01-609

Table of Contents

Page

Preface xvii

About This Book xvii
Summary of Contents xviii
Acknowledgments xix
Comments and Questions xx

Part I OVERVIEW 1

Chapter 1 Introduction 3

Attack of the Giant Worm (and Other Tales) 3
What Is Computer Security? 8
A Broader Definition of Security 9
Secrecy and Confidentiality 9
Accuracy, Integrity, and Authenticity 10
Availability 10
Threats to Security 11
Vulnerabilities 11
Threats 14
Countermeasures 16
Why Buy Security? 18
Government Requirements 19
Information Protection 19
What's A User To Do? 20

FACULTAD DE CIENCIA Y TECNOLOGIA
BIBLIOTECA
Sede Oro Verde - 01
UADER

Chapter 2 Some Security History 23

Information and its Controls 24
Computer Security: Then and Now 25
Early Computer Security Efforts 27
Tiger Teams 29
Research and Modeling 30
Secure Systems Development 31
Building Toward Standardization 31
Standards for Secure Systems 32
Standards for Cryptography 36
Standards for Emanations 37
Computer Security Mandates and Legislation 38
NSDD 145 39
NTISSP 2 39
Computer Fraud and Abuse Act 40
Computer Security Act 41
Searching for a Balance 42
Recent Government Security Initiatives 42
Privacy Considerations 44
International Security Activity 46
The Growth of Modern Standards 47

Part II COMPUTER SECURITY 53

Chapter 3 Computer System Security and Access Controls 55

What Makes a System Secure? 55
System Access: Logging Into Your System 57
Identification and Authentication 57
Protecting Passwords 62
Data Access: Protecting Your Data 66
Discretionary Access Control 67
Mandatory Access Control 72

Chapter 4 Viruses and Other Wildlife 79

Viruses 79
Worms 82
Trojan Horses 83
Bombs 84
Trap Doors 85
Spoofs 86
Other Wildlife 86
Remedies 88

Chapter 5 Secure System Planning and Administration 89

Administrative Security 89
Overall Planning and Administration 91
  Analyzing Costs and Risks 91
  Planning for Disaster 93
  Setting Security Rules for Employees 94
  Training Users 94
Day-to-day Administration 96
  Performing Backups 96
  Performing a Security Audit 99
Separation of Duties 100

Chapter 6 Inside the Orange Book 103

Introduction to the Orange Book 104
A Summary of Security Concepts 105
  What's a Trusted System? 105
  Measuring Trust 106
  Trusted Computing Base 107
  Security Policy 108
  Security Model 108
  Security Kernel 109
  Security Perimeter 110
Orange Book Evaluation Classes 110
  Comparison of Evaluation Classes 112
  Complaints About the Orange Book 112

Evaluations of Secure Systems 115
Security Policy Requirements 115
Discretionary Access Control 116
Object Reuse 118
Labels 119
Mandatory Access Control 124
Accountability Requirements 124
Identification and Authentication 124
Trusted Path 126
Audit 128
Assurance Requirements 133
Operational Assurance 134
Life-cycle Assurance 141
Documentation Requirements 149
Security Features User's Guide 150
Trusted Facility Manual 151
Test Documentation 152
Design Documentation 153
Summary of Classes 155
D Systems: Minimal Security 155
C1 Systems: Discretionary Security Protection 155
C2 Systems: Controlled Access Protection 156
B1 Systems: Labeled Security Protection 157
B2 Systems: Structured Protection 157
B3 Systems: Security Domains 158
A1 Systems: Verified Design 159
Compartmented Mode Workstations 159
Government Computer Security Programs 161

Part III COMMUNICATIONS SECURITY 163

Chapter 7 Encryption 165

Some History 166
What is Encryption? 169
Why Encryption? 171
Transposition and Substitution Ciphers 172
Cryptographic Keys: Private and Public 175
Key Management and Distribution 177
One-time Pad 178
The Data Encryption Standard 179

What is the DES? 182
Future of the DES 185
Other Cryptographic Algorithms 188
Variations on the DES 188
Public Key Algorithms 188
The RSA Algorithm 189
Digital Signatures and Notaries 190
Government Algorithms 192
Message Authentication 192
Encryption in Banking and Financial Applications 193
Government Cryptographic Programs 196
NSA 196
NIST 197
Treasury 197
Cryptographic Export Restrictions 197

Chapter 8 Communications and Network Security 201

What Makes Communication Secure? 202
Communications Vulnerabilities 204
Communications Threats 204
Modems 205
Networks 207
Network Terms 207
Some Network History 210
Network Media 212
OSI Model 215
Network Security 218
Trusted Networks 218
Perimeters and Gateways 221
Security in Heterogeneous Environments 221
Encrypted Communications 222
The Red Book and Government Network Evaluations 226
TCSEC Requirements 228
Other Security Services 228
Some Network Security Projects 232
DISNet and Blacker 232
SDNS 232
Kerberos 233
Project MAX 233
Secure NFS 234

Part IV OTHER TYPES OF SECURITY 235

Chapter 9 Physical Security and Biometrics 237

Physical Security 238
Natural Disasters 238
Risk Analysis and Disaster Planning 241
Locks and Keys: Old and New 241
Types of Locks 243
Tokens 243
Challenge-response Systems 244
Cards: Smart and Dumb 244
Biometrics 246
Fingerprints 249
Handprints 250
Retina Patterns 250
Voice Patterns 251
Signature and Writing Patterns 251
Keystrokes 252

Chapter 10 TEMPEST 253

The Problem of Emanations 254
The TEMPEST Program 255
How To Build TEMPEST Products 257
TEMPEST Standards and Restrictions 259
TEMPEST Standards 259
TEMPEST Export Restrictions 260
Who Cares About TEMPEST? 261
Is TEMPEST Needed? 262
Changing TEMPEST Concepts 263
Government TEMPEST Programs 265

Part V APPENDICES 267

Appendix A Acronyms 269

Appendix B Computer Security Legislation 277

Appendix C Orange Book and Other Summaries 289

Orange Book (TCSEC) Requirements 289
Compartmented Mode Workstation (CMW) Requirements 313
System High Workstation (SHW) Requirements 315
International Security (ITSEC) Requirements 318

Appendix D Government Security Programs 323

Computer Security Programs 323
The Role of the NCSC 324
The Role of NIST 325
Trusted Product Evaluation Program (TPEP) 326
Evaluation of Network Products 331
Evaluations of Database Management Systems 332
Evaluations of Security Subsystem Products 333
Formal Verification Systems Evaluation Program (FVSEP) 336
Degausser Products List 338
Rating Maintenance Phase (RAMP) Program 338
System Certification and Accreditation 339
DOCKMASTER 340
Technical Vulnerability Reporting Program 341
Communications Security Programs 341
Commercial COMSEC Endorsement Program 342
CCEP Eligibility 343
CCEP Program Steps 344
Government Endorsed DES Equipment Program 345
EFT Certification Program 346
Protected Network Services List 346
Off-line Systems List (OLSL) 347

Restrictions on Cryptographic Products 347
TEMPEST Security Programs 348
Industrial TEMPEST Program and Preferred Products List 349
Endorsed TEMPEST Products Program 351
Endorsed TEMPEST Test Services Program 356
Endorsed TEMPEST Test Instrumentation Program 357

Appendix E A Security Source Book 359

Government Publications 360
The Rainbow Series 360
Other NSA Publications 369
FIPS PUBs 370
NIST Special Publications 374
Other NIST Publications 385
Compartmented Mode Workstation (CMW) Publications 385
COMSEC Program Publications 386
TEMPEST Program Publications 386
Other Security-relevant Government Publications 387
Government Program Contact Points 387
Computer Security (COMPUSEC) Programs 388
Communications Security (COMSEC) Programs 389
TEMPEST Programs 390
Other Government Contacts 390
Emergency Organizations 391
Standards Organizations 391
Security User Groups 393
Electronic Groups 397
USENET 397
Commercial Bulletin Boards 397
NCSC DOCKMASTER 398
NIST Computer Security Bulletin Board 398
Computer Security Periodicals 399
Computer Security Books 401
Conference Proceedings 401
Computer Security Textbooks 401
Viruses and Other Programmed Threats 402
Computer Crime and Ethics 402
Of General Interest 403

Glossary 405

Index 429