Different Approaches in the Teaching of Information Systems Security

William Yurcik
David Doss
Department of Applied Computer Science
Illinois State University
Normal, IL, 61790, USA

Abstract

We describe innovative new approaches to teaching information systems security that may be used individually or in combination. Information system security is a difficult course to teach and these approaches provide resources to both novice and experienced educators to enhance their courses. We conclude that more educational development work needs to done to uniformly improve information systems security education to counterbalance pressures for technical training over fundamental concepts and this paper provides a start by synthesizing the current state-of-the-art.

Keywords: Information security, security education

Much has been reported about the urgent need for more information systems security professionals. In (Bishop 1999), Matt Bishop contrasts the views of the major players:

- Universities need educators who can communicate underlying theory to students in order to have them apply design principles to security mechanisms.
- Industry, driven by fiduciary duty to stockholders, needs immediate help in protecting investments in people, equipment, and most importantly information assets.
- Government needs professionals to design tools to protect national economic and defense infrastructures from existing and conjectured cyberterrorists as documented in (Yurcik 2000).
- General public awareness – Is the public aware a problem exists? (Bishop 2000)

These different viewpoints are all valid.

This situation has created pressure on the system that has filtered down to students. One effect is the hiring of students before academia is "done with them" (Osterman 1998). Undergraduate students are being hired before finishing their degrees, graduate students are lured away from Ph.D. studies, and universities are scrambling to hire new faculty. Perhaps worst of all is the pressure on university education to skip some of the *less useful* theory to focus on the latest trends in web programming, certification or Microsoft applications. This just makes a non-tenable situation worse, and this combination of pressures together will have significant ramifications if left unchecked.

To counterbalance these pressures, the we feel obligated to propose information systems security pedagogy ideas for the long term while there is still time for a correction. There has been little previous work about *best practices* or different approaches to teaching information system security.

Of course, an information system security course is not the only course that poses difficulties to educators, but we posit that information systems security is unique because of the wide range of domains involved: computer architecture, criminology/law, cryptography, database, human-computer interaction, information retrieval, information theory, management/business, mathematics, military science, mobile computing, networks, operating systems, philosophy/ethics, programming languages, software engineering, statistics/probability, and web programming (Spafford 1998). It has been reported as not uncommon for an instructor to take ten or more hours to prepare a two-hour security lecture. This is a function of not only the sheer amount of diverse information but also the dynamic nature of the rapidly moving field. Several instructors even report significant security events (newspaper headlines) occurring during their courses, which presents both a positive relevance to students but may also be a challenge to the instructor if not previously covered in the course (in which case the instructor and class learn together) (Irvine 1997).

This paper synthesizes recent disparate ideas on teaching information system security. The remainder of this paper is organized as follows: Section 2 reviews the literature on previous work in computer security education. Section 3 highlights the new and exciting approaches to information systems security education that have recently been documented. We close with a summary and future directions in Section 4.

1. PREVIOUS WORK

To the authors' knowledge, (Neugent 1982; Highland1982) are the first papers on information systems education. These papers, along with slightly more recent papers (Higgins 1989; Spillman 1991; Arsenault & White 1991), start by justifying the need for such a course in the overall undergraduate curriculum and then go on to describe course specifics, including instructional materials, such as textbooks, rationale for topic selection, individual lectures, and course flow over a semester for coherence. While the field has drastically changed from this timeframe, this initial work laid the groundwork for later efforts.

The undergraduate courses proposed up to this point were survey courses that provided orientation but not the technical depth needed for professional specialization. Most of the information system security courses needed by professionals are more appropriate at the graduate level after prerequisite instruction in core computer science concepts. The underlying problem is that universities are producing software engineers that do not design with security as an integral part of the process, instead relying on post-release patches and retrofitting when necessary (Bishop 2000).

At a higher level than individual course descriptions, a consensus, starting with Cook (1985) and later with Irvine (1997) and Irvine, Chin, and Frincke (1998), began to emerge that information system security should not be limited to one- or two-elective undergraduate courses, but rather should be integrated into the entire curriculum. In fact, Bishop states, "Computer Security is not merely a technical subject, but requires a broad knowledge of the practice of engineering and organization, psychology, history, philosophy/ethics, and other humanistic fields."[1] Ideally textbooks, course materials, and hands-on laboratory exercises should have information security integrated into appropriate topics across the curriculum rather than being treated separately but this does not yet exist (Irvine, Chin, & Frincke).

2. DIFFERENT APPROACHES

The different approaches we document here have been identified from two primary sources: (1) Aviel Rubin's list of cryptography and security courses[2] and (2) Heather Hinton's Listing of Computer and Information Security Educational Activities.[3] The goal is to describe each approach in enough detail such that strengths and weaknesses are apparent. We start with approaches common to most computer science/information system courses but quickly progress to approaches unique only to an information system security course.

Traditional Lecture Approach

The traditional lecture (passive) approach dominates the current teaching of information system security. There has been open debate about the content and level of topics in information system security courses - we found that there are three basic types: (1) a survey breadth course; (2) a cryptography course focused on mathematical foundations; and (3) a systems course translating theory into real systems (Bishop 1993). Emphasis on fundamental concepts allows higher-level courses to be more robust to security technology advances, as well as providing general skills that can be later applied to specific practical systems (Amoroso 1993).

The major challenge with teaching an information system security survey course is selecting topics from among many important and interesting possibilities. While we will not attempt to define a consensus topic list in this paper, we can comment on some common educational characteristics. We only comment on feedback received in introductory survey courses here.

First, there is no such thing as too many cryptography examples. Students learn this material with different learning styles, and examples allow students to adjust as well as learn at their own pace (repeating the examples covered in class).

Second, many instructors find that undergraduates learn best with a hands-on approach with examples (virus programs) to engage students and then generalize to theory. Instructors report that students are attracted to analyzing programs for problems but are not keen on theoretical topics. Also at this level, informal explanations dominate over formal mathematical proofs and examples of computer applications security are

[1] <http://www.cs.ucdavis.edu/~bishop/scriv/1999-ncisse/tsld004.htm>

[2] <http://avirubin.com/courses.html>

[3] before Heather Hinton moved to from Ryerson University to Tivoli Systems, this list was previously maintained at this URL <http://www.ee.ryerson.ca:8080/~hhinton/compsec/security>

especially well received. Students learn best when having fun, so breaking ciphers in class and assigning crypto puzzles (with hints) have also been reported with good feedback.

Lastly, an unexpected finding is that the use of real-life examples of cryptography in history via case studies has received positive feedback, especially if integrated tightly with the course. The historical examples are often intuitive, and the insights they provide transcend to more sophisticated systems (Rubin 1997). Many examples can be identified from military history or espionage that have been documented on television (such as the History Channel), popular books, and movies. Two of the most popular examples are from World War II: (1) the Nazi enigma machine and how the U.K. efforts at Bletchley Park revealed its secrets and (2) how the U.S. revealed the Japanese Purple code at the Battle of Midway Island. Of course, history is filled with many examples of the use of encryption all the way back to ancient times, and it is up to the instructor to find the appropriate example for the current concepts being conveyed in the class.

One criticism of the traditional lecture approach is that students may become too passive and not actively attempt to internalize difficult material. Another criticism is that ideas about intelligent malicious attacks (thinking *outside of the box*) are not included, instead focusing more on providing protection against brute force attacks at obvious attack points.

Scribe Approach

Many of the courses using the traditional approach provide active learning by assigning student scribes responsible for taking careful notes during lectures and subsequently producing a web-accessible presentation of the lecture for fellow students and the instructor. Some of these web-accessible presentations have taken the form of board graphics and classroom videotapes. Examples can be found for a course by Aviel Rubin.[4] The web-accessible presentations are graded and of varying quality, but the feedback to the instructor and students have proven very useful. This technique has also been extended to information system security conferences and current events (Steinberg 1991). This has also helped to turn instructor lectures into future textbooks (Amoroso 1993; Rubin 1997).

Expert/Mentor Approach

Depending on the situation (availability and location), educational experiences can be enhanced by having multiple experts instruct on their individual specialties. For instance, the Information Warfare course taught by Lance Hoffman at George Washington University utilizes a dozen outside speakers who happen to be national experts in their respective areas (Hoffman et al. 1999).

Tutorial Approach

This approach consists of self-learning utilizing the increasing number of computer self-study texts on various topics including security. The goal of these texts is primarily certification in different specialties. The certified information systems security professional (CISSP) is the most respected in the field of computer/network security and many resources related to the test are available online.[5] Tutorial essays on most security topics can be found on the World-wide Web by using a search engine. Obtaining original information from leading experts is often worth the hassle and delay factor compared to misinformation from potentially untrusted sources.

Project Approach

Most traditional courses include a project component, whether it is a term paper, experimental project, or some form of topic presentation. Good instructors require hands-on projects—students must understand principles enough to apply them, but this is not always an option based on resources. Examples of projects from Bishop (1993) include:

- securing a web server
- analyzing a virus
- comparing Windows NT and Unix security
- penetration analysis of a particular system
- improving security of a specific organization

As one unique example, Mitchener and Vahdat (2001) document a *chat room* project that represents some of the ideal characteristics for such an activity: it is small but can grow incrementally, it is basic but can grow in complexity, it is analogous to practical business or military applications, it engages students with interactivity and entertainment value, and there is room for creativity in the interfaces, architecture, and protocols (Mitchener & Vahdat 2001). This activity requires a prerequisite networking background that provides the necessary skills to explore security in depth, specifically basic network client/server programming and security protocols (Kerberos, PGP, SSL, secure multicast, and public key infrastructure). The *chat room* has been assigned in two ways: (1) working source code is distributed for students to reverse engineer and describe their operation or to modify and implement their own protocols; and (2) the software engineering design of the *chat room* is assigned for students to implement either alone or in groups. The National Science Foundation supported this project and the code is available.[6]

Lindskog et al. (1999) assigned a project to construct a system that could be used to automatically detect attacks against a file transfer (FTP) server. For evaluation of the system they had designed, students were given a large file containing recorded network data representing

[4] <http://www.cs.nyu.edu/rubin/course/>

[5] <https://www.isc2.org/cissp_studyguide.html>

[6] <http://www.cs.duke.edu/~vahdat>

actual FTP transactions and intrusions and the students had to identify the intrusions.

One criticism of course projects is that some students may not have the background to intelligently select an appropriate topic, instead choosing too easy or too difficult material. One option is for the instructor to prepare an approved list of acceptable projects to eliminate confusion and fear early in the semester. Rubin reports that although some of his student projects have been failures, others have lead to Ph.D. theses and jobs with employers eager to follow through with a student project (Rubin 1997).

Research/Teaching Synergy Approach

The authors believe it is extremely important for students to remain attuned to information system security research so that they will be able to incorporate the latest techniques into their future products and processes. While it is the goal of most university-level educational programs to benefit from the synergy of research and teaching, in the area of information systems education this is difficult due to the level of complexity in specialized security research. Lindskog et al. (1999) document a course that incorporates both research and education on three different types of laboratory research projects: intrusion experiments, intrusion analysis and remediation, and intrusion detection. Via empirical surveys, it was found that students were motivated by this research connection in addition to producing unique research data. Specifically, students role played as attackers and defenders and research measurements were made on the effort used to break into systems and the reward or motivating force behind successful intrusions. This research was eventually published.[7] Students discovered it was not as difficult as they thought to break into UNIX systems and the experience raised their awareness of security problems (Lindskog et al. 1999).

Attack/Defend Isolated Laboratory Approach

In the attack/defend approach, students are divided into offensive teams and defensive teams with the goal of the offensive teams to compromise machines managed and monitored by the defensive teams. The offensive teams are allowed to utilize any attack within a defined set of rules specific to the local environment. The goal of the defensive team is to make target machines secure to intrusion while constantly looking to detect and trace any unauthorized intrusions.

Texas A&M University has been teaching a graduate class in Computer Security using the attack/defend approach since 1995 (Hill et al. 2001). The defensive team has never been successful in preventing penetration teams from compromising one or more of the target machines. Attacks have ranged from social engineering to protocol vulnerabilities, well-known established attacks to creative new attacks, from coordinated group attacks to isolated individual attacks.

This class utilizes an isolated network security laboratory (isonet) to provide a safe active learning environment separated from campus and departmental networks such that no attacks can be launched into or out from the laboratory and no sensitive data or vulnerability information is inadvertently released (Bishop & Heberlein 1996). The network security laboratory is isolated by a combination of safeguards: (1) all components of the laboratory connect to a single router; (2) the router's gateway is through a proxy firewall server. Students can access the laboratory remotely only by logging into the firewall. There is a problem with this approach in that significant resources are required to build and maintain an isolated network security laboratory with a mix of operating systems at different levels of security.

Essentially, this isonet is a playground without concern for negative consequences.[8] Machines may be rebooted, operating systems re-installed, and malicious code tested. Most important of all, students on isonet do not attack passive static systems. Instead, isonet provides a dynamic environment where fellow students actively defend systems.

Chalmers University of Technology also has been teaching a series of courses using the same attack/defend paradigm. As described in Lindskog et al. (1999), the classes are divided into attackers, experimental coordinators, and system administrators (defenders). Target systems included Unix with SunOS 4.1.3, PCs with DOS 6.2, Windows 3.1/NT, and a network file server configured with Novell Netware 3.12. The attackers have to show three things: (1) evidence they were able to circumvent security on the target machine; (2) why the intrusion works (vulnerability); and (3) how to make the target system secure from this type of intrusion. Defenders have to answer three questions: (1) How did the intrusion (if any) enter the system?; (2) When did the intrusion (if any) enter the system?; and (3) How was the intrusion manifested in the system? Students learn information security by doing it. While the goal is to learn about protecting systems against skilled attackers, this is best accomplished with insight into the methods and mindset of attackers—you need to know how to attack to defend well. Students learned that, even unskilled as they were, they could still perform technically advanced attacks with exploit scripts downloaded from the hacker websites.

[7] 11 total papers of which 2 examples include: (1) "On Measurement of Operational Security," by Sarah Brocklehurst et. al., in 9th Annual Conference on Computer Assurance (COMPASS), 1994, pp. 257-266 and (2) "An Empirical Model of the Security Intrusion Process," by Erland Jonsson and Lech Janczewski in 11th Annual Conference on Computer Assurance (COMPASS), 1996, pp. 176-186.

[8] nicknamed "the sandbox"

In general, students find the attack/defend approach fun and exciting[9] while simultaneously making them aware of the common threats to networked information systems. Common student complaints include lack of hints and instructions from the instructors. This lack of direction was purposeful; instructors wanted students to learn for themselves either individually or in groups—the only direction was access to an isolated network containing target machines for a limited timeframe and external access to the Internet (outside of the isonet) where they could seek information. Students must research, code, and implement solutions themselves, applying classroom lessons in order to pass the course, thus elevating their learning beyond lectures.

In most cases, students must work together in teams, because attacking and defending information systems is too complex and time consuming for one student to solve. In the end, students learn more from each other than they would ever learn from a lone instructor.

One criticism of this approach is that students are being trained to be computer criminals. However, throughout the course students were continuously informed about what constitutes computer crime according to appropriate national laws and why certain behavior maybe illegal, unethical, or inappropriate. At the 21st National Information Systems Security Conference (1998), there was a panel organized by Deborah Frincke entitled, "Do Attack/Defend Exercises Belong in the Classroom?" It turned out that it was difficult to find a participant (panelist or audience member) who did not support such activities. While such attack/defend security training is a highly effective tool that could be used for good or evil, it was pointed out that the lack of such training might be more dangerous as students graduate and eventually assume security positions of critical importance. If other approaches prove to be as effective, then this approach may not be justifiable but to date this is not the case—this is the future of information security education.

3. SUMMARY

Education is the number one problem in producing information systems security professionals. This paper has presented specific educational approaches to enhance courses and facilitate information systems security curricula to meet the growing demand for information system security professionals. These different approaches are not mutually exclusive but rather may be most effective when used in combination. More educational work needs to be done to provide specific active teaching tools to instructors, such as more exercises with solutions, cryptographic puzzles, projects, and attack/defend simulations.

[9] "Fun" and "exciting" were two key words frequently found in course evaluation reports

4. REFERENCES

Amoroso, Edward G., 1993, A Graduate Course in Computing Security Technology, ACM Technical Symposium on Computer Science Education (SIGCSE), pp. 251-255.

Arsenault, A and G. White, Oct. 1991, Teaching Computer Systems Security in an Undergraduate Computer Science Curriculum, Fourteenth National Computer Security Conference, pp. 582-597.

Bishop, Matt, Oct.-Dec. 2000, Education in Information Security, IEEE Concurrency, pp. 4-8.

Bishop, Matt, Oct. 1999, What Do We Mean by "Computer Security Education"? 22nd National Information Systems Security Conference.

Bishop, Matt, May 1993, Teaching Computer Security, Ninth IFIP Intl. Symposium on Computer Security (IFIP SEC), pp. 43-52.

Bishop, Matt and L. Todd Heberlein, Oct. 1996, An Isolated Network for Research, 19th National Information Systems Security Conference, Baltimore MD, pp. 349-360

Cook, Janet M., 1985, Increasing Students' Security Awareness: Article 1, ACM Technical Symposium on Computer Science Education (SIGCSE), pp. 155-165.

Higgins, J, Oct. 1989, Information Security as a Topic in Undergraduate Education of Computer Scientists, Twelfth National Computer Security Conference, pp. 553-557.

Highland, H., Spring 1982, A College Course in Cryptography and Computer Security, Security and Audit Control Review, Vol. 1, No. 2, pp. 34-37.

Hill, John M.D., Curtis A. Carver, Jeffrey W. Humphries, and Udo W. Pooch, 2001, ACM Technical Symposium on Computer Science Education (SIGCSE). Charlotte NC, pp. 36-40.

Hoffman, Lance J., Jerrold Post, John Markey, Kyle Hettinger, 1999, Teaching Information Warfare to a Multidisciplinary Class: Lessons Learned, National Information Systems Security Conference.

Irvine, Cynthia E., Oct. 1997, Challenges in Computer Security Education, IEEE Software, pp. 110-111.

Irvine, Cynthia E., Shiu-Kai Chin, and Deborah Frinke, Dec. 1998, Integrating Security into the Curriculum, IEEE Computer, pp. 25-30.

Lindskog, Stefan, Ulf Lindqvist, and Erland Jonsson, June 1999, IT Security Research and Education in Synergy, First World Conference on Information Security Education (WISE1), Stockholm Sweden.

Mitchener, W. Garrett and Amin Vahdat, Feb. 2001, A Chat Room Assignment for Teaching Network Security, ACM Technical Symposium on Computer Science Education (SIGCSE), Charlotte NC., pp. 31-35.

Neugent, William (Bill), Spring 1982, A University Course in Computer Security, Security Audit and Control Review, Vol. 1, No. 2, pp. 17-33.

Osterman, Shawn, 1998, Please Don't Eat All the Dough, ACM SIGCOMM, Vancouver BC.

Rubin, Aviel, April 1997, An Experience Teaching a Graduate Course in Cryptography, Cryptologia.

Spafford, Eugene F., June 1998, Teaching the Big Picture of InfoSec, 2nd National Colloquium for Information System Security Education, James Madison University.

Spillman, Richard, 1992, A Computer Security Course in the Undergraduate Computer Science Curriculum, Collegiate Microcomputer, Vol. 10, pp. 91-96.

Steinberg, Steve, Feb. 1991, A Student's View of Cryptography in Computer Science, Communications of the ACM, Vol. 34, No. 2, pp. 15-17.

Yurcik, William and David Doss, Nov. 2000, Information Security Educational Initiatives to Protect E-Commerce and Critical National Infrastructures, Information Systems Education Conference (ISECON). Philadelphia, PA.