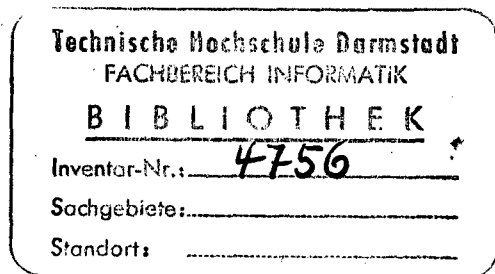


# Database Security and Integrity

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

# Contents

## **CHAPTER 1 INTRODUCTION**

1.1	The need for database security and integrity .....	1
1.2	The value of information .....	1
1.3	Misuse of computers .....	3
1.4	Security and integrity of databases .....	4
1.5	Definitions .....	5

## **CHAPTER 2 PRIVACY REQUIREMENTS**

2.1	Introduction .....	11
2.2	The privacy concept in the United States .....	11
2.3	The history of information privacy legislation .....	13
2.4	Current privacy developments and issues .....	16
2.5	Implementation of systems for privacy .....	19

## **CHAPTER 3 DATABASE CONCEPTS**

3.1	What is a database? .....	25
3.2	Data independence .....	28
3.3	Database architecture .....	29
3.4	Data models .....	29
3.5	Advantages of the database approach .....	34
3.6	Database security and integrity .....	35

3.7	Sample systems .....	36
3.8	Summary .....	37

**CHAPTER 4  
DATABASE SECURITY IN PERSPECTIVE**

4.1	A fictional case of attempted unauthorized access .....	39
4.2	Security threats and defenses in computer systems .....	40
4.3	Estimating the costs and benefits of security measures .....	47
4.4	Security evaluation of a database system .....	50
4.5	Summary .....	52

**CHAPTER 5  
POLICIES FOR DATABASE SECURITY**

5.1	Introduction .....	55
5.2	Policies and mechanisms .....	56
5.3	Policies for database security .....	57
5.4	Summary .....	64

**CHAPTER 6  
MODELS OF DATABASE SECURITY**

6.1	Introduction .....	65
6.2	A basic model of database access control .....	66
6.3	Extensions to the basic model .....	71
6.4	Multilevel models .....	73
6.5	An information-flow model .....	76
6.6	Comparison of models .....	78

**CHAPTER 7  
AUTHORIZATION**

7.1	Introduction .....	83
7.2	The authorizer .....	85
7.3	Subjects .....	85
7.4	Objects .....	86
7.5	Access types .....	90
7.6	Specifying subsets and conditions .....	90
7.7	Auxiliary procedures .....	93
7.8	Authorization language and displays .....	93
7.9	The use of classes .....	98
7.10	Consistency and effect of new rules .....	102
7.11	Summary .....	103

**CHAPTER 8  
DATA INTEGRITY**

8.1	Introduction .....	107
8.2	Transactions .....	107
8.3	Semantic integrity .....	109
8.4	Concurrency control .....	122
8.5	Recovery .....	134

**CHAPTER 9  
AUDITING AND CONTROLS  
IN A DATABASE ENVIRONMENT**

9.1	Introduction .....	149
9.2	Basic concepts .....	149
9.3	Common forms of computer fraud .....	154
9.4	Control practices .....	155
9.5	The audit trail .....	161
9.6	Computer auditing techniques .....	163
9.7	Developing reliable application systems .....	170
9.8	DBMS support of audit and control .....	176
9.9	Conclusion .....	177

**CHAPTER 10  
ENFORCEMENT DESIGN**

10.1	Introduction .....	183
10.2	Design principles for secure systems .....	184
10.3	Detection and analysis of access requests .....	185
10.4	Access validation .....	187
10.5	IMS .....	191
10.6	IDMS .....	194
10.7	LASC proposal .....	195
10.8	System R .....	197
10.9	INGRES .....	199
10.10	A kernel design for a secure DBMS .....	203
10.11	Enforcement of multilevel security in DBMSs .....	205
10.12	Database machines .....	209
10.13	Summary .....	213

**CHAPTER 11  
PROTECTION MECHANISMS**

11.1	Introduction .....	217
11.2	The DBMS and the operating system .....	218

11.3	Protection problems	219
11.4	Protection matrix	221
11.5	Mechanisms	223
11.6	Several protection systems	230
11.7	<i>Information-flow control and trusted operating systems</i>	239
11.8	Authentication	247
11.9	Encryption	249
11.10	Summary	258

**CHAPTER 12  
SECURITY AND INTEGRITY IN DISTRIBUTED  
DATABASE SYSTEMS**

12.1	Introduction	267
12.2	The architecture of distributed database systems	267
12.3	Decentralized authorization	272
12.4	Distribution of access rules	275
12.5	Nondiscretionary systems	276
12.6	Integrity in a DDS	279
12.7	Summary	285

**CHAPTER 13  
SECURITY OF STATISTICAL DATABASES**

13.1	Introduction	289
13.2	Compromise of a database	290
13.3	Query overlap	295
13.4	Queries that return a database value	296
13.5	Security mechanisms	296

**CHAPTER 14  
THE FUTURE OF DATABASE SECURITY**

14.1	Changing needs and technology	299
14.2	Sources for the database security art	300

<b>ANSWERS TO SELECTED EXERCISES</b>	303
--------------------------------------	-----

<b>INDEX</b>	309
--------------	-----