What Do We Mean By “Computer Security Education”?

Matt Bishop
Department of Computer Science
University of California at Davis
Davis, CA 95616-8562
email: bishop@cs.ucdavis.edu

The cry of “we need more, and better, computer security education” is now rampant. Those who paid little attention to the need for secure computing have discovered, how necessary it is. But what “computer security education” means is unclear. This talk will highlight some ambiguities.

Academics emphasize the principles underlying computer security. These range from the theoretical (such as the HRU result [1]) to the applied (such as Saltzer’s and Schroeder’s Design Principles for security mechanisms [2]). The goal is to be able to apply those principles to situations; in other words, to practice the science, and art, of computer security.

Good instructors use exercises to drive the ubiquity of these principles into the students. This type of teaching requires equipment and software that reflects the principles being taught, or to which the students can apply the principles and achieve an improvement, or visible alteration, to the system being modified. The students then see that they understand the principles well enough to apply them.

Industry needs to protect its investments in people, equipment, and its intangibles – bank balances, availability of services, proprietary information, *etc*. The security mechanisms must do this effectively. The principles they embody are less important.

In this realm, computer security is applied and practical. The goal of this type of computer security education is to be able to analyze a site, balance (internal and external) threats to the company with costs of implementing security measures, and achieving a balance between the two, with a minimum cost in training to the company. Understanding principles helps develop and implement policies and mechanisms, but the results are what matter.

Government uses computer security as one of many tools to protect the national interest (we assume this is well defined). The threats arise from external attackers and from government employees who act against the best interests of the citizenry or who abuse their authority. The specific protections are legally mandated, and not subject to the same cost-benefit analysis industry can afford. Hence computer security education focuses on developing policies and systems to implement laws and regulations, and less on cost balancing.

This position paper argues that “computer security education” encompasses many different avenues, with different goals. Our challenge is to understand what methods of education – classroom, tutorial, mentoring, or some other form – can best impart the information and understanding required for students to function well in these environments.

References

[1] M. Harrison, W. Ruzzo, and J. Ullman, “Protection in Operating Systems,” *Communications of the ACM* **19** (8) (Aug. 1976), pp. 461-471.

[2] J. Saltzer, and M. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE*, **63**(9) (1975) pp. 1278-1308.