Cybersecurity Education in Universities

Fred B. Schneider
Associate Editor in Chief

An educated workforce is essential to building trustworthy systems. Yet, issues about what should be taught and how are being ignored by many of the university faculty who teach cybersecurity courses—a problematic situation.

Absent an accepted authority on cybersecurity education at the university level, it is difficult for faculty to affect cybersecurity education beyond their home institutions. For sure, professional societies (such as ACM and IEEE) are concerned with defining university curriculum, but they are not accepted by faculty members as being authorities on cybersecurity curriculum, in part, because top technical researchers are typically not involved in the discussions. Curriculum development suffers without input from the full spectrum of faculty members—the absence of leading technical thinkers means that topics needed to prepare students for adopting new trends and directions are unlikely to be incorporated into a curriculum. The curriculum also suffers when we ignore people from industry and government, who have experience with real systems, users, and attackers; and their input is largely absent from these university curriculum initiatives, too.

Several conferences and workshops do have cybersecurity education as their focus, so you might hope that they could serve as an organizing authority. The representation at these meetings, however, is light on practitioners from industry and government, and it is also largely disjoint from the attendees at our leading technical conferences. We could eliminate this disconnect by coalescing several of our conferences into a single community-wide annual meeting. A conference with such a wide view of cybersecurity also would help overcome today's trend of creating specialized workshops and conferences that, unfortunately, is further fracturing the research community and impeding discussion about broader matters, like curriculum.

Another impediment to cybersecurity curriculum development is that research universities do not place a high value on pedagogy when it comes to making tenure and promotion decisions or dispensing other rewards to faculty. Consequently, cybersecurity researchers are not incentivized to write textbooks or survey articles, even though this activity is a form of research because it leads to discovery of new categorizations and unification of ideas. The Saltzer-Schroeder article had an enormous impact on the field by offering a set of generalizations rather than specific technical solutions.[1] We need to incentivize researchers to undertake this kind of thinking and writing—something that requires a change in values.

Even if university teaching were informed by surveys and textbooks by top researchers, there is a debate about what should be taught to future software developers (and, for that matter, to future researchers). Some see the role of university cybersecurity courses as teaching adversarial thinking, so that system builders can view system designs through the same lens attackers do. Others believe these courses should focus on principles and abstractions that bring discipline to the art of building secure systems. Courses in which adversarial thinking is central are quite different from those organized around principles and abstractions.

Case studies are prevalent in cybersecurity courses that teach adversarial thinking. Students are taught about specific attacks, which often requires spending time on idiosyncratic implementation details (though attack taxonomies exist and might also be covered). Some students are able to generalize from this material, and they develop an intuition for identifying assumptions that can be violated to achieve some goal—the essence of any attack. Other students, who don't make the leap from specific attacks to adversarial thinking, are not well served. George Santayana's thinking

1540-7993/13/$31.00 © 2013 IEEE

("Those who cannot remember the past are condemned to repeat it") ignores the reality that fundamentally new kinds of attacks are constantly developed and fielded, so only knowing about (and defending against) known attacks is insufficient. Finally, as with most things, expertise in disassembling some class of artifacts does not imply facility with building new artifacts from scratch.

A class organized around cybersecurity abstractions and principles might well employ case studies of extant systems, but mastery in using the abstractions and principles comes only from the design and implementation of new systems. Evaluating those new systems, however, requires facility with adversarial thinking. You might argue that a student could learn adversarial thinking from studying cybersecurity abstractions and principles, because these ideas concern defenses against attacks. That would suggest organizing our cybersecurity courses around abstractions and principles.

Note that the relationship and—in some cases—tension between synthesis and analysis of cybersecurity also is present when teaching students about safety-critical systems, where starting off from abstract properties can miss important details (such as sources of harm and opportunities for mitigation) but relying on specific hazards risks overlooking other hazards and makes for a weak safety case. Yet, there is little of the same tension visible when teaching about national security or military engagements; somehow, these more-mature subjects succeed in combining the two views. Adversarial thinking can be seen as the very essence of game theory. In it, actions by each player are completely specified; for cybersecurity and safety-critical systems, identifying possible player actions is part of the central challenge.

Can adversarial thinking for cybersecurity even be taught, or is it an innate skill that only some can develop? The answer, which is neither known nor aggressively being sought by those who study cybersecurity education, seems central to the development of an effective cybersecurity course. In the meantime, debate about how best to teach cybersecurity is limited to recounting anecdotes about our collective classroom experiences. Generalization from anecdotes is a risky business.

The evolution of a university-level cybersecurity curriculum is being stunted by the culture and values in universities as well as by our ignorance. Change is needed on all of these fronts. The failure of faculty to take action leaves a door open to others who will. And those outsiders are waiting—not only does the private sector offer cybersecurity training that could easily encroach, but governments (such as the US National Initiative for Cybersecurity Careers and Studies; www.niccs.us-cert.gov) show a growing interest in cybersecurity education at all levels. ■

Reference

1. J.H. Saltzer and M.D. Schroeder, "The Protection of Information in Computer Systems," *Proc. IEEE*, vol. 63, no. 9, 1975, pp. 1278–1308.