Editorial: Special Issue on Resources for the Computer Security and Information Assurance Curriculum: Issue 1

D. FRINCKE, S. OUDEKIRK

Pacific Northwest National Laboratory, Richland, WA

AND

B. POPOVSKY

University of Washington, Seattle

This editorial introduces a set of articles in the JERIC special issue on resources for the computer security and information assurance curriculum. It begins with a discussion of why such a special edition is needed and continues by outlining the articles in this volume, as follows: an innovative model for security education based on teaching hospitals; teaching context in computer security through metaphors; tools supporting exploration of cryptography; suggestions for a hands-on Linux course geared towards a student population that includes noncomputer scientists; and finally, projects suitable for a course in computer forensics.

Categories and Subject Descriptors: K.3 [Computing Milieux]: Computers and Education; K.3.2 [Computers and Education]: Computer and Information Science Education; K.4.1 [Computers and Society]: Public Policy Issues--Abuse and crime involving computers; C.2.0 [Computer Communication Networks]: General; D.4 [Software]: Operating Systems; D.4.6 [Operating Systems]: Security and Protection

General Terms: Security, Experimentation

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

1. INTRODUCTION

Welcome to this special issue of the *Journal on Educational Resources in Computing* (JERIC). The special issue presents a collection of articles around the broad topic of providing resources for a computer security and information assurance curriculum. The intent of the publication is to support departments and campuses seeking to devise new programs; in addition, there are ideas for educators who may be seeking new classroom exercises or new approaches to presenting materials, particularly at the introductory level. This issue is paired with another set of articles, to appear in the next issue of JERIC, on the same theme; the second issue has greater emphasis on network and infrastructure security.

Why a special issue on a security-oriented curriculum? Not much more than a decade ago, it was rare for a campus to have even one or two faculty regularly teaching information assurance or computer security courses. Most of these faculties came to sec-

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 1531-4278/07/0600-ART1 \$5.00.

urity from other disciplines, rather than continuing from foundations established during their graduate studies. As to the security concepts being taught, if they were taught at all, they were more likely to be incorporated in database, operating system, or network courses than as stand-alone courses. A special topics course might focus on security, but this was not the norm. Partly because of the newness of the field, the preparation time required teach computer security courses time-consuming. Faculty in this area estimated (anecdotally) that it would take double or triple the time needed for them to prepare their security courses, in contrast to what they spent development traditional computer science classes. In one of the earliest workshops discussing security education, the faculty responsible for teaching these early security courses and concepts indicated that they could find very few textbooks that could be used in their classes. When it came time to publish articles or provide research references to their students, they could reference only one or two journals that focused on security [Frincke and Bishop 2004]. Due in large part to individual faculty members' belief in the importance of the subject of computer security, and with the support of a few dedicated government and commercial representatives, a mutually supportive community was born. This community worked collectively and individually to devise and share teaching methodologies, materials, and philosophies; to evolve standards for a core security/information assurance curriculum; and to advance the field by writing textbooks and establishing conferences, workshops, and journals.

Much has changed in the past fifteen years. It is now common to find computer security courses listed in catalogs as part of the regular offerings – and increasingly the faculty teaching these subjects emphasized security during their graduate studies. There are numerous textbooks, and a plethora of conferences to attend. Security courses and topics are still most commonly found in computer science, engineering, and business – but many are also offered through economics, law, and even philosophy departments, to name a few.

So is there still a need for resource sharing and a special focus from JERIC?

We contend that the answer is still yes. Although the number of security/information assurance educators is growing rapidly and the resources available to academics are far superior to those of the early 90s and before, the field itself is growing even faster than the resources. A course that provided a solid understanding of basic cryptographic techniques, UNIX vulnerabilities, standard malware categories, and software assurance techniques used to go a long way towards satisfying demand, but would barely qualify as entry-level knowledge today. Despite the proliferation of specialized courses in forensics, secure e-commerce, security under resource constraints, and autonomic security (to name just a few new concepts), the gap between what we *need to know* as security educators and professionals and what we *are able to teach* remains wide, and continues to widen.

This widening gap may be attributed, in part, to the natural progression of a maturing discipline. The security education community still wrestles with how to teach about system vulnerabilities (e.g., some teach entire courses devoted to writing viruses, including methods on how to evade detection). We also struggle with how to balance the need to develop skills and the need to educate. These struggles are partly due to the changing environment. To the simpler concerns of the early 1990s we have added more technology (wireless, SCADA, nano, grid), new and varied stakeholders (scientific computing, e-commerce, smart houses), and we have raised the stakes (e-government,

disaster recovery, counter terrorism). Ensuring that course materials and examples remain relevant in the face of dramatic shifts in technology and society, still keeps course preparation a challenge, despite the availability of more materials. In short, we still need to talk – and continue to share ideas as a community – to improve security and information assurance education. Hence, the motivation for this special edition.

We begin this pair of special issues with discussion of teaching methodologies and perspectives – “*how*” to balance the educational goals of a computer security program. The article by **Goel et al.**, called, “Innovative Model for Information Assurance Curriculum: A Teaching Hospital,” gives a model of a teaching hospital as a good metaphor for computer security education. The authors begin with a discussion of philosophical perspectives, models, and learning theories in information assurance classrooms: training versus education, “hear-see-do” paradigms (objectivism and constructivism being a few). They then introduce the concept of a teaching hospital as a useful metaphor for computer security education. As in the earlier article Goel et al. begin with the need to “crystallize theoretical knowledge into field knowledge” in medicine, and progress to the observation that information assurance educators likewise should teach students how to link theory with a rapidly changing practice. The teaching hospital paradigm in use at the New York State Center for Information Forensics Assurance is used as an example. In addition to presenting the teaching hospital model itself, this article provides an assessment of how effectively the technique has been in practice, based on experiences at New York State, and describes as well the degree to which the approach was accepted by students.

Next, we consider the importance of incorporating a societal perspective in the classroom itself. In his article, “Teaching Context in Information Security” **Bishop** emphasizes the holistic nature of computer security education. His perspective is that security policies and mechanisms should not be isolated from the environment in which they are used, and especially should not be discussed (or used) without knowledge of the specific risks considered when they were devised. “Policies need to account for people,” and when they do not, it is unlikely that that they will be successful over the long term. How, then, might a technology-oriented collection of students be coaxed into thinking from this larger perspective rather than lapsing into the potentially more familiar territory of dissecting system calls and hardware to find flaws? Bishop suggests that use of puzzles will discourage formula-based solutions, and can be tied to a broad range of student backgrounds. As an additional benefit, Bishop and his students found the puzzle approach to be enjoyable and approachable, which enhances learning. This article should also be helpful for instructors outside the information assurance area who seek additional ways to develop critical thinking among their students or who want ideas about how to break the traditional lecture mold.

Teaching environments that lead to improvements in critical thinking skills are important, and so is extending student understanding of fundamental principles. Professionals and academics in this discipline are expected to *have* skills and to *understand* concepts. The sheer range of knowledge to be integrated, especially into an entry-level computer security course, can be daunting, and for students computer security courses can be among the most time-consuming. Tools that make it easier to introduce and understand difficult topics are highly beneficial, particularly when they allow experimentation. Continuing with the concept of sharing “*how*” to teach computer security, the article “Ganzua: A Cryptanalysis Tool for Monoalphabetic and Polyalphabetic Ciphers” by **Garcia-Pasquel et al.** provides support for instructors who want to incorporate hands-on cryptanalysis tools in their lectures. *Ganzua*, which means

picklock in Spanish, is a Java-based application designed to assist cryptanalysis of ciphertext. With this tool students can learn for themselves how to solve various cryptograms; the hands-on approach is particularly well suited to introductory courses in cryptology and general computer security. A strong intuitive understanding that different cryptographic systems have different strengths and weaknesses is of great importance for new students, and a hands-on approach serves to demystify cryptanalysis.

The next article is for those interested in how to incorporate a combined skills/knowledge approach. **Shumba** in “Teaching Hands-On Linux Host Computer Security” provides exercises useful for instructors introducing new courses in information assurance to an interdisciplinary audience. These exercises were specifically devised to support a security concepts course, called Cybersecurity Basics, attended primarily by criminology, business, and communications media majors. Teaching students from such diverse majors is a challenge, particularly when the topics are technical and the students are not engineering or computer science majors. Shumba’s article offers a discussion of useful exercises as well as a quantitative assessment of the educational outcomes she observed.

Finally, we include an article on exercises for the study of forensics, **Harrison’s** “A Term Project for a Course on Computer Forensics.” Most forensics classes involve at least a modest use of tools to extract evidence from a hard drive. For instance, students might be given an examination disk with “evidence” to be discovered and retrieved by the student. The authors discuss their experiences in generating and providing examination disks suitable for students in an upper-division undergraduate term project that reinforces classroom discussion of the investigative aspect of disk examination.

Taken together, the articles in this special issue reflect many of the changes in the resource base for security and information assurance educators. We appreciate the time and energy that the authors have put into making their materials available to others in this format. We, and they, hope that our readers find value in what has been produced.

REFERENCES

- FRINCKE, D. AND BISHOP, M. 2004. Joining the security education community. *IEEE Security & Privacy*, (Sept./Oct.), 61-63.