

07-10-00

Contents

Foreword

xvii

Preface

xix

1 Threats to Computer Systems

1

1.1 Threats, Vulnerabilities, and Attacks

2

1.2 Types of Threats

3

 Disclosure Threat

3

 Integrity Threat

4

 Denial of Service Threat

4

1.3 Attacker Intent

5

1.4 Security and Usability

6

1.5 Further Impediments to Security

7

1.6 System Security Engineering

9

Summary

12

Bibliographic Notes

12

Exercises

13

2 Threat Trees

15

2.1 Arbitrary Threat Lists

16

2.2 Threat Trees

17

2.3 Example: Hospital Computer System

18

2.4 Using Threat Trees for Calculation

21

2.5 Using Threat Trees to Support System Security
 Engineering

23

S7054

000000

computer

2.6 Example: Aircraft Computer System	24
Summary	28
Bibliographic Notes	28
Exercises	28

3 Categorization of Attacks	31
3.1 Using an Attack Taxonomy	32
3.2 Considerations in Selecting an Attack Taxonomy	34
3.3 Example: Simple Attack Taxonomy	35
3.4 Example: Risks-Based Empirical Attack Taxonomy	36
External Information Theft	37
External Abuse of Resources	38
External Masquerading	38
Pest Programs	39
Bypassing of Internal Controls	39
Active Authority Abuse	39
Abuse Through Inaction	40
Indirect Abuse	40
Summary	40
Bibliographic Notes	41
Exercises	41

4 Trojan Horses and Viruses	43
4.1 Trojan Horses	44
4.2 Viruses	45
4.3 Self-Reproducing Programs	46
4.4 Code Propagation	48
4.5 Typical Virus Operation	49
4.6 Example: Internet Virus	52
4.7 Trojan Horse Clues	53
Summary	54

Bibliographic Notes	54
Exercises	54

5 Common Attack Methods	55
--------------------------------	----

5.1 Example: Password Spoof Program	56
5.2 Example: Password Theft by Clever Reasoning	58
5.3 Example: Logic Bomb Mail	59
5.4 Example: Scheduled File Removal	60
5.5 Example: Field Separator Attack	60
5.6 Example: Insertion of Compiler Trojan Horse	61
5.7 Simple Attack Prevention Methods	63
Individual Screening	63
Physical Controls	63
Care in Operations	63
Summary	64
Bibliographic Notes	64
Exercises	64

6 Security Labels	67
--------------------------	----

6.1 Security Levels	68
6.2 Security Categories	69
6.3 Security Labels	70
6.4 Subjects and Objects	72
6.5 Clearances and Classifications	73
6.6 Dominates Relation	74
6.7 Example: UNIX System V/MLS Security Labels	76
Summary	78
Bibliographic Notes	78
Exercises	78

7 The Lattice of Security Labels	79
7.1 Basic Properties of Lattices	80
7.2 The Lattice of Security Labels	80
7.3 Example: Military Security Label Lattices	81
7.4 Using Security Label Lattices	85
7.5 Mathematical Security Modeling	85
Summary	86
Bibliographic Notes	86
Exercises	86

8 Security Policies	89
8.1 Reference Monitor Concept	90
8.2 Security Policy Concepts	91
8.3 Informal Security Policy Expression	92
8.4 Example: UNIX System V/MLS Security Policy	93
8.5 Formal Security Policy Expression	94
8.6 Example: Formal Policy Expressions	96
8.7 Expressing a Security Policy with Respect to a Specification	98
Summary	99
Bibliographic Notes	99
Exercises	100

9 The Bell-LaPadula Disclosure Model	101
9.1 Level Diagrams	102
9.2 BLP Model Rules	104
9.3 Tranquility and the BLP Model	106
9.4 Formalized Description of the BLP Model	107
9.5 An Inductive Procedure for the BLP Model	108
9.6 Example: BLP Model-Compliant System	109

Summary	111
Bibliographic Notes	111
Exercises	112

10 BLP Analysis and Debate	113
10.1 Example: Blind Writes	114
10.2 Example: Remote Reads	117
10.3 Example: Trusted Subjects	118
10.4 Example: System Z	119
Summary	120
Bibliographic Notes	121
Exercises	121

11 Nondeducibility and Noninterference Security	123
11.1 Nondeducibility Security	124
11.2 Example: Nondeducibility Secure Parity System	126
11.3 Noninterference Security	129
11.4 Example: Parity System Not Noninterference Secure	131
11.5 Remarks on Disclosure Definitions	132
Summary	133
Bibliographic Notes	133
Exercises	133

12 The Biba Integrity Model	135
12.1 Mandatory Integrity Model	136
12.2 Subject Low-Water Mark Model	137
12.3 Object Low-Water Mark Model	138

12.4 Formalized Description of the Biba Model	139
12.5 Example: Biba Model-Compliant System	140
12.6 Assessment of the Biba Model	142
12.7 Combining Security Models	142
12.8 Example: Biba and BLP Model Combination	143
Summary	145
Bibliographic Notes	145
Exercises	145

13 The Clark-Wilson Integrity Model

13.1 Preliminary CW Concepts	148
13.2 CW Model Rules	150
13.3 Assessment of the CW Model	154
13.4 Combining the CW Model with the Biba Model	155
Summary	157
Bibliographic Notes	158
Exercises	158

14 Denial of Service

14.1 DOS Concept Definitions	159
14.2 Example: DOS Requirements in Temporal Logic	161
14.3 Mandatory DOS Model	162
14.4 Millen's Resource Allocation Model (RAM)	165
Summary	168
Bibliographic Notes	168
Exercises	169

15 Safeguards and Countermeasures

15.1 Safeguards	172
15.2 Countermeasures	173

15.3 Overview of Security Mechanisms	174
Configuration Management	175
Formal Specification and Verification	176
Enhanced Life Cycle Activities	176
15.4 A Collection of Selection Principles	177
Summary	178
Bibliographic Notes	179
Exercises	179

16 Auditing	181
16.1 Auditing Requirements	182
16.2 Operational Description of Auditing	183
Step 1: Determine What Must Be Audited	184
Step 2: Insert Audit Calls	184
Step 3: Create Protected Log Routines	185
16.3 Example: UNIX System V/MLS Auditing	187
16.4 Example: CMW Auditing	189
16.5 Alternate Auditing Approaches	190
16.6 Attacks Countered by Auditing	191
Summary	191
Bibliographic Notes	191
Exercises	192

17 Intrusion Detection	193
17.1 Intrusion Detection Architecture	194
17.2 Intrusion Detection Concepts	195
17.3 IDES Model	196
Subjects and Objects	197
Audit Records	197
Profiles	198
Anomaly Records	200
Activity Rules	200

17.4 Example: ComputerWatch	201
17.5 Attacks Countered by Intrusion Detection	203
Summary	203
Bibliographic Notes	203
Exercises	204

18 Identification and Authentication	205
18.1 Identification and Authentication Concepts	206
18.2 Identification and Authentication Approaches	207
Something Possessed	208
Something Embodied	209
Something Known	210
18.3 Example: Polonius	211
18.4 User Sessions	213
18.5 Trusted Path	214
18.6 Attacks Countered by Identification and Authentication	214
Summary	215
Bibliographic Notes	215
Exercises	215

19 Passwords	217
19.1 User-Generated Passwords	218
19.2 Computer-Generated Passwords	220
19.3 Tunable Passwords	221
19.4 Password Cracking	221
19.5 Password Encryption	222
19.6 Password Salt	223
19.7 Example: UNIX System Password Management	223
Summary	224
Bibliographic Notes	225
Exercises	225

20 Encryption	227
20.1 Basic Encryption Terminology and Concepts	228
20.2 Example: UNIX <i>crypt</i>	230
20.3 Substitution and Transposition	231
Substitution	231
Transposition	232
20.4 DES Overview	232
20.5 Attacks Countered by Encryption	235
Summary	236
Bibliographic Notes	236
Exercises	236

21 Key Management Protocols	239
21.1 Attacks to Remote Communications	240
21.2 Private Key Protocol	242
21.3 Public Key Protocol	243
21.4 Example: Secure Terminal/Host Communication	245
21.5 RSA Implementation	246
21.6 Arbitrated Protocols with Third Party	247
21.7 Example: Kerberos	249
21.8 Key Distribution	250
21.9 Digital Signatures	250
Summary	251
Bibliographic Notes	251
Exercises	251

22 Access Control	253
22.1 Access Control Mechanisms	254
22.2 Discretionary vs. Mandatory	254
22.3 Access Matrices	255

22.4	Permission Mechanisms	256
22.5	ACL and Capability Mechanism	257
22.6	Example: Secure Xenix ACLs	258
22.7	Capabilities and the BLP Model	259
22.8	Mandatory Label-Based Mechanisms	259
22.9	Example: UNIX System V/MLS Access Control	262
22.10	Example: Trusted Mach Access Control	264
22.11	Example: Secure Tunis Access Control	264
22.12	Attacks Countered by Access Control	266
	Summary	267
	Bibliographic Notes	267
	Exercises	267

23	Covert Channels	269
23.1	Definition of Covert Channels	270
23.2	Covert Storage Channels	271
23.3	Covert Timing Channels	273
23.4	Information Flow Approach	274
23.5	Resource Matrix Approach	275
23.6	Example: Covert Channels in SAT	276
23.7	Computers as the Weakest Link	277
	Summary	278
	Bibliographic Notes	278
	Exercises	278

24	Composing Security	281
24.1	Security Composibility	282
24.2	Nondeducibility Composition Scenario	283
24.3	Composing Nondeducibility	287
24.4	Noninterference Composibility Scenario	289
24.5	Composing Noninterference	290

24.6 Security Composibility Implications	291
Summary	292
Bibliographic Notes	293
Exercises	293

25 Privileges and Roles	295
25.1 Privilege and Role Definitions	296
25.2 Role-Based Attacks	297
25.3 Principle of Least Privilege	298
25.4 Transformation and Revocation	299
25.5 Example: Least Privilege on UNIX-Based Systems	300
25.6 Example: Least Privilege in Program Development	301
Summary	303
Bibliographic Notes	303
Exercises	303

26 Security Kernels	305
26.1 Security Kernel Organization	306
26.2 Principles of Kernel Design	307
26.3 Example: Kernelized Secure Operating System (KSOS)	308
26.4 Trusted Computing Base (TCB)	309
26.5 Example: UNIX System V/MLS TCB	311
26.6 Example: SCOMP TCB	311
26.7 TCB Layering	313
Summary	314
Bibliographic Notes	314
Exercises	314

27 Network Security	317
27.1 Network Security Overview	318
27.2 Network Attacks	320
27.3 Encryption Strategies	321
27.4 End-to-End vs. Link Encryption	324
Link Encryption	325
End-to-End Encryption	327
27.5 Network Security Policy Issues	329
27.6 Example: MLS/TCP	330
27.7 Example: Secure Data Network System (SDNS)	331
Summary	333
Bibliographic Notes	333
Exercises	333

28 Database Security	335
28.1 Database Attacks	335
28.2 Database Inference Problem	337
28.3 Database Aggregation Problem	340
28.4 Polyinstantiation	341
28.5 Database Applications on Secure Base	342
28.6 Example: SeaView Database	343
28.7 Integrity Lock Approach	344
28.8 Integrity Mechanisms for Secure Databases	344
Summary	346
Bibliographic Notes	346
Exercises	346

29 Security Evaluation	347
29.1 Goals of Security Evaluation	348
29.2 Orange Book Overview	349

D Division (Minimal Protection)	353
C Division (Discretionary Protection)	353
B Division (Mandatory Protection)	353
A Division (Verified Protection)	353
29.3 Trusted Network Interpretation (TNI)	353
29.4 NCSC RAMP	354
29.5 Alternate Security Criteria	355
Summary	355
Bibliographic Notes	356
Exercises	356

Annotated Bibliography	357
-------------------------------	-----

Twenty-Five Greatest Works in Computer Security	389
--	-----

Subject Index	391
----------------------	-----

Author Index	399
---------------------	-----

Credits	403
----------------	-----