Contents

Foreword by Changjun Jiang vii

Foreword by Yale Li ix

Preface xi

About the Author xv

1. An Introduction to Data Security 1

1.1 What Is Data Security? 3
1.1.1 Definition of data 4
1.1.2 Data lifecycle 5
1.1.3 Data security requirements 11
1.1.4 Overall goal of data security 13
1.2 Principles and Implementation of Data Classification 20
1.2.1 Standards for data classification 23
1.2.2 Data classification framework 27
1.2.3 Data classification implementation steps 30
1.2.4 Regulatory-based data classification 33
1.2.5 Strategies for effective data classification 37
1.2.6 Examples of data classification for organizations 39
1.2.7 Example of cloud data classification 40
1.2.8 Example of Microsoft data classification 47
1.2.9 Smartphone data classification example 49
1.3 Identity Authentication and Data Access Control 52
1.3.1 User authentication 53
1.3.2 Service authentication 59

1.3.3 Device authentication 60
1.3.4 Data access control system 61
1.4 Summary of Data Security System 63

2. Data Security Risk Challenges and Responses 65

2.1 Risks and Challenges of Data Security 65
2.1.1 Data security in the Internet era 66
2.1.2 Data security in the era of convergence of everything 66
2.1.3 Frequent data leakage incidents 72
2.1.4 Growing concerns about data security 81
2.1.5 Data security has become a hot topic in the industry 82
2.1.6 Where is the sensitive data located? 85
2.1.7 Behind the data security issues 87
2.1.8 Evolution of data security attack surface 89
2.1.9 Typical attack scenarios and types 93
2.1.10 Major threats to data security 98
2.2 Data Security Response Mechanism 102
2.2.1 Risk assessment method 102
2.2.2 Analysis of business impact 104
2.2.3 Data flow analysis 105
2.2.4 Selection, implementation, and evaluation of control measures 111
2.2.5 Overview of threat modeling 119
2.2.6 STRIDE threat model 125
2.2.7 Data-centric threat modeling 129
2.2.8 Anomaly and event detection 137
2.2.9 Continuous monitoring 140
2.2.10 Response planning and implementation 142
2.2.11 Recovery plan and crisis management 144

3. Data Security Architecture and Design 147

3.1 Design and Implementation of Data Security Architecture 148
3.1.1 Security architecture project establishment and requirements analysis 151
3.1.2 Security architecture design and delivery 155
3.1.3 Visual presentation of security architecture . . . 161

3.1.4 Security architecture from different perspectives 165
3.2 Organizational Data Security Architecture Model 170
3.2.1 Overview of data security governance framework 171
3.2.2 Data governance strategies and standards 174
3.2.3 Security data collection policy 178
3.2.4 Data retention strategy 181
3.3 Data Security Governance Framework 184
3.3.1 Identify 189
3.3.2 Protect 191
3.3.3 Detect 192
3.3.4 Respond 193
3.3.5 Recover 194
3.3.6 Summary of data security governance framework 195
3.4 Excellent Cases of Security Architecture 196
3.4.1 Defense in depth architecture 196
3.4.2 Data-centric security architecture 199
3.4.3 CSA enterprise architecture 202
3.4.4 NIST cloud computing security architecture 207
3.4.5 Zero trust security architecture 212
3.5 Security Design Principles and Cases 217
3.5.1 Economy of mechanism 218
3.5.2 Fail-safe defaults 220
3.5.3 Complete mediation 222
3.5.4 Open design 224
3.5.5 Separation of privilege 226
3.5.6 Least privilege 227
3.5.7 Least common mechanism 228
3.5.8 Psychological acceptability 229
3.6 Trust Basis for Data Security 232
3.6.1 The principle and application scenarios of HSM 233
3.6.2 The principle and application scenarios of TPM 236
3.6.3 Principles and application scenarios of TEE . . 238
3.6.4 Summary of trust basis for data security 242

3.7 Key Technologies of Encryption and Access Control . . 244
3.7.1 Endpoint encryption technologies 244
3.7.2 File encryption technologies 249
3.7.3 Database encryption technologies 252
3.7.4 Format preserving encryption technology 257
3.7.5 Data-centric encryption 260
3.7.6 Access control technology 262
3.7.7 File monitoring technologies 267
3.7.8 Database monitoring technologies 272
3.8 Data Security Business Scenarios 278
3.8.1 DRM technologies and applicable scenarios . . . 278
3.8.2 MDM technology and applicable scenarios . . . 281
3.8.3 DLP technology and applicable scenarios 284
3.8.4 Introduction of CASB and integration with DLP 287
3.9 Chapter Summary 291
4. The Cornerstone of Data Security: Cryptography and Encryption 293
4.1 Origin and Evolution of Cryptography 296
4.1.1 Caesar cipher 297
4.1.2 Simple substitution ciphers 298
4.2 The Birth of Modern Cryptography 303
4.3 Key-based Encryption 309
4.3.1 One-time password 309
4.3.2 Symmetric encryption 311
4.3.3 Block ciphers 313
4.3.4 Modes of operation of block ciphers 317
4.3.5 Stream ciphers 328
4.4 Public Key Encryption 334
4.4.1 Key exchange 334
4.4.2 Public-key cryptography 336
4.4.3 Man-in-the-middle attack and protection 339
4.4.4 Replay attack and defense 340
4.4.5 Elliptic curve cryptography 342
4.5 Key Management System 349
4.5.1 The importance and principles of key management 350
4.5.2 Key lifecycle management 352

4.5.3 Regulatory requirements for key management 359
4.5.4 Regulatory compliance for key management 360
4.5.5 Problems with key exchange 363
4.5.6 Key distribution center 364
4.5.7 Public key management 366
4.5.8 Key escrow 367
4.6 Public Key Infrastructure 368
4.6.1 PKI system 368
4.6.2 Certificate authority 370
4.6.3 Registration authority 371
4.6.4 Digital certificates 372
4.6.5 Lightweight directory access protocol 374
4.6.6 New PKI system 374
4.7 Hash Algorithm 375
4.7.1 MD5 378
4.7.2 SHA-1 378
4.7.3 SHA-2 379
4.7.4 Keccak and SHA-3 380
4.7.5 Password storage 380
4.7.6 Hash tree 383
4.8 Message Authentication Code 383
4.8.1 Secure MAC 384
4.8.2 Keys in MAC algorithm 385
4.8.3 HMAC introduction 386
4.8.4 Authentication encryption mode 387
4.9 Digital Signature 389
4.10 Security Protocols Based on Cryptography 391
4.10.1 Identification and login protocol 391
4.10.2 Authenticated key exchange 394
4.10.3 Zero-knowledge proof 396
4.10.4 Secure multi-party computation 401
4.10.5 Homomorphic encryption 403
4.11 Cryptography and Key Management in the Quantum Era 405
4.11.1 Quantum key distribution 406
4.11.2 Asymmetric cryptography in the quantum era 408

4.11.3 Symmetric cryptography in the quantum era 408
4.11.4 Post-quantum cryptography algorithms and their standardization 409
4.11.5 The rise of quantum supremacy 409
4.11.6 Prospects of post-quantum cryptography 411
4.12 Cryptography Technology Practice 412
4.12.1 Apple iOS data security 412
4.12.2 AWS key management service 414

5. Privacy Protection and Data Security Compliance 419

5.1 The Concept and Regulation of Privacy 419
5.1.1 Privacy challenges 421
5.1.2 Privacy regulatory trends 423
5.2 OECD Eight Principles of Privacy Protection 428
5.2.1 Collection limitation principle 431
5.2.2 Data quality principle 432
5.2.3 Purpose specification principle 433
5.2.4 Use limitation principle 433
5.2.5 Security safeguards principle 434
5.2.6 Openness principle 434
5.2.7 Individual participation principle 435
5.2.8 Accountability principle 435
5.3 Privacy Protection Technologies 435
5.3.1 Overview of anonymization and pseudonymization technologies 436
5.3.2 Randomization techniques 441
5.3.3 Differential privacy 443
5.3.4 Generalization techniques 447
5.3.5 Encryption technologies 452
5.3.6 Hash technologies 452
5.3.7 Tokenization technology 453
5.3.8 Summary of privacy protection technologies 456
5.4 General Data Security Compliance Requirements 458
5.4.1 National and regional legal compliance requirements 459

5.4.2 International and national standards compliance requirements 467
5.4.3 Industry standard compliance requirements 471
5.5 Industry Data and Privacy Compliance Requirements 476
5.5.1 Financial data supervision requirements 476
5.5.2 Medical and health data security regulatory requirements 481
5.5.3 Children's data supervision requirements 488
5.5.4 Manufacturing security supervision requirements 489
5.5.5 Media industry safety supervision requirements 491
5.5.6 Energy industry safety supervision requirements 492
5.5.7 Education industry security supervision requirements 493
5.6 Evolution of Data Security and Privacy Protection Supervision in China 494
5.6.1 Legislative trends of data security and privacy protection 495
5.6.2 Interpretation of cybersecurity law 497
5.6.3 Interpretation of data security law 500
5.6.4 Interpretation of personal information protection Law 502
5.6.5 National standards for data security and personal information protection 509
5.6.6 Network security level protection 512
5.7 Chapter Summary 515
6. Emerging Technologies and Data Security 517
6.1 AI and Data Security 517
6.1.1 Artificial intelligence, machine learning, and deep learning 519
6.1.2 Artificial intelligence and data security 524
6.1.3 AI data threat model 526
6.1.4 Privacy protection of artificial intelligence . . . 533
6.1.5 Artificial intelligence and network security . . . 536

6.2 Emerging Applications Represented by Blockchain . . . 537
6.2.1 Basic concepts of blockchain 538
6.2.2 Consensus algorithm and its application 542
6.2.3 Merkle tree data structure 546
6.2.4 Comprehensive application of cryptographic algorithms 548
6.2.5 Data structure of blockchain 551
6.2.6 Bitcoin mining algorithm 553
6.3 IoT Data Security 556
6.3.1 Concept of internet of things 557
6.3.2 Data security risks of the internet of things . . . 559
6.3.3 IoT data security response 563
6.4 5G and Data Security 565
6.4.1 5G data security standards 567
6.4.2 Security of 5G new network architecture 570
6.4.3 Security of 5G new service scenarios 571
6.4.4 Formal analysis of 5G authentication protocol 571
6.5 Outlook for 6G and Data Security 573
6.5.1 6G research direction 574
6.5.2 Evolution of 6G security 575
6.5.3 Attack and defense of terahertz network 577
6.6 Chapter Summary 580

Bibliography 581

Index 593