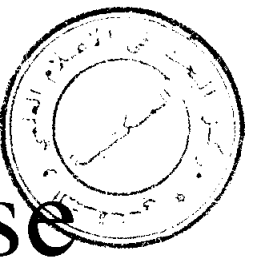
THE
SYSTEMS
PROGRAMMING
SERIES

Database Security and Integrity

E.B. FERNANDEZ
R.C. SUMMERS
C. WOOD



Database Security and Integrity

EDUARDO B. FERNANDEZ
RITA C. SUMMERS
CHRISTOPHER WOOD
International Business Machines Corporation

ADDISON-WESLEY PUBLISHING COMPANY
Reading, Massachusetts · Menlo Park, California
London · Amsterdam · Don Mills, Ontario · Sydney

This book is in the
Addison-Wesley Systems Programming Series

Consulting editors: IBM Editorial Board

Library of Congress Cataloging in Publication Data

Fernandez, Eduardo B 1936-
Database security and integrity.

(The Systems programming series)
Includes bibliographies and index.
1. Data base management. 2. Computers—Access control. I. Summers, Rita C., joint author. II. Wood, C., joint author. III. Title.
QA76.9.D3F47 001.64 80-15153
ISBN 0-201-14467-0

ISBN 0-201-14467-0
DEFGHIJK-HA-89876

THE SYSTEMS PROGRAMMING SERIES

*The Program Development Process Part I—The Individual Programmer	Joel D. Aron
The Program Development Process Part II—The Programming Team	Joel D. Aron
*Mathematical Foundations of Programming	Frank Beckman
*Structured Programming: Theory and Practice	Richard C. Linger Harlan D. Mills Bernard I. Witt
*Coded Character Sets: History and Development	Charles E. Mackenzie
*The Structure and Design of Programming Languages	John E. Nicholls
*The Environment for Systems Programs	Frederic G. Withington
*Communications Architecture for Distributed Systems	R. J. Cypser

An Introduction to Database Systems, Third Edition	C. J. Date
*Database Security and Integrity	Eduardo B. Fernandez Rita C. Summers Christopher Wood
Interactive Computer Graphics	James Foley Andries Van Dam
*Compiler Design Theory	Philip M. Lewis II Daniel J. Rosenkrantz Richard E. Stearns
*Sorting and Sort Systems	Harold Lorin
*Operating Systems	Harold Lorin Harvey M. Deitel

*Recursive Programming Techniques	William Burge
*Modeling and Analysis: An Introduction to System Performance Evaluation Methodology	Hisashi Kobayashi
Conceptual Structures: Information Processing in Mind and Machines	John F. Sowa

*Published

Foreword

The field of systems programming primarily grew out of the efforts of many programmers and managers whose creative energy went into producing practical utilitarian systems programs needed by the rapidly growing computer industry. Programming was practiced as an art where each programmer invented his own solutions to problems with little guidance beyond that provided by his immediate associates. In 1968, the late Ascher Opler, then at IBM, recognized that it was necessary to bring programming knowledge together in a form that would be accessible to all systems programmers. Surveying the state of the art, he decided that enough useful material existed to justify a significant codification effort. On his recommendation, IBM decided to sponsor The Systems Programming Series as a long term project to collect, organize, and publish those principles and techniques that would have lasting value throughout the industry.

The Series consists of an open-ended collection of text-reference books. The contents of each book represent the individual author's view of the subject area and do not necessarily reflect the views of the IBM Corporation. Each is organized for course use but is detailed enough for reference. Further, the Series is organized in three levels: broad introductory material in the foundation volumes, more specialized material in the software volumes, and very specialized theory in the computer science volumes. As such, the Series meets the needs of the novice, the experienced programmer, and the computer scientist.

Taken together, the Series is a record of the state of the art in systems programming that can form the technological base for the systems programming discipline.

The Editorial Board

ABOUT THE AUTHORS

Eduardo B. Fernandez

Eduardo B. Fernandez is an Advisory Industry-Specialist Scientific at the Hamden, Connecticut, Branch Office of IBM Corporation, where he deals with scientific and academic uses of computers.

Dr. Fernandez received a degree in Electrical Engineering from the Universidad Tecnica F. Santa Maria, Valparaiso, Chile, in 1960, followed by a Master's Degree in Electrical Engineering from Purdue University in 1963, and a Ph.D. in Computer Science from UCLA in 1972.

Between 1961 and 1965, he worked for the university of Chile at the NASA Satellite Tracking Station in Santiago, involved in maintenance and training. In 1966 he joined the Electrical Engineering and Computer Science Department of the University of Chile, where he taught and did research on circuit theory and digital systems. In 1973 he joined the Los Angeles Scientific Center of IBM Corporation, where he was involved in research on database systems, in particular on security and performance aspects.

He is the author or coauthor of 25 technical papers, several research reports, and 13 invention disclosures. He has lectured at places such as Stanford University, Yale University, Bell Labs, University of the Philippines, Politecnico di Milano, as well as in many conferences and symposia. He has taught at the University of Chile and Catholic University (Santiago, Chile), UCLA, Instituto Tecnologico de Monterrey (Mexico), and Asian Institute of Technology (Bangkok, Thailand).

Rita C. Summers

Rita Summers is a Senior Programmer at the IBM Los Angeles Scientific Center. Since joining IBM in 1964 she has designed and implemented systems for interactive applications, computer-assisted instruction, and numerical control, and has worked on multicomputer operating systems and language for database access. She received two IBM Outstanding Contribution Awards for her work on virtual memory systems. Her work in the area of database security includes leadership of a project that developed a design for a secure database system. She has participated in the development and teaching of courses on database security, both within IBM and in universities. She is the author of many technical reports, conference papers, and articles. Recent publications include "Data base security: Requirements, policies, and models" (with C. Wood and E. B. Fernandez), *IBM Systems Journal*, **19**, 2 (1980); "Authorization in multilevel database models" (with C. Wood and E. B. Fernandez), *Information Systems*, **4**, 2 (1979); and "A System Structure for Data Security" (with E. B. Fernandez), Report G320-2687, IBM Los Angeles Scientific Center, April 1977.

Before joining IBM Ms. Summers worked as a systems analyst and programmer at Ramo Wooldridge. She received B.A. and M.A. degrees from UCLA. She is a member of Phi Beta Kappa, the Association for Computing Machinery, and the Institute of Electrical and Electronics Engineers.

Christopher Wood

Christopher Wood is located at the Los Angeles Scientific Center, where he has been working in database security and performance since 1976. He joined IBM in 1970 as a systems engineer in London, England, specializing in the database area. In 1966 he obtained a B.S. in physics from Imperial College, London University, and in 1969 a Ph.D. from Balliol College, Oxford University, in theoretical physics. Dr. Wood is a member of the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers.

Preface

This book is concerned with the security and integrity of information that is maintained in databases. Topics that are central to this concern are treated in depth, and important related topics are introduced. The book is aimed at a reader with some technical background in the computing field and with a serious interest in database security. Some background in database systems is also desirable; this could be a college course, experience in using or managing a database system, experience in designing or implementing a database management system, or a general cultural acquaintance with databases combined with other systems experience.

We have in mind three classes of readers:

- students
- system designers and programmers, and
- people responsible for managing and auditing the security of database systems.

The book may be used in different ways by these different groups of readers.

For the student

The book is designed to be useful for a senior level or graduate course in computer science or management science. All chapters are appropriate for study, but a shorter course can be obtained by skipping special topics, such as privacy (Chapter 2), distributed databases (Chapter 12), or sta-

tistical databases (Chapter 13). Integrity (Chapter 8) is a self-contained unit that could be omitted if the course is restricted to security.

For the system designer and programmer

For these readers the book provides a conceptual framework plus a comprehensive analysis of useful principles and techniques. The security designs of important database systems are covered. Again, special topics can be skipped.

For the security administrator or auditor

These readers can skip the more theoretical chapters and those dealing with design and programming technology. These are Chapters 6, 8, 10, 11, and 13. The remaining chapters should be useful for explaining why database security and integrity are important, creating an awareness of security and integrity threats and defensive measures, providing a conceptual framework, and relating auditing and control to that framework.

For all readers, and for the researcher as well, the references and the annotated bibliographies should be valuable.

Structure of the Book

Chapter 1 defines the topics of the book, argues for their importance, and introduces basic terminology. Chapter 2 reviews privacy concepts, privacy legislation, and current privacy issues. Chapter 3 summarizes the basic concepts and terminology of database systems. Chapter 4 is an overview of the entire computer security problem, showing where database security fits in. Chapter 5 discusses possible security policies, while Chapter 6 introduces models of database security. One of these models is used to structure some of the remaining chapters. The next chapter considers issues of authorization; that is, how users' rights to access the database are specified. Problems and techniques of integrity are described in Chapter 8. In Chapter 9 the topic of auditing and control is introduced and its relation to database security is discussed.

Chapter 10 introduces some basic design principles for systems that enforce security, discusses design choices, and describes the designs of a number of systems. Chapter 11 continues the treatment of security enforcement by describing operating-system and hardware mechanisms that support database security.

The special characteristics of security and integrity in distributed systems are considered in Chapter 12. The security of statistical databases is treated in Chapter 13. Finally, Chapter 14 speculates on the future of database security.

Acknowledgments

We gratefully acknowledge the help we have received from many sources. Encouragement and administrative support were provided by the editorial board of the Systems Programming Series and by the IBM Los Angeles Scientific Center. We especially would like to thank Kathy Hanson, Betsey Barnes, and Sal Matos, librarians at the Center, for their help in locating publications, and Roberta Tseng and Katy Piskur for their skilled use of a text-editing system. IBM's System Research Institute provided an opportunity to test the material of the book in a short course taught by the authors. A draft of the book was used in a longer course taught at California State University at Northridge. Marvin Schaefer, who taught that course, supplied valuable criticisms and references. A course based on sections of the book was taught at the Instituto Tecnologico de Monterrey, Mexico.

Our students in these courses helped us to clarify the presentation. Paula Newman and D. P. Beresford-Redman provided helpful comments on Chapter 9, Dick Attanasio on Chapter 11, Jim Gray on Chapter 8, and Patricia Griffiths on Chapters 10 and 12. Stan Kurzban read and commented on the entire manuscript. Tomas Lang supplied a detailed critique of an early version of the book.

We have been impressed by the skill of the editorial staff at Addison-Wesley, and by the care taken in the production of the book. We are grateful to IBM for supporting our work in many ways, but responsibility for the content of the book and for the views expressed is completely ours.

Hamden E.B.F.
Los Angeles R.C.S.
November 1980 C.W.

Contents