

Table of Contents

Part One

Challenges and Basic Approaches	1
---------------------------------------	---

1. Introduction	3
-----------------------	---

1.1 The Need for Security	3
---------------------------------	---

1.2 Fundamental Aspects of Security	6
---	---

1.3 Informational Assurances	7
------------------------------------	---

1.3.1 The Information Society	7
-------------------------------------	---

1.3.2 A General Framework	7
---------------------------------	---

1.3.3 Privacy and Informational Self-Determination	10
--	----

1.3.4 Enforcement of Informational Self-Determination	12
---	----

1.3.5 Legislation	13
-------------------------	----

1.3.6 Security Evaluation Criteria and Security Agencies	14
--	----

1.4 Notions of Security	16
-------------------------------	----

1.4.1 Outline of a Formal Theory	16
--	----

1.4.2 A Practical Checklist for Evaluations	18
---	----

1.5 The Design Cycle for Secure Computing Systems	19
---	----

1.5.1 Compositionality and Refinement	19
---	----

1.5.2 Construction Principles	23
-------------------------------------	----

1.5.3 Risk Assessment	25
-----------------------------	----

1.6 The Life Cycle of Secure Computing Systems	26
--	----

1.7 Bibliographic Hints	27
-------------------------------	----

2. Fundamental Challenges	29
---------------------------------	----

2.1 Information Flow from Senders to Receivers	29
--	----

2.1.1 Message Transmission	30
----------------------------------	----

2.1.2 Inferences	32
------------------------	----

2.1.3 Inspections and Exception Handling	34
--	----

2.1.4 Control and Monitoring	39
------------------------------------	----

2.2 Security Interests	40
------------------------------	----

2.2.1 Availability	40
--------------------------	----

2.2.2 Integrity: Correct Content	41
--	----

2.2.3 Integrity: Unmodified State	41
---	----

2.2.4 Integrity: Detection of Modification	42
--	----

2.2.5 Authenticity	42
--------------------------	----

2.2.6 Non-Repudiation	42
-----------------------------	----

2.2.7	Confidentiality	43
2.2.8	Non-Observability	44
2.2.9	Anonymity	44
2.2.10	Accountability	45
2.2.11	Evidence	45
2.2.12	Integrity: Temporal Correctness	45
2.2.13	Separation of Roles	45
2.2.14	Covert Obligations	46
2.2.15	Fair Exchange	46
2.2.16	Monitoring and Eavesdropping	46
2.3	Trade-Offs	47
2.3.1	Autonomy and Cooperation	47
2.3.2	Trust and Threats	49
2.3.3	Confidence and Provision	50
2.4	Bibliographic Hints	51
3.	Computing Systems and Their Basic Vulnerabilities	53
3.1	Architecture	53
3.1.1	Physical Devices	56
3.1.2	Virtual Vertical Layers	59
3.1.3	Virtual Digital Objects and Implementing Bit Strings	60
3.1.4	Horizontal Distribution	61
3.1.5	Personal Computing Devices	63
3.2	Complexity of Computations	63
3.3	Bibliographic Hints	64
 Part Two		
Fundamentals of Information Flow and Inference Control		65
4.	Messages, Inferences, Information and Knowledge	67
4.1	A General Perspective	67
4.2	Simple Mathematical Models	71
4.2.1	Inversion of Functions and Solving Equations	72
4.2.2	Projections of Relations	76
4.2.3	Determination of Equivalence Classes	80
4.2.4	Impact of Message Sequences	80
4.2.5	Implications in Classical Logics	82
4.2.6	Logics of Knowledge and Belief	86
4.2.7	Probability-Oriented Models	87
4.3	Inference Control	88
4.4	Bibliographic Hints	92
5.	Preventive Inference Control	93
5.1	Inference Control for Sequential Programs	93
5.1.1	An Example	94

5.1.2	A Classification of Information Flows	97
5.1.3	Computational Challenges	97
5.1.4	An Adapted Relational Model for Carriers and Blocking	100
5.1.5	Introducing Labels	102
5.1.6	Carriers, Labels and Expressions	106
5.1.7	Examples of Dynamic Monitoring	107
5.1.8	Examples of Static Verification	114
5.1.9	Resetting and Downgrading Dynamic Labels	124
5.1.10	The Programming Language Jif	126
5.2	Inference Control for Parallel Programs	126
5.3	Inferences Based on Covert Channels	127
5.4	Inference Control for Information Systems	129
5.5	Inference Control for Statistical Information Systems	134
5.5.1	The Summation Aggregate Function	135
5.5.2	Selector Aggregate Functions	139
5.6	Inference Control for Mandatory Information Systems	141
5.6.1	A Labeled Information System with Polyinstantiation	142
5.6.2	Inference-Proof Label Assignments	145
5.7	Noninterference in Trace-Based Computing Systems	146
5.7.1	Noninterference Properties	147
5.7.2	Verification by Unwinding	150
5.8	Bibliographic Hints	152
 Part Three		
	Security Mechanisms	155
 6. Key Ideas and Examples		
6.1	Redundancy	157
6.1.1	Spare Equipment and Emergency Power	158
6.1.2	Recovery Copies for Data and Programs	159
6.1.3	Deposit of Secrets	159
6.1.4	Switching Networks with Multiple Connections	160
6.1.5	Fault-Tolerant Protocols	160
6.1.6	Error-Detecting and Error-Correcting Codes	162
6.1.7	Cryptographic Pieces of Evidence	163
6.2	Isolation	164
6.2.1	Spatial Separation and Entrance Control	164
6.2.2	Temporal Separation and Isolated Memory	166
6.2.3	Memory Protection and Privileged Instructions	167
6.2.4	Separate Process Spaces	171
6.2.5	Object-Oriented Encapsulation	172
6.2.6	Security Kernels	173
6.2.7	Stand-Alone Systems	173
6.2.8	Separate Transmission Lines	174

6.2.9	Security Services in Middleware	174
6.2.10	Firewalls	174
6.2.11	Cryptographic Isolation	175
6.3	Indistinguishability	175
6.3.1	Superimposing Randomness	175
6.3.2	Hiding among Standardized Behavior	178
6.4	Bibliographic Hints	180
7.	Combined Techniques	181
7.1	Identification or Classification, and Proof of Authenticity	182
7.1.1	Some Idealized Non-Computerized Situations	183
7.1.2	Local Identifiers	184
7.1.3	Global Identifiers	186
7.1.4	Interoperable Classification	187
7.1.5	Provisions for Authentication and Proof of Authenticity	187
7.2	Permissions and Prohibitions	191
7.2.1	Specification	193
7.2.2	Representation, Management and Enforcement	194
7.3	Requirements and Mechanisms	199
7.4	Bibliographic Hints	202
8.	Techniques of Control and Monitoring: Essentials	203
8.1	Requirements, Mechanisms and their Quality	203
8.2	Essential Parts	203
8.2.1	Declaration of Permissions and Prohibitions	204
8.2.2	Control Operations	205
8.2.3	Isolation, Interception and Mediation of Messages	206
8.2.4	Proof of Authenticity	206
8.2.5	Access Decisions	206
8.2.6	Monitoring	207
8.2.7	Root of Trust	208
8.3	Bibliographic Hints	208
9.	Conceptual Access Rights	209
9.1	Conceptual Models of Discretionary Approaches	210
9.1.1	Refining the Granted Relationship	213
9.1.2	Differentiating Controlled Objects	215
9.1.3	Programs, Processes and Masterships	217
9.1.4	Differentiating Operational Modes	218
9.1.5	Qualifications and Conditions	221
9.1.6	Managing Privileges with Collectives	222
9.1.7	Role-Based Access Control (RBAC)	224
9.2	Semantics for Access Decisions	225
9.2.1	Informal Semantics	226
9.2.2	Formal Semantics	228
9.2.3	The Flexible Authorization Framework (FAF)	228

9.2.4	The Dynamic Authorization Framework (DAF)	236
9.3	Policy Algebras	241
9.3.1	A Basic Policy Algebra	242
9.3.2	An Algebra on Policy Transformations	246
9.4	Granting and Revoking	249
9.4.1	A Conceptual Model	249
9.4.2	A Formalization of Granting	252
9.4.3	Formalizations of Revoking	253
9.4.4	Recursive Revocation	256
9.5	Dynamic and State-Dependent Permissions	261
9.5.1	Control Automata	262
9.5.2	Role Enabling and Disabling	263
9.5.3	Information Flow Monitoring	265
9.5.4	Process Masterships and Procedure Calls	269
9.5.5	Discretionary Context Selection	272
9.5.6	Workflow Control	274
9.6	Analysis of Control States	275
9.6.1	Task and Abstract Model	275
9.6.2	Undecidability	280
9.6.3	Take-Grant and Send-Receive Control Schemas	284
9.6.4	Typed Control Schemas	289
9.7	Privileges and Information Flow	290
9.8	Conceptual Model of Mandatory Approaches	293
9.8.1	Dynamic Mandatory Access Control	295
9.8.2	Downgrading and Sanitation	297
9.8.3	A Dual Approach to Enforcing Integrity	298
9.9	Bibliographic Hints	299
10	Elements of a Security Architecture	303
10.1	Establishing Trust in Computing Systems	305
10.2	Layered Design	308
10.2.1	Integrity and Authenticity Basis	310
10.2.2	Establishing the Trustworthiness of an Instance	313
10.2.3	Personal Computing Devices	317
10.2.4	Hardware and Operating System with Microkernel	320
10.2.5	Bootstrapping and Add-On Loading	325
10.2.6	Network and Middleware	326
10.2.7	Programming Languages and Programming	330
10.3	Certificates and Credentials	334
10.3.1	Characterizing and Administrative Properties	336
10.3.2	Evaluating Trust Recursively	339
10.3.3	Model of Trusted Authorities and Licensing	340
10.3.4	Model of Owners and Delegation	342
10.3.5	Converting Free Properties into Bound Properties	345
10.4	Firewalls	348

10.4.1	Placement and Tasks	348
10.4.2	Components and their Combination	350
10.5	Bibliographic Hints	352
11.	Monitoring and Intrusion Detection	355
11.1	Intrusion Detection and Reaction	356
11.1.1	Tasks and Problems	356
11.1.2	Simple Model	359
11.2	Signature-Based Approach	362
11.3	Anomaly-Based Approach	365
11.4	Cooperation	365
11.5	Bibliographic Hints	366
12.	Techniques of Cryptography: Essentials	369
12.1	Requirements, Mechanisms and their Quality	369
12.2	Cryptographic Isolation and Indistinguishability	371
12.3	Cooperation in the Presence of Threats	374
12.4	Basic Cryptographic Blocks	374
12.4.1	Encryption	375
12.4.2	Authentication	378
12.4.3	Anonymization	382
12.4.4	Randomness and Pseudorandomness	387
12.4.5	One-Way Hash Functions	388
12.4.6	Timestamps	390
12.5	Quality in Terms of Attacks	391
12.6	Probability-Theoretic Security for Encryption	395
12.7	Probability-Theoretic Security for Authentication	400
12.8	Information Gain about a Secret Encryption Key	407
12.9	Complexity-Theoretic Security for Encryption	412
12.9.1	One-Way Functions with Trapdoors	412
12.9.2	RSA Functions	415
12.9.3	ElGamal Functions	418
12.9.4	Elliptic-Curve Functions	421
12.10	Cryptographic Security	425
12.11	Bibliographic Hints	425
13.	Encryption	429
13.1	Survey and Classification	429
13.1.1	Definition and Application Scenario	429
13.1.2	Classification	431
13.1.3	A Tabular Summary	434
13.2	One-Time Keys and Perfect Ciphers (Vernam)	436
13.3	Stream Ciphers with Pseudorandom Sequences (Vigenère)	438
13.4	The RSA Asymmetric Block Cipher	442
13.5	The ElGamal Asymmetric Block Cipher	444
13.6	Asymmetric Block Ciphers Based on Elliptic Curves	446

13.7	The DES Symmetric Block Cipher	446
13.8	The IDEA Symmetric Block Cipher	452
13.9	The AES–Rijndael Symmetric Block Cipher	455
13.10	Stream Ciphers Using Block Modes	460
13.10.1	Electronic Codebook (ECB) Mode	461
13.10.2	Cipher Block Chaining (CBC) Mode	462
13.10.3	Cipher Feedback (CFB) Mode	464
13.10.4	Output Feedback (OFB) Mode	465
13.10.5	Counter-with-Cipher-Block-Chaining Mode (CCM)	466
13.10.6	A Comparison of Block Modes	467
13.11	Introduction to a Theory of Encryption	468
13.11.1	The Symmetric/Single-Usage Setting	469
13.11.2	The Asymmetric/Single-Usage Setting	474
13.11.3	The Settings for Multiple Key Usage	475
13.11.4	Constructions	476
13.12	Bibliographic Hints	477
14.	Authentication	479
14.1	Survey and Classification	479
14.1.1	Classification	481
14.1.2	A Tabular Summary	482
14.2	One-Time Keys and Perfect Authentication (Orthogonal Arrays)	484
14.3	RSA Asymmetric Digital Signatures	488
14.4	ElGamal Asymmetric Digital Signatures	491
14.5	DSA, the Digital Signature Algorithm	494
14.6	Digital Signatures Based on Elliptic Curves	495
14.7	Undeniable Signatures	496
14.8	Symmetric Message Authentication Codes Based on CBC Mode	501
14.9	Introduction to a Theory of Authentication	502
14.9.1	Definition of Unforgeability	503
14.9.2	Impact of Length-Restricted Schemes	505
14.9.3	Constructions	507
14.10	Bibliographic Hints	512
15.	Anonymization	513
15.1	Survey	513
15.2	Blind Signatures and Unlinkable Obligations	514
15.3	Superimposed Sending	517
15.4	MIX Networks	519
15.5	Bibliographic Hints	525
16.	Some Further Cryptographic Protocols	527
16.1	Survey	527
16.2	Covert Commitments	529
16.2.1	Application Scenario and Security Requirements	529
16.2.2	A Mechanism Based on Symmetric Encryption	530

16.2.3	A Mechanism Based on a One-Way Hash Function	531
16.3	Secret Sharing	532
16.3.1	Application Scenario and Security Requirements	532
16.3.2	A Mechanism Based on Distributing Linear Equations	533
16.4	Zero-Knowledge Proofs	535
16.4.1	Application Scenario	535
16.4.2	Security Requirements	538
16.4.3	A Mechanism Based on an NP-Complete Problem	541
16.5	Multiparty Computations	544
16.5.1	Application Scenario and Security Requirements	544
16.5.2	Employing Homomorphic Threshold Encryption	548
16.5.3	Employing Boolean Circuits	553
16.6	Design and Verification of Cryptographic Protocols	555
16.7	Bibliographic Hints	556
Part Four		
Implementations		559
17. Design of Selected Systems		561
17.1	UNIX Operating System	561
17.1.1	Basic Blocks	562
17.1.2	Conceptual Design of the Operating System Functionality ...	562
17.1.3	Conceptual Design of the Security Concepts	565
17.1.4	Refined Design	567
17.1.5	Components of Local Control and Monitoring	569
17.2	Oracle/SQL Database Management System	576
17.2.1	Basic Blocks	576
17.2.2	Conceptual Design of the Database Functionality	577
17.2.3	Conceptual Design of Access Rights	581
17.2.4	Components of Local Control and Monitoring	586
17.3	CORBA Middleware	591
17.3.1	Basic Blocks	591
17.3.2	Conceptual Design of the Client-Server Functionality	592
17.3.3	Conceptual Design of the Security Concepts	593
17.4	Kerberos	599
17.4.1	Basic Blocks	599
17.4.2	Conceptual Design	600
17.4.3	Simplified Messages	604
17.5	Simple Public Key Infrastructure (SPKI/SDSI)	606
17.5.1	Basic Blocks	607
17.5.2	An Application Scenario	608
17.5.3	Certificates and their Semantics	609
17.5.4	Certificate Chain Discovery	612
17.6	Pretty Good Privacy (PGP)	615

17.6.1	Basic Blocks	616
17.6.2	Conceptual Design of Secure Message Transmission	616
17.6.3	Key Management	619
17.6.4	Assessment of Public Keys	620
17.7	Bibliographic Hints	622
Appendix		625
A.1	Entity–Relationship Diagrams	625
A.2	First-Order Logic	628
A.3	Random Variables and Entropy	630
A.3.1	Random Variables and Probability Distributions	630
A.3.2	Entropy	631
A.4	Number Theory	632
A.4.1	Algebraic Structures Based on Congruences	632
A.4.2	Finite Fields Based on Prime Congruences	633
A.4.3	Algorithms for Operations on Residue Classes	635
A.4.4	Randomized Prime Number Generation	637
A.5	Finite Algebras	639
References		643
Index		669