

Educating Students to Create Trustworthy Systems

Computer science’s long-standing tradition of computer security education has focused primarily on designing secure and reliable systems that can ensure information confidentiality, integrity, and availability. This tradition is geared toward preparing students

this material only if driven to do so. This arises both from their interests and the availability of funding, which enormously impacts the direction of educational emphasis.

Given that the main source of long-term research funding for information security has been defense agencies, computer science (CS) and computer engineering (CE) departments dominated early security research. They addressed fundamental issues, such as designing secure cryptographic algorithms, communication systems, and multilevel systems. From this research tradition emerged the *component model of security*: requirements, policy, and mechanisms.¹ Edward Crowley offered the following definition:²

- a precisely articulated security policy describing the management, protection, and distribution of sensitive information by an organization; and
- a set of functional mechanisms sufficient to enforce the policy and assure that these mechanisms enforce it.

This focus on verifying an independent system’s conformance to a design specification or regulation is consistent with a CE or CS approach to security education.³ This vein of research led to fundamental breakthroughs, including intrusion detection systems, access control models, capability maturity models, and theoretical models such as the schematic protection model (SPM).

Academic research centers in in-

RICHARD S. SWART
Utah State University

ROBERT F. ERBACHER
Utah State University

for typical paradigms, such as writing secure code, providing authentication and access control, and developing policies to limit exposure to vulnerabilities and protect users’ rights.

Computer science research focuses on both applied and theoretical aspects of these areas. This differs greatly from the management information systems (MIS) approach to information security education, which focuses on operational aspects, such as

- risk analysis and mitigation—identifying potential data loss or system compromises, their cost to the organization, and how to reduce such risks;
- human factors—identifying how users will react to security techniques and policies, and how they will attempt to get around them;
- legal requirements—examining the various legal requirements for integrating security and reporting, and how to implement such requirements; and
- policy—creating corporate-wide policies to mitigate security risk and exposure, thus limiting potential monetary and public-image damage.

More succinctly, the goal of MIS computer security efforts is to prepare the next generation of business leaders to manage security issues from a high level of abstraction and to provide broad oversight. In contrast, the goal of computer science security education is to provide the technical expertise to develop secure software and defend against low-level attacks.

Faculty and industry must find novel, cross-disciplinary approaches to educating security professionals to fully address this array of issues. In this article, we analyze barriers to effective security education and offer suggestions for improving cooperation among computer science, business management, information systems, and other technology departments.

Old paradigms, new challenges

The status quo in computer security education doesn’t include cross-cutting aspects such as managing computer security, risk analysis, security architecture design, or the human factors and usability of secure systems; yet, even if source materials were to include such elements, many instructors would likely use

formation assurance and security have recruited faculty members from IT departments, MIS departments, and other core business areas to join academic research centers in computer security, but security hasn't been a traditional part of the business management or information systems curricula, and very few faculty members in business or IT departments receive academic preparation in security. For clarity, consider the following. In general, computer scientists are primarily interested in creating trustworthy computing environments. MIS professionals, on the other hand, tend to consider how users might undermine security controls. *The New York Times* recently reported that doctors at major hospitals were subverting security controls put in place for compliance with the Health Insurance Portability and Accountability Act (HIPAA) by emailing themselves copies of patient records via Gmail and Yahoo mail.⁴ Although the system was well-designed and apparently secure, users could easily circumvent the designers' intentions to facilitate their own work.

Grand challenges

Recognizing that industry and academia are failing to adequately address computer security educational needs, the Computer Research Association (CRA; www.cra.org) convened a unique conference in 2003. Participants identified four grand challenges in computer science and engineering:⁵

- Develop tools and principles for constructing large-scale systems for important societal applications that are highly trustworthy despite being attractive targets.
- Develop quantitative information-systems risk management to be at least as good as quantitative financial risk management within the next decade.
- Eliminate epidemic-style attacks within 10 years.

- Give end users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future.

Dealing with epidemic-style attacks will require focused effort in software engineering to develop secure code, but the solution will also require systems that account for the human factors that spread such attacks, including social engineering and end-user psychology. CS students can elect to take human-computer interaction (HCI) courses, but these courses rarely consider security. Most CS students lack a foundation in psychology or user behavior, which makes approaching these problems very difficult from within the CS paradigm.

Top problems in information security

Security faculty have a key role in identifying and preparing students for the challenges the field faces, but they can do so only if there is agreement about the top issues in information security. Researchers at Auburn University conducted a comprehensive international survey in conjunction with the (ISC)² organization to identify those problems.⁶ The study identified the following issues, based on responses from professionals holding the Certified Information System Security Professional (CISSP) designation:

5. Vulnerability and risk management
6. Policy-related issues
7. Organizational culture
8. Access control and identity management
9. Internal threats
10. Business continuity/disaster preparation

The researchers found the top five issues were consistent across all industry sectors, geographical regions, and respondents' technical or management levels, but educators' scores showed the least correlation with the full results.⁶ In fact, CS security courses rarely cover more than three or four of these topics.

A review of funded grants through the US National Science Foundation's CyberTrust program reveals that the vast majority of the money continues to flow to the development of resilient and survivable systems, access control, intrusion detection, and other technical solutions. If CS and CE departments broadened their research and teaching to include these top 10 issues, the next generation of technical security professionals would be better prepared to meet the challenges of today's security environment. MIS and IT faculty, on the other hand, must ground their students in the fundamentals of operating systems, networks, and software engineering so that they can better understand technical security challenges. Lack-

Security education must bridge the gap between users and underlying mechanisms and focus on building systems that protect privacy, ensure security, and engender trust.

1. Top management support
2. User awareness training and education
3. Malware
4. Patch management

ing this, MIS and IT students risk developing policies that can't be implemented or failing to recognize or comprehend risks deriving from technical sources.

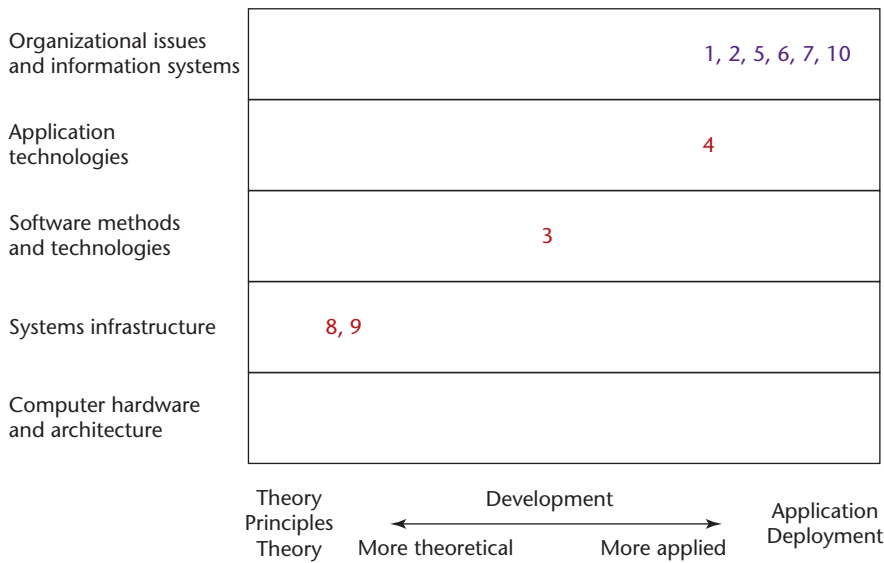


Figure 1. Top 10 information security issues, mapped to the conceptual space of computing. Note the mismatch between the majority of funding, research, and applied teaching, which focuses on theoretical work in software methods, architectures, and hardware, and the majority of the problems, which are organizational and systemic. (ADAPTED FROM THE COMPUTING CURRICULA 2005 REPORT,⁸ COPYRIGHT ACM AND IEEE. USED WITH PERMISSION.)

Bridging the gap

Figure 1 maps the top 10 information security problems onto the map of the conceptual space of computing from the IEEE Computer Society/ACM/Association for Information Systems joint task force on the Model Curricula for Computing’s “Computing Curricula 2005” report, which covers undergraduate degree programs in computer engineering, computer science, information systems, information technology, and software engineering.^{7,8} Strikingly, the vast majority of funding, research, and applied teaching is in theoretical work in software methods, architectures, and hardware, whereas most of the problems are organizational and systemic.

The fact that we don’t understand how security arises from users’ interactions with systems is a major problem.⁹ Part of this gap arises from issues in measurement and focus. Traditionally, the CS and CE approaches to information assurance

have been concerned with verifying system requirements. In contrast, information systems professionals’ strength is in studying decision-making behavior and IT management and strategies. However, all information assurance and security programs must be founded on educating students to appreciate the hardware, software, systemic, and organizational factors that lead to risk.

Including risk assessment and modeling in traditional CS and CE classes would vastly improve security curricula. Business faculty must respond to the challenge by doing the necessary empirical research in quantitative cost-benefit modeling for IT and by teaching their undergraduate and graduate students to use these sophisticated models to guide security investments and decision-making. The CRA report succinctly describes the problems with current approaches to risk:

“Envisioning large-scale information systems from one

limited disciplinary perspective is not effective. Each domain-expert group brings more focus and attention to select system dimensions, but we must consider all these visions in an integrated and systemic way to do justice to the modeling process. The evolution of risk sources in software and information assurance calls for a paradigm shift from conducting one-time, static risk identification.”⁵

Computer security education can no longer focus on static systems. The dynamic IT landscape is heading toward ubiquitous and pervasive computing in which user needs will be much broader than traditional security models, and users will use and misuse technologies in ways designers simply can’t envision. Security education must therefore bridge the gap between users and underlying mechanisms and focus on building systems that protect privacy, ensure security, and engender trust.

Traditional CS majors must be equipped to understand organizational, institutional, and end-user sources of risk. Information system students, especially in MIS programs, need sufficient grounding in networking, coding, and operating systems to understand the sources of risk from hardware and software. In either camp, students learning system analysis and design must be exposed to two key concepts: the secure software development life cycle and explicit modeling of risk.

As a guiding principle, we propose that all security programs expose students to multiple sources of risk early in the educational program. All students need early exposure to systems-of-systems thinking in which complexity can be traced to both structural issues (such as

hardware, structures, and facilities) and human-based complexity (institutions, culture, training, language, organizational behavior, and so on). Mechanisms for doing so include team teaching, case studies, and cross-disciplinary collaborative projects. Students in CS and CE programs need explicit instruction in HCI principles and in the emerging field of security and usability. Advanced system development courses need to introduce cybernetic and systems-of-systems thinking to challenge the traditional paradigms of validation, verification, and auditing for compliance. The development of more effective risk models will enable educators to impart to students effective methods of managing the complex sources of risk inherent in security, and to start breaking down the domain-specific approaches to risk assessment.

Adequately preparing the next generation of computer and information security professionals requires comprehensive security education programs that combine traditional courses in networking, software engineering, and cryptographic systems, as well as human factors and risk assessment. □

References

1. G. Spafford, "What *Is* Information Security?" *ACM SIGCSE Bulletin*, vol. 36, no. 1, 2004, p. 342.
2. E. Crowley, "Information System Security Curricula Development," *Proc. 4th Conf. Information Technology Curriculum*, ACM Press, 2003, pp. 249–255.
3. C.E. Irvine et al., "Integrating Security into the Curriculum," *Computer*, vol. 31, no. 12, 1998, pp. 25–30.
4. B. Stone, "Firms Fret as Office E-Mail Jumps Security Walls," *The New York Times*, 11 Jan. 2007; www.nytimes.com/2007/01/11/technology/11email.html?ei=5070&en=c7865d64c9cbfb3a&ex=1178078400
5. "Four Grand Challenges in Trustworthy Computing," white paper, Computing Research Assoc., 2003; www.cra.org/reports/trustworthy.computing.pdf.
6. K.J. Knapp et al., "Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness," white paper, Int'l Information Systems Security Certification Consortium (ISC)², 2005; www.isc2.org/download/auburn_study2005.pdf.
7. R. Shackelford et al., "Computing Curricula 2005: The Overview Report," *Proc. 37th SIGCSE Technical Symp. Computer Science Education*, 2006, pp. 456–457.
8. *Computing Curriculum 2005*, tech. report, ACM/IEEE, 2005; www.computer.org/portal/cms_docs_ieeeecs/ieeecs/education/cc2001/CC2005-March06Final.pdf.
9. G. Conti et al., "A Comprehensive Undergraduate Information Assurance Program," *Proc. 3rd World Conf. Information Security Education (WISE3)*, Kluwer Academic Publishers, 2003, pp. 243–260.

Richard S. Swart is a doctoral candidate in the management information system (MIS) Department at Utah State University. His research interests include information security management, corporate governance, methods of vulnerability assessment, and security of health information technology. A former healthcare professional and administrator, Swart has an MSW from the University of Utah and an MS in MIS from Utah State University. He serves on the board of directors for the Utah chapter of the Information Systems Security Association. Contact him at richard.swart@usu.edu.

Robert F. Erbacher is an assistant professor in the computer science department at Utah State University. His research interests include digital forensics, computer security, intrusion detection, information visualization, and cyber command and control. Erbacher has an ScD in computer science from the University of Massachusetts, at Lowell. Erbacher is a member of the IEEE and the ACM, as well as the editorial board for the Journal of Electronic Imaging. Contact him at robert.erbacher@usu.edu.



PURPOSE: The IEEE Computer Society is the world's largest association of computing professionals and is the leading provider of technical information in the field. Visit our Web site at www.computer.org.

EXECUTIVE COMMITTEE

President: Michael R. Williams*
President-Elect: Rangachar Kasturi;* **Past President:** Deborah M. Cooper;* **VP, Conferences and Tutorials:** Susan K. (Kathy) Land (1ST VP);* **VP, Electronic Products and Services:** Sorel Reisman (2ND VP);* **VP, Chapters Activities:** Antonio Doria;* **VP, Educational Activities:** Stephen B. Seidman;† **VP, Publications:** Jon G. Rokne;† **VP, Standards Activities:** John Walz;† **VP, Technical Activities:** Stephanie M. White;* **Secretary:** Christina M. Schober;* **Treasurer:** Michel Israel;†
2006–2007 IEEE Division V Director: Oscar N. Garcia;† **2007–2008 IEEE Division VIII Director:** Thomas W. Williams;† **2007 IEEE Division V Director-Elect:** Deborah M. Cooper;* **Computer Editor in Chief:** Carl K. Chang†

* voting member of the Board of Governors

† nonvoting member of the Board of Governors

BOARD OF GOVERNORS

Term Expiring 2007: Jean M. Bacon, George V. Cybenko, Antonio Doria, Richard A. Kemmerer, Itaru Mimura, Brian M. O'Connell, Christina M. Schober
Term Expiring 2008: Richard H. Eckhouse, James D. Isaak, James W. Moore, Gary McGraw, Robert H. Sloan, Makoto Takizawa, Stephanie M. White
Term Expiring 2009: Van L. Eden, Robert Dupuis, Frank E. Ferrante, Roger U. Fujii, Anne Quiroz Gates, Juan E. Gilbert, Don F. Shafer

Next Board Meeting: 9 Nov. 2007, Cancún, Mexico

EXECUTIVE STAFF

Associate Executive Director: Anne Marie Kelly; **Publisher:** Angela R. Burgess; **Associate Publisher:** Dick J. Price; **Director, Administration:** Violet S. Doan; **Director, Finance and Accounting:** John Miller

COMPUTER SOCIETY OFFICES

Washington Office: 1730 Massachusetts Ave. NW, Washington, DC 20036-1992
 Phone: +1 202 371 0101 • Fax: +1 202 728 9614
 Email: hq.ofc@computer.org

Los Alamitos Office: 10662 Los Vaqueros Circle, Los Alamitos, CA 90720-1314
 Phone: +1 714 821 8380 • Email: help@computer.org
 Membership and Publication Orders:
 Phone: +1 800 272 6657 • Fax: +1 714 821 4641
 Email: help@computer.org

Asia/Pacific Office: Watanabe Building, 1-4-2 Minami-Aoyama, Minato-ku, Tokyo 107-0062, Japan
 Phone: +81 3 3408 3118 • Fax: +81 3 3408 3553
 Email: tokyo.ofc@computer.org

IEEE OFFICERS

President: Leah H. Jamieson; **President-Elect:** Lewis Terman; **Past President:** Michael R. Lightner; **Executive Director & COO:** Jeffrey W. Raynes; **Secretary:** Celia Desmond; **Treasurer:** David Green; **VP, Educational Activities:** Moshe Kam; **VP, Publication Services and Products:** John Baillieul; **VP, Regional Activities:** Pedro Ray; **President, Standards Association:** George W. Arnold; **VP, Technical Activities:** Peter Staecker; **IEEE Division V Director:** Oscar N. Garcia; **IEEE Division VIII Director:** Thomas W. Williams; **President, IEEE-USA:** John W. Meredith, P.E.

revised 1 May 2007

