Categories and Subject Descriptions
K.3 [Computers & Education]: Computer & Information Science Education - Computer Science Education.

General Terms

Keywords
Security, Projects.

1 Summary
Computer science educators are increasingly being asked to provide education in the area of computer security, and a number of institutions are offering computer security courses and developing computer security programs. However, there is a need for computer security educators to develop “hands-on” projects that enable their students to move beyond a theoretical understanding of the field and develop practical skills that can be used in implementing secure computer systems for their future business and government employers.

This 75-minute panel session will discuss current and future ideas for computer security course projects in a typical computer science undergraduate curriculum. The emphasis of this panel is on practical course projects that emphasize issues and techniques in computer security and that can be used either in a stand-alone course on computer security, or as projects in other related courses at the undergraduate level.

The panelists will demonstrate a consistency of purpose but also a wide variety of approaches among the projects selected and the courses in which they can be used. The schools represented vary from medium to large state universities to a private college to a large independent institute.

The projects to be discussed vary across a number of dimensions. They range from low-level programming exercises (e.g. buffer overflow) to conceptual policy development and implementation (e.g. password policies). The projects deal with computer security from the point of view of the system administrator, the security officer, and the programmer. They touch on a number of other computer science topics, including networking, database systems, and software development, and thus have potential applicability in a variety of courses.

The unifying theme of the panel – the desire to provide “off the shelf” computer security course projects that other undergraduate computer science programs can adopt and implement with ease – will be evident throughout. By presenting a wide variety of projects and approaches to achieve this end, it is hoped that any audience participants who wish to create a cyber security thread or project in their own programs will find some ideas to help them.

The program for the panel will allow each panelist a maximum of 12 minutes to outline their projects and approaches. The remaining 30 minutes will then be reserved for general discussion and questions and contributions from the audience.

2 D. Paul Benjamin
Benjamin’s project is intended to teach the concept of a buffer overflow, and how it can be used to attack a machine. It will also illustrate the usefulness of assembly language programming. This project will be included in our computer architecture course, because that is where we teach assembler programming. It could also be part of an operating system course or a security course.
Each student will program a simple function call in C, and then list the assembly language output of the C compiler. A simple alteration of the assembler code will permit the student to return to a different part of the calling code. Then the student will learn how to insert assembler code so that calling the function causes a shell to execute. This shows the student how a buffer overflow can permit an attacker to run commands on a server.

3 Charles Border

Border is creating a project involving the development and implementation of a policy regarding user passwords. Given a mixed Microsoft Windows 2000 and Linux network this lab exercise will require students to design and then implement a new password policy. The goals for this exercise are to:

1. enhance the students' understanding of what constitutes an effective policy, and
2. demonstrate the difficulties that can arise from a seemingly innocuous change.

The steps in the process include:

First, developing an outline of requirements by surveying existing applications and infrastructure;
Second, writing a policy statement, and
Third, implementing the policy through a script.

Border will discuss the structure and details of this laboratory exercise, including how the heterogeneous Windows/Linux environment affects the policy that is ultimately implemented.

4 Robert Montante

Network administrators have an increasing range of tools available to monitor activity and performance on a network segment. Capturing and displaying the traffic is useful for studying how a network operates, and also for developing skills in administering and maintaining it.

Montante is developing a lab module for a networks administration course that applies packet sniffing tools to administrative tasks. The initial exercise is the installation and basic configuration of appropriate software. This is a basic task for any system administrator. The second and central exercise uses filters to extract interesting and unusual packet streams. A significant issue for this lab is to define what "interesting" and "unusual" packets are. Supportive lecture material for this point covers the formats and construction of data packets, malformed packets, and possible system behaviors when malformed packets are received.

Finding interesting packet streams is a practical problem with this lab. For basic activities it is sufficient to conduct basic network operations on an isolated, pedagogical LAN. But generating malformed packets may be an inappropriate academic activity, and is completely unacceptable on a "production" network. An effective solution to this is to use actual packet streams, recorded from networks that were attacked, as training data sets. Some sources will be discussed.

5 Paul J. Wagner

Wagner is currently developing a database security module and project to be used in either a database systems course or a computer security course. The module focuses on database security in a networked/web-based environment. More specifically, it involves analysis of the security issues related to the individual technologies of database systems, web servers and networks, as well as issues raised by the integration of these technologies. The module also includes examples of particular problems found in Oracle/Apache and Oracle/Internet Information Server (IIS) environments.

The module concludes with a class project involving the security analysis of a particular database system installation in a networked environment on his campus. Students will have an opportunity to examine a particular installation and develop a report outlining the security status of the installation, any problems they’ve found, and recommendations for security enhancements. The students will use several available vulnerability analysis tools as well as analysis techniques suitable to the web/database environment.

Wagner will describe in more detail the major issues and tools to be used in this module and project, as well as his progress on this work.