IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5122

Innovative Model for Information Assurance Curriculum: A Teaching Hospital

Sanjay Goel and Damira Pon

NYS Center for Info. Forensics & Assurance, BA 310b, 1400 Washington Ave., Albany, NY 12222, USA, {goel,dp1252}@albany.edu

ABSTRACT

The paper presents a novel idea for information security education based on a teaching hospital concept. The model envisages real information security problems from industry and government solved and abstracted into living-cases used for training and education of university students and public-sector employees. 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 involving faculty and students. The paper presents the curriculum and cases developed as a part of this endeavor and discusses the partnerships with government and private organizations. The paper also describes the architectures of the laboratories built to support this "teaching hospital".

INTRODUCTION

There is a strong need for information assurance (IA) education, which stems from the pervasiveness of information technology in business and society. Government and private industry have become dependent on information systems, as they are widespread across all business functions (e.g., procurement, data management, design, analysis and manufacturing). Disruption of critical operational information systems can have serious financial impacts. Losses from security breaches have risen rapidly over the last several years and exceeded $200 million in 2003 (CSI/FBI Report, 2004). Greater concerns include threat to human life and property from disruption of network-dependent critical infrastructure operations for elements such as dams, power grids, and radar controllers. Organizations are cognizant of these information security risks and attempt to protect information assets through controls based on industry standard guidelines and advisories that are issued by security agencies. However, security threats continue to escalate and organizations continue to lose money. Sources of security threat are not necessarily external malicious hackers, but also trusted insiders (disgruntled employees or employees with ideological agendas). In fact, many security breaches are caused by human errors (e.g., network misconfiguration and careless password disclosures). Each employee with network access poses a threat to an organization. Most employees are expected to use computers to fulfill primary job requirements and they learn the use of computers out of necessity. However, security does not influence their employment directly, nor are there serious negative consequences of accidentally causing security breaches. As a result, employees do not have strong incentives to gain security education. Although the information security competency of the workforce ranges from the largely amateur to advanced, all users hold responsibility for and need to be trained in security.

One priority of the President's National Strategy to Secure Cyberspace (United States, 2003) was to promote and ensure that "businesses, general workforce, and the general population" were able to "secure their own parts of cyberspace", training and education programs that supported the "Nation's cyber security needs" were developed, current federal cyber security programs were improved, and industry-supported certifications were 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 country's critical infrastructure is controlled by private industry. Training private industry workforce needs to be a national priority to ensure information systems and critical infrastructure protection. Other segments of the population also need training. Children in K-12 grades are increasingly exposed to information technology and though adept at using computers, are very gullible and make easy targets for Internet criminals and pedophiles. Similarly, our elderly are easily swayed by lack of technical understanding, as well as awareness of computer crimes and become easy victims of hackers. Universities need to be dissemination catalysts for curricular material across society by directly providing education, or training educators in schools and community colleges that cater to a large segment of the population. Bishop (2000) describes the necessity for information security education at multiple levels (training, undergraduate, masters, and doctoral) and the varying types of skills learned for each, all of which are relevant in information security education.

Dissemination of IA education encompasses distinctive issues. Technology changes quickly and new threats are constantly emerging. Consequently, knowledge rapidly becomes obsolete and the workforce needs to be regularly reeducated. Institutions providing IA training 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 disciplines such as computer science, business, information science, engineering, education, psychology, criminal justice, public administration, law, and accounting The broad interdisciplinary nature of IA requires several specialists to collaboratively teach the curriculum and integrate different perspectives and teaching styles into cohesive delivery. For effective collaboration, different departments should contribute and benefit mutually. If not crafted carefully, such a multidisciplinary environment can lead to non-integrated disparate courses.

We present a pedagogical model based on a "teaching hospital" concept that addresses the issues introduced above and discuss its implementation at the Center for Information Forensics and Assurance (CIFA) at the University at Albany. The subsequent content is organized as follows: Section 2 reviews existing IA programs, Section 3 presents the "teaching hospital" model, Section 4 describes curriculum developed for the teaching hospital and Section 5 presents cases developed for teaching hospital education. Section 6 contains concluding remarks and future plans.

EXISTING IA PROGRAMS

Several universities have active programs focused on developing IA curriculum, such as, Purdue University (Dark & Davis, 2002), Carnegie Mellon University, University of Oklahoma, and United States Military Academy (Hoffman, et al., 2003). These institutions have developed a comprehensive set of curricula that spans several departments and is varied based on strengths and capabilities of existing faculty and curricula. Most have developed IA educational laboratories that allow

students to have hands-on experience to launch and protect against different attacks. In addition, most of these schools have utilized government grants created to foster IA education as well as to improve the security of the nation.

The National Security Agency and the Department of Homeland Security sponsor the creation of National Centers of Academic Excellence in Information Assurance (National Security Agency, 1999). This program follows through on some statutes listed within the National Strategy to Secure Cyberspace. To become one of these centers, there are criteria for measurement of acceptable IA programs. Within these evaluation criteria, the need for an interdisciplinary program is established, citing beneficial contributions from various fields such as law and management instead of solely 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). This model is based on federal regulations and is composed of three different levels of instruction: Awareness, Training, and Education. For each of these instructional levels, there is an associated learning objective; 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, demos, case studies, and hands-on learning and Education furthers training with discussions, readings, and research. As the level of instruction is applied to audiences within IT and information security, there is more emphasis on practical hands-on learning. Several other models exist 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 with lectures, group collaboration, guest speakers from industry, and case studies. Hoffman et al. (2003) discuss the "hear-see-do" paradigm within technological fields and the estimation 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 for students to both learn in and do research.

TEACHING HOSPITAL MODEL

Teaching hospitals have been used extensively for medical training since the twentieth century. They enabled control on medical students production, and medical education quality monitoring. Training is provided to medical students and doctors-in-training through direct clinical experience of treating actual patients under the supervision and guidance of attending physicians in medical wards. Medical teaching hospitals are important because their students need hands-on experience; otherwise, it is very difficult to translate the abstract knowledge from the literature into a diagnosis. This practice enables residents to crystallize theoretical knowledge into field knowledge, which they can utilize when practicing 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 is learned within the classroom in the outside world. Teaching hospitals tend to offer "a comprehensive array of facilities" as well as possess sufficiently high volumes of patients from whom students can gain experience. Teaching hospitals have also traditionally "conducted 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 eventual application of theory into practice.

At Kansas State University's Engineering Learning Center (Azadivar & Tucker, 2000; Kramer et al., 2002), a teaching hospital model is implemented. Azadivar and Tucker (2000) detail reasons for incorporating this concept within the engineering education. They describe the teaching hospital method; medical students help real patients with medical illnesses and problems under the supervision of experience professionals. This practice allows for application of what is learned within the classroom to live subjects in the "real world" environment with "real world" constraints (time and budget). A teaching hospital analogy (Kramer et al., 2002) is made where the teaching hospital model is converted into a teaching factory. The hospital is replaced with the Engineering Learning Center (ELC), the medical doctors with experienced engineers, the medical interns with engineering/business interns, patients with manufacturing companies, and the medical equipment with engineering tools and manufacturing equipment. Within their model, the ELC also incorporated cooperation among engineering, business, and computer science students and the results were "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 becomes obsolete quickly 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 propose a "teaching hospital" for training students in the IA field where students receive hands-on experience by working on real problems under the supervision of researchers and practitioners in the field. Our model attempts to emulate a teaching hospital by structuring an integrated program in IA research and education through collaboration with other organizations (problem-rich in the area of information security). Since the IA potential student population is large and few researchers in the area are available, it is not feasible to send students to directly apprentice with researchers in the field. As an alternative, cases from state and law enforcement agencies are utilized. Real problems are abstracted into living cases, which are used for classroom instruction; a constant stream of cases can thus be generated. This approach allows the context of real problems to be introduced into education and maintains the currency of the curriculum as newer cases replace (or supplement) older cases. An active research program and a mechanism for abstraction of projects into teaching cases are required for the constant infusion of new material.

Partnerships

CIFA has strong partnerships with the New York State (NYS) Police Computer Crime Laboratory (CCL) and the New York State Office for Cyber Security & Critical Infrastructure Coordination (CSCIC) and is responsible for employing this "teaching hospital" model for IA research and education. The primary responsibility of CCL is to investigate computer crimes (i.e., computer fraud, theft of information, pornography, malicious code, music piracy, and unauthorized intrusions into networks) in NYS. Most work involves forensic analysis of data, hardware, and networks. These practices draw heavily from literature on computer architectures, software design, networking, and law. A large portion of data is sensitive due to legal underpinnings. However, once 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 NYS agencies to which it issues advisories when new information security threats are identified. CSCIC also creates and disseminates security policies to NYS agencies and acts as an advisor for policy implementation. CCL is a source of computer forensics and incident handling cases and CSCIC is a resource for cases in the area of security policies and security risk assessment.

Facilities

In medical hospitals, implementation of a "teaching hospital" is easier as a large number of medical wards already exist where physicians treat patients and residents can shadow physicians. In the IA field, there is no such network of existing facilities where security problems are actively solved. Similar to teaching hospitals, institutions that educate in IA should have appropriate facilities with sufficient equipment to enable

hands-on learning. Instead of a hospital with beds, x-ray machines, and blood analysis labs, our facilities consist of computer laboratories for both teaching and research. Some fundamental issues with the design of security laboratories are in ensuring that laboratory exercises do not accidentally cause disruption of services in other networks. For this reason, implemented network architecture allows the labs to be disconnected from the university network whenever experiments or labs with the potential of causing network damage are executed. In addition, Internet access using a connection independent of the university to support activities such as deployment of honey nets is integrated. Both educational and research laboratories are connected to each other through a network connection independent of the university network to allow communication and sharing of files between both labs. Wireless networks allow research in wireless security and to enable flexible reconfiguration of lab architecture.

Laboratory hardware and software needs to be diverse so the environment in which a real problem occurred can be replicated. The educational laboratory is designed to facilitate rapid reconfiguration of machines changes that occur as a part of laboratory exercises can be eliminated to return the laboratory its normal setting.

CURRICULUM DEVELOPED

Course material development for IA requires experts from several disciplines. Students interested in the curriculum also come from various backgrounds including, public policy, law, computer science, business, and information science. Therefore, it is often difficult to design three-credit courses where all material is relevant to all students. Furthermore, since 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. These courses coincided with the interests of our major partners. Incident Handling interested CCL employees and Risk Analysis appealed to the CSCIC workforce. A diverse team developed these courses. Domain experts acted as content developers for the teaching material. A pedagogy expert provided advice on the structure, evaluation, and organization of courses. Practitioners evaluated content and provided examples and cases. Much content required for the courses was relatively new and not available in textbooks; hence, content was compiled from various sources. The courses had strong hands-on components and classes were separated into 50% classroom instruction and 50% 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 and analyzing log files, and writing policies.

The first set of courses offered were taught by an instructor who did not participate in the development of the curriculum. There was strong interest in enrollment from both government employees and university students. However, many students had to be declined due to roster limitations. *Glen Martin Associates*, an independent consulting firm, performed curriculum evaluations. The firm prepared student questionnaires and interviewed students as well as curriculum developers to perform their assessment. The course feedback was positive with a satisfaction rating of more than 2 out of three for most categories dealing with course content as well as instruction. In the Risk Analysis course, the survey showed that the student knowledge varied significantly at the beginning of the course from none to good. However, at the end of the course their knowledge invariably went up to 80% good and 20% very good (the primary goal of the course). The course received a rating of 5.4 out of 6 for the category in which students would recommend the course to others and for instructor presentations, a rating of 5.7. Incident Handling course ratings were similar: lower 2's out of 3 for knowledge/skills learned from the course, and ratings between 4-5 out of 6 for the differing course components.

One comment was that the curriculum was content-dense and contained too many topics. For instance, the Risk Analysis module contained material on security policies as well as some security fundamentals. In addition, due to their varying backgrounds, some students were already familiar with some subtopics of the courses. To address this issue, the curriculum is being expanded into five course offerings by splitting the content of the initial two offerings. The five modules are: 1) Security Fundamentals, 2) Risk Analysis, 3) Incident Handling, 4) Computer Forensics, and 5) Security Policies. These topics will be narrowly focused and all the background material will be covered in the prerequisite security fundamentals class.

To achieve more widespread dissemination of our curriculum, we are working with our partner CERIAS at Purdue University to offer these courses in distance delivery format. The courses will be available via WebCT with instructor audio, video, and PowerPoint inset as a student goes through the curriculum. In the online dissemination, students work alone on the material without interaction among peers or instructors and it is more difficult to maintain attention. To retain student attention, each lecture is divided into 20-minute segments with a clear set of objectives at the beginning of each segment and evaluation material at the conclusion of each segment. At the termination of an entire lecture, either a case or an elaborate quiz is provided for the student to assess retention and understanding of the material.

Cases Developed

The effectiveness of case-based learning has been highly researched. Case-based education has been used for instruction within many schools for various disciplines and is an established method of teaching. 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, generalization of cases through recognition of similarities, and relation of cases to tasks at hand. Using case studies within a teacher education program, Tomey determined that there are many advantages to case-based learning. This learning style "blends aspects of the cognitive and social constructivist models of teaching and learning" (Mayo, 2002) and promotes "active, self-directed learning" and there is 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). While case-study incorporation may decrease lecture time, it is determined to be a rational "trade-off between breadth and depth of knowledge covered" (Sudzina, 1997). When doing a case study on a UK business school, Needham (2001) stated one of the problems with case studies is keeping them current and relevant due to time-consuming and expensive production. CIFA deals with this issue by incorporating public and private collaborators, as well as a research component. Real problems from these organizations are continually being introduced within the research lab and abstracted into cases, thereby ensuring relevance and currency within the field.

To support hands-on exercises, two types were developed: 1) basic skill exercises, and 2) context-based cases. Basic skill exercises were primarily focused on use of tools for network monitoring, penetration testing, password auditing, etc. Context-based exercises were derived from real cases our partners experienced in the field. Cases for risk analysis were developed from the audit reports of public and private organizations. Fictitious names for the organizations were introduced to prevent cases from adversely affecting the security of these organizations. Real cases from the CCL are being actively investigated for computer forensics and incident handling curriculum.

CONCLUSIONS

We have developed an innovative paradigm of information security education at the University at Albany in partnership with the CCL and CSCIC. This learning paradigm utilizes a "teaching hospital" approach whereby real problems from government agencies and industry are brought into our research laboratory, made into "living cases", and

solved by teams of faculty, 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 are then documented and disseminated to the state agencies. By working closely with the public-sector agencies in developing information security curriculum, we provide a unique and rich learning environment for university students taking courses, and ensure that government employees are well trained in the practices of information security.

ACKNOWLEDGEMENTS

This work is done with partial support of NSF 01-67 Grant 020657151 and FIPSE Grant P116B020477. The authors would also like to acknowledge the other team members of CIFA, including, Laura Iwan, Thomas Hurbanek, Robert Bangert-Drowns, Jagdish Gangolly, Peter Bloniarz and George Berg for their support in this work.

REFERENCES

Azadivar, F., & Tucker, J. (2000). An Engineering Learning Center: Description, Results, and Lessons Learned, *In the Proceedings of the 30th ASEE/IEEE Frontiers in Education Conference*, 1-5.

Bishop, M. (2000). Education in Information Security. IEEE Concurrency, Retrieved on September 21, 2004 from http://nob.cs.ucdavis.edu/~bishop/papers/2000-educieee/2000-educieee.pdf

Dark, M.J., & Davis, J. (2002). Report on Information Assurance Curriculum Development. Curriculum Development Workshop, CERIAS, Retrieved on September 21, 2004 from http://www.cerias.purdue.edu/education/post_secondary_education/undergrad_and_grad/curriculum_development/information_assurance/report_info_assurance_cur_dev.pdf

Gilbert, C. (2003). Developing an Integrated Security Training, Awareness, and Education Program GSEC Practical Assignment version 1.4b, SANS Institute. Retrieved on September 21, 2004 from http://www.sans.org/rr/papers/47/1160.pdf

Hoffman, L.J., Dodge, R., Rosenberg, T., & Ragsdale, D. (2003). Information Assurance Laboratory Innovations. 7th Colloquium for Information Systems Security Education, Washington, DC.

Hsu, C. & Backhouse, J. (2002). Information Systems Security Education: Redressing the Balance of Theory and Practice. Journal of Information Systems Education, 13(3), 211-218. Retrieved on September 21, 2004 from http://www.jise.appstate.edu/13/211.pdf

Kramer, B.A., Tucker, J., Jones, T., Beikmann, M., & Windholz, R. (2002). The Engineering Learning Center: A Model for Mentored Product Innovation. *In the Proceedings of the 32nd ASEE/IEEE Frontiers in Education Conference*, Boston, MA, 24-29.

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. Retrieved on September 24, 2004 from 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.

National Security Agency. (1999). Criteria for Measurement. Centers of Academic Excellence, Retrieved on September 25, 2004 from 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*.

Russell, S.J., & Norvig, P. (1995). *Artificial Intelligence: Modern Approach.* Upper Saddle River, NJ: Prentice Hall.

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. *J Contin Educ Nurs, 34*(1), 34-38.

United States. (2003). Priority III: A National Cyberspace Security Awareness and Training Program. The National Strategy to Secure Cyberspace, Retrieved on September 28, 2004 from http://www.whitehouse.gov/pcipb/priority_3.pdf