Computer Security Curriculum at Small Colleges Panel Discussion

Charles Ashbacher
Department of Mathematical Sciences
Mount Mercy College
Cedar Rapids, Iowa 52402
cashbacher@yahoo.com

Abstract

It is no exaggeration to say that the conflict between the people who are using computers for malicious purposes and those who try to stop them is a war. At stake is the very survival of computers as a useful tool. For example, the current fraction of e-mail messages that are unsolicited is approaching eighty percent. Network managers now spend an enormous amount of time doing nothing more than managing the security patches that vendors send out on a regular basis. The purpose of this panel discussion is to provide a forum for computer instructors at small colleges to share their experiences and thoughts on how the principles of computer security can be effectively incorporated into the computer science major.

Position Statement

All teachers of computing must incorporate the basics of computer security into their lesson plans. The ongoing battle between the people who are using computers for malicious ends ("black hats") and those who use them for good ("white hats") has tilted in favor of the "black hats" in recent years. Computer viruses still abound in the wild, junk e-mail is now the overwhelming majority of all messages sent, and companies such as Microsoft are constantly scrambling to issue patches to repair security holes. Some observers believe that at this time the "black hats" rather than the "white hats" are doing the greatest amount of innovation in computing. There are estimates that put the annual worldwide cost of fighting the "black hats" at over a trillion dollars annually.

The events of 9-11 have brought the threat of terrorism from something that is an occasional tragedy to an item that is part of the daily lives of Americans. Cyberterrorism is by definition the use of a computer to commit of an act of terrorism. In general, the definition includes only acts committed remotely, specifically using the Internet. Most of the critical infrastructure of modern industrial societies is controlled by computers, with the equivalent of trillions of dollars being moved electronically on a daily basis. Given this dependence, it is clear that a significant disruption of this flow could have catastrophic consequences.

Over the last three years, I have taught three classes that included a great deal of material related to computer security. In CS 400 Software Engineering in the spring semester of 2003, the class project was the creation of a program to obfuscate Java code. Code obfuscation is the process where source code is modified into a functionally equivalent form, but made much more difficult to read. The purpose of code obfuscation is to make it much more difficult for a "black hat" to decompile and understand the Java bytecode. The program was written in Java and is open source.

In CS399 Special Topics: Computer Security, that I taught in the January term of 2004, the basic principles of computer security were examined. The primary areas covered were:

*) Buffer overflows.
*) Security from the perspective of the client.
*) Security from the perspective of the server.
*) Understanding the IP protocol and how to use that knowledge to launch an attack.

*) The various methods whereby messages can be securely sent from one location to another.
*) How to examine programs with the goal being to carry out an exploitation.

In CSS 400 Software Engineering in the spring semester of 2004, the class project was to create a program that will scan C source code searching for potential security problems. The people at the computer security company Cigital were kind enough to provide their database of identified security issues in C.

With limited monetary and time budgets, instructors at small colleges find it difficult to incorporate security into their offerings in a timely manner. The purpose of this panel discussion is to provide an opportunity for instructors to discuss and share their experiences, both positive and negative, when they have included computer security material in their courses. Other areas of discussion will be thoughts on the future. Points such as:

*) Are we professionally obligated to offer courses in computer security?
*) Where do courses in computer ethics fit into the issue of computer security?
*) How can computer science departments cooperate with philosophy and business departments to offer combined courses in ethical behavior?

can also be examined.