing sites become available. As with any blacklist, there is also a "whitelist" of known legitimate sites.

Lab questions - Consider the PayPal e-mail in the figure (an email is provided to the students, please see website for the complete module) . The Web address in the box, http//211.248.156/Paypal/cgi-bin/webscrcmd_login.php, appears when the user mouse-over the "Click here to verify your account" link.

1. Complete the following checklist for this e-mail.

2. List any sentence, phrase or word that makes the e-mail a suspected phish.

Security Checklist	
Vulnerability: Phishing **Course:** Computer Literacy	
Task – Read the e-mail carefully; answer yes/no in the space provided	**Yes/No**
1. Were there suspicious words, phrases or sentences	
2. Were there suspicious links?	
3. Are there grammatical or spelling errors in the e-mail?	
4. Does the e-mail start with a generic greeting?	
5. Does the e-mail contain any pop-up boxes or attachments?	
6. Does the e-mail contain an air of urgency or a need to respond immediately?	
7. Does the email ask you for personal information such as passwords and social security number?	
If you answered yes to any of the above questions, then the e-mail is a suspected phishing mail.	

Discussion questions

1. Play at least two games of Anti-Phishing Phil at http://wombatsecurity.com/antiphishingphil. Create a "blacklist" of the phishing Web site addresses you encountered, and a "whitelist" of the legitimate Web sites. (Hint: see the section on Anti-phishing Technologies.) Describe how the Anti-Phising Phil experience has helped you to better recognize phishing Web sites. What are your likes and dislikes about the game? Are there any suggestion(s) that you would like to provide so as to improve it? If so, explain.

2. Take the "SonicWall Phishing and Spam IQ Test" a couple of times (http://www.sonicwall.com/phishing/). What was your maximum score? Look at the test result sheet, and give the name that appears in the "Subject" column for three of the questions. For each of the subjects, click on the "Why?" link that appears under the "Explain Answer Column." The e-mail you viewed for that question should re-appear—this time with explanations. Copy one of the given explanations for each of the e-mails.

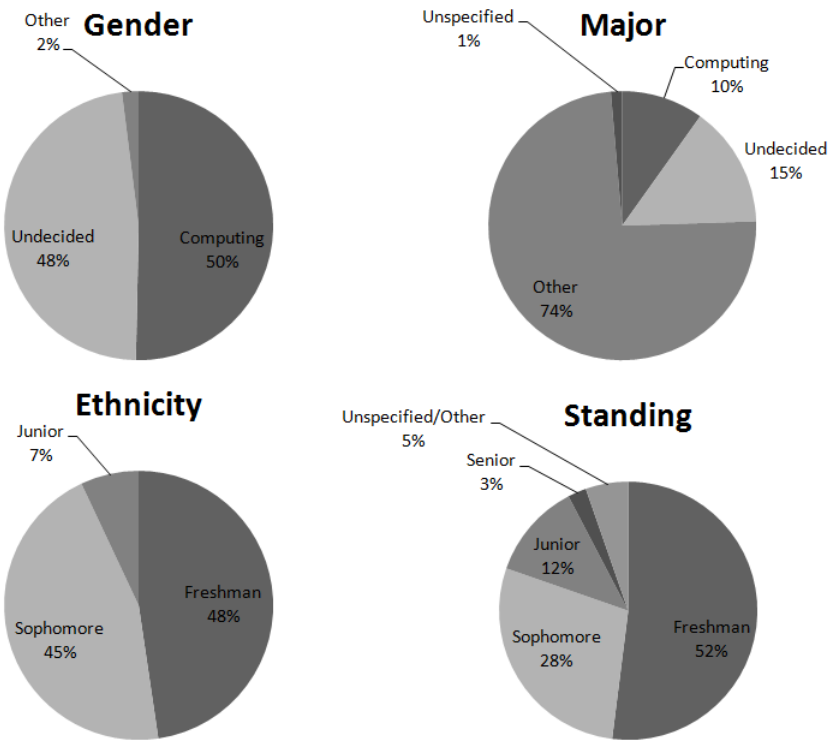

Figure 1. Demographics of survey respondents

4.3 Survey Results

This assessment involved class sections in five institutions and we found that it was difficult to get a similar response rate for both the pre-surveys and the post-surveys. There were 300 survey responses with 86 in the pre-survey and 214 in the post-survey. In line with our Institutional Review Board requirements, the survey did not contain any information that could identify the student or pair the responses between the pre and post tests. Each question in the survey was a multiple choice question with three or more options (the T/F questions had a unsure option) and one correct option. The score of each survey was calculated by counting the number of correct answers from a total of 14 questions (including general security and module specific questions). We picked the Mann-Whitney non-parametric test to compare the mean rank of the scores in the two groups (pre and post). This was done because of two primary reasons – 1) the n for the groups is different and 2) the Kolmogorov-Smirnov and Shapiro-Wilk test showed that the scores were not normally distributed. Figure 2 summarizes the results. The average score obtained in the pre-surveys was 9.09 and the average score in the post-surveys was 10.67. It was found that this was a statistically significant increase ($p < 0.001$) . These results look promising and support H1.

For individual modules, it was found that there was a statistically significant increase ($p < 0.001$) in the scores obtained in the questions targeted at each of the modules with a 34.71% increase in knowledge related to the phishing module, 25.82% increase in the cryptography module, and 9.14% increase in the password module. This supports H2.

Deeper analysis on the data showed that the significant increase in overall scores persisted across gender and ethnicity. Additionally, we found that women started significantly lower than men, yet, caught up in the post-test; and at the end of the semester there was no significant difference in their scores. Further analysis of this data is in progress.

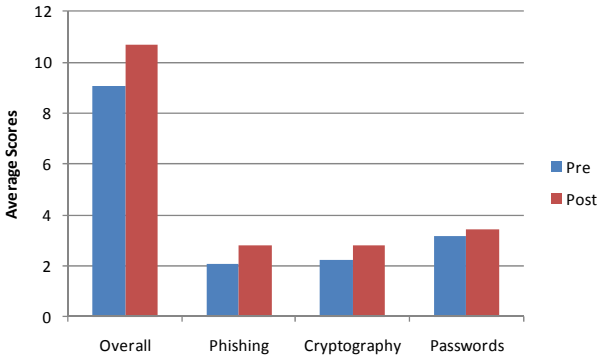

Figure 2. Survey results for pre and post surveys

5. Conclusion

Many colleges offer specialized security courses and tracks for students in computing majors since computer security is recognized as an essential topic for computer scientists. For the non-computing majors, there are few offerings in information security. Increasingly, information security is becoming critical in many fields and the current computer literacy courses insufficiently address the security challenges faced by our

graduates. This paper discussed the development and impact of a set of modules designed to integrate security into computer literacy across two universities and several community colleges in the state of Maryland. Results from our comparative analyses based on pre and post test results showed statistically significant improvements in the post-tests. Overall scores improved 17.37%; phishing module related scores increased 34.71%; cryptography related scores increased 25.82%, and password related scores increased 9.14%. Also of interest, females, who scored lower on the pre-tests, caught up with males on the post-tests.

6. ACKNOWLEDGMENTS

This project is partially supported by the NSF Course Curriculum and Laboratory Improvement (CLLI) grant number DUE-0817267. We greatly appreciate our colleagues and partners at Bowie State University, Harford County Community College, Community College of Baltimore County, and Anne Arundel Community College. In particular, we are grateful to Harry Hochheiser, Mike O'Leary, Shiva Azadegan, AC Chaplin, Patricia Gregory, Jack McLaughlin for their contributions.

7. REFERENCES

[1] Bacon, T. and Tikekar, R. Experiences with developing a computer security information assurance curriculum. *Journal of Computing Sciences in Colleges 18*, 4 (2003), 254 - 267.

[2] Bartholomew, K.W. Computer literacy: is the emperor still exposed after all these years? *Journal of Computing Sciences in Colleges 20*, 1 (2004), 323.

[3] Bogolea, B. and Wijekumar, K. Information security curriculum creation: a case study. *Information Security Curriculum Development*, ACM (2004), 59-65.

[4] Epperson, A. Computer literacy revisited: a comprehensive investigation of computer literacy. *ACM Inroads 1*, 2 (2010), 30-33.

[5] Gawande, A. *The checklist manifesto: how to get things right*. Metropolitan Books, 2009.

[6] Hoffman, M., Blake, J., McKeon, J., Leone, S., and Schorr, M. A critical computer literacy course. *Journal of Computing Sciences in Colleges 20*, 5 (2005), 163.

[7] Irvine, C. and Chin, S. Integrating security into the curriculum. *IEEE Computer 31*, 12 (1998), 25-30.

[8] Kaza, S., Taylor, B., Hochheiser, H., Azadegan, S., O□Leary, M., and Turner, C.F. Injecting Security in the Curriculum – Experiences in Effective Dissemination and Assessment Design. *The Colloquium for Information Systems Security Education (CISSE)*, (2010).

[9] McConnell, J. Active Learning and its use in computer science. *Proceeds of the 1st conference on Integrating Technology into computer science education*, (1996), 52-54.

[10] Multiple. Being Fluent with Information Technology. 1999, 128. http://www.amazon.com/Fluent-Information-Technology-Committee-Literacy/dp/030906399X.

[11] Shelly, G.B. *Computer Concepts - Discovering Computers: Living in a Digital World, Fundamentals*. Course Technology, 2010.

[12] Sloan, L. and Halaris, A. Towards a definition of computing literacy for the liberal arts environment. *Technical Symposium on Computer Science Education*, (1985), 320.

[13] Snyder, L. *Fluency with Information Technology: Skills, Concepts, and Capabilities*. Pearson, 2011.

[14] Taylor, B., Hochheiser, H., Azadegan, S., and O'Leary, M. Cross-site Security Integration: Preliminary Experiences across Curricula. *13th Colloquium for Information Systems Security Education (CISSE)*, (2009), 158-165.

[15] Taylor, B., Hochheiser, H., Azadegan, S., and O'Leary, M. Cross-site Security Integration: Preliminary Experiences across Curricula. *13th Colloquium for Information Systems Security Education (CISSE)*, (2009), 158-165.

[16] Taylor, B. and Azadegan, S. Using Security Checklists and Scorecards in CS Curriculum. *National Colloquium for Information Systems Security Education*, (2007), 4-9.

[17] Taylor, B. and Azadegan, S. Teaching Security through Active Learning. *Proceedings of Frontiers in Education: Computer Science and Engineering, Las Vegas*, (2007).

[18] Taylor, B. and Azadegan, S. Moving beyond security tracks: integrating security in CS0 and CS1. *SIG Computer Science Education (SIGCSE)*, ACM (2008).

[19] Turner, C., Hochheiser, H., Feng, J., Taylor, B., and Lazar, J. Cooperative Information Assurance Capacity Building. *13th Colloquium for Information Systems Security Education (CISSE)*, (2009), 44-50.