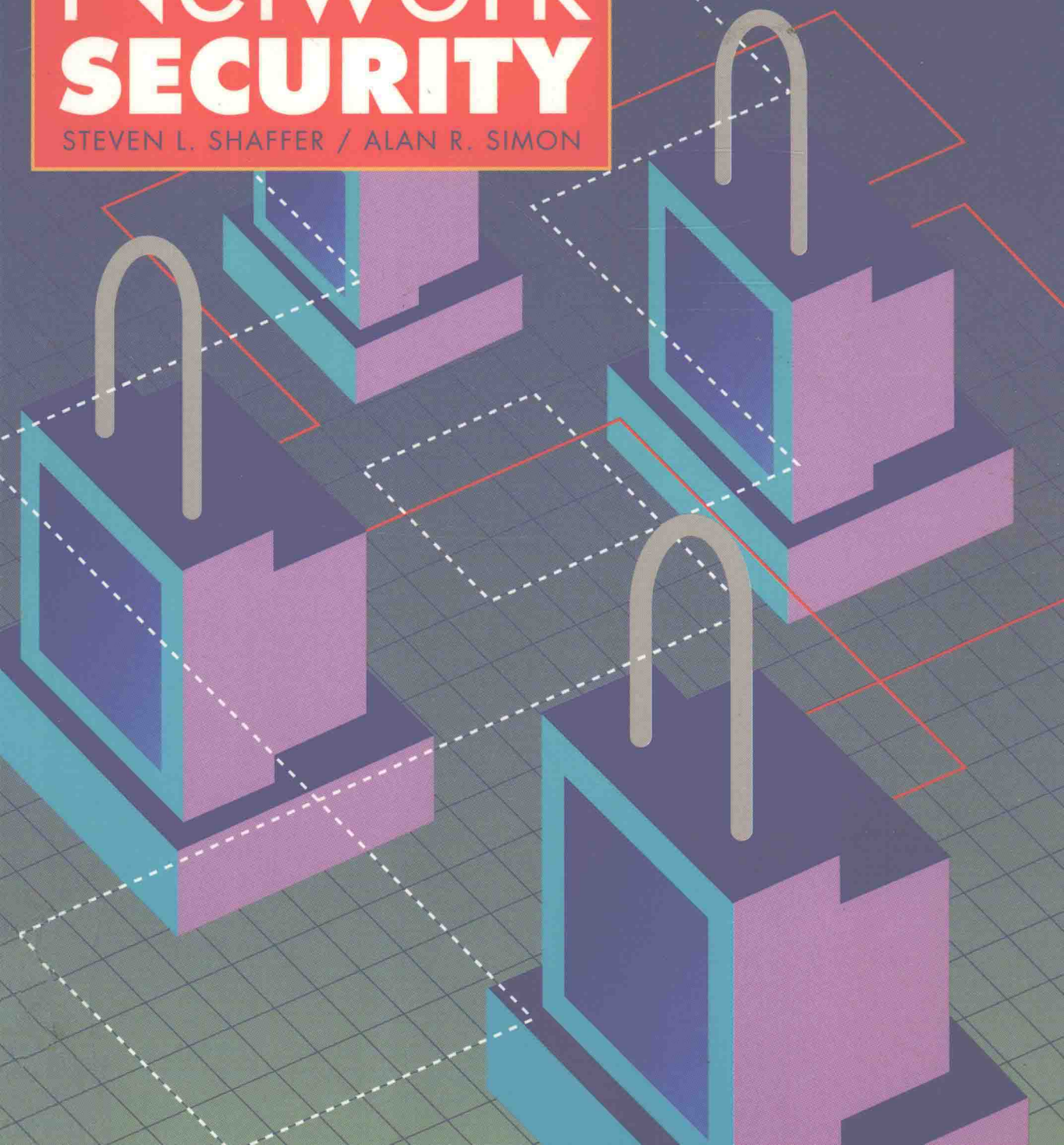


# Network **SECURITY**

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. ∞

Copyright © 1994 by Academic Press, Inc.

All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

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*

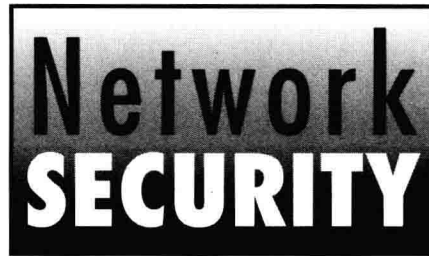
ACADEMIC PRESS LIMITED

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



*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 acronyms 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

---

Preface	vii
Acknowledgments	ix
1 Principles of Distributed Computing and Networks	1
1.1 Introduction	1
1.2 The Network Computing Revolution	3
1.3 Focus and Objective	4
1.4 Secure Distributed Processing	5
Many Existing Views of Distributed Processing	6
Notions of a Distributed System	7
1.5 Distributed Systems Elements Structure for this Book	11
Elements of Distribution	11
Distributed Users	12
Distributed Communications	13
Distributed Processes	15
Distributed Data	15
Distributed Control	16
Distributed Security	17
1.6 Distribution	18
Proximity	18
Number of Nodes	18
Cooperation within and among Elements	19
1.7 Summary	19
End Notes	19
2 The Need for Network Security	21
2.1 Introduction	21
2.2 Information Services and Value	24
2.3 Classified Information	24

2.4	Proprietary and Sensitive Information	25
2.5	Total Dependence	26
2.6	Economics	26
2.7	Summary	27
	End Notes	28
3	The Network Security Challenge	29
3.1	Introduction	29
3.2	The Fundamental Paradox	29
	Tradeoffs 30 • Principal Issues 30	
3.3	Reclusive and Tightly Held Science	32
3.4	Inadequate Funding and Management Commitment	33
3.5	Organizational Opposition	33
3.6	Operational Opposition and Costs	34
3.7	Technical Complexity and Rapid Change	34
3.8	A Moving Target	35
3.9	The Lack of Network Security Standards	37
3.10	Legal Inadequacies	42
3.11	Summary	43
	End Notes	44
4	Network Security Services	45
4.1	Introduction	45
4.2	Security Control Objectives	46
	Policy 46 • Accountability 47 • Assurance 47	
4.3	Continuity of Operations Services	47
	Network Security Mechanisms—Continuity of Operations	48
4.4	Integrity Services	48
4.5	Authentication Services	49
	Identification and Authentication 50 • Distributed Identification and Authentication Services 50 • Cascading Authentication 51 • Goals 52 • Trusted Path Propagation 54 • Privilege Passing 54 • Network Security Mechanisms—Authentication 54	
4.6	Access Control Services	55
	Mandatory Access Controls 56 • Distributed MAC 56 • Discretionary Access Controls 56 • Distributed DAC 57 • Access Control Lists 57 • ACL Issues 57 • Information/Data Labels 59 • Capabilities/Functions—Based Access Control 60 • Logical Networking Controls 61	

4.7	Confidentiality Services	61
	Network Security Mechanisms—Confidentiality	61
4.8	Nonrepudiation Services	70
	Network Security Mechanisms—Nonrepudiation	71
4.9	Assurance	71
4.10	Summary	72
	End Notes	72
<b>5</b>	<b>Network Security Disciplines</b>	<b>75</b>
5.1	Introduction—Security Engineering Disciplines	75
5.2	Physical Security	75
5.3	Personnel Security	76
5.4	Information Security	77
5.5	TEMPEST	78
5.6	Network and Computer Security	79
5.7	Communications Security	80
5.8	Industrial Security	80
5.9	Operations Security	81
5.10	Life-Cycle Security Engineering	81
5.11	Summary	82
<b>6</b>	<b>Network Security Approaches and Mechanisms</b>	<b>83</b>
6.1	Introduction	83
6.2	The ISO/OSI Reference Model	83
	Physical Layer—Layer 1	84 • Data Link Layer—Layer 2
	Network Layer—Layer 3	86 • Transport Layer—Layer 4
	Session Layer—Layer 5	87 • Presentation Layer—Layer 6
	Application Layer—Layer 7	88 •
6.3	Network Security Services Revisited	88
6.4	Network Security Mechanisms	89
	Specific Security Mechanisms	90 • Pervasive Security Mechanisms
6.5	Layering and Placement of Network Security Services and Mechanisms	92
	Physical Layer	93 • Data Link Layer
	Network Layer	95 • Transport Layer
	Session Layer	96 • Presentation Layer
	Application Layer	97
6.6	An Example of a Network Security Implementation	98
6.7	Summary	101
	End Notes	101

- 7 Personal Computer Networking—Security Issues and Approaches 103
  - 7.1 Introduction—The PC Networking Revolution 103
  - 7.2 Practical Guidance for PC Networking 106
  - 7.3 PC Physical Security Concerns 106
  - 7.4 Identification and Authentication—Network Operating Systems 107
    - Passwords 108 • Mandatory Access Controls 111 • Discretionary Access Controls 111 • Novell NetWare File and Directory Security 112 • Banyan VINES File and Directory Security 113 • Simultaneous Log-ons 114 • Encryption 115
  - 7.5 Application Protection in a PC Networking Environment 116
    - Security for Network Applications 117
  - 7.6 Summary 119
    - End Notes 119
- 8 Controlling Viruses and Trojan Horses 121
  - 8.1 Introduction 121
  - 8.2 Viruses 122
    - Virus Advancement 123 • Virus Protection 125 • Software Acquisition 126 • Secure Systems 126 • Network Performance Alarms 126 • Preventative Program Utility 127 • Gateways and Filters 127 • Detective Software 127 • Computer Emergency Response Teams 128 • NOS Virus Protection 128 • Practical Virus Advice 129 • Practical Virus Prevention 129 • Specific and Practical Actions 131 • Ongoing Activities 132 • Government 132 • Commercial 132 • Summary—The Virus Threat 133
  - 8.3 Trojan Horses 133
    - Introduction 133 • Types of Trojan Horses 134
  - 8.4 Techniques for Introducing a Trojan Horse into Systems 136
    - Introducing a Trojan Horse in Hardware 136 • Introducing a Trojan Horse in Software 137 • Introducing a Viritic Trojan Horse 138 • Introducing a Trojan Horse through the Use of a Trap Door 139
  - 8.5 Exploitation 139
    - System Vulnerabilities Exploited by Trojan Horses 140 • Absence of Security Policy 140 • Inadequate Security Policy or Countermeasures 141 • Lack of Support for Security Features 141 • Discretionary Access Controls 142 • Mandatory Access Controls 142 • Programming Environment 143 • The Insider Threat 144

8.6	Examples of Trojan Horses	145										
	Case 1—Space Physics Analysis Network	146 • Case 2—A Money Order Trojan Horse	147 • Case 3—A Trojan Horse in a Pharmaceutical Company	148								
8.7	Identification of Trojan Horses	149										
	Observation	149 • Automated Comparison Assessment	150 • Audit Control	152 • Centralized Control	152							
8.8	Prevention	153										
	Mandatory Access Controls	153 • Integrity Controls	155 • Discretionary Access Controls	155 • Management of Software Development	156 • Logic Flow Diagrams	156 • Documentation	157 • Techniques to Eliminate Trojan Horses in User Code	158 • Restricted User Software Development or Isolation	158 • Manual Review of Logic/Source	158 • Behavioral Observation	159 • Risk Management Scheme	159
8.9	Maintaining “Trojan Horse–Free” Code	160										
	Training	160 • Encryption	160 • Read-Only Memory	161 • Configuration Management and Control	161							
8.10	Summary	162										
	End Notes	163										
9	Covert Channels	165										
9.1	The Covert Channel Threat	165										
	Causes for Covert Channels	166										
9.2	General Concepts	166										
	Storage and Timing Channels	167 • Definition of Covert Channels	169									
9.3	Covert Channel Taxonomy	169										
	Defined Covert Channels	169 • Undefined Covert Channels	170									
9.4	Exploitation of Covert Channels	170										
	Identification of a Covert Channel Candidate	170 • Channel Exploitation after Identification	171 • Channel Access	172 • Channel Modulation	173 • Covert Protocols	173 • Information Reception	174 • Information Usage and Benefit	174				
9.5	System Vulnerabilities Exploited by Covert Channels	174										
	Covert Storage Channels—Examples	175 • Covert Timing Channels	177									

9.6	Covert Channel Analysis and Measurement Techniques	177
	The Access Control Method 178 • Informal Methodologies 178 • The Information Flow Method 178 • The Shared Resource Matrix Method 179 • Formal Methodologies 180 • Formal Verification 180	
9.7	Practice and Examples	180
	NCSC Certified Systems 181 • NCSC Practices 181	
9.8	Guidance to Developers and Evaluators	181
	Measurement by Analysis and Engineering Estimate 182 • Measurement by Experiment 184 • Bursty Channels 185 • Considerations in Design 186 • Considerations during Implementation 187 • Identification of Covert Channels 187	
9.9	Countermeasures	188
9.10	Elimination of Covert Channels	188
	Bandwidth Reduction Techniques 189 • Limited Access 189 • Channel Sterilization 190 • Noise Introduction 190 • Encryption 191	
9.11	Damage Confinement	191
	Monitoring Techniques for Remaining Covert Channels 191 • Configuration Management and Control 193	
9.12	Summary	194
	End Notes	194
10	Practical Approach to Network Security	197
10.1	Introduction	197
10.2	Practical Network Security Objectives	198
10.3	Senior Management Commitment	198
10.4	Network Risk Analysis	200
	Benefits 202 • Security Perimeter 202 • System Decomposition 202 • Risk Analysis Team 205 • Sensitivity Assessment 206 • Technically, Logically, and Organizationally 207 • Valuation of Information Assets 207 • Identification of Threats 209 • Threat Environment 210 • Threat Categories 213 • Threats—LAN Communications 215 • Threats—Long-Haul Communications 215 • Threat Logic Tree 215 • Threat Rejection Logic 216 • Determining Vulnerability to Threats 216 • Degree of Risk 217 • Countermeasure Application 218 • Residual Risk 219 • Process Iteration 219 • Certification Process 221 • Network Accreditation 222 • Continuance 222	

10.5	Network Security Policy	222
	Discretionary Access Controls	224 • User ID and Passwords 225 •
	Host Discretionary Access Controls	225 • Biometric—Discretionary
	Access Control	225 • Mandatory Access Controls 226 •
	MAC—Physical Separation	226 • MAC—Segmentation 227 •
	MAC—Resource Isolation	227 • Marking Policy 227 • Physical
	Security	227 • Accountability 228 • Assurance 228
10.6	Security Management Personnel	229
	Network Security Manager	229 • Network Security Officer(s) 230 •
	Network Security Administrators	230
10.7	Network Security—Policies and Procedures	231
	Training and Awareness	231 • Software Development and
	Introduction	233 • System Backups 233 • Reporting of Security
	Incidents	234
10.8	Maximize Inherent Security Capabilities in Design	234
	Common Sense	235 • Principle of Least Privilege 235 • Physical
	Separation	235 • Segmentation 236 • Heterogeneous
	Implementations	236 • Filtering Bridges and Routers 237 •
	Dedicated Network Resources	237 • Selective Service/Access
	Menus	238 • Security Overhead and Transparency 238
10.9	Summary	239
11	Advanced Network Security Strategies	241
11.1	Introduction	241
11.2	Integrity—The New Network Security Frontier	242
11.3	Denial of Service—Dependence on Reliability, Maintainability, and Availability	242
11.4	Accountability	243
11.5	Network Security Integration	244
11.6	Network Security Standards	244
11.7	Security Overhead and Transparency	246
11.8	High-Performance Systems	246
11.9	Public Disclosure of Security-Relevant Information	246
11.10	Intrusion Detection Systems (IDS)	247
11.11	Security Mechanism Communalities	248
11.12	Uniform Use of Encryption Mechanisms	248
11.13	Uniform Labeling	249
11.14	Covert Channels	249
11.15	Upward Compatibility of Security Services	250

**xviii    Contents**

11.16	Composability of Security Properties	250
11.17	Capability-Based Protection	250
11.18	Modeling Distributed Systems	251
11.19	Summary	251

**12 Network Security Standards    253**

12.1	Introduction	253
12.2	SNMP V2.0	253
12.3	IEEE 802.10	255
	802.10 Parts 255   •   Secure Data Exchange (SDE) 256   •   Layer 2	
	Security Services versus those of OSI 258   •   Key Management 258	
12.4	Summary	259
	End Notes	259

**Appendix: Representative Network Security Programs    261**

**Bibliography    303**

**Index    309**

# 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.”<sup>1</sup>

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.

## 2 Network Security

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