TEACHING INFORMATION SECURITY TO ENGINEERING MANAGERS

Julie J.C.H. Ryan

Abstract — The concepts and practice of information security have for the most part been contained within Computer Science or Electrical Engineering departments in academia. However, as the information age matures and pervasive IT supports every engineering discipline, a requirement to teach information security to engineering managers emerges. The challenges of presenting concepts, theories, and approaches to engineering managers are many when those concepts have been developed from a decidedly computer-oriented perspective. This paper explores experiences, challenges, and innovative solutions based on the last five years of educational efforts at the graduate level.

Index Terms — Computer Security, Education

INTRODUCTION

There are two traditional fields of academic research and education related to information security: computer security and electrical engineering. This makes sense from a technology research and development point of view, in that the enabling technologies for information security are predominately constructed from software and hardware.

This worked well from a practitioner point of view as well, until recently. During the era of mainframes and segregated computing centers, specialists in information security needed to be computer scientists or electrical engineers.

A change, however, has occurred in both the ubiquity of computing equipment and in the level of specialization required to operate such equipment. As such, it is not uncommon to see system administrators whose highest level of formal education is high school, application developers whose area of specialization is in graphics arts or sociology, and Chief Information Officers (CIO) whose education is in business administration.

The challenge in the information systems security field lies in the fact that while each of these individuals needs to understand and be able to apply the principles of information security while performing her or his job, none of them is qualified to enroll in an educational program offered through a computer science or electrical engineering academic department. Nor would they likely benefit in a career sense from advanced education in computer science or electrical engineering.

This is where the opportunity of expanding the traditional reach of information security education arises. There is a demand for information security education beyond computer science and electrical engineering, but challenges exist when transferring concepts out of the language of computer engineering and applied mathematics to more general concepts and business focused solutions.

BACKGROUND

The field of information security encompasses the practices of communications security, computer security, operations security, administrative security, physical security, personnel security, and environmental security. The practice of information security is normally defined as protecting the security attributes of information assets, detecting a compromise or attack on those security attributes, and being able to react to and correct such situations. Security attributes are normally defined as comprising the confidentiality, integrity, and availability requirements of information assets or systems.

The need for a formalized profession in computer security is regarded as first publicized by the Defense Science Board in the landmark 1970 document "Security Controls for Computer Systems." Besides calling for the education of professionals in the techniques and processes associated with computer security, the report also pointed out that "[p]roviding satisfactory security controls in a computer system is in itself a system design problem [requiring a] combination of hardware, software, communication, physical, personnel, and administrative-procedural safeguards…"[1]. In a word, the complexity of the information security problem was characterized as requiring the specialty of systems engineering.

Three decades later, the growth of computing capabilities has been explosive and characterized by inter-connectivity. Ubiquitous networks link every kind of computer imaginable, from the navigation system in cars [2] to the pacemakers in hearts [3]. The use of computers is pandemic in every engineering field. Program managers use computer networks to manage geographically dispersed and asynchronous workforces [4]. Doctors, lawyers, and accountants use computers as fundamental and important tools in their professions. Once an expensive investment reserved for wealthy corporations, now computer systems are necessary adjuncts to even the smallest businesses [5].

---


0-7803-7961-6/03/$17.00 © 2003 IEEE

33rd ASEE/IEEE Frontiers in Education Conference

F4C-1
And the security considerations are extraordinary. As stated succinctly by the Joint Economic Committee (JEC) of the US Congress:

Computer networks connect and control everything from pipelines to stock exchanges. At a speech given on March 23, 2001, to the Partnership for Critical Infrastructure of the U.S. Chamber of Commerce, Condoleezza Rice, United States National Security Advisor said, “Today, the cyber economy is the economy. . . . Corrupt those networks and you disrupt this nation.” [6]

THE CHALLENGE

Engineers, and Engineering Managers, have sufficient other things to do besides worrying about security. Getting them to understand the challenges and reasons why they should be concerned is an enormous challenge. Once they do understand and are interested in educational programs related to security, there is a secondary challenge inherent in turning what has traditionally been a computer science and math oriented approach into material that is meaningful and useful.

At the George Washington University (GWU), we have been teaching information security concepts to engineering managers since 1996. Over this time period, we have developed an approach that provides a comprehensive understanding to the student in six graduate level courses (18 semester credit hours). At the end of the program, the student is awarded a Graduate Education Certificate in Information Security Management. To date, we have awarded over 100 of these certificates and have approximately 100 students enrolled currently at various stages in the program. The courses in the Certificate Program may also be used towards a Master of Science degree.

The program was developed as a direct result of a need in the local community for individuals knowledgeable in the field of information security, particularly in the context of support to federal government programs. It has expanded to the point where the student body represents institutions from around the world and from every profession, including museum sciences.

There are two keys to the success of the program. One is presenting the concepts of information security in a management context, providing the student with the ability to see how security considerations affect management issues. The second is our approach to information security in a systems engineering context, rather than as an add-on or separate consideration.

Underlying the specific elements of the program is a recognition that the concepts of information security need to be explored in the original language of their development but then integrated into an overall holistic approach. This is important in order to give students an appreciation for the science that went into developing the concepts. It is also important in order to give the students a structure in which to parse the concepts in a way that makes sense to each of them, independent of what their background may be. As an example of how we implement this philosophy, the concepts of physical security are taught first in the language of physical security experts, using textbooks written for physical security experts. The course projects, however, require the students to integrate those concepts with other concepts associated with security, such as protection profiles in accordance with the Common Criteria.

This approach requires that the professors be facile with not only all the concepts but also with all the languages of the specialties. Working in group projects enables students to contribute their unique perspectives and skills to the 'accidental' education of their classmates. The result is an education program that fits the requirements of homeland security workers, network administrators for art galleries, and civil engineers. Each learns quite a lot about the history, concepts and applications of information security but is able to explore through projects and research papers the elements that fit most closely to their career requirements.

The Students

The students in the program come from all walks of life and professions. Currently in the program we have students from Brazil, India, Pakistan, Saudi Arabia, Africa, and Indonesia. We have students with jobs as high school teachers, sales representatives for high technology corporations, network administrators, management consultants, radio frequency engineers, government program managers, and members of various militaries.

No single assumption about core knowledge can be made about what the students know (or even should know). There is no common level of math background. Many students have never composed a line of computer code. There is no common appreciation for how computers or networks operate. The understanding of how educational processes work is uneven. Even the ability to write a compound sentence can not be assumed: students with degrees from fairly prestigious undergraduate institutions are as likely as students from less prestigious colleges to write poorly and to make citation errors.

A fascinating insight into the current information technology (IT) workforce is gained through observation of the students. Many of our students came into the IT workforce by chance rather than choice. With the explosion of IT in the workplace and the concomitant demands for an IT workforce, some simply gravitated towards IT-related jobs through talent and natural inclination. Others found that there were no other choices available to them. Others yet saw the IT field as an opportunity for them to escape the binds of a suffocating career choice.

This presents a particular challenge to the educational institution: how to convey a set amount of knowledge to a
student body with no guaranteed level of skill in any particular field. And yet, the necessity for teaching the material and for making sure that the students all achieve the terminal learning objectives is a critical requirement for both the success of the program and for national security in the information age.

**Educational Approaches**

Teaching these responsible yet unevenly skilled students the precepts of information security has been a challenge. Over the past five years, we have developed methodologies that assist in assuring that even the least skilled student achieves the learning objectives of the program.

A varied approach to education in the classroom is naturally part of our approach. One of the first things we learned is that lecture alone doesn't work, even when the professor is amusing and entertaining. We do not focus on lectures as the primary means for conveying information, but relegate lecture to an adjunct position setting the stage for experiential learning processes.

Group exercises are emphasized, with the goal of each exercise being the application of some element of the learning objectives in real life. Some of the exercises are performed in class, while others require a longer term out of class approach.

Practical applications of technologies are required. For example, every student is required to use asymmetric cryptography to exchange emails with professors. This gives the students both the practical knowledge of how the technology works and what can be done with it as well as an intuitive understanding of what user reactions are likely to be when required to use public key infrastructures.

The use of on-line courseware has proven to be remarkably beneficial in managing the enforcement of reading and comprehension requirements. We use Prometheus, which was developed at GWU and is now owned by Blackboard.com [7]. The students can take part in on-line asynchronous discussions, manage group participation in projects, post files, and turn in homework via the Prometheus interface. Additionally, basic knowledge skills can be enforced through use of multiple choice quizzes that are managed through Prometheus. The ability to set dates when the quizzes are available to the students enforces a pace of activity, while the geographic range of the participation enables professional students who are travelling to maintain continuity with the class even while missing classes.

With the incorporation of all these varieties of techniques, we have seen both the effectiveness of instruction and student satisfaction with the program improve.

**Institutional and Professional Liability**

A potentially enormous problem presents itself in the field of information security education. By definition, we can't teach students how to protect and defend information assets and systems without teaching them how to attack (either in theory or in practice). We go out of our way to caution students on laws, regulations, and morality, but there is always a possibility that a student will abuse the knowledge provided either on purpose or by accident.

This potentially opens the door to liability. Liability follows a breach of duty. The duty required of educational institutions and their professors flows from legislation, regulations, and the common law. Colleges and universities, and professors as well, can be found liable for their acts or omissions where such acts or omissions are negligent.

Clearly, when teaching students potentially dangerous material, it is very important that institutions protect themselves from future problems. To counter any potential liability, it is very important that a policy and procedural framework exist in which the education takes place. The policy defines what is acceptable and what is unacceptable while the procedures enforce and reinforce the policy.

Of course, it is not enough for a policy framework to exist in some dusty drawer or filing cabinet. Four things are required to make a policy effective: first, there must be a carefully crafted and clear statement of the policy, ideally in writing. Second, the policy must be actually passed out and advertised to the people affected by the policy – a policy that is created and placed on the shelf rather than distributed to those to whom it applies is ineffective, practically and legally. Ideally, those to whom the policy applies read it and sign a statement to the effect that they have read and understood the policy. This signed statement can later be used in court, if necessary. Third, there must be a process for detecting whether or not the policy is being followed: a policy that the organization or institution does not seek to enforce is ineffective. Finally, there must be sanctions for violations of the policy, and those sanctions must be applied when violations are detected.

At GWU, we manage this by having a written policy document for the program that both refers to University and School policies and clearly states the policies enforced for the program. Key elements of our policy document are requirements for compliance with laws and regulations, compliance with academic integrity standards and procedures, and a discussion of penalties for non-compliance.

Besides requiring all new students to read and sign the policy, we incorporate the elements of the policy document into our educational material. This practice both serves to reinforce the message and to teach the students why policy statements are critically important to practice of information security.
The Program

The six classes in the program are structured around the security engineering phases commonly referred to as Protect, Detect, and Correct. The use of the engineering phases provides a neat way to address the major engineering considerations in a framework that makes intuitive sense and is easily applied. It also nicely divides up the material to be taught into manageable chunks.

The Phases of Information Security Engineering

The Protect phase refers to all the things that are incorporated into a system (however large or small) that are designed to protect the system and its processes from security related problems or failures. Protection elements span computer technologies, such as anti-viral software and firewalls, personnel security procedures, such as background checks on prospective employees, to physical security elements like guards, gates, and locks.

Engineering a systemic solution to the protection problem requires that threats be assessed, vulnerabilities analyzed, failure results considered, and countermeasures applied. The driving concept is risk management rather than risk avoidance. Since it is well recognized that it is impossible to have perfect security, even with unlimited resources, the goal of engineering the elements of protection is to spend whatever resources are available in the best possible manner. Not all the resources available, however: some resources need to be reserved for engineering the elements of the detection and correction phases of the security challenge.

The Detect phase refers to all things that are incorporated into a system to detect problems. There are four classes of problems that need to be considered when designing detection capabilities.

First, there is the class of problem that was protected against. This is the class of problem that was recognized as being worthy of expending resources in order to gain some level of protection. There are two things that need to be detected in this class of problem: the failure of the protection mechanism and the occurrence of the problem which was protected against. Protective mechanisms fail through environmental degradation, mistakes, or malicious behavior. It's a fact of life that they not 100% reliable over time. That makes checking the protective mechanisms a critical element of detection processes. Detecting the failure of the protective mechanism is not enough, however; the occurrence of the problem must be detectable as well.

The second class of problem that should be considered is the problems that were not protected against. The reasons for not protecting against these problems could stem from lack of resources or could reflect a fundamental impossibility of realistic protection. For this class of problem, the only protection the system has is inherent in a speedy detection of the problem occurrence.

The third class of problem that should be considered is the occurrence of stealthy or counter-detection attack activities. These are potential insults to the security attributes of the system that are designed to not be detected. Depending on the sensitivity of the enterprise operations, a comprehensive detection program may need to address these problems.

The fourth class of problem that should be considered is the occurrence of problems which were unknown. It is a truth that no knowledge space is perfect; it is also true that adversaries are unceasingly innovative in finding ways around protection mechanisms and into enterprise operations. A comprehensive detection program, then, must include the ability to detect previously unclassified abnormalities in the operational environment that may indicate an attack or security failure is occurring.

The Correct phase comprises all the elements of reaction and recovery to a security failure or attack. This phase includes business continuity efforts, crisis management, and information asset recovery.

The Classes

The six classes that comprise the core courses for our program in information security management address the challenges of protection, detection, and correction in a system engineering framework that both conveys the engineering challenges inherent in an environment and emphasizes the continuing need to revisit solutions over time. Further, the moral and ethical implications of activities are continually stressed.

The first course in the program is an overview course: Management of Information and Systems Security. This course lays out the framework for systems engineering holistic information security in a modern enterprise and introduces all of the concepts that are covered in the subsequent courses. Technical subjects, such as malicious software, are covered as well as non-technical subjects, such as policy requirements. The purpose of this course is to give the students a broad but not deep comprehension of the subject as a whole so that they will know how each piece fits into the larger framework in later classes.

In this class, the reading and lecture material are supported through three projects. The first project is to install PGP, create a key pair, exchange public keys with the professor, and ultimately exchange an encrypted email. This simple exercise is a remarkably powerful learning experience for non-computer scientists. It is regularly singled out as an 'ah ha' moment by the students. The second project is to research technologies that assist in achieving security goals. The project requires them to analyze the usefulness, the complexity, and the costs associated with the technologies. This gives each the knowledge that a manager would need in order to make rudimentary decisions on how to invest resources in security technologies. The third project is an analysis on the state of
the hack. This research project gives the students an appreciation for the complexity, ease, and reach of contemporary network attacks.

The second course in the program covers the legal and regulatory framework that impacts the practice of information security: Legal Issues for Information Security Managers. This is a critically important class due to the potential for inadvertently running afoul of laws and regulations in a misguided attempt to protect information assets and systems. This class also serves to educate the students on the moral and ethical implications of activities such as unauthorized system access, intellectual property piracy, and other unique challenges of the information age. Students in this course are required to write policies and to analyze intellectual property issues. The final examination is a complex contractual and liability analysis covering electronic commerce, security failures, and software development.

The third course in the program is the first of two courses covering the Protect phase of security engineering: Managing the Protection of Information Assets and Systems. This class requires the overview course as a prerequisite. Because the vast majority of efforts in the information security field have been spent on elements of protection, it would be impossible to do a credible job of addressing every element of protection in only one course. This course covers every protection concept and approach except those related to cryptography. Included in this course are physical security concepts and mechanisms, personnel security concepts and approaches, operational security concepts and approaches, and computer security protections. The computer security protections covered include technologies, such as firewalls, password protections, and access mediators. An overview of the Common Criteria is included as well as the historical development of security concepts. This course provides students with the fundamental skills required to acquire computer security capabilities, manage the security in a complex environment, and be able to judge the levels of protection in an operational context.

There are three projects required in this course, all of which are performed in groups that stay static over the semester. Each group is assigned a hypothetical scenario—a bank, a hospital, a regional air traffic control center, or the like. The first project is for the group to develop a physical security plan for their scenario. The plan must include technologies, egress routes, traffic analyses, and the like. The second project is to develop a personnel security plan and integrate it with the physical security plan. This also includes technologies, procedures, and risk analyses. The final project is to select a unique information technology application that could be used in the environment and develop a Protection Profile in accordance with the Common Criteria at EAL-3 or above. The students are not permitted to select common applications like firewalls or smart cards but must select something much more specific to their hypothetical scenario. As a result of these three projects, students have a very deep appreciation for the contributions of the different specialties of security in an operational environment.

The fourth course in the program is the second of two courses covering the Protect phase of security engineering: Management of Cryptographic Systems. This course covers the critical technology of cryptography and all the security capabilities enabled through use of cryptography. These enabled applications include secret communications, digital signatures, electronic commerce, data integrity assurance, and transaction integrity. Both symmetric and asymmetric cryptographic algorithms are discussed and used in this course. The students use and research many different cryptographic algorithms in the course. As a result, they are extremely conversant with the benefits and challenges associated with the use of cryptography and the life cycle management issues.

The fifth course in the program is a course covering the Detect phase of security engineering: Auditing, Monitoring, and Intrusion Detection for Information Security Managers. This class requires the overview course as a prerequisite. This course covers the practice of auditing (at all levels), the use of technologies for intrusion detection, and the design of detection capabilities in an operational environment. Students are provided with the skills to rationally decide where to put detection support capabilities in order to maximize the effectiveness of the capabilities in the context of the operational environment.

Projects in this class include performing a security analysis of an operational environment, writing an audit plan, and performing forensics analysis on an example data set.

The sixth and capstone course in the program is a course covering the Correct phase of security engineering: Planning, Correction, and Restoration for Infosec Managers. This class requires the overview course as a prerequisite. This course teaches the students how to handle crises from a managerial perspective and with an emphasis on information security related crises. Students develop business continuity plans, dry run crisis management exercises, and examine the state of the art in reactive and corrective technologies. The capstone project for this class is for students to participate in an emergency scenario, structured around an information security failure. The students discover the problem through symptoms revealed by the situation mediators and must analyze their way into discovering what the actual problem is and what steps to take to mitigate the problem. It is a powerful experience that demonstrates to the students the complexities and challenges of experiencing problems in real life, giving them an opportunity to practice their skills in a no-penalty environment.
CONCLUSIONS

Providing information security education to technical and engineering managers is a critical need for the current and future economy. The ubiquity of networking and the growing requirements for interconnectivity in commercial activities of all sorts define the centricity of IT in all aspects of professional life. Managing the vulnerabilities that exist in IT infrastructures requires attention to security engineering.

There are critical elements that must be attended to, however. One element is the provision of security related education to students of various backgrounds and capabilities. Another element is the care inherent in structuring a program that provides information and capabilities while safeguarding the institution and professors.

Developing a program that manages both elements in the context of providing critical skills to the IT workforce can be a valuable addition to existing engineering management programs and to local economies.

REFERENCES