Editorial: Resources for the Computer Security and Information Assurance Curriculum

D. FRINCKE and S. OUDEKIRK
Pacific Northwest National Laboratory

AND

B. POPOVSKY
University of Washington, Seattle

This editorial introduces the articles in this companion issue to the first JERIC special issue on Computer Security and Information Assurance Curriculum. It includes an article that supports making computer security education more accessible through a portable network, and one on lessons learned in developing a workshop for educators. Other articles outline laboratory exercises especially suitable for distance or online education, illustrate ways to teach students about threats, and provide approaches to classroom discussion of disaster recovery.

Categories and Subject Descriptors: K.3 [Computers and Education]; K.3.2 [Computer and Information Science Education]; K.4.1.a [Abuse and Crime Involving Computers]; C.2 [Computer-Communication Networks]; C.2.0 [General]; D.4 [Operating Systems (C)]; D.4.6 [Security and Protection (K.6.5)]

General Terms: Security, Experimentation

Additional Key Words and Phrases: Computer forensics, security, protection

---

1. INTRODUCTION

We begin with a discussion of how to make computer security education more accessible with **Rosenberg and Hoffman's** article, "Taking the Network on the Road: Portable Network Solutions for Computer Security Educators." Many factors make a traditional bricks-and-mortar laboratory difficult to maintain – the premium most campuses place on space, the need to maintain changing technologies, and the difficulty of setting aside a room with enough seats for the often-huge security classes. The authors propose a cost-effective alternative to a permanent classroom or laboratory network: the Portable Educational Network, or PEN. The PEN is a portable, scalable, isolated, and flexible laboratory at The George Washington University, which is built from standard enterprise-grade components to simulate a standard Internet connection. It supports computer network defense exercises by taking the approach of student as attacker and instructor as defender. The instructor can use the PEN to show in real time the effect of attacks on the network, and can walk the class through a range of countermeasures to show their effectiveness (or lack of it).

Authors' addresses: D. Frincke, Computational and Information Sciences Directorate, Pacific Northwest National Laboratory, Richland, WA 99354; S. Oudekirk, Computational and Information Sciences Directorate, Pacific Northwest National Laboratory, Richland, WA 99354; B. Popovsky, The Information School, University of Washington, Seattle, WA 98195.

Permission to make digital/hard copy of part of this work for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage, the copyright notice, the title of the publication, and its date of appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee. Permission may be requested from the Publications Dept., ACM, Inc., 2 Penn Plaza, New York, NY 11201-0701, USA, fax:+1(212) 869-0481, permissions@acm.org
© 2007 ACM 1531-4278/07/1200-ART1 \$5.00.

Because the PEN is an isolated and self-contained network, it is safer to use in typical classrooms than an open connection to an outside laboratory might be. Variations of this lab are in use in a wide range of educational and government institutions, [where](#) they provide a less expensive and highly portable alternative to physically configuring, wiring, and maintaining a fixed-location laboratory.

Wagner and Phillips also address portability issues in their article, “A Portable Computer Security Workshop.” Rather than emphasizing resources for student education, the authors consider the issue of how to efficiently increase the number of educators who can teach security and information assurance classes. They share lessons learned from their experiences in developing and running a computer security workshop for educators. Their target audience is first-time instructors for post-secondary institutions wishing to start a course or laboratory sequence in computer security.

In “Laboratory Exercises in Online Information Assurance Courses,” **Bhagyavati** continues our exploration of how to provide support for information assurance by outlining methods for electronic delivery of security education. In this article the author discusses best practices and experiences drawn from delivering online materials to students over a three-year period.

Once a hands-on network is available and a decision is made to use it to illustrate network weaknesses, the next step is to consider the kinds of experiments to provide. In “Laboratory Experiments for Network Security Instruction,” **Brustoloni** proposes five experiments that illustrate a variety of threats, ranging from eavesdropping, dictionary, and man-in-the-middle attacks to port-scanning, and finger-printing. The sequence concludes with discussion of how to defend computer systems against the threats covered in the earlier exercises. The strategy is “instructor plays the attacker,” which has many of the benefits of the “students attack each other” approach with potentially fewer risks in implementation. The article includes a discussion of student performance before and after working with each experiment, which shows that the exercises did provide a statistically significant (positive) effect on student learning, as well as an increase in student interest and attention.

The last article diverges from traditional security basics. All too rarely do security courses include a section on disaster recovery; the tendency is to discuss recovery only briefly, perhaps as part of the aftermath of dealing with an intruder or with a small amount of physical damage to a facility. However, as shown by **Landry** in “Dispelling 10 Common Disaster Recovery Myths,” disasters happen all the time, and therefore mitigation of and recovery from disasters should be part of the discussion of the physical and virtual threats faced by organizations. There are unique challenges in large scale-disasters. Drawing from personal experience, Landry interweaves lessons learned from his information technology experience in hurricane Katrina with the more traditional topic of threats from attackers. His article is written in a form suitable for classroom discussion and debate for students with a wide range of technical ability.