

MODERN METHODS FOR COMPUTER SECURITY AND PRIVACY

LANCE J. HOFFMAN

University of California
Computer Science Department
Berkeley, California

TECHNISCHE HOCHSCHULE DARMSTADT	
Fachbereich 1	
<u>Gesamtbibliothek</u>	
<u>Betriebswirtschaftslehre</u>	
Inventar-Nr. :	<u>17.103</u>
Abstell-Nr. :	<u>A18 / 1109</u>
Sachgebiete:	<u>1.7.7.6</u>

PRENTICE-HALL, INC., Englewood Cliffs, New Jersey 07632

CONTENTS

Preface	xi
1 Introduction	1
Outline of This Book	1
Definitions	1
Dealing with Extremely Sensitive Information	2
Security Design Principles	3
Nontechnical Areas	4
Summary	4
Questions	4
2 Authentication	6
Identification and Authentication	6
Passwords	8
Question-Answer Method	13
Authenticating Systems to Users	14
General Cautions Concerning Passwords	16
Authentication Procedure	18
User Exits	20
Physical Authentication Methods	20
Actions on Denied Access Attempts	20
Summary	21
Questions	21

3	Authorization	23
	The Authorization Matrix	24
	Authority Levels	27
	Compressing the Authorization Matrix	28
	Restricting Languages Available to the User	29
	Automatic Request Modification	30
	Data-Dependent Access Control Decisions	31
	Using Input/Output Routines for Authorization	32
	Summary	34
	Questions	34
4	Logging	35
	Content of the Log	35
	Uses of Logs	37
	Cost of Logging	39
	Threat Monitoring	39
	Surveillance Programs	40
	Summary	41
	Questions	41
5	Privacy Transformations: Traditional Methods	42
	An Example: The Caesar Cipher	43
	Cryptographic Systems	43
	Substitution Ciphers	45
	A General Framework for Substitution Transformations	48
	Frequency Analysis	49
	Transpositions	51
	Composite Transformations	52
	Summary	52
	Questions	53
6	Privacy Transformations: Computer-Oriented Software Methods	55
	Pseudo-Random Number Generators	55
	Using Pseudo-Random Numbers in Privacy Transformations	56
	Enciphering Random-Access Files	57
	Choosing the Seed Number	57
	Maximizing the Length of the Key Sequence—Choosing a and c	57
	An “Infinite” Key Word Cipher	59
	The Key Sequence	60
	The Known Plaintext Problem	61
	An “Infinite” Key Character Cipher	63
	Compression Methods	65
	Commercially Available Software Packages	67
	Costs of Software Privacy Transformations	67
	Summary	69
	Questions	70

7	Privacy Transformations: Hardware Methods	72
	Linear Shift Register Circuits	72
	LUCIFER	75
	The Federal Standard	78
	Network Encryption Requirements	89
	Commercially Available Hardware	90
	Summary	90
	Questions	91
8	System Programs	92
	Some Problems in Today's Operating Systems	93
	Utility Programs	95
	Protecting Proprietary Programs and Data	96
	Penetration Tests	97
	Costs of Add-On Operating System Security	101
	Protective Overhead	102
	Virtual Machine Monitors—A New Type of Operating System	103
	Application of Security Design Principles	106
	Summary	106
	Questions	106
9	Machine Architecture	108
	Minicomputers as Security Controllers	108
	Microprocessors as Security Aids	110
	Isolation Hardware in Traditional Systems	112
	Other CPU Hardware Features	122
	Summary	123
	Questions	123
10	Statistical Data Banks	124
	Methods for Dossier Extraction	125
	Likelihood Estimators	129
	General Protection Measures for Statistical Data Banks	129
	Summary	132
	Questions	132
11	Mathematical Models	134
	Protection	134
	The ADEPT-50 Model	135
	Hartson's Five-Dimensional Security Space	136
	Covered Security System Model	138
	Finite-State Models	141
	Kernels and Certification	142
	Summary	147
	Questions	147

12	Future Research Areas	148
	Costs and Measurements	148
	Measurement Using Security Ratings	151
	Privacy Cost Model	155
	Security Specification Languages	155
	Bulk Storage Devices	161
	Security-Conscious Terminals	161
	Data Center Security Standards	161
	Summary	161
	Questions	162
13	Nontechnical Aspects of Computer Security	163
	Risk Analysis	170
	Administrative Methods	176
	Physical Security	178
	Codes of Ethics	179
	Legal Methods	179
	Caveat	181
	Summary	181
	Questions	183
14	Laws and Pending Legislation	184
	Historical Phases of Privacy Awareness and Action	185
	Laws Outside the United States	187
	Existing Laws in the United States	187
	Common Features of United States Legislation	192
	Keeping Track of Pending Legislation	192
	Summary	195
	Questions	195
	Appendices	197
	Answers to End of Chapter Questions	224
	Bibliography	235
	Index	251