A Curricular Strategy for Information Security Engineering

Richard Smith
Department of Computer and Information Sciences (formerly QMCS)
University of St. Thomas

Abstract

Existing textbooks and training materials in basic information security do not reflect the actual problem solving techniques and practices in the field of information security engineering. In general, texts focus on memorization of a broad range of facts related to modern information security practice. Analytical techniques, when present, often focus on mathematical foundations of cryptography, the inner workings of security protocols, and perhaps the logical derivation of formal security policy statements. In practice, information security engineering involves a life cycle starting with requirement analysis, progressing through design analysis and deployment, and repeating the cycle following a period of system monitoring and incident response. A fundamental activity in the practice of information security engineering is the assessment of *security perimeters* that divide a system into more-trustworthy and less-trustworthy components. This type of analysis is applied at every level of an information security system to yield an overall assessment of its security. Perimeter assessment requires that a student learn fundamental features of computer systems at the hardware, operating system, application, and network level. This yields a coherent curricular strategy that incorporates certain classical elements of cryptographic analysis (e.g. assessment of key strength), engineering requirements analysis, and fundamental elements of computer engineering.

Introduction

There has been a significant growth in post-secondary courses and majors in information security. This includes the topics of computer security, network security, cryptography, and *information assurance*. Agencies of the US Government, notably the National Security Agency (NSA), often use that final term to capture all aspects of information security. To promote security training at the post-secondary level, the US Government started evaluating course offerings and degree programs in 1998. As of 2007, over a hundred 2-year, 4-year, and graduate programs have been evaluated and certified as meeting the published courseware standards. Colleges and universities that meet additional criteria are designated Centers of Academic Excellence by the NSA. In 1999, seven schools were so designated; as of 2007, over seventy schools had been so designated (NSA, 2007).

However, there is currently a gap in the textbooks, curricula, and training materials for information security. At one end, vendors like Cisco and Microsoft provide specific technical training for their products, and this training often leads to “certifications” of

various sorts. This training focuses on technical proficiency with specific products, and provides a general outlook on information security only as an afterthought. At the other, collegiate textbooks and related curricula educate students in technical aspects of cryptographic algorithms, security policy models, protocol analysis and other abstract elements of information security. These courses focus on the mathematical foundations of security; a typical textbook is (Bishop, 2005). The few books that fall between these extremes (i.e. not specific to products and not focused on mathematical foundation) provide a superficial introduction at best. While such books don't require a background in advanced mathematics, students can't really absorb the material except through memorization, since they rarely provide practical skills to learn.

Many computer science degree programs across the US, including ours at the University of St. Thomas (UST), have far fewer students today than we did at the top of the "dot com boom" in the late 1990s. Our department performed a self-evaluation in 2004 that identified several growing areas that we might develop programs in, including information security. Based on that report, the dean of the College of Arts and Sciences identified information security as a program the department should develop.

The following sections describe the requirements for the program, detail the courses to be offered, and describe the introductory course contents. The introductory course may well be key to the success of the program: it is intended to serve the university at large by providing solid information security training with minimal prerequisites, and it is also intended to help recruit students to the information security major.

Curriculum Requirements and Alphabet Soup

When we started developing an information security curriculum at the University of St. Thomas (UST), we knew that a classical, mathematically-oriented information security curriculum would not be practical. The Department of Computing and Computational Sciences (formerly called "Quantitative Methods and Computer Science") focuses on computing applications, not on theoretical computer science or lower-level computer engineering concerns. We did not have courses in place to prepare students to study abstract security models or to analyze cryptographic algorithms or protocols. Instead, our curriculum would focus on the high-level skills for information security practitioners.

Three factors have determined the curriculum: university requirements, department requirements, and external requirements. Our department resides within the College of Arts and Sciences, and our majors must fulfill the requirements for a liberal arts degree. The department has never sought accreditation for its programs since it provides little coursework in theoretical computer science, as required by a classical computer science major.

The department's majors generally require programming, data structures, applied statistics, and system analysis, plus additional courses depending on their specialty. We are also trying to offer more courses that appeal to non-majors. When we have offered

security courses under “Special Topics” they drew respectable enrollments even without being required for any particular major. Since the department does not try to offer accredited programs, our external influence is primarily from potential employers of our graduates.

In developing the computer security curriculum, we sought input from alumni, from potential employers, and from professionals within UST who had information security responsibilities. We also decided to pursue US government certification of our curriculum.

Government certification involves the following entities and acronyms:

- IACEP – Information Assurance Courseware Evaluation Program – a program administered by the NSA that certifies post-secondary schools that offer courses conforming with US government training requirements
- NSTISSC – National Security Telecommunications and Information Systems Security Committee – a multi-agency committee that originally developed the US Government standards for training information security professionals
- CNSS – Committee on National Security Systems – the committee that replaced the NSTISSC and now publishes the training standards.
- NSTISSI – NSTISSC Instructions – a standard “instruction” originally developed and published by the NSTISSC, and now under the purview of the CNSS.

If an information security education program seeks to be certified under the IACEP, it must meet training requirements for any of the five positions described in the following NSTISSI:

- NSTISSI 4011 – Information Security Professionals – individuals responsible for the analysis, design, specification, and assessment of information security.
- NSTISSI 4012 – Designated Approving Authority (DAA) – a special role in the US Government who has the final authority to approve the security provided by a system and place it in operation.
- NSTISSI 4013 – System Administrators in Information Systems Security – an administrative role that involves a lot of government-specific security expertise.
- NSTISSI 4014 – Information Systems Security Officers (ISSO) – individuals who oversee information security in particular sites and installations independent of the system administrators.
- NSTISSI 4015 – System Certifiers – another special role that analyzes systems before deployment to ensure that they fully conform with the installation security requirements. The DAA uses their analysis to decide on deploying a system.

We decided to focus on training for information security professionals as specified in Instruction 4011 (NSTISSC, 1994). This is because the overwhelming majority of our graduates go to work for private industry, and the other roles implement government-specific security policies that are rarely used in private industry. The DAA, administrator, and certifier roles were clearly too government-specific to appeal to potential employers.

The same appears to be true of ISSOs: while some employers might desire such individuals in the future, it is not currently a position that many seek to fill at present.

Recommendations from alumni and other security professionals focused on the importance of understanding computer networks and information flow. One recommended following the outline of the Common Body of Knowledge for Certified Information System Security Professionals (CISSP). A superficial comparison indicates that we will cover the CISSP requirements if we adequately address NSTISSI 4011 requirements.

Program Development at UST

We combined input from faculty members with industry experience in information security with input from former students and from computing professionals in the UST community to produce a curriculum for a Bachelor of Arts in Information Security. The principal constraints were to 1) fulfill IACEP certification requirements and 2) be practical to implement within the existing computer science programs at UST.

If we compare the UST program with Whitman and Mattord's (2004) categorization of information security programs, the new program is essentially a Scenario 2 technical program. Two courses form the centerpiece of a program that focuses on technical security topics. In addition to these courses, several important elements of the IACEP requirements are fulfilled by separate courses in Networking and in Operating Systems.

The major program was adapted from the course sequence for other computing majors at UST. The new major requires two security specific courses plus courses in Operating Systems and Computer Networking. Here is a summary of all courses required:

- Lower division courses
  - Introductory course to procedural programming and computing
  - Object oriented programming and data structures
  - Applied statistics
  - Elementary information security (Sec 1)
- Upper division courses
  - Operating systems (OS)
  - Computer networks (Net)
  - Information security analysis (Sec 2)
  - System analysis and design
  - Elective course in the major (e-commerce, databases, etc.)
- Allied requirements
  - Discrete math or digital logic design
  - Workplace communications

The two new courses serve differing roles. The first course, Elementary Information Security, will provide a general course open to both majors and non-majors. It will aim to be both practical and engaging in covering the material. Students appear to be interested

in computer security because it suggests a blend of mystery and crime; the first course will try to give students a solid grounding in information security while fulfilling these less academic expectations. The second course, Information Security Analysis, will cover more advanced topics that require either additional knowledge or a stronger commitment to the topic. In other words, students will face less engaging required topics, like national security standards and policies, as well as more engaging activities like an information warfare exercise.

Here is how the required courses fulfill the IACEP requirements. Instruction 4011 Section 14 lists seven curriculum areas, and they are fulfilled by one or more of four required courses: the security courses (Sec 1 and Sec 2), operating systems (OS), or networking (Net).

- Data communications – Sec 1, Net
- Computing basics: hardware, software, firmware – Sec 1, OS
- Security overview and model – Sec 1
- National information security uses, policies, models – Sec 1, Sec 2
- Specific communications systems and policies – Net, Sec 2
- Planning and designing for security – Sec1, OS, Net, Sec 2
- Specific vulnerabilities; technical and policy solutions – Sec 1, OS, Net, Sec 2

In June, 2007, our department participated in a workshop for information security curriculum development hosted by the University of Minnesota and sponsored by the National Science Foundation. During that workshop we compared curricula across existing and proposed programs at the 2-year, 4-year, and graduate level. The only consensus standard identified for information security curricula were the IACEP requirements. Participants noted that the demand was so high for graduates with information security training that employers were satisfied with IACEP certification. In general, employers were most interested in students with hands-on problem solving experience as opposed to more theoretical training.

In the fall of 2007, the department will submit this proposed program for University approval. Once the major and associated courses are approved, we will submit the curriculum for IACEP certification.

The Security Courses

The two security courses will work together to address security issues that can't be covered in topic-specific courses on networking or operating systems. These courses will introduce students to the information security life cycle, and present more specific aspects incrementally. The first course, the elementary course, lays out the critical concepts so that all students will learn about them. The second course, the analysis course, fills remaining gaps in Instruction 4011 requirements and gives the students more experience with security tools and techniques.

The Elementary Course

Existing textbooks and curricular recommendations do not provide a satisfactory strategy for presenting information security to new students. Some take a theoretical approach in which they present the mathematical foundations first, but this doesn't work with the garden-variety undergraduate who hasn't studied number theory or computability theory. Others try to arbitrarily organize the topics around major security topics or concepts, though this is often thwarted by tight coupling between different topics.

The approach developed for the introductory course at UST is essentially geographical. We start with a single computer and a single legitimate user, and then incrementally expand the user population and the network connections. The progression goes like this:

- Single desktop computer – introduce basics of physical security, security policy objectives ("Don't touch my computer!), intrusion recovery, etc.
- Shared desktop computer – introduce user based access control, process protection in operating systems, and then file and volume encryption as an alternative, which leads to cryptography.
- Local area network – introduce networking basics, and the concept of user roles.
- Viruses and worms – malicious logic that tries to spread.
- Wireless networking – introduces "link layer" encryption
- Internet access – the problem of safe browsing on the web, especially from a LAN. This introduces firewalls.
- VPNs – safely connecting LANs across the Internet. This introduces public key cryptography as used in IPSEC/IKE.
- Socket layer encryption – protecting traffic for Web browsers. This introduces RSA public key encryption.
- PKI – this introduces digital signatures, certificates, and their problems.
- E-Commerce – this introduces the risks to a site that provides service to the Internet, particularly Web service. This covers additional features of firewalls.

The latter part of the progression (starting with link layer encryption of wireless traffic) is based on the organization of an introductory book in network cryptography (Smith, 1997).

This progression introduces the students to the problem of assessing security perimeters that divide a system into more-trustworthy and less-trustworthy components. The students start with a simple household-based scenario, then they work with a small business LAN, and incrementally build up to more sophisticated systems. At each level, the students review fundamental features of computer hardware and software at all levels of a system.

Information security engineering involves a life cycle starting with requirement analysis, progressing through design analysis and deployment, and repeating the cycle following a period of system monitoring and incident response. At each point in the progression,

students will look at specific problems that are solved by particular security measures applied to the system at that level. The problem drives the requirements specification, and the available technologies drive the design development.

Students will work with security concepts in a practical context by performing additional analyses that are used by information security professionals: risk assessments, vulnerability assessments, and security plans. They will learn how to use some basic scanning tools to survey small networks and assess possible vulnerabilities. They will perform simple risk assessments in which they must balance the impact of security measures against the potential reduction in risk. They will also write security plans in which they describe the security measures that must be implemented to block specific weaknesses in a system.

The course is intended to be open to both majors and non-majors. The prerequisites will include at least one introductory computing course and a practical math prerequisite. The introductory computing course may be a general course on computing (here at UST we teach such a course for business school students) or a programming course. Qualified students may waive that prerequisite if they are already sufficiently knowledgeable about computers. The practical math course may either be the UST course in discrete mathematics or the course in applied statistics. These courses are required for many science and engineering majors in addition to computer science majors. A desirable side-effect would be for this class to excite students' interest in a major in computing or information security.

As part of a college-wide revision of undergraduate course requirements, UST has started promoting the concept of "Writing Across the Curriculum." This concept reflects the belief that students learn concepts better when they have to work with them in the context of serious written assignments. In support of this, every major is supposed to include one or more major courses in which over 50% of the grade is based on written works. The elementary computer security course may become one of these courses since much of the work involves assessment and argument.

The point of this course is to provide students with a broad and useful understanding of information security. It is not intended to be comprehensive, and it will not by itself fulfill Instruction 4011 curriculum requirements. This course will provide a structure for learning about information security and a series of exercises in which the students will practice what they learn.

The Analysis Course

This course has two goals: 1) give students more in-depth experience with information security concepts through more sophisticated labs and projects, and 2) cover national information security policies required for compliance with Instruction 4011.

Additional in-depth experience will involve both study and labs. The study activities will focus on recent security incidents and on the latest information sources and tools for

keeping ahead of evolving threats. The labs will cover more sophisticated types of weaknesses and possible attacks. A final lab will be an "information warfare" scenario in which students use tools to attack and defend computers on an isolated subnetwork.

National security policies can be incredibly dry topics, especially for undergraduates destined to work in private industry. It may be possible to make this an interesting topic by portraying it as "extreme security." While national policies are driven in general by a high perceived value of various military, intelligence, and diplomatic secrets, the technical details are often driven by notorious incidents, like the Walker spy ring. It may be possible to teach the material more effectively by tying it to specific causes or historic incidents. In any case, the material must be covered to comply with Instruction 4011.

Conclusion

This is clearly just the first step in developing a successful information security curriculum. We have used a number of resources to develop a curriculum that fulfills the needs of our department and of UST students. The elementary course will serve the undergraduate community at large. The analysis course will serve as a capstone to complete students' coverage of federally mandated security topics. The course will also give them distinctive hands-on experiences that will be of value to information security professionals. The overall structure yields a coherent curricular strategy that incorporates certain classical elements of cryptographic analysis (e.g. assessment of key strength), engineering requirements analysis, and fundamental elements of computer engineering.

We are confident that the proposed program will meet with UST approval and earn IACEP certification.

Acknowledgements

The initial development of the security curriculum was the work of a QMCS Department Committee consisting of Dr. Pat Jarvis and Dr. Rick Smith, with Dr. Mari Heltne as department chair. Certain improvements in topic coverage and in lab exercises should be credited to the University of Minnesota Summer School on Information Assurance (UMSSIA), which was hosted by Dr. Youngdae Kim and Dr. Mark Hopper, with Dr. Zhi-Li Zhang serving as principal investigator. The UMSSIA was funded by a grant from the National Science Foundation. The elementary course topic development was in part the result of a Research Assistance Grant funded by the University of St. Thomas.

References

Bishop, Matt (2005). Introduction to Computer Security, Addison Wesley, Boston.

National Security Telecommunications and Information Systems Security Committee – NSTISSC (1994). National Trainingn Standard for Information Security (INFOSEC) Professionals. NSTISS Instruction 4011.

National Security Agency – NSA (2007). National IA Education and Training Program, web site, http://www.nsa.gov/ia/academia/acade00001.cfm (retrieved 27 June 2007).

Smith, Richard E (1997). Internet cryptography. Addison Wesley: Boston.

Whitman, Michael, and Mattord, Herbert (2004). Designing and teaching information security curriculum. Proceedings of the InfoSecCD Conference '04, October 2004, Kennesaw, GA.

Biography

Dr. Richard Smith is an assistant professor of computer science at the University of St. Thomas, St. Paul, MN. Before joining the faculty of UST, Dr. Smith was an information security professional and the author of two book and numerous articles.