PANEL TITLE: UNIVERSITY APPROACHES TO INFORMATION SECURITY EDUCATION - CHALLENGES, ISSUES, SUCCESSES, AND OPPORTUNITIES

PANEL CHAIR: Dr. Rayford Vaughn (Mississippi State University): Dr. Vaughn teaches computer security classes to undergraduate and graduate students at MSU. He is actively involved in establishing a Software Engineering degree program, which will include security training as a required component. He has taught computer security courses at the US Naval Academy and the University of Maryland. He is a former member of the National Computer Security Center of NSA.

PANELISTS:

- **Professor Allan Berg (**James Madision University): Professor. Berg is the Director of the JMU INFOSEC program – a Master of Science program with a strong concentration in information security. This program began in January 1997 in the Northern Virginia area under a grant from NSA. The program has been very successful in teaching through innovative delivery methods – primarily involving web-based instruction. The program is structured for professionals in the workforce.
- **Dr. Matt Bishop** (University of California, Davis): Dr. Bishop's main research area is computer security, in which he has been active since 1979. He is especially interested in vulnerabilities analysis, intrusion detection, the design of secure systems and software, network security, formal models of access control, and user authentication. He has also worked extensively on the security of the UNIX operating system. He is a faculty member in the UC Davis Computer Security Laboratory where faculty and students undertake numerous security-related projects.
- **Dr. Virgil Gligor** (University of Maryland): Dr. Gligor's research interests are in the general area of computer, distributed system, and network security. His current research activities are focussed on cryptographic protocol analysis, in particular, message integrity and authentication protocols in large computer networks. Message integrity research includes both the cryptographic protection of message content and the authentication of the message origin. He lists research interests as operating systems, distributed systems, and computer security.
- **Dr Cynthia Irvine** (Naval Postgraduate School): Dr. Irvine is Director of the Naval Postgraduate School Center for INFOSEC Studies and Research. Prior to joining the faculty of the Computer Science Department at the Naval Postgraduate School in 1994, she worked at Gemini Computers on several projects to utilize Class A1 technology for applications ranging from file systems to messaging prototypes. She received her undergraduate and Ph.D. degrees from Rice University and Case Western Reserve University, respectively. She has participated in the development and review of several interpretations of and guidelines for the Trusted Computer System Evaluation Criteria and has provided critical comments on emerging standards for the evaluation of trusted systems. Her current research interests are in the area of network security architectures and high assurance multilevel distributed systems. Dr. Irvine has published several key papers in the area of computer security education – most recently a paper entitled "Integrating Security into the Curriculum", IEEE Computer, Dec 1998.

PANEL ABSTRACT:

Not many years ago, there was little or no information security course instruction available in academic computing science programs. Today, there is a proliferation of security instruction and textbooks to accommodate it, but it is being delivered in several different ways – seemingly successfully. Some universities make no change to existing computer science curriculum but include a brief discussion of security topics in classes such as operating systems, database, and perhaps software engineering. Other institutions have adopted programs that lead to a degree having a recognized concentration in information security. Some have created computing security labs while others ban such research. Training this Nation's computer science, computer engineering, software engineering, and management information systems graduates is critically important to their future employers and to the safety of our next generation information infrastructure. This panel consists of five representatives from universities offering computer security training, but not all in the same manner. The purpose of the panel is to allow each member describe their program, their student population, problems in establishing the program, and their expectations for its future success. The panel members represent academia across the United States. The approaches taken at each university are somewhat different – yet each is seen as successful by the Departments involved. The audience for this panel will gain an appreciation for the diversity of security training approaches in academia and greater insight into the issues being addressed by security faculty.

REMOTE LEARNING FOR INFORMATION SECURITY PROFESSIONALS

Professor Allan Berg
James Madison University
Department of Computer Science
Harrisonburg, VA 22807
allan_berg@cs.jmu.edu
(540) 568-8772

To serve as a professional in information security requires a commitment to life-long education. This commitment is critical in light of the rapid advancement of underlying technologies that affect information security, which are changing rapidly. Yet the traditional academic classroom setting often does not meet the needs of the information security professional because of time constraints and distance. In many cases the traditional academic classroom treats the student as a passive recipient of knowledge filtered through the instructor; it requires that the student and the instructor be in the classroom at the same time; and,in many cases, forces the student to live in the geographical vicinity of the university or to commute.

Over the past three years, the Computer Science faculty in the College of Integrated Science and Technology at James Madison University has offered an Internet-based remote electronic graduate program that leads to the Master of Science degree in Computer Science concentrating in Information Security. This program was initiated in January 1997 with 28 participants. Under an NSA grant a second group (cohort) of 20 students was launched in June 1997. Two cohorts were launched in August 1998, and five cohorts of 20 each will start August 1999 with enrollees from across the nation and Europe.

Graduate programs leading to or expanding professional degrees are ideal for conversion into Internet-based distance education formats as they address the unique needs of the adult learner. Programs should target professionals already working in their fields or professionals in corollary occupations who wish to expand their knowledge or to move into new occupations.

Participants in JMU's Internet-based asynchronous-taught distance education program are actively involved in assigned tasks that are completed over a period of several days or several weeks and submitted electronically to the instructor for comment; thus, participants are not required to synchronize with regular classroom attendance. Because communication is remote and electronic, participants are not required to live in the geographic vicinity of the university delivering the program. The program avoids the shortfalls of the correspondence school model because it treats participants as professionals who are able to teach and learn from each other as much as from the instructor by encouraging regular electronic interaction between the participants.

In March 1999 James Madison University was recognized as a Center of Excellence in Information Assurance Education.

What Do We Mean By "Computer Security Education"?

Matt Bishop
Department of Computer Science
University of California at Davis
Davis, CA 95616-8562
email: bishop@cs.ucdavis.edu

The cry of "we need more, and better, computer security education" is now rampant. Those who paid little attention to the need for secure computing have discovered how necessary it is. But what "computer security education" means is unclear. This talk will highlight some ambiguities.

Academics emphasize the principles underlying computer security. These range from the theoretical (such as the HRU result [1]) to the applied (such as Saltzer's and Schroeder's Design Principles for security mechanisms [2]). The goal is to be able to apply those principles to situations; in other words, to practice the science, and art, of computer security. Good instructors use exercises to drive the ubiquity of these principles into the students. This type of teaching requires equipment and software that reflects the principles being taught, or to which the students can apply the principles and achieve an improvement, or visible alteration, to the system being modified. The students then see that they understand the principles well enough to apply them.

Industry needs to protect its investments in people, equipment, and its intangibles - bank balances, availability of services, proprietary information, etc. The security mechanisms must do this effectively. The principles they embody are less important. In this realm, computer security is applied and practical. The goal of this type of computer security education is to be able to analyze a site, balance (internal and external) threats to the company with costs of implementing security measures, and achieving a balance between the two, with a minimum cost in training to the company. Understanding principles helps develop and implement policies and mechanisms, but the results are what matter.

Government uses computer security as one of many tools to protect the national interest (we assume this is well defined). The threats arise from external attackers and from government employees who act against the best interests of

the citizenry or who abuse their authority. The specific protections are legally mandated, and not subject to the same cost-benefit analysis industry can afford. Hence computer security education focuses on developing policies and systems to implement laws and regulations, and less on cost balancing.

This position paper argues that "computer security education" encompasses many different avenues, with different goals. Our challenge is to understand what methods of education - classroom, tutorial, mentoring, or some other form - can best impart the information and understanding required for students to function well in these environments.

References

[1] M. Harrison, W. Ruzzo, and J. Ullman, "Protection in Operating Systems," Communications of the ACM 19 (8) (Aug. 1976), pp. 461-471.

[2] J. Saltzer, and M. Schroeder, "The Protection of Information in Computer Systems," Proceedings of the IEEE, 63(9) (1975) pp. 1278-1308.

The NPS CISR Approach to Information System Security Education

Cynthia E. Irvine
Computer Science Department
Naval Postgraduate School, Monterey, California

The Naval Postgraduate School Center for INFOSEC Studies and Research (NPS CISR) represents a **success** in graduate-level education in computer and network security for military officers and government civilians. NPS CISR offers a program that includes: a curriculum ranging from introductory to advanced graduate-level courses; a research efforts addressing critical security and information assurance issues; a laboratory supporting both research and education; visiting professors; invited lectures; and academic exchange. The NPS CISR vision is to use foundational material in computer science, including, computer security, as a cornerstone for modern research and instructional programs. The program uses principles-based science and engineering to teach students how to require, specify, design and implement information systems with assurance of correct security policy enforcement.

NPS CISR has grown since its inception in the early 1990s. FY99 enrollments in computer and network security courses totaled over 300. Several factors have contributed to this success. We have been able to establish a critical mass of both instructional and research faculty and staff. Our sponsors have provided NPS CISR with both continuing support and benign oversight. We have a security track in the computer science curriculum and at least one computer security class is required for several other curricula. Increasingly, NPS students have recognized the importance of computer security and have elected to take computer and network security classes as well as conduct thesis work. The ability to plan on greater than annual intervals has been essential, particularly in a locale where INFOSEC job hopping is difficult.

NPS CISR's success invites reflection on **issues** and **challenges** in computer security education.

The first is academic manpower. Where are the professors who are able to teach computer security? Finding a instructor to teach crypto-math and protocols or to drone through a survey text is insufficient. Professors need to know, and students need to learn, the principles underpinning the design and implementation of secure systems — systems of computers — computers at the endpoints and multiple points in-between. Can sufficient talent be found to take this coherent approach? The lure of industry for those with advanced degrees and expertise in system security includes high salaries, interesting work, and, in start-ups, the possibility of fame and fortune. How can academe compete?

Another challenge is academic advancement. At the 1997 Workshop on Education in Computer Security, one educator noted that the road to academic success does not include computer security: tenure committees are not conversant in this area and/or believe that the important research topics have already been mined. A young professor might think twice before choosing to hitch his wagon to the security star.

Curriculum is an issue. For better or worse, many teachers believe that they can create a course syllabus. Thus, despite good intentions, government/industry standards specifying

course material may be dismissed as “interference” with academic freedom. However, course content may be influenced:

- Summer internships or fellowships in government or industry for both students and faculty members.
- Research grants to faculty on security topics that provide latitude for the exploration of new ideas.
- Faculty opportunities for INFOSEC and information assurance continuing education.
- Teaching start-up packages, such as the NPS CISR CD: *Introduction to Computer Security*.
- Workshops for and by educators on computer security education topics and techniques.

With sponsor support, NPS CISR has an **opportunity** to continue to create a cadre of military officers who appreciate the imperative for, and challenges of computer security and understand the value of science, engineering, and management to achieve sound technical system security solutions. The interplay between faculty, students, and the active military will permit the further development of relevant and timely course materials, an ongoing program of academic exchange, and a vibrant research program that addresses emerging security concerns of DoD and Government.

Computer Security Training and Emerging Software Engineering Degree Programs

Rayford B. Vaughn, Jr.
Associate Professor
Mississippi State University
vaughn@cs.msstate.edu
(662) 325-07450

It is rare to find computer security course offerings at most academic institutions today. There are exceptions, of course, and some institutions are offering concentrations in this area of study. For example, the Naval Postgraduate School Center for Information Systems Security Studies and Research (NPS CISR) – as represented by Dr. Cynthia Irvine, George Mason's Laboratory for Information Security Technology, and the James Madison University (JMU) concentration in Information Security Master's degree program (http://www.infosec.jmu.edu) – represented by Professor Allan Berg, are three examples of increased academic interest. Additionally, Dr. Matt Bishop has developed a strong program and laboratory at UC Davis and Dr.Virgil Gligor has taken his vast experience into the classroom at the University of Maryland. Each has a different approach to bringing this instruction to our graduating students.

A typical computer science program today includes the normal introductory courses, database, software engineering, data structures and algorithms, operating systems, and a few electives. There is no requirement and, certainly no guarantee that a graduating student will come away with any appreciation whatsoever for security issues or how one may address them. Essentially the same situation exists in computer engineering programs. It is generally only when faculty happens to have an interest in this area that the subject of information protection becomes a topic included on the course syllabus in any way other than a cursory treatment. At Mississippi State University, we have introduced a single course in this area – an elective for CS majors and a required course for our new software engineering BS program. It is important to note at this point in the paper that there is a strong movement within many academic institutions to offer degree programs in the field of software engineering. While most such programs are staffed and managed by Computing Science departments – this is not universally the case. Software engineering, as a separate degree program, offers us an opportunity to integrate a strong information security focus into these curricula. It is this author's opinion that information security is both an architectural requirement and a user requirement – both issues of software engineering interest. This leads to a conclusion that a security-engineering course should be a required course in both undergraduate and graduate software engineering degree programs. It is also the authors opinion that the computer security emphasis area is not sufficient to build a degree around, but that a certificate program incorporated into computer science, computer engineering, or software engineering degree programs is appropriate.