

# Computer Security

THIRD EDITION

Dieter Gollmann

*Hamburg University of Technology*



A John Wiley and Sons, Ltd., Publication

# Contents

Preface	xvii
<b>CHAPTER 1 – History of Computer Security</b>	<b>1</b>
1.1 The Dawn of Computer Security	2
1.2 1970s – Mainframes	3
1.3 1980s – Personal Computers	4
1.3.1 An Early Worm	5
1.3.2 The Mad Hacker	6
1.4 1990s – Internet	6
1.5 2000s – The Web	8
1.6 Conclusions – The Benefits of Hindsight	10
1.7 Exercises	11
<b>CHAPTER 2 – Managing Security</b>	<b>13</b>
2.1 Attacks and Attackers	14
2.2 Security Management	15
2.2.1 Security Policies	16
2.2.2 Measuring Security	17
2.2.3 Standards	19
2.3 Risk and Threat Analysis	21
2.3.1 Assets	22
2.3.2 Threats	23
2.3.3 Vulnerabilities	24
2.3.4 Attacks	24
2.3.5 Common Vulnerability Scoring System	26
2.3.6 Quantitative and Qualitative Risk Analysis	26
2.3.7 Countermeasures – Risk Mitigation	28
2.4 Further Reading	29
2.5 Exercises	29
<b>CHAPTER 3 – Foundations of Computer Security</b>	<b>31</b>
3.1 Definitions	32
3.1.1 Security	32
3.1.2 Computer Security	34
3.1.3 Confidentiality	34
3.1.4 Integrity	35
3.1.5 Availability	36
3.1.6 Accountability	37
3.1.7 Non-repudiation	38

## CONTENTS

3.1.8	Reliability	38
3.1.9	Our Definition	39
3.2	The Fundamental Dilemma of Computer Security	40
3.3	Data vs Information	40
3.4	Principles of Computer Security	41
3.4.1	Focus of Control	42
3.4.2	The Man–Machine Scale	42
3.4.3	Complexity vs Assurance	44
3.4.4	Centralized or Decentralized Controls	44
3.5	The Layer Below	45
3.6	The Layer Above	47
3.7	Further Reading	47
3.8	Exercises	48
<b>CHAPTER 4 – Identification and Authentication</b>		<b>49</b>
4.1	Username and Password	50
4.2	Bootstrapping Password Protection	51
4.3	Guessing Passwords	52
4.4	Phishing, Spoofing, and Social Engineering	54
4.4.1	Password Caching	55
4.5	Protecting the Password File	56
4.6	Single Sign-on	58
4.7	Alternative Approaches	59
4.8	Further Reading	63
4.9	Exercises	63
<b>CHAPTER 5 – Access Control</b>		<b>65</b>
5.1	Background	66
5.2	Authentication and Authorization	66
5.3	Access Operations	68
5.3.1	Access Modes	68
5.3.2	Access Rights of the Bell–LaPadula Model	68
5.3.3	Administrative Access Rights	70
5.4	Access Control Structures	71
5.4.1	Access Control Matrix	71
5.4.2	Capabilities	72
5.4.3	Access Control Lists	72
5.5	Ownership	73
5.6	Intermediate Controls	74
5.6.1	Groups and Negative Permissions	74
5.6.2	Privileges	75
5.6.3	Role-Based Access Control	76
5.6.4	Protection Rings	78

5.7	Policy Instantiation	79
5.8	Comparing Security Attributes	79
5.8.1	Partial Orderings	79
5.8.2	Abilities in the VSTa Microkernel	80
5.8.3	Lattice of Security Levels	81
5.8.4	Multi-level Security	82
5.9	Further Reading	84
5.10	Exercises	84
<b>CHAPTER 6 – Reference Monitors</b>		<b>87</b>
6.1	Introduction	88
6.1.1	Placing the Reference Monitor	89
6.1.2	Execution Monitors	90
6.2	Operating System Integrity	90
6.2.1	Modes of Operation	91
6.2.2	Controlled Invocation	91
6.3	Hardware Security Features	91
6.3.1	Security Rationale	92
6.3.2	A Brief Overview of Computer Architecture	92
6.3.3	Processes and Threads	95
6.3.4	Controlled Invocation – Interrupts	95
6.3.5	Protection on the Intel 80386/80486	96
6.3.6	The Confused Deputy Problem	98
6.4	Protecting Memory	99
6.4.1	Secure Addressing	100
6.5	Further Reading	103
6.6	Exercises	104
<b>CHAPTER 7 – Unix Security</b>		<b>107</b>
7.1	Introduction	108
7.1.1	Unix Security Architecture	109
7.2	Principals	109
7.2.1	User Accounts	110
7.2.2	Superuser (Root)	110
7.2.3	Groups	111
7.3	Subjects	111
7.3.1	Login and Passwords	112
7.3.2	Shadow Password File	113
7.4	Objects	113
7.4.1	The Inode	113
7.4.2	Default Permissions	114
7.4.3	Permissions for Directories	115

7.5	Access Control	116
7.5.1	Set UserID and Set GroupID	117
7.5.2	Changing Permissions	118
7.5.3	Limitations of Unix Access Control	119
7.6	Instances of General Security Principles	119
7.6.1	Applying Controlled Invocation	119
7.6.2	Deleting Files	120
7.6.3	Protection of Devices	120
7.6.4	Changing the Root of the Filesystem	121
7.6.5	Mounting Filesystems	122
7.6.6	Environment Variables	122
7.6.7	Searchpath	123
7.6.8	Wrappers	124
7.7	Management Issues	125
7.7.1	Managing the Superuser	125
7.7.2	Trusted Hosts	126
7.7.3	Audit Logs and Intrusion Detection	126
7.7.4	Installation and Configuration	127
7.8	Further Reading	128
7.9	Exercises	128
<b>CHAPTER 8 – Windows Security</b>		<b>131</b>
8.1	Introduction	132
8.1.1	Architecture	132
8.1.2	The Registry	133
8.1.3	Domains	134
8.2	Components of Access Control	135
8.2.1	Principals	135
8.2.2	Subjects	137
8.2.3	Permissions	139
8.2.4	Objects	141
8.3	Access Decisions	142
8.3.1	The DACL	143
8.3.2	Decision Algorithm	144
8.4	Managing Policies	145
8.4.1	Property Sets	145
8.4.2	ACE Inheritance	145
8.5	Task-Dependent Access Rights	147
8.5.1	Restricted Tokens	148
8.5.2	User Account Control	149
8.6	Administration	150
8.6.1	User Accounts	150
8.6.2	Default User Accounts	150

8.6.3	Audit	152
8.6.4	Summary	152
8.7	Further Reading	153
8.8	Exercises	153
<b>CHAPTER 9 – Database Security</b>		<b>155</b>
9.1	Introduction	156
9.2	Relational Databases	158
9.2.1	Database Keys	160
9.2.2	Integrity Rules	161
9.3	Access Control	162
9.3.1	The SQL Security Model	163
9.3.2	Granting and Revocation of Privileges	163
9.3.3	Access Control through Views	164
9.4	Statistical Database Security	167
9.4.1	Aggregation and Inference	168
9.4.2	Tracker Attacks	169
9.4.3	Countermeasures	170
9.5	Integration with the Operating System	172
9.6	Privacy	173
9.7	Further Reading	175
9.8	Exercises	175
<b>CHAPTER 10 – Software Security</b>		<b>177</b>
10.1	Introduction	178
10.1.1	Security and Reliability	178
10.1.2	Malware Taxonomy	178
10.1.3	Hackers	178
10.1.4	Change in Environment	179
10.1.5	Dangers of Abstraction	179
10.2	Characters and Numbers	179
10.2.1	Characters (UTF-8 Encoding)	179
10.2.2	The rlogin Bug	181
10.2.3	Integer Overflows	181
10.3	Canonical Representations	183
10.4	Memory Management	184
10.4.1	Buffer Overruns	185
10.4.2	Stack Overruns	186
10.4.3	Heap Overruns	187
10.4.4	Double-Free Vulnerabilities	187
10.4.5	Type Confusion	189
10.5	Data and Code	191
10.5.1	Scripting	191
10.5.2	SQL Injection	192

10.6	Race Conditions	193
10.7	Defences	194
10.7.1	Prevention: Hardware	194
10.7.2	Prevention: Modus Operandi	195
10.7.3	Prevention: Safer Functions	195
10.7.4	Prevention: Filtering	195
10.7.5	Prevention: Type Safety	197
10.7.6	Detection: Canaries	197
10.7.7	Detection: Code Inspection	197
10.7.8	Detection: Testing	199
10.7.9	Mitigation: Least Privilege	200
10.7.10	Reaction: Keeping Up to Date	201
10.8	Further Reading	201
10.9	Exercises	202
<b>CHAPTER 11 – Bell–LaPadula Model</b>		<b>205</b>
11.1	State Machine Models	206
11.2	The Bell–LaPadula Model	206
11.2.1	The State Set	207
11.2.2	Security Policies	208
11.2.3	The Basic Security Theorem	210
11.2.4	Tranquility	210
11.2.5	Aspects and Limitations of BLP	211
11.3	The Multics Interpretation of BLP	212
11.3.1	Subjects and Objects in Multics	213
11.3.2	Translating the BLP Policies	214
11.3.3	Checking the Kernel Primitives	214
11.4	Further Reading	216
11.5	Exercises	216
<b>CHAPTER 12 – Security Models</b>		<b>219</b>
12.1	The Biba Model	220
12.1.1	Static Integrity Levels	220
12.1.2	Dynamic Integrity Levels	220
12.1.3	Policies for Invocation	221
12.2	Chinese Wall Model	221
12.3	The Clark–Wilson Model	223
12.4	The Harrison–Ruzzo–Ullman Model	225
12.5	Information-Flow Models	228
12.5.1	Entropy and Equivocation	228
12.5.2	A Lattice-Based Model	229
12.6	Execution Monitors	230
12.6.1	Properties of Executions	231
12.6.2	Safety and Liveness	232

12.7	Further Reading	232
12.8	Exercises	233
<b>CHAPTER 13 – Security Evaluation</b>		<b>235</b>
13.1	Introduction	236
13.2	The Orange Book	239
13.3	The Rainbow Series	241
13.4	Information Technology Security Evaluation Criteria	242
13.5	The Federal Criteria	243
13.6	The Common Criteria	243
13.6.1	Protection Profiles	244
13.6.2	Evaluation Assurance Levels	245
13.6.3	Evaluation Methodology	246
13.6.4	Re-evaluation	246
13.7	Quality Standards	246
13.8	An Effort Well Spent?	247
13.9	Summary	248
13.10	Further Reading	248
13.11	Exercises	249
<b>CHAPTER 14 – Cryptography</b>		<b>251</b>
14.1	Introduction	252
14.1.1	The Old Paradigm	252
14.1.2	New Paradigms	253
14.1.3	Cryptographic Keys	254
14.1.4	Cryptography in Computer Security	255
14.2	Modular Arithmetic	256
14.3	Integrity Check Functions	257
14.3.1	Collisions and the Birthday Paradox	257
14.3.2	Manipulation Detection Codes	257
14.3.3	Message Authentication Codes	259
14.3.4	Cryptographic Hash Functions	259
14.4	Digital Signatures	260
14.4.1	One-Time Signatures	261
14.4.2	ElGamal Signatures and DSA	261
14.4.3	RSA Signatures	263
14.5	Encryption	264
14.5.1	Data Encryption Standard	265
14.5.2	Block Cipher Modes	266
14.5.3	RSA Encryption	268
14.5.4	ElGamal Encryption	269
14.6	Strength of Mechanisms	270
14.7	Performance	271
14.8	Further Reading	272
14.9	Exercises	273



<b>CHAPTER 15 – Key Establishment</b>	<b>275</b>
15.1 Introduction	276
15.2 Key Establishment and Authentication	276
15.2.1 Remote Authentication	277
15.2.2 Key Establishment	278
15.3 Key Establishment Protocols	279
15.3.1 Authenticated Key Exchange Protocol	279
15.3.2 The Diffie–Hellman Protocol	280
15.3.3 Needham–Schroeder Protocol	281
15.3.4 Password-Based Protocols	282
15.4 Kerberos	283
15.4.1 Realms	285
15.4.2 Kerberos and Windows	286
15.4.3 Delegation	286
15.4.4 Revocation	287
15.4.5 Summary	287
15.5 Public-Key Infrastructures	288
15.5.1 Certificates	288
15.5.2 Certificate Authorities	289
15.5.3 X.509/PKIX Certificates	289
15.5.4 Certificate Chains	291
15.5.5 Revocation	292
15.5.6 Electronic Signatures	292
15.6 Trusted Computing – Attestation	293
15.7 Further Reading	295
15.8 Exercises	295
<b>CHAPTER 16 – Communications Security</b>	<b>297</b>
16.1 Introduction	298
16.1.1 Threat Model	298
16.1.2 Secure Tunnels	299
16.2 Protocol Design Principles	299
16.3 IP Security	301
16.3.1 Authentication Header	302
16.3.2 Encapsulating Security Payloads	302
16.3.3 Security Associations	304
16.3.4 Internet Key Exchange Protocol	304
16.3.5 Denial of Service	306
16.3.6 IPsec Policies	307
16.3.7 Summary	308
16.4 IPsec and Network Address Translation	308
16.5 SSL/TLS	310
16.5.1 Implementation Issues	312
16.5.2 Summary	313

16.6	Extensible Authentication Protocol	314
16.7	Further Reading	316
16.8	Exercises	316
<b>CHAPTER 17 – Network Security</b>		<b>319</b>
17.1	Introduction	320
17.1.1	Threat Model	320
17.1.2	TCP Session Hijacking	321
17.1.3	TCP SYN Flooding Attacks	322
17.2	Domain Name System	322
17.2.1	Lightweight Authentication	324
17.2.2	Cache Poisoning Attack	324
17.2.3	Additional Resource Records	324
17.2.4	Dan Kaminsky’s Attack	325
17.2.5	DNSSec	326
17.2.6	DNS Rebinding Attack	327
17.3	Firewalls	328
17.3.1	Packet Filters	329
17.3.2	Stateful Packet Filters	330
17.3.3	Circuit-Level Proxies	330
17.3.4	Application-Level Proxies	330
17.3.5	Firewall Policies	331
17.3.6	Perimeter Networks	331
17.3.7	Limitations and Problems	331
17.4	Intrusion Detection	332
17.4.1	Vulnerability Assessment	333
17.4.2	Misuse Detection	333
17.4.3	Anomaly Detection	334
17.4.4	Network-Based IDS	334
17.4.5	Host-Based IDS	334
17.4.6	Honeypots	335
17.5	Further Reading	335
17.6	Exercises	336
<b>CHAPTER 18 – Web Security</b>		<b>339</b>
18.1	Introduction	340
18.1.1	Transport Protocol and Data Formats	340
18.1.2	Web Browser	341
18.1.3	Threat Model	342
18.2	Authenticated Sessions	342
18.2.1	Cookie Poisoning	343
18.2.2	Cookies and Privacy	343
18.2.3	Making Ends Meet	344
18.3	Code Origin Policies	346

18.3.1	HTTP Referer	347
18.4	Cross-Site Scripting	347
18.4.1	Cookie Stealing	349
18.4.2	Defending against XSS	349
18.5	Cross-Site Request Forgery	350
18.5.1	Authentication for Credit	351
18.6	JavaScript Hijacking	352
18.6.1	Outlook	354
18.7	Web Services Security	354
18.7.1	XML Digital Signatures	355
18.7.2	Federated Identity Management	357
18.7.3	XACML	359
18.8	Further Reading	360
18.9	Exercises	361
<b>CHAPTER 19 – Mobility</b>		<b>363</b>
19.1	Introduction	364
19.2	GSM	364
19.2.1	Components	365
19.2.2	Temporary Mobile Subscriber Identity	365
19.2.3	Cryptographic Algorithms	366
19.2.4	Subscriber Identity Authentication	366
19.2.5	Encryption	367
19.2.6	Location-Based Services	368
19.2.7	Summary	368
19.3	UMTS	369
19.3.1	False Base Station Attacks	369
19.3.2	Cryptographic Algorithms	370
19.3.3	UMTS Authentication and Key Agreement	370
19.4	Mobile IPv6 Security	372
19.4.1	Mobile IPv6	373
19.4.2	Secure Binding Updates	373
19.4.3	Ownership of Addresses	375
19.5	WLAN	377
19.5.1	WEP	378
19.5.2	WPA	379
19.5.3	IEEE 802.11i – WPA2	381
19.6	Bluetooth	381
19.7	Further Reading	383
19.8	Exercises	383
<b>CHAPTER 20 – New Access Control Paradigms</b>		<b>385</b>
20.1	Introduction	386
20.1.1	Paradigm Shifts in Access Control	386

20.1.2	Revised Terminology for Access Control	387
20.2	SPKI	388
20.3	Trust Management	390
20.4	Code-Based Access Control	391
20.4.1	Stack Inspection	393
20.4.2	History-Based Access Control	394
20.5	Java Security	395
20.5.1	The Execution Model	396
20.5.2	The Java 1 Security Model	396
20.5.3	The Java 2 Security Model	397
20.5.4	Byte Code Verifier	397
20.5.5	Class Loaders	398
20.5.6	Policies	399
20.5.7	Security Manager	399
20.5.8	Summary	400
20.6	.NET Security Framework	400
20.6.1	Common Language Runtime	400
20.6.2	Code-Identity-Based Security	401
20.6.3	Evidence	401
20.6.4	Strong Names	402
20.6.5	Permissions	403
20.6.6	Security Policies	403
20.6.7	Stack Walk	404
20.6.8	Summary	405
20.7	Digital Rights Management	405
20.8	Further Reading	406
20.9	Exercises	406
	<b>Bibliography</b>	<b>409</b>
	<b>Index</b>	<b>423</b>