Editors: Matt Bishop, bishop@cs.davis.edu
Deborah Frincke, deborah.frincke@pnl.gov

Joining the Security Education Community

Deborah Frincke
Pacific Northwest National Laboratory

Matt Bishop
University of California, Davis

Enthusiasm, exploration, evolving mounds of hardware, and a strong sense of purpose were stalwarts during security education's pioneering days, and although these still form its core, other characteristics are emerging as the discipline's landscape becomes more settled.

One major emerging trend is in curriculum development. The kaleidoscope approach of obtaining curricular excellence primarily from local resources and ideas is giving way to an outward-looking approach that incorporates the growing community experience to gracefully knit anticipated student outcomes, faculty talents, and educational styles together as the underpinnings of a more coherent curriculum. The lessons taught by security education's pioneers can be found in many venues, and although program development remains challenging, there is a larger community available for support.

Future departments will examine the national evolution of security and privacy education and training and how that affects the palette of education and training options; we'll also discuss the campuses that offer such curricula. We begin with a high-level view of community venues for gatherings within and between the security and privacy community and its supporters.

Cooperation and collaboration: Watchwords

Security and privacy education has always been driven by more than intellectual curiosity, creativity, and a wish to support human endeavors, although these are certainly present in no small measure. Security and privacy education is, at its heart, driven by a compelling national and international need. Society's increased dependence on pervasive computer-based communications, infrastructures, and systems makes it imperative that we understand the risk factors, that we learn what it truly means to "secure" the devices upon which we rely, and that with careful thought we balance the technological trade-offs between protection, performance, and neat new features with decisions about how various implementations affect our personal freedoms and privacy. If these decisions are not made deliberately, they'll be made by the de facto implication of whatever structure emerges by happenstance. No single aspect of society will have all the answers, but fortunately, several groups have emerged to support both the pragmatic need to share materials and expertise, and to lead the larger debate about what should be taught and researched.

Colloquium for Information Systems Security Education

One place to seek out answers to the "I wonder how other people do it?"

question is the Colloquium for Information Systems Security Education (www.ncisse.org). CISSE's primary method of influencing and supporting security education is through a yearly conference, alternately sponsored by an academic, industry, or governmental entity. Past hosts have included the executive branch of the US government, the US National Security Agency, the US Military Academy at West Point, Microsoft, IBM, James Madison University, and George Mason University. Formerly the National Colloquium for Information Systems Security Education, CISSE has streamlined both its name and its mission: its goals are built on the recognition that the US requires a "information-literate work force that is aware of its vulnerability" as well as education of the next generation. Furthermore, CISSE emphasizes partnership.

"The Colloquium's value is built upon developing academic contacts for courseware development and sharing, the potential value of scholarships for research and academic ventures, and the benefit of supporting a clearinghouse of academic issues," says Allan Berg, CISSE treasurer and secretariat director.

Founded in 1997, CISSE brings leaders in academia, government, and industry together to support information systems' security education issues. Questions remain much the same today as in the earliest days, although the responses now include more "worked examples":

- What really belongs in a security curriculum?
- Who are the stakeholders?
- How can faculty rapidly gain expertise in a fast-paced field?
- How can we attract students to the study?
- How should the community seek to influence the national agenda to better support security education?

Security and privacy education has always been driven by more than intellectual curiosity, creativity, and a wish to support human endeavors.

Recent meeting discussions emphasize methods for achieving educational goals, and focus on growing centers of excellence in information assurance education. Participants regularly discuss curriculum and program development in academia—as well as desirable goals—for new governmental policies. A recent addition to a typical conference-style agenda is a hands-on boot camp for faculty, which is an intense and focused course held just prior to the general conference. This boot camp provides both the information content and teaching techniques for a specific topic.

IFIP WISE

Another forum for influencing information security education and training is through the International Federation of Information Processing (IFIP) Working Group 11.8 on Information Security Education (WISE). Established in 1991 as an international resource center for the exchange of information about education and training in information security, WISE's aim, according to Helen Armstrong, senior lecturer at the School of Information Systems at Curtin Business School in Perth, Australia and one of the primary organizers of the program committee, is "to promote information security education and training at the university level in academia, government, and industry." The group is international in scope and attendance.

Since 1999, there have been three WISE world conferences; WISE4 will be held in Moscow in May 2005. In addition to its conferences, WISE has sponsored several international workshops. The WISE Web site (www.fis.mephi.edu/wise4/) includes registration information for the next meeting as well as a call for papers.

Workshop on Education in Computer Security

Led by Cynthia Irvine of the computer and network security faculty at the Naval Postgraduate School in Monterey, California, the Workshop on Education in Computer Security (WECS) was one of the earliest formal meeting groups for security educators. As with the earliest NISSCE/CISSE meetings, the first WECS held in Monterey, California, in 1997, featured formal conversations mixed with sidebar discussions that foreshadowed the emergence of modern NSF programs to support security faculty development; public cyberwar games for educational purposes; the original ideas behind the national centers of excellence; and the Cyber Corps, which trains computer security experts to form the US's first line of defense against global cyber threats.

WECS continues to be a high-value forum for information exchange between newcomers and experienced security educators. Meeting sizes are deliberately limited—on the order of a few dozen participants—but the smaller participant list does not significantly limit breadth. By balancing attendees between veterans, newcomers, and recent WECS alumnae, and by seeking representation from different campuses, the meetings provide a nice balance between freshness and

experience. A few representatives of government and industry are usually present, but most participants are drawn from academia.

Although WECS meetings address broad national issues, their primary purpose is to emphasize practical programmatic and curriculum development for immediate classroom use. Practical tutorial tracks often accompany WECS meetings to accommodate focused discussion of some key capability that might be difficult for new security educators to learn on their own (such as techniques for using live exercises in the classroom). Scholarship attendees are encouraged to return and present the results of their efforts in subsequent WECS meetings, so that knowledge about teaching is constantly tested, assessed, shared, freshened, and refined.

WECS-06 (http://cisr.nps.navy.mil/WECS6/overview.html) was held in July 2004; Irvine says that WECS-07 will occur during summer 2005.

Centers of Academic Excellence

No discussion of the community of security educators would be complete without mention of the National Centers of Excellence. In November 1998, the NSA established the Centers of Academic Excellence in Information Assurance Education (CAEIAE, or CAE, institutions). The original program was driven primarily by the Clinton administration's May 1998 Policy on Critical Infrastructure Protection, Presidential Decision Directive 63 (PDD 63). This year, the US Department of Homeland Security and the NSA agreed to cosponsor the program and have changed the designation to indicate its broad national caliber, renaming the program the National Centers of Academic Excellence in Information Assurance Education (www.nsa.gov/ia/academia/acade00001.cfm). This new designation is tied to the US National Strategy to Secure Cyberspace. Although space does not permit a full discussion of the CAE program here, the growth in number and sophistication of centers—and how they interact—is a key factor behind how security education is offered in the United States today, and deserves a column of its own.

Security education has arguably left the pioneer stage, so the question before us now is what comes next? How will we balance education and training? How much influence should educators exert on national and international legislation and vice versa? How do we as a community support lifelong learning? What about the need to quickly learn skills that are both complex and could have a short useful lifespan, and the dissemination of key underlying principles? There is still much to do, and security and privacy education will remain a fascinating and malleable field of study for years to come. The underlying need to answer the grand challenge problems of security and privacy remains a practical and time-driven one, and ultimately success will depend on how well we can work together. One thing remains clear: teaching and practicing security and privacy is a joint venture requiring solid partnerships and discussion between academia, government, and industry. Equally necessary is the informed participation of the citizenry who will have to live with the answers we deliver. □

Deborah Frincke *is chief scientist for the Pacific Northwest National Laboratory's cybersecurity group in Richland, Washington. She is currently on leave from the University of Idaho, where she is an associate professor and was director of the Center for Secure and Dependable Systems. Her research interests emphasize system defense, especially intrusion detection, and the security of high-speed systems. Contact her at deborah.frincke@pnl.gov.*

Matt Bishop *is an associate professor in the Department of Computer Science at the University of California, Davis, and a codirector of the Computer Security Laboratory there. His research interests include vulnerabilities analysis, the design of secure systems and software, network security, formal models of access control, and intrusion detection. Contact him at bishop@cs.ucdavis.edu.*