Panel on Integrating Security Concepts into Existing Computer Courses

Paul Mullins
Slippery Rock University
mullins@granite.sru.edu

Jim Wolfe
Indiana University of Pennsylvania
jlwolfe@grove.iup.edu

Michael Fry
Lebanon Valley College
fry@lvc.edu

Erik Wynters
Bloomsburg University
erik@bloomu.edu

William Calhoun
Bloomsburg University
wcalhoun@bloomu.edu

Robert Montante
Bloomsburg University
bobmon@bloomu.edu

William Oblitey, Moderator
Indiana University of Pennsylvania
oblitey@iup.edu

Summary

Recently, computer security has come to the forefront of public awareness. With the onslaught of worms such as Code Red, national (U.S.) concern has increased about cyber terrorism and the information infrastructure. One educational response has been the emergence of a number of computer security degree programs - at the undergraduate level, e.g., East Stroudsburg State University of PA, and at the graduate level, e.g., the Heinz School at Carnegie-Mellon University.

The panel members were all participants in the Cyber security faculty development Workshop[1] held at Indiana University of PA in August, 2001. Among the goals of the workshop was the development of courses that would teach the theory and application of security, including the use of specially designed (quarantined) "attack" and "defend" computer labs. Additional goals include development of modules related to security for CS core courses, and an interdisciplinary minor for Computer Science and Criminology majors.

It was the consensus of the panel participants that many institutions would be unable to implement special degree programs or tracks, and, in a significant number of cases, might be unable to immediately implement even one specialized course. Yet, all the participants also believed strongly that security-related content in our computer courses can, and should, be improved. Even if no security-based courses are added, major and non-major courses in computer science, CIS, etc., can do a better job of raising awareness of threats, vulnerabilities, and risks.

SIGCSE'02, February 27- March 3, 2002, Covington, Kentucky, USA.
ACM 1-58113-473-8/02/0002.

Each panel member will address a specific course or sub discipline and describe how security was infused or added to the current curriculum. The intent is to foster discussion regarding appropriateness and pedagogy while relating individual experiences, successes and failures. Audience and panel members will be encouraged to discuss the relative merits of this approach.

Position Statement of Paul Mullins

Computer security is a multidisciplinary area that includes reliability, fault tolerance, software engineering, system administration and a number of other traditional computer science areas. Security issues must be addressed in courses ranging from CS1 to theory of computations if students are to understand the relationship security has with the rest of their education.

Security issues have been experimentally included in several courses by the author without the need for a new program or umbrella curriculum. Most recently, a module has been developed for an undergraduate course in File Processing. Added topics include policies, protection models, access control, maintaining integrity, log files, hiding and detecting malicious code, and denial of service.

Position Statement of James Wolfe

By the time computer science students reach their third or fourth year, they should have developed a good set of ethics regarding the use of computer hardware and software, especially if those of us teaching the courses provide encouragement along the way. In the junior- and senior-level courses such

as Network Administration, System Administration, Systems Programming and Operating Systems, we can introduce discussions of information security vulnerabilities without promoting hacking. We can present the flaws in access protection mechanisms and protocols, the hazards of stack overflow and the use of privileged programs, the weaknesses of relying on encryption, and profiles of how these can be exploited. For "administration" courses, the presentation of vulnerabilities can be followed up with techniques and laboratory exercises using security assessment and hardening tools. For "systems" courses, a discussion of the theory behind information security shows its limitations; this leads naturally to discussion of risk assessment - identify vulnerabilities, estimate probability of exploitation, and consider responses and costs.

Position Statement of Michael Fry

Two directions: security-related content can be used as a motivating pedagogical tool, where the goal is better learning of computer science concepts that are not specific to security. A junior/senior course in Computer Networks will include experiments with port scanning, and student presentations on research into how certain D.O.S. attacks work. Better understanding of IP as well as security issues should result.

On the other hand, security consciousness, as part of good citizenship, can be recognized as an important goal for an introductory course in computer science. Content on operating systems and network security (which currently touches on the encryption, privacy law, etc.) will be supplemented with material on malicious attacks, risk, and the roles (perhaps role playing) of system administrators, information security officers, and law enforcement officers, in an attempt to raise awareness of risks and responsibilities. Of course, adding such content means something else will have to be sacrificed.

Position Statement of Erik Wynters

Although technical details related to information security have at times been treated like closely guarded military secrets, entrusted only to those with a "need to know", we believe a free exchange of information benefits users more than secrecy. Knowledge of the issues, vulnerabilities, and means of addressing security concerns is clearly important for computer specialists, but some knowledge in this area is essential for every computer user whether at work or at home.

Given the view delineated above, we strove to include a basic exposure to information security concepts in our basic computer literacy course for majors in all areas. We discuss our experience teaching this information security-augmented version of the literacy course, including difficulties encountered and attainment of goals.

Position Statement of William Calhoun

Security issues should be discussed throughout the undergraduate computer science curriculum. Discussing security in our courses can enliven standard topics while making students more aware of security risks. Even in the more theoretical courses, there are appropriate places to connect the course material with security.

For example, topics discussed in Organization of Programming Languages relate to the buffer overflows that can make a computer vulnerable to "crackers". There are also several places in the Theory of Computation where connections can be made to security issues. Public-key cryptography is based on empirically tested conjectures from computational complexity, and decidability and solvability constraints limit what is possible in fighting viruses.

Position Statement of Robert Montante

Computer Networking is evolving from a specialized topic to a unifying theme for most of the issues in computer systems. An early networking course can touch on practical aspects of operating systems and system architecture, along with technical data communications concepts and topics in network administration.

Security-oriented issues are sometimes added to a course curriculum as a distinct topic, but this can give the ideas an unnatural and foreign flavor.

The most effective way to incorporate security-oriented issues into the curriculum is to include them as natural aspects of normal course topics.

The Bastille Linux Project's hardening script, for example, supplies a smooth application of numerous security concepts to a realistic, hands-on lab activity.

[1] NSF-Grant-01-11: Cybersecurity Education and Research Center for Western Pennsylvania.