J.Natn.Sci.Foundation Sri Lanka 2006 34(2): 109-110

BOOK REVIEW

Security in Computing (Third edition) by Charles Pfleeger and Shari Pfleeger (2004), Pearson Education (Singapore) Pte. Ltd., India Branch, ISBN 81-297-0042-5. 746 pages. Index. Bibliography.

Received: 06 December 2005; Accepted: 20 January 2005

This publication on Security in Computing by Charles Pfleeger and Shari Pfleeger also discusses other areas of computing, in general and readers with particular interests can find information easily. The chapters of this book are arranged in an orderly manner, commencing with general security concerns followed by the particular needs of specialized applications, and finally management and legal issues. The authors deal with the following five key areas: introduction (threats, vulnerability and control), encryptions, code, management & law and privacy & ethics. This is a very useful book for graduate level students and novices in the field of Computer Security.

In the first chapter, the authors attempt to explain the fundamental concepts of Computer Security. They have introduced most of the concepts very clearly but some important concepts are not outlined completely. (i.e., the full ranges and types of controls). The authors discuss real world problems (i.e.,"Hollywood at Risk") rarely seen in other books written on Computer Security. However, it is not clear why the authors have divided threats into four classes: interception, interruption, modification and fabrication rather than simply deal with the opposites of confidentiality, integrity, and availability.

An attempt is also made to provide an understanding of what encryption is and how it can be used or misused. This chapter is useful for users of encryption but not for designers of new encryption schemes. The books listed as additional reading material is helpful to obtain additional information.

Secure systems development is explained in chapter three. This is an important but often neglected topic and is covered reasonably well. First, the authors write about programming errors (buffer overflows and incomplete access control) and then move on to give the information on viruses, worms and Trojan horses. Naturally, none of these would be useful without some software engineering principles and practices. Authors have explained this fact as well. However, the material is not always completely clear and rigorous. For example, it is implied that Thompson, rather than Cohen, was the first to investigate viruses.

In the fourth chapter, authors have explained protection in general purpose operating systems. Initially there is an introduction to the history of protection in operating systems and later there is an overview of protection features provided by general-purpose operating systems: the protection of memory, files and the executing environment. There are numerous figures in this chapter and they compliment the text well. The authors close the chapter giving information on the control of access to general objects, file protection mechanisms and user authentication. The part dedicated to passwords is particularly well written and covers the topic in great depth. In fact, the information given in this chapter is largely theoretical and I would have liked to see it as an expanded chapter for different practical situations (for example, Protecting Memory in Windows 2000 Operating System).

Trusted Operating Systems Design explained in chapter five, begins with, "What is a Trusted System?" This explanation is transparent and real world examples are given to clarify the content. The whole chapter is very well organized by dividing it into 4 parts. An attempt has been made to explain the content using examples. The implementation section provides several examples, but the explanations are not satisfactory, as design issues are not discussed (for example, Security designs in Unix