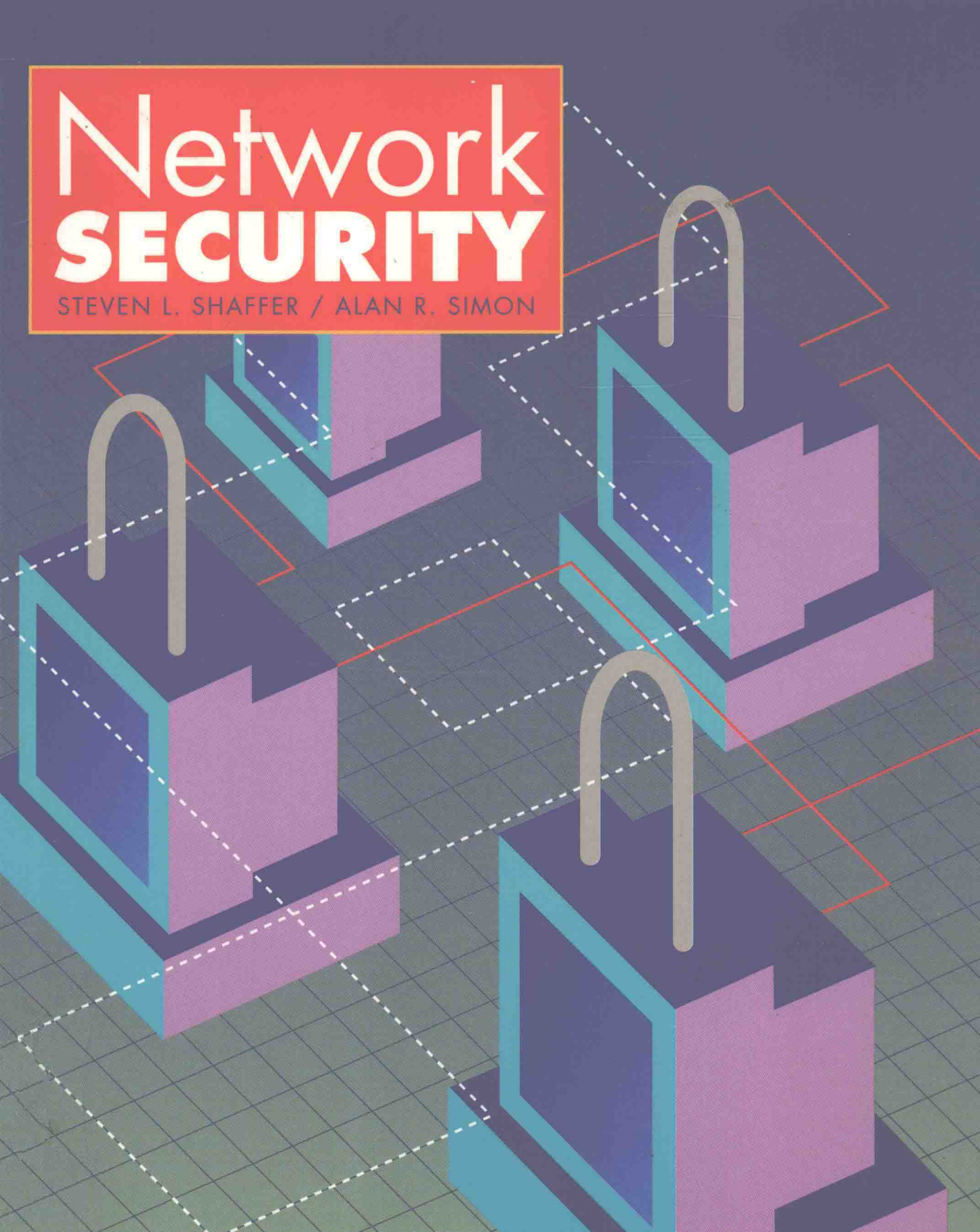
Network SECURITY

STEVEN L. SHAFFER / ALAN R. SIMON



Network SECURITY

Steven L. Shaffer
SSDS Inc.
Inglewood, Colorado

Alan R. Simon
Jackson, New Jersey

AP PROFESSIONAL
A Division of Harcourt Brace & Company
Boston San Diego New York
London Sydney Tokyo Toronto

This book is printed on acid-free paper. ♾

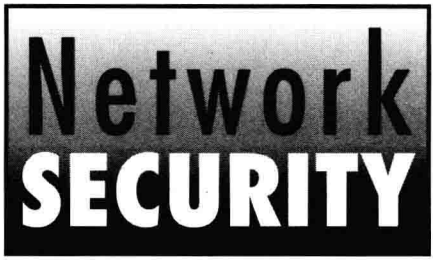
AP PROFESSIONAL
955 Massachusetts Avenue, Cambridge, MA 02139

An Imprint of ACADEMIC PRESS, INC.
A Division of HARCOURT BRACE & COMPANY

United Kingdom Edition published by
ACADEMIC PRESS LIMITED
24–28 Oval Road, London NW1 7DX

ISBN 0-12-638010-4

Printed in the United States of America
93 94 95 96 97 98 EB 9 8 7 6 5 4 3 2 1


Network
SECURITY

This book is the direct result of the generous time given to me and substantial sacrifice by my lovely wife, Joan, my daughter, Jordan, and my son, Dylan.
—Steven L. Shaffer

For Ann, my parents, and my brother.
—Alan R. Simon

Preface

This book is an attempt to bring network security out of the closet. As with many technical disciplines, network security has been the domain of the "network security expert." As a result, a separate language filled with acronymns and unique jargon has developed. There have been a number of very good technical reference books written that effectively address fundamental security mechanisms such as encryption, trusted computing bases (TCBs), auditing, access control, and the like. There have also been a number of security books written about security utilities and secure operating systems.

The specific purpose of this book is to provide those individuals who are responsible for network security in their organization with a practical approach to network security. This book will appeal to system and system security administrators, both in the government and commercial sectors. Many corporate MIS departments have recently seen an upsurge in network security awareness and visibility. In some cases, larger corporations have created an MIS security position and allocated substantial budgets to support overall system and network security programs.

Many corporations are in the process of transitioning their closed and proprietary information processing infrastructure to open, standards-based, integrated enterprises. For the transitioning organization, the ability to maintain and extend security is of paramount importance. Federal, state, and local governments are increasing the importance of network security. This book will also appeal to the average network security practitioner who is interested in understanding practical security approaches and implementation techniques for networks. In addition, several colleges are offering graduate courses in network security as part of an MS degree in MIS or computer science, and the material in this book will be of value to students and faculty members.

Acknowledgments

Pete Wiedemann (Chief Engineer at SSDS, Inc.) provided invaluable insight in the areas of trusted distributed processing and covert channels.

Contents

1

Principles of Distributed Computing and Networks

1.1 INTRODUCTION

In *The Papers of James Madison* in the U.S. Library of Congress, there is a letter written from Thomas Jefferson to James Madison on August 2, 1787. In the letter, Jefferson includes a curious mix of words and numbers that at first glance appears to be meaningless. The third and fourth presidents of the United States were, in fact, exchanging writing using coded communications due to the sensitive nature of its content. In the case of this particular letter, the discussion was of the "king and queen" (presumably of England), the "king's passion for drink" (which was encoded as "the 1647' 678.914. for 411.454"), and similar statements. In the body of the message, Jefferson tells Madison, "I cannot write these things in a public dispatch because they would get into a newspaper and come back here." (My, how things haven't changed much in over 200 years!) In that last sentence expressing his concern, even the word "newspaper" was encoded as "1039.7.207."[1]

It's important to understand that the subject matter of this book—network security—actually can be more broadly defined as "security of communications" and in fact dates back thousands of years. The above example is simply one of thousands, perhaps millions, of encoded communications that have been passed through the ages.

Encoding, or encryption, is simply one of the most highly visible aspects of communications security that has been formalized into security for computer networks, but, as we will see, the discipline encompasses much more.

The need for network security, and measures in that area, roughly parallels the evolution of computing from centralized, mainframe-based to distributed. Initially, most network security strategies were based around physical security measures such as the isolation of terminals and other access devices, guarded access to computer rooms, and similar steps. A large portion of those strategies revolved around personnel requirements, such as issuing security clearances, providing adequate security-oriented training, and so on.

As interception of messages became a major problem (as it had always been even for noncomputer-based communications), encryption began to play an important role. In addition to front-end communications processors, many computers passed their communications streams through encryption and decryption devices. Accompanying hardware-oriented solutions were software security mechanisms, typically hosted on mainframe computers. All access to computer systems and any application and maintenance of security mechanisms were totally under the back room control of the data processing department, which had the effect of centralizing the security function.

As distributed processing—based around workstations and PCs on the desktops and departmental midrange systems—became widely adapted, each system needed its own hardware and software security measures, and two problems surfaced:

- each different system type had its own security requirements and solutions, and all were not compatible, and
- most of the security measures remained under the control of the centralized MIS data center, which resulted in problems similar to those experienced in the early days of the distribution of computing resources in general: slow communications, overplanning for simple functions like deploying a PC, and so on. In fact, most early deployments of desktop resources were blissfully absent of any security procedures, especially dealing with remote system access.

As mission-critical applications (not just the departmental mailing lists) became rehosted onto decentralized, distributed resources, the centralized communications security mechanisms, which had been for terminal-to-host or interhost access, needed to be redeployed to take into account the use of workstations and PCs as terminal emulators.

Network technology that virtually front-ends devices to provide access to a shared bus or a network became popular. Examples included terminal servers both for terminals and for workstations and PCs. Gateways were provided