Learning modules for security, privacy and information assurance in undergraduate engineering education†

Daniel Manson[1], Sigurd Meldal[2], Carol Sledge[3], Stephen M. Maurer[4], John C. Mitchell[5], Erich Spengler[6], Janos Sztipanovits[7], and Javier Torner[8]

Abstract – **Computer trustworthiness continues to increase in importance as a pressing scientific, economic, and social problem. In today's environment, there is heightened awareness of the threat of well-funded professional cyber hackers and the potential for nation-state sponsored cyber warfare. An accelerating trend of the last decade has been the growing integration role of computing and communication in critical infrastructure systems that now have complex interdependencies rooted in information technologies. These overlapping and interacting trends force us to recognize that trustworthiness of our computer systems is not an IT issue anymore; it has a direct and immediate impact on our critical infrastructure. Security is often a collective enterprise, with complicated interdependencies and composition issues among a variety of participants. This poses a challenge for traditional engineering education models and curricula. The panel will discuss experiences and strategies to establish curricular foundation elements providing CSET graduates with an understanding of the interaction between cyber security, critical infrastructure systems and public policy.**

Index Terms – security, engineering education, privacy, information assurance.

PANELISTS' POSITION STATEMENTS

Daniel Manson, Cal Poly Pomona

Government directives, federal and state legislation, and industry requirements are all driving the need for more information assurance (IA) professionals. While CSET curricula prepare students for the workplace in general, there is an increasing need for CSET programs to integrate information assurance into the curriculum.

Presidential Decision Directive 63 on Critical Infrastructure Protection (May 1998) highlighted the critical shortage of information assurance professionals and the need for national standards. In January 2000, the NSTISSC initiated the Information Assurance Courseware Evaluation (IACE) Program to establish standards establishing the requirements for various categories if IA professionals.

National Centers of Academic Excellence in Information Assurance Education (CAEIAE) promote higher education in IA, and produce a growing number of professionals with IA expertise.

Cal Poly Pomona became a CAEIAE in 2005, and we will discuss the process of achieving a CAEIAE designation.

Carol Sledge, Software Engineering Institute, CERT

Administrators need a way to think about information assurance and security issues, and they need a set of skills to help them integrate security policies, practices, and technologies into their operational infrastructure. The SEI has defined a three-course Survivability and Information Assurance (SIA) curriculum to educate IT administrators about IA and security issues and to provide ways to integrate IA into their routine tasks.

The curriculum is based upon 10 principles emphasized throughout each course. These form a foundation extending beyond any specific technology – technologies change over time – and the curriculum provides a basis for assessing new technologies as they become available.

In concert with the "adapt and adopt" philosophy espoused in the CERT Program's educational outreach effort, the courses in the SIA curriculum (www.cert.org/sia) can form the basis for a certificate program at the graduate level, or specific materials from the various courses can be integrated into existing degree courses and curricula. One of our goals is for institutions of higher education to adapt, adopt, and expand

† This work was supported in part by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia and United Technologies.

[1] Cal Poly Pomona
[2] San José State University, NSF STC TRUST
[3] Carnegie Mellon University, Software Engineering Institute, CERT
[4] UC Berkeley, Goldman School of Public Policy
[5] Stanford Computer Security Lab, Stanford University, NSF STC TRUST
[6] Center for Systems Security and Information Assurance
[7] The Institute for Software Integrated Systems, Vanderbilt University, NSF STC TRUST
[8] CSU San Bernardino

1-4244-0257-3/06/$20.00 © 2006 IEEE **October 28 – 31, 2006, San Diego, CA**
36th ASEE/IEEE Frontiers in Education Conference

what we provide to best suit their particular curricular objectives.

Stephen Maurer, UC Berkeley

Since 2004, I have taught three public policy courses aimed primarily or exclusively at engineers for the NSF Science and Technology Center for Research on Ubiquitous Secure Technologies (*TRUST*) and CITRIS. These include IT and Public Policy, Introduction to Homeland Security, and Public Policy for Engineers.

The boundaries that divide academic subjects are deep but also artificial. Once engineers enter the workforce, "pure" engineering problems are few and far between.

The challenge is to find social science topics that engineering students find useful. A favorite example is *innovation economics*. Engineers do innovation for a living, and finding a precise language for this subject is very important to them. A student who successfully internalizes how innovation economists look at the world immediately sees problems much more clearly and analytically – and students also find the subject entertaining.

John Mitchell, Stanford University

The Stanford computer security curriculum includes ten-week courses on cryptography, computer security, network protocols, and advanced cryptography. CS155, *Computer Security*, is the basic undergraduate course, focusing on application security, operating systems security, and network security. The course gives students experience in finding security vulnerabilities and covers methods for design and construction of secure software systems. The essentials of cryptography, from a user's perspective, are covered in *a single lecture*, and we have found that this provides sufficient background for studying other computer security topics.

Since CS155 covers a wide range of topics, we combine in-depth programming projects with simple homework assignments that follow up on lecture topics. Three projects from a typical year are (i) finding buffer overflows, (ii) finding vulnerabilities and redesigning an application or web server, and (iii) intrusion detection and mitigation. These are programming projects that require significant understanding and effort, and many students say they will never look at programming the same way again.

Erich J. Spengler, Center for Systems Security and Information Assurance

The current and critical need for innovation in cyber security related disciplines exists throughout educational programs from K-12 through the graduate level. Three career areas must be addressed: (1) the focused cyber security practitioner specializing in their field of study, (2) the IT professional not dedicated to security but charged with the protection of critical information and infrastructure, and (3) non-IT-related professionals (e.g., healthcare personnel).

The NSF ATE Center for Systems Security and Information Assurance (CSSIA) promotes innovation and collaboration among institutions, business and industry in the following areas to significantly reduce the time and cost of cyber security program development: (1) curriculum standardization, modularization and sharing mechanisms, (2) innovative remote laboratories, management and deployment systems, (3) on-going faculty development and enrichment opportunities, (4) articulation agreements between K-12, two-year colleges and university entities, (5) effective K-12 outreach programs, (6) student and faculty internship and externship opportunities, and (7) engaging collaborative capstone activities such as the Collegiate Cyber Defense Competition (CCDC) consortium.

Janos Sztipanovits, Vanderbilt University

One of the objectives of the Education Program of the NSF TRUST Science and Technology Center is to facilitate the insertion of security components in engineering courses. The primary motivation for this objective is coming from the pervasive application of information technology as universal integrator in large systems. Consequently, security vulnerabilities in the IT infrastructure may introduce system-wide vulnerabilities. Engineering courses focusing on safety-critical systems (e.g. chemical processes control, robotic systems and automotive systems) need expose these potential vulnerabilities and explain to students the core principles that help designing, building and operating secure systems. The proper insertion of IT security topics in engineering courses is a challenge. The abstract security concepts developed in computer science and engineering need to be presented in a highly context dependent manner – but without loosing the semantic clarity and clear link to security mechanisms offered by computation and communication platforms. The Education Program of TRUST intends to facilitate this by developing on-line learning resources that can be used by educators to address security issues in multiple disciplines and multi-disciplinary contexts. Based on our ongoing experiments in chemical process control, we feel that this goal is feasible.

Javier Torner, CSU San Bernardino

Compliance with federal and state legislation has become the driving force behind initiatives in formation security at both the public and private sector. However, the success of many of these initiatives has been jeopardized due to the lack of security professionals at all levels, and the lack of awareness among stakeholders.

The shortage of security professionals can only be resolved by revamping higher education programs in information technology and other disciplines by integrating principles of information security and assurance in the curriculum. The Information Assurance Courseware Evaluation (IACE) Program has been developed, but is yet to be widely adopted by higher education.

The panel will discuss the benefits and mechanisms for professional development opportunities for faculty and staff through a stronger collaboration between faculty members and the information security and assurance office at a university.