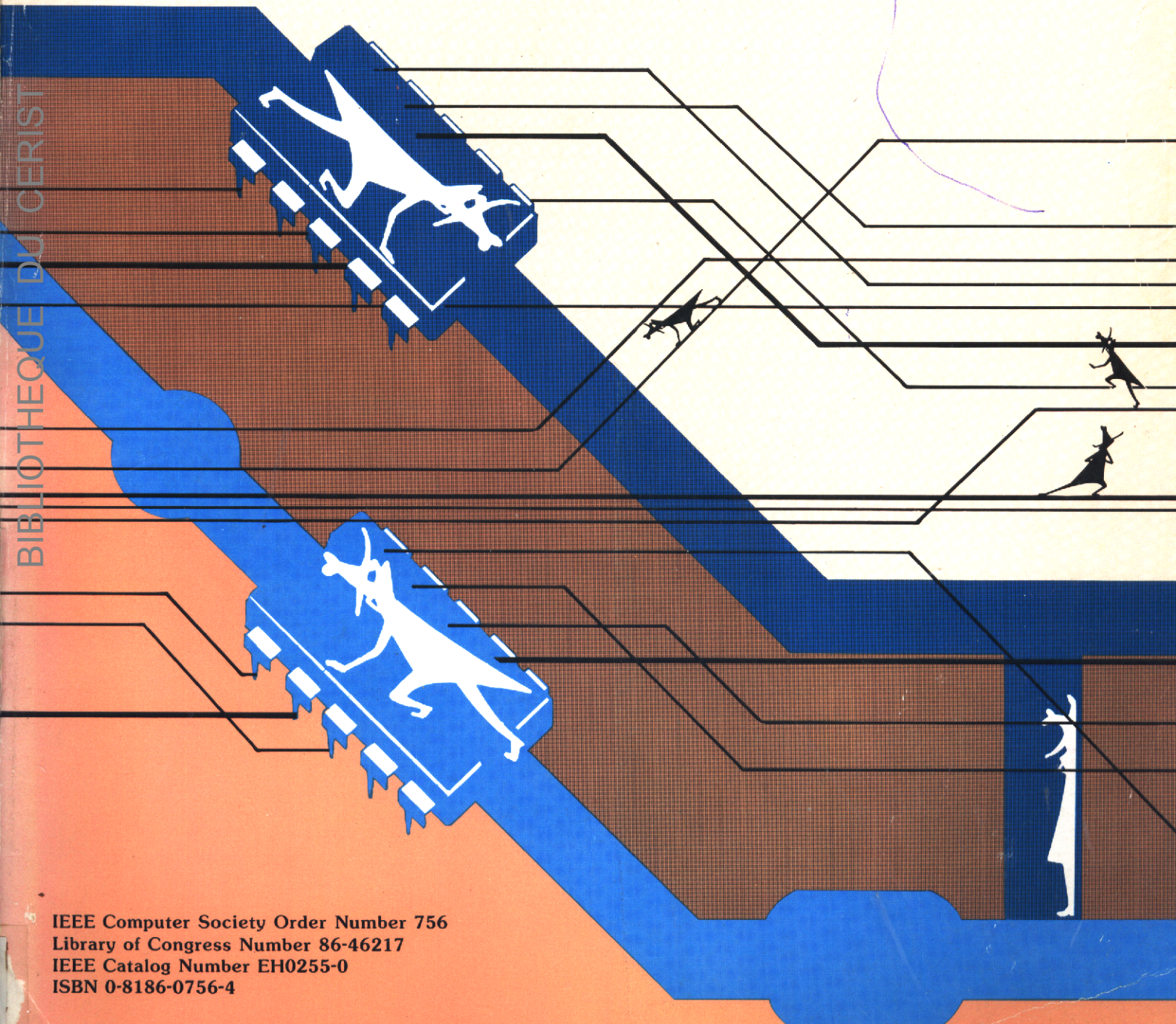


c 1994

TUTORIAL COMPUTER AND NETWORK SECURITY


Marshall D. Abrams and Harold J. Podell



BIBLIOTHEQUE DU CERIST

IEEE Computer Society Order Number 756
Library of Congress Number 86-46217
IEEE Catalog Number EH0255-0
ISBN 0-8186-0756-4

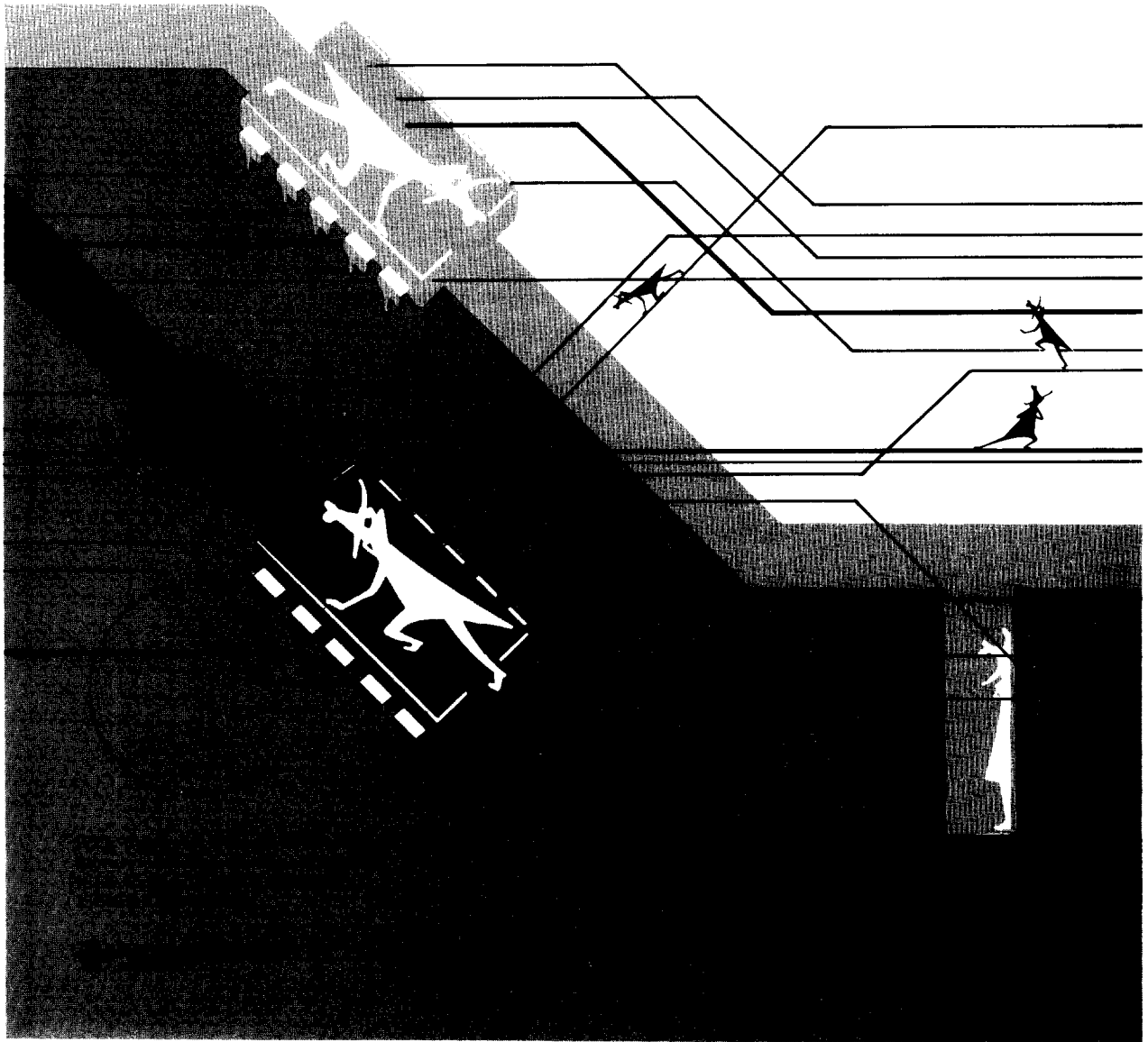
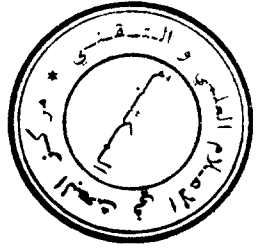
 THE COMPUTER SOCIETY
OF THE IEEE

 THE INSTITUTE OF ELECTRICAL
AND ELECTRONICS ENGINEERS, INC.

IEEE
COMPUTER
SOCIETY
PRESS 

TUTORIAL
**COMPUTER
AND
NETWORK SECURITY**

Marshall D. Abrams and Harold J. Podell



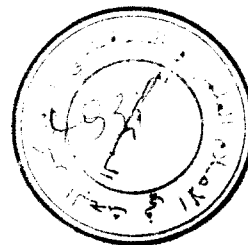
BIBLIOTHEQUE DU CERIST

Published by IEEE Computer Society Press
1730 Massachusetts Avenue, N.W.
Washington, D.C. 20036-1903

COVER DESIGNED BY JACK I. BALLESTERO

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limits of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 29 Congress Street, Salem, MA 01970. Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication permission, write to Director, Publishing services, IEEE, 345 E. 47 St., New York, NY 10017. All rights reserved. Copyright © 1987 by The Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number 756
Library of Congress Number 86-46217
IEEE Catalog Number EH0255-0
ISBN 0-8186-0756-4 (Paper)
ISBN 0-8186-4756-6 (Microfiche)



Order from: IEEE Computer Society
Post Office Box 80452
Worldway Postal Center
Los Angeles, CA 90080

IEEE Service Center
445 Hoes Lane
Piscataway, NJ 08854

IEEE Computer Society
Avenue de la Tanche, 2
B-1160 Brussels,
Belgium



THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

Preface

This tutorial text is written for those who are concerned with security in automated systems, and those who should be concerned. We have tried to bridge the gaps between civil government, military, and private sector. Actually, we think these gaps are more apparent than real. All three groups are concerned with security policy, cost/effectiveness, risk management, and residual risk acceptance. Their emphases may differ, but the concerns are there. Different vocabularies emphasize differences rather than similarities. This book is about information system security, which includes data security, computer security, and network security. Though we often refer to information system security as computer security, we intend to imply the broader context.

We think that computer security has reached a "critical mass." *The Trusted Computer Security Criteria* (TCSEC), the *Orange Book*, has become very well known. It has also become a Defense Department Standard. The annual National Computer Security Conference has outgrown the facilities at the National Bureau of Standards. Other conferences are also experiencing growth pressures. The National Computer Security Center is working to extend the application of the TCSEC to networks and databases. The *Evaluated Products List* is growing. Many interesting and useful computer systems have been evaluated or are in the process. There should be a goodly number of secure systems available in the next few years.

The state-of-the-art is changing very rapidly. This is reflected in the literature. Textbooks rapidly become obsolete. We offer this tutorial text as one small way to disseminate knowledge about computer security. We hope you find it useful. Your comments and suggestions for the next edition will be appreciated.

The book is organized into five major sections: Introduction, Computer System Security, Network Security, Glossary, References, and Recommended Readings. The first three sections are subdivided.

Section 1.1 provides an introduction to the various concepts and considerations that constitute computer and network security. Many important subjects are covered lightly; additional treatment occurs in subsequent sections. Each section is written as a stand-alone discussion of a topic; therefore, there is some redundancy between related sections. Introductory overview papers have been selected to help establish a framework for what follows. Perhaps you will want to pass one of these papers, appropriately highlighted, up the management chain!

Section 1.2 takes a closer view of the context for our concerns with security. Issues of public policy, national defense, individual privacy, and property rights are all constituent parts.

Section 2.1 addresses management issues in computer system security. A basic framework to establish a structure for viewing computer systems security is established. Three aspects of the structure are discussed: management responsibility and authority; managerial; physical: administrative, technical, and communications controls and management decision-making for systems under development.

Formal models; the basis for proofs of correctness and trustworthiness, are discussed in Section 2.2. The concept of a formal model for computer security is central to (1) the development of trusted computer system evaluation, (2) the implementation of the controls specified by the criteria into a trusted computing base (TCB) of hardware and software, and (3) the verification and, in some cases, testing that the TCB implementation is a correct implementation of the model.

Standards provide a basis for comparison, interoperation, and evaluation. Section 2.3 provides a guide to this aspect of computer network security. The sections on standards are adapted from key papers and documents pertaining to the security standards issues. There are very few national standards and guidelines available for use in defining levels of computer and network security. Important computer security standards and guidance from the National Bureau of Standards and the National Computer Security Center (NCSC) are discussed. In addition, the security aspects of draft guidance on network security from the International Organization for Standardization Open Systems Interconnection seven-layer reference model and the Consultative Committee for International Telegraph and Telephone standards are presented.

Application requires technology and methodology. These are discussed in Section 2.4. TCB specific issues are presented by adapting selected work from the NCSC and Stanley Ames, Morrie Gasser, and Roger Schell.

Security of computerized databases is an area of current interest and is discussed in Section 2.5, where selected database security issues pertaining to NCSC criteria are presented and unresolved security issues related to DBMS are resolved.

Examples of commercially available systems and the concerns of their developers are extremely important to practitioners in separating theory from practice. Section 2.6 contains a number of such examples. NCSC publishes an *Evaluated Products List* and individual product evaluation reports. The discussion provides a sample of NCSC's activity with respect to evaluating security products against NCSC criteria.

Having achieved some degree of success with monolithic computer systems, one of the next security concerns is networks. Section 3.1 provides an overview of this topic. Issues are addressed concerning the nature of a network, network architecture, and security services.

Encryption, discussed in Section 3.2, is the most important mechanism in computer and network security. In fact, it is so important that it is often confused with a service. This section contains a cryptographic overview, including keys, single (secret) key cryptosystems, two (public) key cryptosystems, block and stream ciphers, link and end-to-end encryption, standards, network protocol security, message authentication, and the Commercial COMSEC Endorsement Program.

Access control and authentication are extended to the network environment in Section 3.3. After reviewing individual user identification and authentication, the concept is extended to messages, also discussed in conjunction with encryption in Section 3.2. Several approaches and products are discussed. Although introduced earlier, network protocols are given their own Section, 3.4. Protocol security is discussed in terms of the *Open System Interconnection Protocol Reference Model*. Specific security systems and mechanisms are identified and related to the layered protocol model. As we did with computer systems, we conclude the discussion of network security with examples and applications. Section 3.5 summarizes the importance of standards, followed by discussions of applications in financial institution key distribution, space shuttle security, and development of a multilevel secure local area network. The conclusions, which follow Section 3.5, reflect our initial observation that computer security has reached a "critical mass."

The glossary has been amalgamated from definitions in the papers considered and from several pre-existing glossaries. We believe it serves as a baseline that integrates selected computer and network security terms. The recommended readings and other references conclude the book.

Marshall D. Abrams
Harold J. Podell
Silver Spring, MD
October 1986

Table of Contents

Section 1: Introduction	1
Section 1.1: Overview	3
An Overview of Computer Security.	9
<i>R.C. Summers (IBM Systems Journal, Volume 23, Number 4, 1984, pages 309-325)</i>	
Security Considerations for Personal Computers.	26
<i>W.H. Murray (IBM Systems Journal, Volume 23, Number 3, 1984, pages 297-304)</i>	
NBS Perspectives on Risk Analysis: Past, Present, and Future.	34
<i>S.W. Katzke (Minutes of the Federal Information Systems Risk Analysis Workshop, 1985, pages 2-3-2-5)</i>	
Section 1.2: Society and Policy	37
Computer Privacy in America: Conflicting Practices and Policy Choices	45
<i>B.G. Matley (Proceedings of the 1985 Symposium on Security and Privacy, 1985, pages 219-223)</i>	
DoD Overview: Computer Security Program Direction	50
<i>J.S. Greene, Jr. (Proceedings of the 8th National Computer Security Conference, 1985, pages 6-10)</i>	
COMSEC in Transition	55
<i>O.C. Lewis (Signal, August 1985, pages 122-124)</i>	
Section 2: Computer System Security	59
Section 2.1: Management Issues	61
An Analysis of the Differences between the Computer Security Practices in the Military and Private Sectors	71
<i>L.S. Chalmers (Proceedings of the 1986 Symposium on Security and Privacy, 1986, pages 71-74)</i>	
An Economically Feasible Approach to Contingency Planning	75
<i>R.H. Courtney, Jr. (Proceedings of the 9th National Computer Security Conference, 1986, pages 237-244)</i>	
Section 2.2: Formal Models	83
Proving a Computer System Secure.	88
<i>W.D. Young, W.E. Boebert, and R.Y. Kain (Scientific Honeyweller, July 1985, pages 18-27)</i>	
Section 2.3: Standards	99
Department of Defense Trusted Computer System Evaluation Criteria	117
<i>Department of Defense Computer Security Center (Department of Defense CSC-STD-001-83, 1983, pages 1-5, 91-92, 107)</i>	
A Status Report on the Development of Network Criteria	128
<i>S. Brand (Proceedings of the 8th National Computer Security Conference, 1985, pages 145-151)</i>	

Section 2.4: Technology and Methodology	135
Security Kernel Design and Implementation: An Introduction	142
<i>S.R. Ames, Jr., M. Gasser, and R.R. Schell (Computer, July 1983, pages 14-22)</i>	
A Security Kernel for a Multiprocessor Microcomputer	151
<i>R.R. Schell (Computer, July 1983, pages 47-53)</i>	
Issues in Discretionary Access Control	158
<i>D.D. Downs, J.R. Rub, K.C. Kung, and C.S. Jordan (Proceedings of the 1985 Symposium on Security and Privacy, 1985, pages 208-218)</i>	
Section 2.5: Database Security	169
On the Logical Extension of the Criteria Principles to the Design of Multilevel Database Management Systems	173
<i>M. Schaefer (Proceedings of the 8th National Computer Security Conference, 1985, pages 28-30)</i>	
Design Overview for Retrofitting Integrity-Lock Architecture onto a Commercial DBMS	176
<i>R.D. Graubert and K.J. Duffy (Proceedings of the 1985 Symposium on Security and Privacy, 1985, pages 147-159)</i>	
Commutative Filters for Reducing Inference Threats in Multilevel Database Systems	189
<i>D.E. Denning (Proceedings of the 1985 Symposium on Security and Privacy, 1985, pages 134-146)</i>	
Integrity in Trusted Database Systems	202
<i>R.R. Schell and D.E. Denning (Proceedings of the 9th National Computer Security Conference, 1986, pages 30-36)</i>	
Section 2.6: Computer System Applications	209
Data Security: A Growing Concern	213
<i>P.M. Roberts (Honeywell Information Systems, Inc., Monograph, 1985, pages 1-6)</i>	
Scomp: A Solution to the Multilevel Security Problem	220
<i>L.J. Fraim (Computer, July 1983, pages 26-34)</i>	
An EMACS Based Downgrader for the SAT	228
<i>J. McHugh (Proceedings of the 8th National Computer Security Conference, 1985, pages 1-10)</i>	
Secure Computing: The Secure Ada Target Approach	238
<i>W.E. Boebert, R.Y. Kain, and W.D. Young (Scientific Honeyweller, July 1985, pages 1-17)</i>	
Designing the GEMSOS Security Kernel for Security and Performance	255
<i>R.R. Schell (Proceedings of the 8th National Computer Security Conference, 1985, pages 108-119)</i>	
SE/VMS: Implementing Mandatory Security in VAX/VMS	267
<i>S. Blotcky, K. Lynch, and S. Lipner (Proceedings of the 9th National Computer Security Conference, 1986, pages 47-54)</i>	
Section 3: Network Security	275
Section 3.1: Overview	277
Data Security in Computer Networks	282
<i>S.C. Kak (Computer, February 1983, pages 8-10)</i>	
Network Security Overview	285
<i>S.T. Walker (Proceedings of the 1985 Symposium on Security and Privacy, 1985, pages 62-76)</i>	

Networks Are Systems: A Discussion Paper.	300
<i>J. Rushby (Proceedings of the Department of Defense Computer Security Center Invitational Workshop on Network Security, 1985, pages 7-24-7-38)</i>	
Observations on Local Area Network Security	317
<i>M.D. Abrams (Proceedings of the Aerospace Computer Security Conference: Protecting Intellectual Property in Space, 1985, pages 77-82)</i>	
Section 3.2: Cryptography	323
Cryptography: Encryption and Authentication	332
<i>Analysis Communications Systems Corp. (Everything You Wanted to Know about DES Security But Did Not Know Who to Ask, 1984, pages 3-1-3-9)</i>	
Requirements for Key Management Protocols in the Wholesale Financial Services Industry	341
<i>M.B. Greenlee (IEEE Communications Magazine, September 1985, pages 22-28)</i>	
Section 3.3: Access Control and Authentication	349
Electronic Document Authentication.	354
<i>R.R. Jueneman (To be submitted to IEEE Communications Magazine, 1987)</i>	
Section 3.4: Protocols	367
Security in High-Level Network Protocols	371
<i>V.L. Voydock and S.T. Kent (IEEE Communications Magazine, July 1985, pages 12-24)</i>	
Section 3.5: Network Applications	385
Automated Distribution of Cryptographic Keys Using the Financial Institution Key Management Standard	387
<i>D.M. Balenson (IEEE Communications Magazine, September 1985, pages 41-46)</i>	
Space Shuttle Policies and Programs	393
<i>E.L. Keith (Proceedings of the Aerospace Computer Security Conference: Protecting Intellectual Property in Space, 1985, pages 11-20)</i>	
Development of a Multilevel Secure Local Area Network	403
<i>D.D. Schnackenberg (Proceedings of the 8th National Computer Security Conference, 1985, pages 97-104)</i>	
Section 4: Conclusions	411
Section 5: Glossary	413
Section 6: References/Other Readings	425
Section 7: Recommended Readings	429