Information Security Curricula in Computer Science Departments: Theory and Practice

Alec Yasinsac
Department of Computer Science
Florida State University
214a James Jay Love Building
Tallahassee, FL 32306-4530
yasinsac@cs.fsu.edu
850.644.6407
850.644.0058 (fax)

Abstract

Information Security college-level education efforts received a financial shot in the arm late last year with the announcement of a federal funding program to train an information security workforce. In this paper, we address issues surrounding development of a viable Computer Science, Information Security curriculum that meets the varying needs of the federal government, industry, and academia. The foundation of our program is research and education on information security and the underlying enabling technologies such as cryptography.

Keywords: Security, NSTISSC, INFOSEC Training and Education, Security Curriculum, E-commerce

Author Bio: Alec Yasinsac is an assistant professor of Computer Science at Florida State University. He is a Senior Member of IEEE, a member of the IEEE Computer Society, ACM, the IEEE Computer Society Technical Committee on Security and Privacy, and the Internet2 Security Work Group. His research interests focus on network security, primarily associated with providing logically secure channels through application of cryptography and has publications in the areas of intrusion detection, security protocol verification, and cryptography.

Track: GENERAL.

Information Security Curricula in Computer Science Departments: Theory and Practice

Abstract

Information Security college-level education efforts received a financial shot in the arm late last year with the announcement of a federal funding program to train an information security workforce. In this paper, we address issues surrounding development of a viable Computer Science, Information Security curriculum that meets the varying needs of the federal government, industry, and academia. The foundation of our program is research and education on information security and the underlying enabling technologies such as cryptography.

I. Introduction.

In the Internet age, protecting information is beginning to get the attention that it has long deserved. Turning to E-Commerce, many large corporations base their business plans on their ability to deliver their E-goods electronically. Since their ability (or lack of ability) to protect electronic methods translates directly into pocketbook gains and losses, corporate executives are now paying attention to information security. A similar phenomenon has occurred in government based on various efforts to *reinvent government*. These efforts largely became initiatives to replace traditionally manual functions with more efficient electronic methods. It can safely be said that many governments, large and small, would come to a standstill were they to loose their computer capabilities nowadays.

The greatest threat to the benefits allowed by electronic computing and the Internet is that of security concerns. One necessary path towards ensuring secure computing is through development of an information security workforce. In late 2000, the federal government approved a multi-million dollar, four year program aimed at developing such a workforce[NSF01-11]. This program targeted funding for student scholarships, faculty development, and infrastructure enhancement at academic institutions. Previously, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) established training standards for Information Systems Security professionals and a program to certify academic institutions that can map their curriculum to these standards [NSTISSC].

Meeting these training standards in academia is not straightforward. While the NSTISSC focus is on providing practical, vocational skills; mainstream colleges and universities have goals that are not necessarily parallel nor compatible with those of the NSTISSC standards and

training programs. For example, training programs are vocationally focused, based on core competencies, while educational objectives are much more broad, usually given in terms of covering a certain educational or knowledge discipline.

This problem is particularly acute for the information security field. As a result, some academic programs have chosen to address security from a multi-disciplinary approach [CERIAS], others from the application area, such as E-Commerce [NCSU] [RH].

In this paper we address the challenges and issues relating to establishing an Information Security curriculum within a computer science department at a Research I university.

II. Information Security Program In a Computer Science Department

Vaughn suggests that there three models for academic security curricula [Vau00] :

1. Incorporated topics within existing courses
2. Integration of security into software engineering program
3. Creation of a degree focus on computer security

Without discounting the viability of the first and second options, the purpose of this paper is to extend the discussion of the latter option; creation of an Information Security Degree Program within a computer science department at a Research I institution. We qualify the institution type to draw focus to our fundamental premise: *Any new degree program must contribute to the overall goal of the University*. We do not justify this premise, rather accept it unequivocally. This allows us to highlight several fundamental issues in establishing a security curriculum within a Computer Science Department.

We begin by addressing a canonical dilemma of academia: Teaching the theoretical versus the practical, which may also be known as the "Education versus Training Dilemma".

In the computer field, there is a struggle within institutes of higher learning to ensure that curricula distinguish themselves from training by reflecting a proper level of academic abstraction. This is accomplished by, among other things, maintaining a proper distance from commercial products and focusing on theoretical concepts rather than practical problems and case studies.

Conversely, university educators must maintain a practical balance in the curriculum to ensure that their graduates are employable. Fortunately, much theoretical computer science information contributes directly to practical computer scientist competencies. Unfortunately, there are numerous divergent areas between theory and practice where tradeoffs must be made. At the undergraduate level, the tradeoffs may be best resolved by a reversion to the practical, providing challenging information that equally meets the practical competencies of employers.

This is good for teaching institutions where new degree programs likely need only attract a significant student client constituency to be seen as successful. Security administrators are in high demand and interest in hacking and counter-hacking technologies make suggestions of careers in practical computer security resonate among young students.

For a Research I institution, while the curriculum must attract students, the program must also enhance the University's research posture. Potentially, the target student population growth may be closely refined, e.g. it may only advance the University's goal if the students it attracts are graduate students, or possibly even only Ph.D. students. Moreover, for Research I institutions, any new security curriculum will likely only be seen as successful if it produces

quality graduate students and a body of knowledge that will produce two results for the university

1. Increased research result visibility (refereed publications) and
2. Increased external funding (federal grants).

To meet these objectives, it would seem that the security curriculum must first focus at the graduate level. This graduate curriculum must be sufficiently rigorous to enable the students to conduct quality security research, yet it must also be sufficiently appealing to attract a sufficient number of qualified students. Based on these observations, we may believe that we should focus on practical security at the undergraduate level, and more on the theoretical at the graduate level.

While these are noble goals and it is reasonable to visualize a situation where a curriculum can be fabricated that produces a population of students that guarantees that this goal will be accomplished. Unfortunately, such a curriculum may yet be difficult to map to the practical training standards formed by NSTISSC, nor may such a curriculum well-prepare its students for immediate induction into the NSTISSC-target workforce.

It is also not clear that a theoretical graduate program would be sufficiently supported by a highly practical undergraduate program[1]. It is unlikely that a practical undergraduate program would efficiently prepare graduates for the rigors of theoretical coursework and research. Specifically, the prerequisite mathematical foundation demanded for a theoretical graduate security curriculum would likely not be met by a more practical undergraduate program. Additionally, while a practical undergraduate program may produce students that are motivated regarding information security, it may not adequately filter out students that are not suited to a theoretical curriculum.

We are detail the options for the focus of security curricula reflected in Table 1. We posit that these foci need not be terminal; for example, it may be prudent to begin a program with Option 1 (practical focus) to allow the program to build up a suitably sized student constituency, then to migrate to a more theoretical focus at the graduate level or at both the graduate and undergraduate levels.

We see option #3 as the weakest combination. While the theoretically-focused undergraduate curriculum would provide excellent technical preparation for the follow-on graduate program, it would likely necessitate that elementary security topics that would not be appropriate for a theoretical undergraduate program, be introduced into the graduate program as a regular course. Additionally, the number of students attracted to a theoretically-focused undergraduate program would likely not provide a good pipeline of students for the practical graduate program, forcing the institution to depend on an inordinate number of students from other programs to fill the seats.

Similarly, option #4 falls from favor for fear of its likely inability to attract a sufficient number of students into the program in its early stages.

---

[1] We suggest that it is advantageous for institutions that support information security programs at both undergraduate and graduate levels that the two programs be mutually supporting. For example, the undergraduate program should provide its students with relevant and sufficient skills to matriculate to the graduate program. Similarly, the graduate program should allow students from the undergraduate program to matriculate without extensive unfilled prerequisites.

The pros and cons separating the first and second options are founded in their ability to meet research quality and quantity goals. Option #2 plays directly to the advantages outlined so far, by attracting a large number of undergraduates that will be easily employable by challenging graduate students to contribute to theoretical and research goals, and through the focus on theoretical, providing a core constituency of research-focused students to extend the publication and fund-attracting capabilities of the department.

Option #1, on the other hand, has the advantages that

1. It will attract more graduate students.
2. It will attract them more quickly
3. From the larger population of graduate students the institution will be able to generate more research
4. The quantity of students drawn will include high quality students as well

For these four reasons, we believe it may be advantageous to select option #1 to start such a program.

	Undergraduate	Graduate
1	Practical focus	Practical focus
2	Practical focus	Theoretical focus
3	Theoretical focus	Practical focus
4	Theoretical focus	Theoretical focus

Table 1

III. Information Security Curricula

Figure 1 offers a list of topics applicable to Information Security curricula. This list was devised based on a topical analysis of the existing state of security research, practice, and education. While this course subject list is based on topical analysis, other categorizations were derived from roles of security principles [ICF98] and other emphasis [IWC97], but with little meaningful variation from our list.

At the core of these curricula are the two courses dealing with the content specific topical areas of computer security and network security. These courses provide a foundation that is essential for understanding the computer science context of security issues. The Computer Security course must address protection of the computer itself, including issues such as operating system vulnerabilities, physical security, virus protection, security administration, application security, and so on. These topics handicapped in terms of the depth of coverage without the knowledge provided in computer architecture and operating systems.

Similarly, the Network Security course should investigate the vulnerabilities and protection methods of electronic transmissions across the seven layers of the Open Systems Interconnect model, from firewalls to intrusion detection technologies and beyond. This course relies upon having students familiar with the fundamental technology and functions of computer networks and would be constrained if students do not understand fundamental network technologies such as how packets are routed between networks and how network directory service operate.

Beyond these two core courses, the distinction between information security and other computer science courses required for practical versus theoretical programs is fairly straightforward. Theoretical programs will tend to focus on mathematically intensive educational and research topics such as Number Theory, Formal Methods, Computational Complexity (Algorithms), and Cryptography. Conversely, programs with a more practical

Information Security Curriculum Elements

	Course Title	Some Relevant Topics
1.	Security Management	Accreditation Risk Assessment
2.	Internet Security, tools & techniques	Firewalls, IDS, PKI, email security, filtering Communication Security Network Auditing and Forensics
3.	Models of Security	Security Policies Security Metrics
4.	Database Security	Flow/Inference/Access Control
5.	Computer Security	Operating System Protection Malicious code Security Administration Legal and ethical issues
6.	Network Security	Cryptographic methods Security Protocols Protection Methodologies
7.	Formal Methods for Ensuring Security	Verifying Security Policies Security Protocol Analysis
8.	Cryptography	Cryptographic Algorithms Number theory Cryptanalysis Cryptographic Protocols Modern topics

Figure 1

intent, will slant towards tools and techniques courses on Internet Security, Database Security, and Security Management and Administration. Figure 1 is ordered based on our opinion beginning with the more practical courses (security administration) progressing to the more theoretical (cryptography).

Even with standard security course lists, topical variances within courses can be broad and deep, with actual course content driven by textbook selection or instructor interests. While the National INFOSEC Education and Training Program certification effort provides a baseline of content for an overall program desiring certification, specific course content remains relatively unstructured. Even among institutions certified to meet the same NSTISSC training standard, courses with the same names may not provide the same required competencies. Thus, students

desiring to achieve NSTISSC certification are unlikely to be able to share courses between schools. Greater uniformity would be necessary to allow such class sharing between institutions.

We achieve uniformity among core Computer Science courses in standard academic curricula through the accreditation process of the Accreditation Board for Engineering and Technology, but have no similar mechanism for achieving vocationally-focused goals through academic curricula. Neither am I aware of any previous or ongoing effort to establish such uniformity beyond the NSTISSC program. Whether such uniformity is achievable is debatable and would likely depend on establishment of a consortium of organizations from industry, government, and the military as well as from academia.

IV. Blending Computer Science and Information Security Curricula

While curricula in computer science departments around the world may vary, we provide an overview of canonical computer science curriculum courses in Figure 2. While unremarkable, when balanced against the courses suggested as elements of a security curriculum, a trend of requisite knowledge is quickly recognized. For example, the network security course depends

Computer Science Curriculum Elements

1. Software Engineering
2. Fault Tolerance
3. Theory of Computation
4. Automata
5. Algorithms
6. Discrete Mathematics
7. Compilers
8. Programming Languages
9. Data Structures
10. Data communications
11. Computer Networks
12. Operating Systems
13. Computer Architecture
14. Digital Logic
15. Artificial Intelligence
16. Neural Networks
17. Expert Systems
18. Database systems
19. Graphics/Visualization
20. Real Time Systems
21. Systems Administration

Figure 2

on students having a suitable understanding of how computer networks work, given in the networks course. Similarly, study of database security issues presume understanding of database systems characteristics and operation. It is not surprising that most security topics relate to a fundamental issue of computer science.

An exception to this trend is the subject of security policies. Rather than being founded on some other computer science discipline, security policies appears to be a separate, necessary element of computer science. Access control, information flow, multi-level security, etc. do not directly align with any other mainstream computer science topic. Rather they are a discipline of their own and have been the topic of extensive research [BL73], [Jon78] and many others. Nonetheless, no security curriculum could be considered comprehensive without presenting extensive material on security policies, and one or more courses on security policies would be appropriate in a security curriculum within a computer science department.

Figure 3 identifies a relationship between the canonical computer science and information security courses. It is this relationship that lead us to a mapping from our curriculum to the NSTISSC Training Standard for Information Security Specialists (NSTISSC 4011) [NSTISSC].

Our existing Computer Security and Network Security courses provide detailed security specific knowledge applicable to a security professional, while the systems administration and data communication courses fill the computer science specific knowledge necessary to complete the required competencies.

Correspondingly, we are preparing an additional course corresponding to the Internet Security course that when combined with the network and computer security classes will completes the competencies for the NSTISSC 4013 (Security Administrator). We are also deciding whether to pursue a security management course that will contain sufficient

Information Security Courses with Relevant Computer Science Elements

1.	Security Management:	Systems Administration
2.	Internet Security, tools & techniques	Systems Administration
3.	Models of Security	None
4.	Database Security	Database systems
5.	Computer Security	Operating Systems Systems Administration
6.	Network Security	Computer Networks
7.	Formal Methods for Security	Software Engineering
8.	Cryptography	Discrete Mathematics Algorithms

Figure 3

information to fulfill the competencies of the Designated Approving Authority (4012) and Systems Security Officer (4014) positions.

Bibliography

[BL73] D. E. Bell and L. LaPadula, "Secure Computer Systems: Mathematical Foundations and Model, M74-244, MITRE Corp. Bedford, MA, 1973

[CERIAS] The Center for Education and Research in Information Assurance and Security, http://www.cerias.purdue.edu/

[ICF98] Cynthia Irvine, Shiu-Kai Chin, and Deborah Frincke, "Integrating Security into the Curriculum", *IEEE Computer*, December 98, Vol. 31, Num 12.

[IWC97] Cynthia Irvine, Daniel Warren, and Paul Clark, The NPA CISR Graduate Program in INFOSEC: Six Years of Experience", *Proceedings of the 20th NISSC*, Baltimore, MD, Oct 97, pp. 22-30

[Jon78] Anita Jones, "Protection Mechanism Models: Their Usefulness", In *Foundations of Secure Computation*, 1978, pp. 237-252

[NCSTATE], The E-Commerce Learning Center @ NC State University, http://www.ecommerce.ncsu.edu/

[NSF01-11] National Science Foundation Solicitation NSF 01-11, "Federal Cyber Service: Scholarships for Service (SFS) A Federal Cyber Service Training and Education Initiative Program Solicitation", Fall 2000

[NSTISSC] National Security Telecommunications and Information Systems Security Committee , National INFOSEC Education & Training Program, http://www.nsa.gov/isso/programs/nietp/corseval.htm

[RH] Royal Holloway, University of London, http://www.isg.rhbnc.ac.uk/#MSc

[Vau00] Rayford B. Vaughn, "Building a Computer Security Emphasis in Academic Programs", *NCISSE 2000*