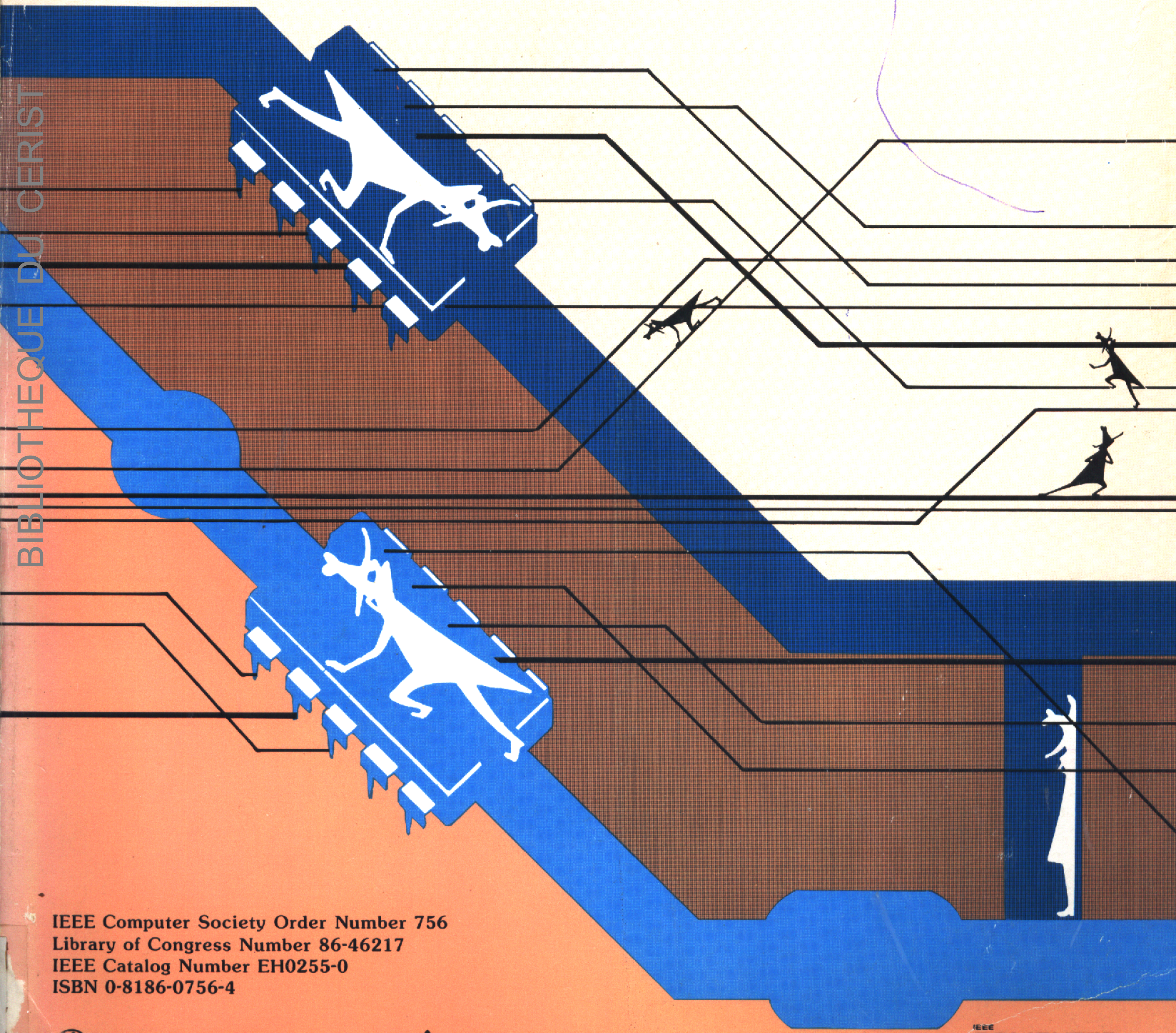
c 1994

TUTORIAL

COMPUTER AND NETWORK SECURITY

Marshall D. Abrams and Harold J. Podell



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

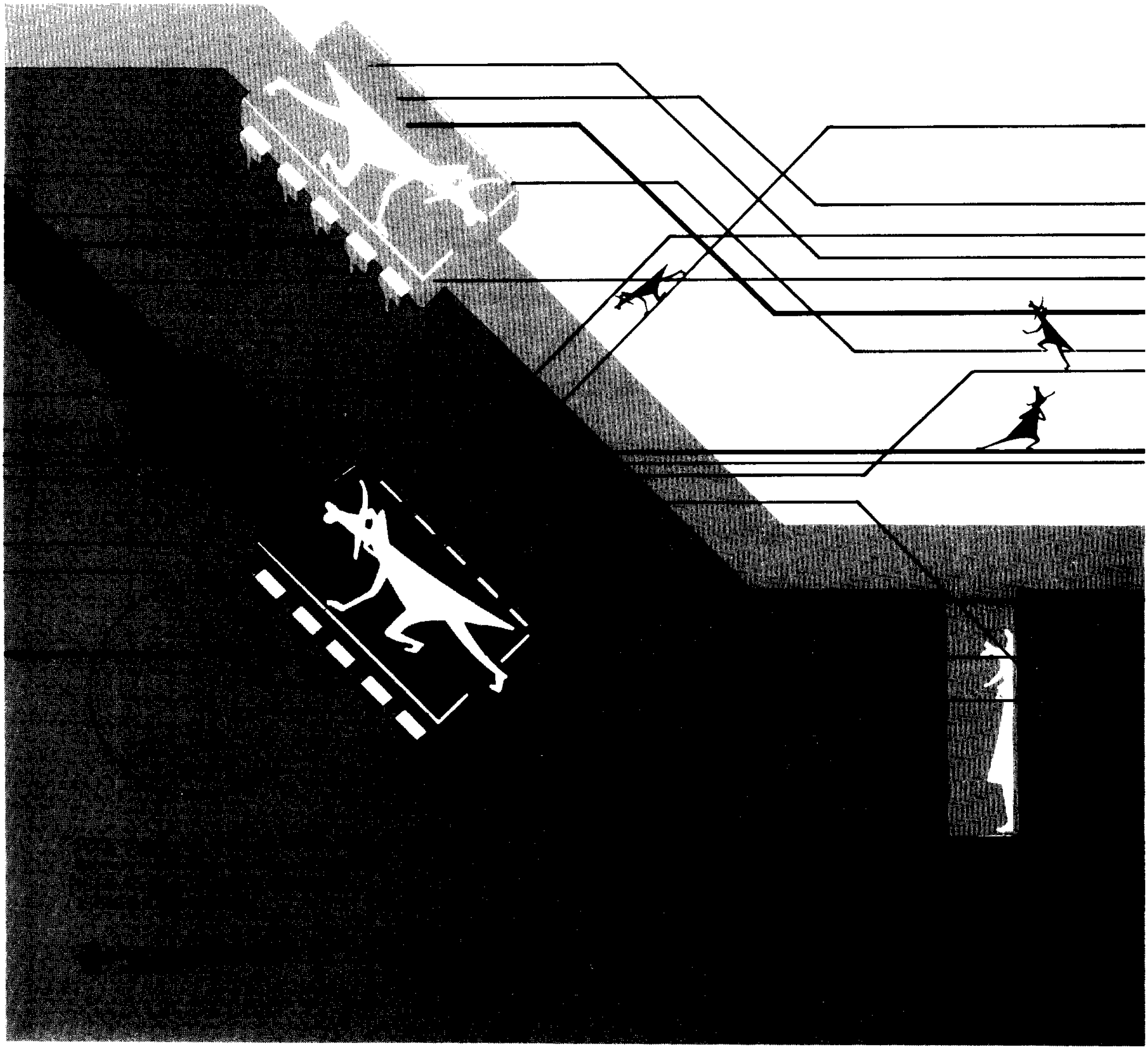
IEEE
THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

IEEE COMPUTER SOCIETY PRESS

TUTORIAL

COMPUTER AND NETWORK SECURITY

Marshall D. Abrams and Harold J. Podell



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

COVER DESIGNED BY JACK I. BALLESTERO

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

IEEE
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