Back to School

Deborah Frincke
Pacific Northwest National Laboratory

Matt Bishop
University of California, Davis

As summer draws to an end, faculty and students turn their attention to academic planning. This used to be a very tough task—faculty developed most of their materials from scratch. Now, rather than a handful of items to draw on when planning a security and privacy course, there is a plethora of sample syllabi, textbooks, and other supportive materials. The question is: where are they? For all the busy academics out there readying their courses—and the students who are about to join you, we have written this article, with help from the Centers of Excellence in Information Assurance Education, in the hope that it will make your preparations a trifle less hectic.

Classroom icebreakers

In academics, as in marketing, first impressions stick. A good first-day icebreaker goes a long way toward setting the stage for a positive learning experience. Here are some possible ways to ease the transition from summer to the classroom:

- Choose a common summer experience and analyze it using security or privacy principles associated with the class theme. A class emphasizing privacy might consider credit-card-based summer travel purchases—what might the credit-card company's files indicate about personal preferences?
- Assign students teams to analyze their own systems for spyware, incoming vulnerability scans, and randomly roaming worms. Use caution—over enthusiasm might lead students to analyze resources they don't own, or put an important resource in harm's way. There's nothing like learning that IRC pirates have 'borrowed' a classmate's computer to get students' attention.
- Have students learn as much as they can about themselves, their classmates, or an unknown volunteer on the Internet armed only with a name and a browser. This exercise is suitable for a privacy class, if handled within university guidelines with due consideration. Be careful in your choice of target.

The key to a successful icebreaker is to refocus student attention from summer while personalizing the topic, thus establishing a positive and "seeking" mindset among the students and setting a precedent for interactive problem solving. These vignettes can be used all semester, in many ways—for example, to distinguish between what ought to be possible (policy) or what is desirable versus actual experience with what is possible (enforcement mechanisms). They also provide a vehicle for gently introducing informal public speaking when appropriate—something many technical students can use. Finally, modern learning styles reinforce what many of us know from years in the classroom, many individuals must understand a concept's relevance before they are able to focus well on the topic.

University policies affect classroom mechanisms

There are many "gotchas" lurking for those running security courses involving hands-on activities, more so than in most computer science disciplines. Earlier departments in *IEEE Security & Privacy* and elsewhere have discussed specifics involving computer laboratory exercises. Recent media events, ranging from discussions of individual security practices to coverage of individual classes on viruses and ethical hacking should be convincing evidence that preparation for external attention is warranted. In that spirit, we suggest these best practices for security educators:

- Introduce yourself to the individual responsible for the campus IT security. It's helpful to be on a first-name basis with this person, especially if it should turn out your stand-alone classroom experiments aren't really stand-alone. Campus IT administrators can also help you stay within university policies for appropriate computer use. You might also ask if there are any real-world tasks with pedagogical value that your students could perform.
- A good relationship with your campus media relations specialists and your campus legal counsel can be invaluable. Trust us on this one.
- Campus definitions of and re-

quirements for interacting with human subjects range widely. Many have a strict paper trail that must be filed well in advance, and sometimes a committee must review the request and sign off on it. Our advice is, whether running a honeynet or sniffing network data via a network scanner or using potato-chip cans as part of your wireless security's hands-on experimentation, make sure your activities meet campus guidelines for human subjects. Consider completing the forms a class exercise, and use the opportunity to discuss the safety, privacy, and ethical issues embodied in the human subjects' requirement documents.

- Use discretion in planning those practicum exercises, particularly when they involve critical infrastructures, social engineering, or gathering personal information. One student team went out to visually assess their local dam and railway system for vulnerabilities. Those students subsequently spent a rather unpleasant hour being questioned by local law enforcement afterwards, due to an (appropriate) call by a concerned citizen. We recommend that you discuss such excursions with campus authorities in advance—who you know by first name by now, right?—and make sure your ideas are acceptable, that you've given your students good guidance for their activities, and that you provide a description of the assignment to your chair or dean in case something goes awry when you are out of town.
- Make sure your laboratory has a "fair and ethical" use policy. Devising one of these can be an exercise in itself.

These preparations might seem cumbersome—you've never needed them before, and you're sure you won't need them in the future so all this discussion is just paranoia… doesn't that sound like 'reasoning' you've heard before?

Codes of conduct

Course introductions normally include warnings about consequences for unprofessional or illegal conduct. Such prohibited conduct ranges from plagiarism to violation of appropriate computer-usage policy to other campus conduct codes.

With creativity, we can use these awkward topics to achieve pedagogical goals. Consider plagiarism—an ever-increasing concern for educators. Even students who have a general understanding of citation basics might not know how to handle trickier cases, such as citing an author's quotation from a second paper, so they need more information. There are easy techniques to relay such information without detracting from class content.

- Identify a paper from the first week's reading assignment. Devise a set of proper, and improper, citations from that work. Require students to check these—in such a way that they must at least scan the paper to find the remarks. Having the citations involve a definition you want to emphasize adds even more value.
- Divide students into teams and have them make up their own examples of easy, and more difficult, citations based on quotes from this paper.

You might wish to periodically return to the issue from other angles:

- Consider a "forensic-style" programming assignment that looks for unauthorized transfer of protected material to an offsite location.
- Discuss the techniques behind identifying authors of malware as it compares to identifying plagiarism.
- Require students to serve as reviewers for each other's final written papers, and score students as reviewers as well as authors. Tell them that one of their tasks is to ensure that the material is original (as they would for a professional journal or magazine), and to assist the author in correcting any errors before the paper gets to you for final review.

Many other ways to handle plagiarism discussions exist; these are some that the authors and other center of excellence leaders have used successfully in the past.

Organizing guest lecturers

Students welcome a change behind the podium from time to time. Besides providing variety, practitioner-role models are beneficial at all levels of education. The down side is the expensive plane fares and lodgings, and shrinking campus budgets often mean there is no funding for such activities. Fortunately, there are ways to host guests without breaking the bank.

Federal and state agencies

Some federal and state agencies encourage employees to serve as guest speakers; some have a limited budget for travel and lodging costs. The US Federal Bureau of Investigations, the US National Institute of Standards and Technology, and the US Attorney General's Office have been mentioned as being particularly accommodating in visiting campuses. It's helpful if you make the request well in advance, and are flexible about the date—perhaps have it coincide with the active recruiting pe-

Besides providing variety, practitioner-role models are beneficial at all levels of education.

riod. When working with federal agencies, be sensitive to regulations that govern the gifts these individuals are allowed to accept. Make sure the financial arrangements are understood by all in advance.

Corporate speakers

Many companies provide personnel for speaking engagements; some will contribute to expenses. For example, Cisco funds a guest lecture program (www.cisco.com/security_services/ciag/initiatives/education/guestlecturers.html). Some companies give speakers kudos on their yearly reviews when they receive this kind of invitation, so sending a thank-you letter to the speaker (and his or her supervisor) is a nice way to show appreciation for any time spent with your class.

Local university community

Your new friend, the campus IT administrator, has a wealth of stories about everything from insider misuse to the financial realities of handling a campus security system when budgets are shrinking and IT demands are increasing. Your advisory board—departmental, college, or university—includes someone with a useful perspective on security and privacy, and board members often welcome an opportunity to participate in the education process.

Professional organizations

Several professional organizations have speaker programs. The ACM provides speakers through its Distinguished Lectureship Series (www.acm.org/top/lect.html) on a cost-sharing basis. The Computer Research Association's Committee on Women in Computing Research (CRA-W) also has a funded distinguished lecturer series; its specific intent is to increase the number of female graduate students (www.cra.org/Activities/craw/dist_lect.html). The IEEE Computer Society's Distinguished Visitor Program (www.computer.org/chapter/dvp/) provides similar programs.

Alumni and students

Alumni often return to watch their friends graduate, and a panel of returning students employed in the security arena can be quite enjoyable for both participants and audience.

Curriculum development

There have been many positive developments in curriculum development over the last 10 years and in an upcoming column, we will expand on this topic. For now, in the interests of brevity, we recommend you start here:

- Purdue University's Center for Education and Research in Information Assurance and Security (www.cerias.purdue.edu/).
- The University of Tulsa's Center for Information Security (www.cis.utulsa.edu).
- National Information Assurance Training and Education Center (www.niatec.info).
- Virginia Alliance for Secure Computing & Networking (www.vascan.org).

And, for those who want a more interactive experience, we suggest you attend these events:

- Colloquium on Information Systems Security Education (every June).
- Kennesaw State University's Information Security Curriculum Development Conference (September 2004).
- Workshop on Education in Computer Security (every July).
- IFIP Working Group 11.8 on Information Security Education (WISE) Workshop on Information Security Education, (biannual, May 2005).

Improvements largely sprang from grass-roots determination that security education was a community responsibility.

These sites and forums only scratch the surface of what's out there—a welcome contrast to the state of the art only a dozen years ago. These improvements largely sprang from grass-roots determination that security education was a community responsibility—and the results are impressive. We hope you take advantage of these materials and contribute yourselves. ▢

Acknowledgments

We gratefully acknowledge the help we received from members of the Centers of Excellence in Information Assurance Education, who emailed us with many of the suggestions here and others we've saved for future columns. We also thank the busy (often volunteer) individuals who answered questions about their programs and offerings. You are all wonderful colleagues and we appreciate all you do.

***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.*