THE FIRST ACM WORKSHOP ON EDUCATION IN COMPUTER SECURITY

Cynthia E. Irvine[‡]

A successful first ACM Workshop on Education in Computer Security (WECS) was held in Monterey, California on January 29-31 of 1997. The workshop was sponsored by ACM SIGSAC, the National Security Agency, the Defense Information Systems Agency, and the Naval Postgraduate School. Procceedings from the workshop are in preparation and should be available later in 1997.

After weeks of unremitting rain, flooding, and mud slides, the weather cleared and participants enjoyed the sunny skies and blue seas of the beautiful Monterey Peninsula. The Workshop was international, with participants from Canada, Mexico, Sweden, Germany, Belgium, the United Kingdom, the Netherlands, and the United States. For many, it was the first time we had met in person. Attendees came from from academe, government, and industry. Although educators comprised the majority, participation by potential employers of INFOSEC professionals helped to focus pedagogical objectives. The confluence of perspectives resulted in interesting discussions.

Program Committee members were Heather Hinton (Ryerson Polytechnic University, Canada), Matt Bishop (University of California, Davis), Ron Ross (Institute for Defense Analyses(IDA)), Erland Jonsson (Chalmers University of Technology, Sweden), and Dennis Volpano (Naval Postgraduate School (NPS)). Daniel Warren (NPS) served as the treasurer as well as a participant. Led by co-chairs Cynthia Irvine (NPS) and Hilarie Orman (DARPA) the workshop was organized to maximize interaction between participants. Instead of a succession of relatively similar presentations with a potential for "death by viewgraph," short panel discussions were used as a starting point for plenary discussions and breakout sessions.

The theme of the first day was the **Scope and Content of INFOSEC Curricula: Defining the Core.** After welcoming remarks, we began with a panel chaired by Ron Ross. Intended to provide motivation for what would follow, it was entitled **Generating Demand for INFOSEC Education.** The first panelist was Daniel Faigin (Aerospace Corp.)[§] who suggested that a partnership should exist between government and industry in INFOSEC education. Academe can provide a foundation through a well planned curriculum, while industry can show students how principles learned in class are applied to real security problems. Next, Vic Machonachy (U.S. Department of Defense(US DoD)) presented the goal of INFOSEC education as producing a continuum of results from simple awareness to the significant knowledge and expertise of skilled professionals. He suggested that government, academe, and industry work together to insure that a common baseline of INFOSEC skills and knowledge are defined for specific points in this education continuum. Derek Simmel (Software Engineering Institute, Carnegie Mellon University) described a bleak future with increasing demand for security-knowledgeable management and technical personnel being unmet. He suggested that instead of continuing to react to the exploitation of flaws, systems must be designed with security from their inception. This approach will require security professionals who can build such systems and a user population able to use them properly. Bruce George (US DoD) presented an overview of the security engineering classes taught at the National Cryptologic School. The last panelist was John McCumber (Trident) who described both his need as an employer of INFOSEC professionals as well as training and educational offerings of his company.

The second panel session was chaired by Cynthia Irvine and entitled **A View of the Core: The Content of INFOSEC Education**. Jim Alves-Foss (University of Idaho) outlined a program providing both undergraduate and graduate education for three different career paths: system administrator, system developer, and security researcher. In addition to injecting INFOSEC issues into the overall computer science curriculum, two INFOSEC courses define a computer security core at each educational level. Students also take a specified set of additional computer science courses chosen to meet career path objectives. Jens Luessum (University of Bonn, Germany) described an innovative program to provide computer security education to high school teachers. Motivation for this work is the need for teachers to protect their information and the almost universal connection of schools to the Internet. He suggested that since so many individuals become their own security administrators that a new term and requirement, *security ergonomics*, was needed to insure that security administration was easy, not overlooked, and made sense to users. Panelist Heather Hinton (Ryerson) observed that many computer science curricula are already crowded with required courses and introducing a new course, whatever the topic, can be challenging, even when it is an elective. At the university where she first offered a computer security course, she was not paid for teaching it. With a mixture of practical experiments and assignments, discussion

[‡]Cynthia Irvine is with the Naval Postgraduate School and can be reached at irvine@cs.nps.navy.mil

[§]To save space, the names and affiliations of co-authors are not listed in this summary and, unless specified, the country of the individuals is USA.

of historical and current works, she has constructed an upper level graduate course. Cynthia Irvine described how the Reference Monitor Concept constituted the fundamental notion around which a curriculum of introductory and advanced graduate-level courses has been structured. A number of courses are accessible by a large population of engineering students within the context of a rigorous program for computer science students. Jean Ramaekers (Inst. d'Informatique, Namur, Belgium) described a graduate-level course designed with a careful balance between a highly abstract, academic approach and one that focused on the immediate problems a student would face in industry. His talk emphasized a tension between training and formal education all INFOSEC educators must address.

A discussion followed in which Stan Kurzban (consultant) described his interest in computer security education for the legal profession. (In light of the fact that in some states digital signatures are considered legally binding, his objectives carry a significant degree of urgency.) Following extensive discussion, it was agreed that extensive courses in ethics belonged to the philosophy departments and courses focusing on legal issues to the law schools.

After lunch, the breakout session was launched. Five sub-groups, each charged with formulating and later presenting a plan for the content of a curriculum in computer security, were formed. Each was to describe the prerequisites for and the educational objectives of their courses. Later in the afternoon a plenary session convened to discuss the results. Since computer literacy courses are becoming commonplace requirements for all students, the groups agreed that *information responsibility* should be included in all such courses. There was also general agreement that every undergraduate computer science student should be introduced to computer security concepts: policies and their enforcement in computer systems, vulnerabilities, etc. Programs aimed at preparing students for MIS careers should have a greater emphasis on organizational aspects of computer security, while those teaching future system developers and researchers should have a stronger technical emphasis. The variety of topics to be covered in a specialized computer security course or courses at the undergraduate level was large: access control, database security, vulnerabilities, risk analysis, network security, encryption and key management, security policies, construction of secure systems, etc. It was clear that educators will be challenged to cover all of these topics and that, at the graduate level, focused courses on specific aspects of INFOSEC would be required.

The theme for the second day was **INFOSEC Curricula: Novel Approaches to Delivering the Product.** Matt Bishop chaired a session on **Spicing up INFOSEC Education.** Erland Jonsson (Chalmers University) spoke first, describing intrusion experiments permitting students to evaluate the security of selected target systems. Students learn a methodical approach to examining system security properties and are required to keep extensive records and prepare reports on their work. Next David Oppenheimer (Princeton) told us about their class on cryptography and protocols. This presentation was particularly interesting because David was a satisfied student, not an instructor. The course, taught by Ed Felten, was conducted at the advanced undergraduate level. Students read papers and examined flawed protocols and implementations to determine where they failed and how they could be corrected. Hilarie Orman asked "Why does the devil have all the good tunes?" and explained why a class with initial exercises taking a spy vs spy approach to security both capture the interest of students and lead to a better understanding of how to build defensible systems. Finally Paul Olson (US DoD) described an introductory course which had been modularized into on-line micro-courses, thus enabling students to take a subset of the modules (organized as a logical sequence) as time permits and to build up prerequisites for the most advanced modules.

Heather Hinton chaired a panel session asking **Should Computer Security be Multi-Disciplinary?** Suggesting that it is never too early to learn the principles leading to secure systems, Matt Bishop described how software engineering notions can be incorporated into an introductory programming course. Larry Leibrock (University of Texas) is with the Graduate School of Business where an interdisciplinary course in information security with a strong practitioner orientation is presented. Students view computers as the repositories of a corporation's *knowledge assets* and learn that security requires cooperation of a *team* comprised of both technical and managerial personnel. Deiter Gollman (Royal Holloway, University of London) described a large, ongoing program involving a partnership between education and industry. In addition to several courses, students must complete an MSc project which often relates to a real problem of an industrial partner. Art Duncan (Rensalaer Polytechnic Inst.) provided arguments for all technical education to be placed in the context of legal, managerial, and ethical responsibilities. Posed as questions, his talk forced listeners to consider the larger goals of civilization, for which technology is a tool not an end in itself. Ron Ross suggested that when computer science departments teach computer security, they should focus on computer science rather than a wide variety of other topics. Marcel Spruit (Delft University of Technology) suggested that computer

security education could be divided into: organizational, technical, legal, and ethical areas. Today most educational efforst are applied to the technical area; however, organizational aspects of security, founded in system theory, are essential. To find the time to explore organizational issues, he suggested that simulators and other tools could be employed to provide practical experience in technical areas.

In the afternoon, breakout groups were charged with suggesting potential teaching approaches in delivery methods for INFOSEC curricula as well as pros and cons for the proposed method or approach. In the plenary session that followed, several groups suggested that students should be formed into teams assigned with solving a specific security problem. Each team might involve several roles: manager, technologist, and a legal/ethics liaison. Teams might be told to develop a security policy for a specific situation and then be required to describe and justify a system to enforce that policy. It was recognized that, if carefully designed and monitored, a project-oriented approach to teaching had the benefit of engaging students in a way that would permit them to "own" the knowledge that they gained. A drawback to this method is the time required to monitor student activity and design new exercises. Concepts to be demonstrated in labs included anticipatory techniques such as policy formulation and risk assessment, defensive strategies such as intrusion detection, and proactive, engineering approaches to security including fault hypothesis studies and architectures. An important skill that students should learn is how to sell their security solutions to decisions makers with limited budgets.

Organizing and Building the INFOSEC Education Infrastructure was the third day's theme. Following a brief review of the progress of the first two days, Hilarie Orman chaired a panel session entitled **Preparing INFOSEC Education for the 21st Century.** Marie Wright (Western Connecticut State University) suggested that educators should organize and share information as follows: a Web site for INFOSEC educators and an associated journal, an annual workshop or conference, and increased publisher awareness of the need for INFOSEC education materials. Deborah Frinke (University of Idaho) described challenges to the use of distance learning facilities for computer security education: differing system resources of remote students; the difficulty of assisting students with laboratory exercises; knowing who your students are, i.e. benign or malicious: and the ethics of providing information for exercises associated with system vulnerabilities on the Web. Blaine Burnham (US DoD) presented a talk on behalf of Terry Mayfield (IDA), who was unable to attend the workshop. He discussed serious pressures on computer security education programs: increasing demand for highly qualified computer scientists, a need for a rigorous curriculum in computer science as a foundation for computer security studies in the face of continuing dilution of computer science programs at the university level, and pressure by academic departments to add more courses. The recommendation was to keep computer security curricula rigorous, avoid adding what many would call security training courses, and avoid large doses of multi-disciplinary material. Adrian Spalka (University of Bonn, Germany) spoke about the challenge in attracting graduate students to take up computer security as the focus of an academic career. He noted that computer security does not have a reputation as a productive area for computer science research. Consequently, students gravitate toward topics for which the prospect of academic success is higher. Finally John Cordani (James Madison University) described the program beginning at JMU to use distance learning techniques for computer security education. He cited the rate of technological change and the complexity of modern software systems as challenges that the developers of INFOSEC education programs must strive to address.

A lively discussion on attracting new teachers into the field and the perilous route to academic success (tenure) ensued. It became evident that many of the workshop participants were spending substantially longer to prepare computer security lectures (e.g. ten hours for a two hour lecture) than is required for many other courses such as data structures or algorithms. Participants agreed that because our field is so challenging, particularly in the area of creating laboratory exercises and projects reflecting current security problems, that sharing of course materials would be a big help.

The meeting ended with plans for the future.

- It was decided to hold the workshop again in Monterey at the beginning of 1998.
- Ed Felton (Princeton) offered to start a list server for a discussion group on computer security education topics. The list is now set up. To subscribe, send E-mail to Majordomo@CS.Princeton.EDU with the following subject line: subscribe compsec-education or subscribe compsec-education <desired email address>
- Heather Hinton is organizing a Web site which will list computer security education programs and resources.

In summary, the first workshop was a success, but there is much work to be done at many levels to insure that there are permanent improvements in computer security education.