Innovative Model for Information Assurance Curriculum: A Teaching Hospital

SANJAY GOEL AND DAMIRA PON
The University at Albany, State University of New York, and New York State Center for Information Forensics and Assurance
PETER BLONIARZ, ROBERT BANGERT-DROWNS, GEORGE BERG, VINCE DELIO, LAURA IWAN, THOMAS HURBANEK, SANDOOR P. SCHUMAN, JAGDISH GANGOLLY, ADNAN BAYKAL, AND JON HOBBS
New York State Center for Information Forensics and Assurance

A novel idea for information security education created by the New York State Center for Information Forensics and Assurance (CIFA) is presented. This new approach incorporates a teaching hospital model originally developed for medical training. In this model, information security problems from industry and government are solved and abstracted into living-cases used for training and education of university students and public-sector employees. Such a model helps ensure that the curriculum stays current even as the field of information assurance continues to evolve. Solving industry problems hones research skills, while exposing students to living cases helps build context for concepts in information assurance. The success of this approach is contingent upon strong partnerships with government and private organizations that have real security issues as well as an active research program in information security that involves faculty and students. This article presents an implementation of this approach at CIFA. Development of the curriculum, observations gleaned through dissemination of the curriculum, and the infrastructure developed to support this concept are discussed. Evaluation of students has demonstrated the effectiveness of the "teaching hospital" concept and provided us with feedback to further refine its implementation.

Categories and Subject Descriptors: K.3.1 [**Computing Milieux**]: Computer Uses in Education – *Collaborative learning; Distance learning;* K.3.2 [**Computing Milieux**] Computer and Information Science Education – *Computer science education; Curriculum; Information systems education;* K.6.m [**Management of Computing and Information Systems**]: Miscellaneous – *Security*

General Terms: Design, Experimentation, Human Factors, Measurement, Performance, Security, Theory

Additional Key Words and Phrases: Education, learning, constructivism, case-based learning, problem-based learning, cases, teaching hospital, information security education, information assurance

This research was supported in part by the National Science Foundation, NSF 01-67 grant 020657151, and by the United States Department of Education, FIPSE grant P116B020477.
Authors' addresses: S. Goel, Department of Information Technology Management, The University at Albany, State University of New York, BA 310b, 1400 Washington Ave., Albany, NY 12222; email: goel@albany.edu; D. Pon, Department of Informatics, The University at Albany, State University of New York, BA 310, 1400 Washington Ave., Albany, NY 12222. P. Bloniarz, R. Bangert-Drowns, G. Berg, V. Delio, L. Iwan, T. Hurbanek, S. P. Schuman, J. Gangolly, A. Baykal, and J. Hobbs are with the New York State Center for Information Forensics and Assurance

1. INTRODUCTION

The need for widespread dissemination of information assurance (IA) education is clearly understood, and several researchers have elegantly elucidated these concerns [Bishop and Frincke 2004; Dark and Davis 2002; Hsu and Backhouse 2002].

As technology continues to permeate the fabric of society and our dependence on technology increases, the demand for such education will continue to escalate. Estimates of financial losses resulting from security breaches are substantial [Gordon et al. 2004]; but the potential losses could be catastrophic (e.g., threats to human life and property by disruption of supervisory control and data acquisition systems that control the nation's critical infrastructure). In the past, most efforts to improve security have focused on technological innovations, and substantial improvements have been made with basic security tools such as the use of intrusion detection systems and firewalls. By themselves, such improvements have been inadequate in controlling the worsening security environment. Security is a socio-technical problem that requires active user participation and technology development to control the proliferation of attacks as well as to prevent human errors. Because information technology is inextricably linked to the domain to which it is applied, the study of IA in isolation is ineffectual. It is thus essential to integrate IA into existing curricula rather than to create isolated silos of course material [Irvine et al. 1998]. Education in information technology itself is slowly moving towards an interdisciplinary model, and several new programs are being established around this concept.

To promote and ensure that "businesses, general workforce, and the general population" are able to "secure their own parts of cyberspace." is a priority of the President's National Strategy to Secure Cyberspace [United States 2003]. As a result, training and education programs that support the "Nation's cyber security needs" were developed, current federal cyber security programs were improved, and industry-supported certifications promoted. Federal and state governments are investing significant amounts of money in workforce education through classes, web casts, and advisories. Eighty-five percent of the nation's critical infrastructure is controlled by the private sector. Training the private sector workforce needs to be a national priority to ensure the protection of information systems and critical infrastructure. Other segments of the population also need training. Children in the K-12 grades are increasingly exposed to information technology, and while adept at using computers, they can be very gullible and easy targets for Internet criminals and pedophiles. Similarly, older people who are not experienced users of computers and have a limited awareness of computer crimes can easily become victims of hackers. Hence, universities must become catalysts for disseminating curricular material across society by providing education directly or by training educators in schools and community colleges that cater to large and diverse segments of the population. Bishop [2000] describes the necessity for information security education at multiple levels (training, undergraduate, and postgraduate) and the varying types of skills for each, all of which are relevant in information security education.

Dissemination of IA education involves distinct issues. Technology changes quickly, and new threats emerge constantly. As a consequence, knowledge becomes obsolete very quickly, and the workforce must be re-educated continuously. Institutions providing IA education face difficulties in keeping curriculum innovative and relevant, as the course material has a very short shelf life. The information security field is very diverse and combines the disciplines of computer science, business, information science, engineering, education, psychology, criminal justice, public administration, law, and accounting. Its broad interdisciplinary nature requires several specialists to collaboratively teach the

curriculum and integrate different perspectives and teaching styles into a cohesive delivery. For effective collaboration, different departments should contribute and benefit mutually. If not crafted carefully, such a multidisciplinary environment can lead to nonintegrated, disparate courses.

Because IA is a complex subject that spans several disciplines, it is important to build a rich context so that concepts can be assimilated rapidly across multiple disciplines. Researchers have recognized this need and have attempted to build such a context via hands-on exercises that reinforce the concepts taught in the classroom [Conti et al. 2003]. These exercises are difficult to develop, expensive to maintain, and have a short lifespan. Virtual environments are being employed to mitigate the cost and maintenance [Kumar et al. 2005]; but the rapid rate of obsolescence and the need to introduce new information increase the cost of developing hands-on exercises. While expensive and a useful enhancement to the curriculum, these learning aids alone are still not sufficient in providing the rich context necessary for a security curriculum. To give a comprehensive IA learning experience, cases developed from real-world experiences must complement classroom curricula and hands-on security exercises. Irvine et al. [1998] lists two key outcomes of IA education: (1) it trains graduates to address security problems in their professional work; and (2) ensures that the learning fits well in the larger engineering context. The "larger engineering context" [Irvine et al. 1998] refers to the domains to which the learning is related (e.g., computer science, business, etc.). The pedagogical model of a teaching hospital addresses the learning outcomes by facilitating the creation of a rich set of cases based on problems from both the public and private sectors. In addition, this model compensates for material obsolescence because new cases are constantly being produced as new problems appear.

In this article we present this "teaching hospital" concept and discuss what we have learned from its implementation at the New York State Center for Information Forensics and Assurance (CIFA) at the University at Albany. The rest of the article is organized as follows: Section 2 reviews existing IA programs; Section 3 discusses the different learning approaches; Section 4 presents the "teaching hospital" model; Section 5 describes curricula developed for the teaching hospital; and Section 6 contains concluding remarks and future plans.

2. EXISTING IA PROGRAMS

Several universities have active programs focused on developing IA curricula (e.g., Purdue University [Dark and Davis 2002], Carnegie Mellon University, University of Oklahoma, the Naval Post Graduate School [Irvine 2003], and the United States Military Academy [Hoffman et al. 2003]). These institutions have developed a comprehensive set of curricula that span several departments and are varied based on the strengths and capabilities of the faculty and course material. Most have developed IA educational laboratories that allow students to gain hands-on experience in both launching and protecting against various attacks. In addition, most of these programs have resulted from collaboration and sharing among early IA educators in forums such as the Colloquium for Information Systems Security Education and the Workshop on Education in Computer Security [Bishop and Frincke 2004]. Government grants for fostering IA education and improving national security were also crucial to IA program development.

The National Security Agency and the U.S. Department of Homeland Security sponsored the creation of National Centers of Academic Excellence in Information Assurance [National Security Agency 1999]. This program follows through on some statutes in the National Strategy to Secure Cyberspace. To become one of these centers,

an IA program is evaluated against established criteria. Within these evaluation criteria, the need for an interdisciplinary program must be established, citing beneficial contributions from various fields such as law and management instead of just computer science. In addition, the guidelines focus on the importance of dissemination using distance-delivery methods to reach beyond geographic boundaries. Incorporating faculty research and practitioner contributions to IA literature is stressed, as well as the availability of state-of-the-art resources and a designated center for IA education or research.

One of the instructional best practices for information security education is the NIST SP 800-16-IT Security Instructional Model [Gilbert 2003]. It is based on federal regulations and is composed of three levels of instruction: awareness, training, and education, with an associated learning objective fir the three levels. Awareness is associated with "recognition and retention," training with "skill," and education with "understanding." Sample teaching methods for each level are detailed. Awareness is more rudimentary (videos and posters); while training incorporates lectures, demonstrations, case studies, and hands-on learning; and education furthers training with discussions, readings, and research. Because the level of instruction is adapted to information technology and information security audiences, there is an emphasis on practical hands-on learning. There has been considerable debate on the merits of education versus training in several fields, including chemistry [Moore 1998], computer science [Ben-Ari 1998], and information assurance [Irvine 1999; Bishop and Frincke 1998]. Training is usually a narrowly focused program that leads to high proficiency in a specific skill. It prepares a student for a specific activity, but it may not provide a broad perspective, which is useful in adapting learning to other situations. On the other hand, education has a wider focus that involves teaching general theories, concepts, and approaches to problem solving, thereby inculcating critical thinking skills in students. The goal of education is to teach a student to learn and explore on their own to solve new problems as they arise. Roles for both training and education exist in information assurance. There are fundamental concepts that must be understood and specific skills that must be learned in order to function in the field.

There are several other models for IA education. Hsu and Backhouse [2002] apply a situated learning strategy to information systems security. This strategy "stresses the importance of enculturation and community of practice." Classes are designed to include lectures, group collaborations, guest speakers from industry, and case studies. Hoffman et al. [2003] discuss the "hear-see-do" paradigm in technological fields and estimate that students "retain only 26% of what they hear, 50% of what they hear and see, and 90% of what they hear, see and do." They use this learning model to support the creation of "optimized" IA laboratories that allow students to both learn and do research. Irvine [1999] also advocates security laboratories to complement classroom education in information assurance, which may help in training but may not adequately build the context for the problems arising from cases. The teaching hospital model blends training and teaching into a seamless integrated process by incorporating hands-on exercise in the context of real problems via cases generated by the teaching hospital.

3. APPROACHES TO LEARNING

Objectivism and constructivism are two distinct theories about learning that can be applied to IA education. Objectivists believe that knowledge and truth exist outside the mind of individuals. Learners are told about the world and are then expected to replicate its content and structure in their thinking [Jonassen 1991]. Traditionally, teachers have

adopted the objectivist approach, using instructional design models that provide a series of steps which, if followed properly, will lead to learning. The models require developers to identify the learners' prior knowledge, expected learning outcomes, performance objectives, instructional strategies, assessment strategies and techniques, and evaluation procedures. Objectivism propagates rote learning via memorization and feed back.. In such a learning environment, instructors attempt to alter student behavior using reward and punishment. The systematic instructional design model [Dick and Carey 1990] is a commonly used model of this kind, in which Gagne's [1985] categories of learning outcomes, learning conditions, and instruction events are used as decision-making tools and as a framework for designing and delivering of instruction.

Constructivists believe that knowledge and truth are constructed by learners and do not exist outside of the learners' minds [Duffy and Jonassen 1992]. In the constructivist approach, students construct their own knowledge by actively participating in learning. This approach values collaboration, the autonomy of the student, reflectivity, and active engagement. Such a teaching philosophy provides a rich learning environment for students, in which they may explore learning independently and draw conclusions for themselves. The constructivist environment presents actual situations to learn from, and mistakes made by learners are mechanisms that provide feedback and understanding [Wilson and Cole 1991]. The constructivist approach is the basis for several learning paradigms, including, case-based learning [Jarz et al. 1997; Merseth 1991; Riesbeck 1997; problem-based learning [Norman and Schmidt 1992; Stepien and Gallaghar 1993; Stepien et al. 1993]; collaborative learning [Totten et al. 1991]. Constructivism is a more recent learning paradigm; and is considered a superior technique for classroom education [Brooks and Brooks 1993].

There are many instructional design models based on constructivist theory (e.g., Bednar et al. [1995]; Hannafin et al. [1999]; Jonassen [1999]; and Willis [1995]). The "constructivist learning environment" model [Jonassen 1999] is popular in computer-based learning environments. It lays out several design principles, including focus on real-world problems, multiple interpretations of these problems, determining instructional goals collectively, and using evaluation as a self-analysis tool. This educational technique is very effective for an audience with some work experience which allows them to superpose their own contexts on to the problem domain. Creating simulated cases based on real-life situations also provides a rich learning environment through which learners can live vicariously by means of the context embedded in the cases.

The constructivist metaphor meshes well with critical thinking [Bloom 1956], through which students investigate problems, ask questions, give new answers that challenge the status quo, discover new information, question traditional beliefs, challenge received dogmas, and create new knowledge in the process. During critical thinking, the brain makes new neural connections that improve focus on a topic, help in learning difficult concepts, and improve memory. Through critical thinking, the brain is able to build context around other knowledge the user has acquired.

Problem-based learning is a tool of the constructivist approach which provides students with problems from practice [Boud and Feletti 1991]. Giving students a rich set of problems kindles their curiosity and motivates them to learn the subject matter on their own [Berlyne 1965]. It challenges students to work cooperatively in groups to seek solutions to real-world problems, and prepares them to think critically and analytically and find and use appropriate learning resources [Duch 1995]. This approach is usually built around a complex abstract problem that may have multiple solutions or no clear solution. The students must anchor the problem in a context and on the assumptions that

they built around it. Problem-based learning promotes active learning, and can be used as a framework for curriculum development [Samford University 2003]. It has some similarities to case-based learning where cases are abstracted from real events.

By examining case studies in a teacher education program, Tomey [2003] determined that case-based learning has many advantages. The case-based learning style "blends aspects of the cognitive and social constructivist models of teaching and learning" [Mayo 2004] and promotes "active, self-directed learning," and provides an emphasis on "active and interactive components of the learning process." In addition, case studies "help build prior knowledge, integrate knowledge, and consider application to future situations" and "encourage teamwork and accountability, and are realistic and motivating" [Tomey 2003].

Cases, which are considered tools for constructivist learning, are best used when the goal is to enable students to react in realistic decision-making situations [Jarz et al. 1997; Merseth 1991; Riesbeck 1997]. Deciding on which didactic design to use is a major one, and depends on the desired goal. If the goal of learning is to ensure that students reach a certain conclusion or acquire a core set of knowledge, a web-based or multimedia case can be used to narrate a story. However, if it is important to provide the students with a realistic experience, an interactive case should be developed through which students can interact with entities that are involved in the case and conduct research to solve the problem at hand. The amount of case detail can be varied to provide different learning experiences. Cases can be designed with complete information, which will allow students to assimilate the subject matter with relatively less introspection, or sparse information can be provided to force students to deduce (or assume) the remaining information to solve the case through research and analysis. Providing open-ended cases will allow the same case to fit several different scenarios and require greater effort from the learner. The decision to use a specific type of case will also depend on the students who are engaged in the exercises and on the content being imparted. When learning basic concepts, it is probably better to use more structured cases; but when learning advanced concepts drawn from several fields, it is more effective to use unstructured cases.

Much research has been done on the effectiveness of case-based learning. Case-based education has been used for instruction in many schools for various disciplines, and is an established pedagogical method. Case studies were first used in 1788 by the Medical Society of New Haven to advance medical knowledge [Tomey 2003]. Russell and Norvig [1995] describe the process of case-based reasoning as involving cases being put into memory, generalizing cases through recognition of similarities, and relating cases to tasks. While incorporating case-studies may decrease lecture time, it is seen as a rational "trade-off between breadth and depth of knowledge covered" [Sudzina 1997]. Needham [2001], while doing a case study of a business school in the UK, stated that one of the problems is keeping the cases current and relevant, which is necessary in IA education. In collaborative learning, students form groups and collectively solve problems by exchanging ideas and pooling their efforts and resources. This active exchange of ideas not only makes the educational experience more entertaining, but it also fosters critical thinking among the participants. A study by Johnson and Johnson [1986] shows that students in collaborative settings retain information longer and that this collaboratively developed understanding is more thorough because the students are able to build a richer context around the problem. According to Totten et al. [1991], shared learning gives students the opportunity to engage in discussion and take responsibility for their own learning, thereby making them critical thinkers. Such learning not only aids in processing

the content, but also improves the social adaptation of the students when they join the work force, thereby increasing their effectiveness in an organization.

In the next section, we introduce the concept of a teaching hospital to develop a unique constructivist design model for IA education. We use traditional tools such as problems, cases, and scenarios; but we also link these tools to active research on current industry problems to ensure that the curriculum stays relevant.

4. THE TEACHING HOSPITAL MODEL

Teaching hospitals have been extensively used for medical training since early historical times. They enable the control and monitoring of medical students' training and the quality of their medical education. Training is provided to medical students and doctors-in-training through direct clinical experience in treating actual patients under the supervision and guidance of attending physicians in medical wards. Teaching hospitals are important because they provide their students with hands-on experience; it would otherwise be very difficult to translate the abstract knowledge from the literature into an actual diagnosis. They enable medical residents to integrate theoretical knowledge into practical, concrete knowledge, which they will use in the practice of medicine. In IA education it is also essential to find a balance between theory and practice. The field not only requires students to be able to conceptualize, but also to practically apply what was learned in the classroom to the outside world. Teaching hospitals usually offer a comprehensive array of facilities as well as possess sufficiently high volumes of patients with whom students can interact to gain experience. Teaching hospitals traditionally conduct a wide variety of clinical research [Management of America, Inc. 1999]. Although derived from medical education, the "teaching hospital" model has been implemented with great effect within the pedagogical practices of other disciplines that require the eventual application of theory to practice.

A teaching hospital model has been implemented at Kansas State University's Engineering Learning Center [Azadivar and Tucker 2000; Kramer et al. 2002]. Azadivar and Tucker [2000] detail reasons for incorporating this concept into engineering education. For example, medical students, supervised by experienced professionals, help real patients with medical illnesses and problems. Thus applying what was learned in the classroom to live subjects in a "real-world" environment with "real-world" constraints (i.e., time and budget). Kramer et al. [2002] use the teaching hospital model as an analogy to a teaching factory, so the hospital is replaced by the Engineering Learning Center (ELC), the medical doctors by experienced engineers, the medical interns by engineering/business interns, patients by manufacturing companies, and the medical equipment by engineering tools and manufacturing equipment. In their model the ELC also incorporated cooperation among engineering, business, and computer science students, resulting in more than 1100 design and manufacturing engineering projects for more than 250 companies.

A fundamental problem with IA curricula, especially with hands-on exercises, is that the curriculum materials quickly become obsolete as threats and vulnerabilities evolve rapidly. It is expensive to create hands-on exercises, and once developed, the costs need to be amortized over several years to remain sustainable. We present the "teaching hospital" model for training students in IA (see Table I), where students receive hands-on experience by working on real problems supervised by researchers and practitioners. The intentions of the IA teaching model is to reflect those of the medical model in integrating research, education, and service. As described in Table I, the traditional medical hospital is replaced by CIFA at the University at Albany; the medical students are replaced by IA

Table I. Medical Teaching Hospital compared to IA Teaching Hospital

ASPECT	Medical Teaching Hospital	IA Teaching Hospital
Purpose	1. Teach medicine 2. Cure patients 3. Develop new cures	1. Teach IA 2. Improve security in public and private sector agencies 3. Develop new methods of defense
Location	Hospital	CIFA (or equivalent)
Supervisors	Medical doctors	IA faculty
Students	Medical students/residents	IA students/professionals
Clients	Medical patients	Public and private sector agencies

students from the university and professional employees from state agencies. Instead of physicians supervising the process, IA faculties act as mentors for the students and the research and education laboratories serve as environments for active work.

Because the potential IA student population is large and few researchers are available, it is not feasible to send most students to directly apprentice with researchers, especially if they are nontraditional. However, some programs do offer such an experience to limited numbers of students. The NSF Scholarship for Service program [McGinnis and Comstock 2003], which gives scholarships for up to two years in exchange for service to federal government agencies, is a good example. Furthermore, the National Security Agency [Conti et al. 2003] and others (e.g., CISCO and Microsoft) offer internships in IA.

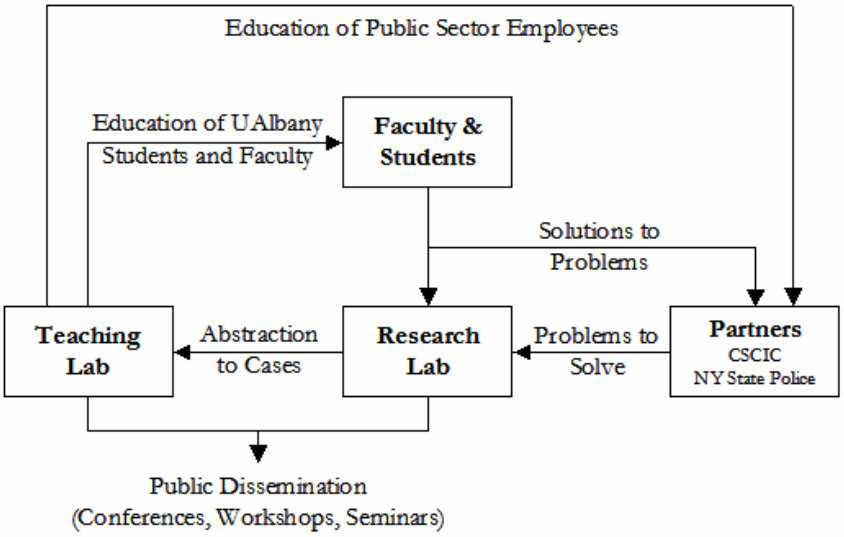

Fig 1. CIFA implementation of the "teaching hospital" model for IA.

As an alternative to these programs, and to incorporate realistic experiences throughout the entire curriculum, cases from state and law enforcement agencies are used. Public and private sector agencies are often unable to devote the resources to develop a solution for a problem that needs to be thoroughly researched and then create a training program to effectively disseminate the results. Figure 1 shows a functional model, in use at CIFA, of a "teaching hospital" for IA.

This model allows for known problems (sanitized due to legal and security constraints) from public and private sector organizations to be transferred to a research laboratory where graduate interns, students, and faculty members can solve them. This population is truly exposed to the "teaching hospital" model, while students at universities and organizations that do not provide such a model experience the context vicariously via abstracted cases developed from problems that have already been solved and incorporated into the teaching material.

4.1 Partnerships

CIFA has strong partnerships with two New York state agencies—the Police Computer Crime Laboratory (CCL) and the Office for Cyber Security and Critical Infrastructure Coordination (CSCIC) — and employs the "teaching hospital" model for IA research and education. CCL's primary responsibility is to investigate computer crime (i.e., computer fraud, theft of information, pornography, malicious code, music piracy, and unauthorized intrusions into networks) in New York State. Most its work involves forensic analysis of data, hardware, and networks (it serves as a source for computer forensics and incident-handling cases). These areas draw heavily from the literature on computer architecture, software design, networking, and law. A large portion of the data is sensitive due to legal constraints, but once the sensitive data is abstracted, these cases are turned into research problems that can be addressed at CIFA. CSCIC is responsible for monitoring the security of all New York State agencies, to which it issues advisories when new information on security threats are identified. It also creates and disseminates security policies to New York State agencies and acts as an advisor for policy implementation, and serves as a resource for cases in the areas of security policies and security risk assessment.

4.2 Facilities

It is relatively easier for medical hospitals to implement a "teaching hospital," as medical wards already exist where physicians treat patients and residents can shadow physicians. In IA there is no such network of existing facilities where security problems can be solved. Similar to teaching hospitals, IA educational institutions should have appropriate facilities with sufficient equipment to enable hands-on learning. But our facilities are computer laboratories for both teaching and research. So a fundamental issue in the design of security laboratories is to ensure that laboratory exercises do not accidentally cause disruption of services in other networks. Hence the implemented network architecture allows the laboratories to disconnect from the university network when experiments with the potential of causing network damage are executed. In addition, Internet access via a connection independent of the university, to support activities such as deployment of honeynets, is integrated into the system. Both educational and research laboratories are connected to each other through a network connection independent of the university network to allow communication and file sharing. Wireless networks allow research in wireless security and enable flexible reconfiguration of laboratory architecture.

Laboratory hardware and software must be diverse, so that the environment in which a real problem occurred can be replicated. The educational laboratory is designed to facilitate rapid machine reconfiguration, so that changes made for laboratory exercises can be eliminated quickly and the laboratory returned to its normal setting.

5. CURRICULUM DEVELOPMENT

Developing course material for IA requires experts from several disciplines. Students interested in the curriculum also come from a variety of backgrounds, including, public policy, law, computer science, business, and information science. Therefore, it is often difficult to design three-credit courses where all the material is relevant to all students. Furthermore, because many students are employed full-time, it is difficult for them to make a prolonged class commitment. To allow students flexibility in planning their curriculum and instructors in designing their courses, our IA curriculum is planned around a series of one-credit courses.

In a spring 2004 pilot program, two information security courses were created: (1) Information Security Risk Analysis and (2) Incident Handling, which coincided with the interests of our major partners. Incident handling interested CCL employees and risk analysis appealed to the CSCIC workforce. The first set of courses was taught by an instructor who did not participate in the development of the curriculum; a diverse team developed these courses. Domain experts acted as content developers for the teaching material and an expert on pedagogy gave advice on the structure, evaluation, and organization of the courses. Practitioners evaluated content and provided examples and cases. Much of the content required for the courses was relatively new and was not available in textbooks; hence, content was compiled from a variety of sources. The courses had a strong hands-on element so classes were separated into half classroom instruction and half hands-on work. Student exercises were comprised of computer-based tools as well as analytic problems, such as using network penetration tools for risk assessment, cases to analyze risks in organizations, forensics tools to analyze data in files, analysis of log files, and on writing policies. There was strong interest in enrollment from both government employees and university students; but many potential students had to be rejected because of roster limitations.

To demonstrate the effectiveness of the teaching hospital as a metaphor, we discuss the creation, implementation, and results of the risk analysis course offered during the pilot program. The risk analysis course (see syllabus in Appendix 1) was intended for information security officers, many of whom were newly transferred from other positions. While they had relatively more competence in information technology compared to their colleagues, they often lacked the knowledge necessary for their primary functions of assessing the risks to their organizations and defining effective security policies. Knowledge of basic security skills was necessary before risk analysis and security policy development could be understood. To provide this comprehensive understanding, the course was divided into three content sections. The first section provided fundamental background on security threats and vulnerabilities, including lectures for conceptual understanding and hands-on laboratories to expose students to hacking and security tools to improve security. The second section introduced risk analysis concepts and included a combination of lecture and case discussion. Making use of the case material was effective because the students were primarily practitioners with much work experience relevant to this material. The third section covered the fundamentals of security policy creation and enactment and familiarized the students with different types of security policies through use of vignettes (small cases).

Several such vignettes were integrated with lecture material throughout all the courses. Most were fictitious cases used to clarify specific concepts and to increase student participation in the class. To keep the cases diverse, the first case was created from data taken from both the public and private sectors. It was based on a security audit of a state agency. To develop the case, the general context of the organization was presented first, so that the scenario could be established. Special care was taken to eliminate any specific references to organizations so that their identities would not be disclosed and exposure to potential hackers avoided. The assets, threats, and vulnerabilities of the organization were presented in the case narrative rather than specified in a structured form. This approach forced the students to comprehend the information and extract the relevant parts for analysis. The students were allowed to discuss the case with each other and with the instructor, which was especially valuable when attempting to identify threats and vulnerabilities, since the students could bring their own individual contexts to the analysis. Each student encountered different threats and vulnerabilities, and through discussion was able to determine a more comprehensive set of data for analysis.

To develop the second case, risk analysis using the same methodology taught in the class [Goel and Chen 2005] was done at General Electric Energy. A team of experts from different divisions of the company performed the analysis. The team worked collaboratively to collect the data for the analysis and completed the analysis through consensus building. As a final assignment, students were expected to use the risk methodology in their own organizations and produce an extensive report. This assignment assisted in consolidating their new knowledge for long-term retention. Since the initial class offering, several cases have been created and published [Goel and Pon; Goel et al. http://www.albany.edu/~goel/research/education.html].[1]

Glen Martin Associates, an independent consulting firm, performed curriculum evaluations to determine the effectiveness of the classes (see summary of results in Appendix 2). To do their assessment, the firm prepared student questionnaires and interviewed students and curriculum developers. The feedback was positive, with a satisfaction rating of more than two out of three for most categories dealing with course content and instruction. In the risk analysis course, the survey showed that student knowledge at the beginning of the course varied significantly, from none to good. However, at the end of the course student knowledge always increased from their knowledge before the class. All students achieved at least "good" results (the primary goal of the class), with 80% stating that they had "good" knowledge of the subject and 20% stating they had "very good" knowledge of the subject. Students gave a rating of 5.4 out of 6 in recommending the course to others and a rating of 5.7 out of 6 for presentations by instructors. While the lecture material was deemed very effective (66.7% strongly agreed), the case studies, in-class discussion, risk analysis project, and the hands-on laboratory activities were considered effective by 100% of the class, although perhaps not as strongly. When compared to the qualitative answers about the least and most valuable parts of the course, the case studies, laboratory activities, and matrix-based risk analysis approach were included in both categories. It can be inferred that while these components were valuable, their execution still needed to be refined. In addition, it emerged from the evaluation that the curriculum was content-dense and contained too many topics. For instance, the risk analysis course contained material on

[1]As new cases and additional information are developed, they will be made available at http://www.albany.edu/~goel/research/education.html.

security policies as well as some security fundamentals. Also, due to their varying backgrounds, some students were already familiar with some of the course subtopics. In order to address this issue, the curriculum is being expanded. The risk analysis course has been split into three: a security fundamentals course, an information security risk assessment course, and a security policies course. It was also found that students strongly preferred online delivery of material, especially those who worked at state agencies. To achieve more widespread dissemination of our curriculum, we are working with our partner CERIAS at Purdue University to offer these courses via distance-delivery format using WebCT. The Information Security Risk Assessment course was offered in fall 2005 as a two-week course (see the syllabus in Appendix 3). The course was available in audio and video, with an instructor and a PowerPoint inset that progressed through the curriculum. The online dissemination format allows students to learn the material without interaction with peers or instructors; but it is more difficult for the student to sustain attention in this format than in a classroom setting. To retain student attention, each lecture was divided into 20-minute segments with a clear set of objectives at the beginning of each segment and material to evaluate the results at the end. At the end of an entire lecture, either a case or an elaborate quiz was given to the students to assess retention and understanding of the material. Online dissemination was made up of an audiovisual experience for the learner, wherein the instructor supplements a written presentation on the material with a narrative one. The video of the online presentation switches between the written presentation and the narrative, and sometimes the instructor appears as an inset in the written presentation.

At first, the courses were offered primarily to the employees of the public sector. However, to amortize the cost of their development and to sustain them over the long run, the courses should be incorporated into a higher education curriculum. But due to its multidisciplinary nature, IA has a problem: the courses can reside in several disciplines and their corresponding departments. In addition, there is significant logistical difficulty in adding more courses to existing departments by displacing other courses. To avoid such problems, the curriculum is being incorporated into segments of existing courses where it can enhance current course content.

6. CONCLUSIONS

In partnership with the CCL and the CSCIC, we at CIFA have developed and implemented an innovative paradigm of information security education at the University at Albany to train professionals and students effectively and economically. This learning paradigm uses a “teaching hospital” approach in which current problems from government agencies and industry are brought into our research laboratory, made into “living cases,” and solved by teams of faculty members, professionals, and students. At the “teaching hospital,” a team categorizes problems and creates treatment regimens or procedures for solved problems so they can be prevented and/or remedied in the future. These treatment regimens or procedures are then documented and disseminated to the state agencies. In today’s changing security environment, it is hard to keep educational material current. CIFA deals with the issue of obsolescence by incorporating real cases from public and private collaborators, as well as from security research conducted in laboratories. The presentation material remains relatively static while the cases are constantly replaced. The cases originate from problems that the public and private organizations face continually; these problems are brought to the research laboratory and abstracted into cases, thereby ensuring relevance for the field. Along with these cases, hands-on laboratory exercises supplement learning through the practical application of

knowledge. By working closely with public-sector agencies in developing an information security curriculum, we provide a unique and rich learning environment for university students and ensure that government employees are well trained in the practices of information security.

ACKNOWLEDGMENTS:

We would like to thank William Pelgrin of CSCI for his support of CIFA. In addition, thanks to Melissa Dark and Ting Zhuang of Purdue University for assisting in the development of the distance-delivery version of the risk analysis curriculum.

REFERENCES

AZADIVAR, F. AND TUCKER, J. 2000. An engineering learning center: description, results, and lessons learned. In *Proceedings of the 30th ASEE/IEEE Frontiers in Education Conference (*Kansas City, MO, Oct.), IEEE Press, New York, 1-5.

BEDNAR, A.K., CUNNINGHAM, D., DUFFY, T.M., AND PERRY, J.D. 1998. Theory into practice: How do we link? In *Constructivism and Technology of Instruction: A Conversation*, T.M Duffy and D.H. Jonassen (eds.), Lawrence Erlbaum Associates, Hillsdale, NJ, 17-35.

BEN-ARI, M. 1998. Constructivism in computer science education. In *Proceedings of the 29th SIGCSE Technical Symposium on Computer Science Education (*Atlanta, GA, Feb.), ACM Press, New York.

BERLYNE, D.E. 1965. Curiosity and education. In *Learning and the Educational Process*, J.D. Krumboltz (ed), Rand McNally, Chicago.

BISHOP, M. 2000. Education in information security. *IEEE Concurrency.* http://nob.cs.ucdavis.edu/~bishop/papers/2000-educieee/2000-educieee.pdf.

BISHOP, M. AND FRINCKE, D. 2004. Joining the security education community. *IEEE Security & Privacy*, (Sept./Oct.), 61-63.

BLOOM, B.S. 1956. *Taxonomy Of Educational Objectives, Handbook 1: Cognitive Domain.* Longmans Green, New York.

BOUD, D. AND FELETTI, G. 1991. *The Challenge of Problem-Based Learning*. Kogan Page, London.

BROOKS, J.G. AND BROOKS, M.G. 1993. *The Case for Constructivist Classrooms.* Association for Supervision and Curriculum Development., Alexandria, VA.

CONTI, G., HILL, J., LATHROP, S., ALFORD, K., AND RAGSDALE, D. 2003. A comprehensive undergraduate information assurance program. In *Security Education and Critical Infrastructures, 3rd Annual World Conference on Information Security Education* (WISE3, Monterey, CA, June), C. Irvine and H. Armstrong (eds.) Kluwer Academic, Boston, MA, 243-260.

DARK, M. AND DAVIS, J. 2002. Report on information assurance curriculum development. *Curriculum Development Workshop, CERIAS.* http://www.cerias.purdue.edu/education/post_secondary_education/undergrad_and_grad/curriculum_development/information_assurance/report_info_assurance_cur_dev.pdf.

DICK, W. AND CAREY, L. 1990. *The Systematic Design Of Instruction.* Harper Collins, New York.

DUCH, B. 1995. Problem based learning in physics: the power of students teaching students. *About Teaching 47*, 6-7.

DUFFY, T.M. AND JONASSEN, D.H. 1992. *Constructivist and the Technology of Instruction: A Conversation.* Lawrence Erlbaum Associates, Hillsdale, NJ.

GAGNÉ, R.M. 1985. *Conditions of Learning*, 4th ed., Holt, Rinehart and Winston, New York.

GILBERT, C. 2003. Developing an integrated security training, awareness, and education program gsec practical assignment version 1.4b, *SANS Institute*. http://www.sans.org/rr/papers/47/1160.pdf.

GOEL, S., BAYKAL, A., AND PON, D. Botnets: the anatomy of a case. *Journal of Information Systems Security* (accepted).

GOEL, S. AND CHEN, V. 2005. Information security risk analysis – A matrix-based approach. In *Proceedings of the Information Resource Management Association (IRMA) International Conference* (San Diego, CA, May), Information Resources Management Association, Hershey, PA.

GOEL, S. AND PON, D. Information security risk analysis: A pedagogic model based on a teaching hospital. Accepted for publication in *Tools for Teaching Computer Networking and Hardware Concepts*, N. Sarkar, ed.

GORDON, L.A., LOEB, M.P., LUCYSHYN, W., AND RICHARDSON, R. 2004. CSI/FBI computer crime and security survey. *Computer Security Institute Publications*, 1-18.

HANNAFIN, M., LAND, S., AND OLIVER, K. 1999. Open learning environments: Foundations, methods, and models. In *Instructional Design Theories and Models: A New Paradigm of Instructional Theory*, Vol. II, C.M.Reigeluth, ed., Lawrence Erlbaum Associates, Hillsdale, NJ.

HOFFMAN, L.J., DODGE, R., ROSENBERG, T., AND RAGSDALE, D. 2003. Information assurance laboratory innovations. In *Proceedings of the 7th Colloquium for Information Systems Security Education* (Washington, D.C., June).

HSU, C. AND BACKHOUSE, J. 2002. Information systems security education: Redressing the balance of theory and practice. *Journal of Information Systems Education 13*, 3, 211-218. http://www.jise.appstate.edu/13/211.pdf.

IRVINE, C.E. 1999. Amplifying security education in the laboratory. In *Proceedings of the IFIP TC11 WC 11.8 First Workd Conference on Information Security Education* (Kista, Sweden, June), 139-146.

IRVINE, C.E. 2003. The SimSecurity Information Assurance Virtual Laboratory. In *Selected Synopses of Paper Presentations at the IEEE Security & Privacy Symposium,* Oakland, CA, May 2003. Retrieved on May 10, 2006, from www.nps.navy.mil/cs/facultypages/faculty/irvine/Publications/Publications2003/SimSecurity%20abstract_IEEE03.pdf

IRVINE, C.E., CHIN, S., AND FRINCKE, D.A. 1998. Integrating security into the curriculum. *IEEE Computer 31*, 12, 25-30.

JARZ, E.M., KAINZ, G.A., AND WALPOTH, G. 1997. Multimedia-based case studies in education: design, development, and evaluation of multimedia-based case studies. *Journal of Educational Multimedia and Hypermedia 6*, 1, 23-46.

JOHNSON, R.T. AND JOHNSON, D.W. 1986. Action research: cooperative learning in the science classroom. *Science and Children 24*, 31-32.

JONASSEN, D.H. 1999. Designing consructivist learning environments. In *Instructional Design Theories and Models: A New Paradigm of Instructional Theory*, Vol. II, C.M. Reigeluth, ed. Lawrence Erlbaum Associates, Hillsdale, NJ.

JONASSEN, D.H. 1991. Objectivist vs. constructivist: Do we need a new philosophical paradigm? *Educational Technology: Research and Development 39*, 3, 5-14.

KRAMER, B.A., TUCKER, J., JONES, T., BEIKMANN, M., AND WINDHOLZ, R. 2002. The engineering learning center: A model for mentored product innovation. In *Proceedings of the 32nd ASEE/IEEE Frontiers in Education Conference* (Boston, MA, Nov.), IEEE Computer Society Press, Los Alamitos, CA, 24-29.

KUMAR, K., WEIQING, S., RANA, P., LI, T., AND SEKAR, R. 2005. V-NetLab: A cost-effective platform to support course projects in computer security. In *The 9th Annual Colloquium for Information Systems Security Education* (CISSE, Atlanta, GA, June), USENIX Association, Berkeley, CA. Retrieved on May 7, 2006 from http://seclab.cs.sunysb.edu/seclab/pubs/papers/ncisse05.pdf, 1-7.

MANAGEMENT OF AMERICA, INC. 1999. Accredited models for clinical training of physicians in medical schools that operate without a teaching hospital under the control of the university. Florida State University. http://med.fsu.edu/pdf/03_clin_training_of_phys.pdf.

MAYO, J.A. 2004. Using case-based instruction to bridge the gap between theory and practice. *Journal of Constructivist Psychology 17*, 137-146.

MCGINNIS, D.R. AND COMSTOCK, K. 2003. The implications of information assurance and security crisis on computing model curricula. *Information Systems Education Journal, 1*, 9, 1-12.

MERSETH, K. 1991. The early history of case-based instruction: Insights for teacher education today. *Journal of Teacher Education 42*, 4, 243-249.

MOORE, J.W. 1998. Education versus training. *Journal of Chemical Education 75*, 135.

NATIONAL SECURITY AGENCY. 1999. Criteria for measurement. Centers of Academic Excellence. http://www.nsa.gov/ia/academia/caeCriteria.cfm?MenuID=10.1.1.2

NEEDHAM, D. 2001. A case study of case studies: Producing real world learning within the business classroom. *ultiBASE Articles*. http://ultibase.rmit.edu.au/Articles/nov01/needham1.htm.

NORMAN, G.R. AND SCHMIDT, H.G. 1992. The psychological basis of problem-based learning: A review of the evidence. *Academic Medicine 67*, 9, 557-565.

RIESBECK, C.K. 1996. Case-based teaching and constructivism: Carpenters and tools. In *Constructivist Learning Environments*, B. G. Wilson, ed., Educational Technology Publications, Englewood Cliffs, NJ.

RUSSELL, S.J. AND NORVIG, P. 1995. *Artificial Intelligence: Modern Approach.* Prentice Hall, Upper Saddle River, NJ.

SAMFORD UNIVERSITY. 2003. PBL background: definitions. *Problem Based Learning at Samford University*. http://www.samford.edu/pbl/definitions.html.

STEPIEN, W. AND GALLAGHER, S. 1993. Problem-based learning: As authentic as it gets. *Educational Leadership*, 25-28.

STEPIEN, W.J., GALLAGHER, S.A., AND WORKMAN, D. 1993. Problem-based learning for traditional and interdisciplinary classrooms. *Journal for the Education of the Gifted 4*, 338-345.

SUDZINA, M.R. 1997. Case study as a constructivist pedagogy for teaching educational psychology. *Educational Psychology Review 9*, 199-218.

TOMEY, A.M. 2003. Learning with cases. *Journal of Continuing Education in Nursing, 34*, 1, 34-38.

TOTTEN, S., SILLS, T., DIGBY, A., AND RUSS, P. 1991. *Cooperative Learning: A Guide to Research.* Garland, NY.

UNITED STATES. 2003. Priority III: A national cyberspace security awareness and training program. The National Strategy to Secure Cyberspace.http://www.whitehouse.gov/pcipb/priority_3.pdf.

WILLIS, J. 1995. A recursive, reflective instructional design model based on constructivist-interpretivist theory. *Educational Technology 30*, 6, 5-23.

WILSON, B.G. AND COLE, P. 1991. Cognitive dissonance as an instructional variable. *Ohio Media Spectrum 43*, 4, 11-21.

Received April 2005; accepted December 2005