## CONTENTS

**Preface and Acknowledgments** xxiii

**About the Companion Website** xxvii

1 WHAT IS SECURITY? 1

1.1 Introduction 1

1.2 The Subject of Security 2

1.2.1 Branches of Security 2

1.2.2 Defining Security by Function 5

1.2.2.1 Risk Avoidance 5

1.2.2.2 Deterrence 5

1.2.2.3 Prevention 6

1.2.2.4 Detection 7

1.2.2.5 Recovery 7

1.2.3 The Common Body of Knowledge (CBK) Security Domains 8

1.2.3.1 Access Control Systems and Methodology 8

1.2.3.2 Application and Systems Development Security 9

1.2.3.3 Business Continuity Planning and Disaster Recovery Planning 10

1.2.3.4 Cryptography 10

1.2.3.5 Information Security and Risk Management 11

1.2.3.6 Legal, Regulations, Compliance, and Investigations 11

1.2.3.7 Operations Security 12

1.2.3.8 Physical Security 13

1.2.3.9 Security Architecture and Models 14

1.2.3.10 Telecommunications and Network Security 14

1.2.3.11 CBK Summary 15

1.3 A Twenty-First Century Tale 15

1.3.1 The Actors 15

1.3.1.1 Bob’s Story 15

vii
2 SYSTEMS ENGINEERING

2.1 So What Is Systems Engineering?
   2.1.1 Similar Systems Engineering Process
      2.1.1.1 Stating the Problem
      2.1.1.2 Investigate Alternatives and Model the System
      2.1.1.3 Develop/Integrate
      2.1.1.4 Launch the System
      2.1.1.5 Assess Performance
      2.1.1.6 Re-evaluate
   2.1.2 Another Systems Engineering View
   2.1.3 Process Variations

2.2 Process Management
   2.2.1 ISO 9000 Processes and Procedures
   2.2.2 Capability Maturity Model (CMM)

2.3 Organization Environments
   2.3.1 Economic, Legal, and Political Contexts
      2.3.1.1 Regulations/Legislation
      2.3.1.2 Market-Based Regulations
      2.3.1.3 Technology Evolution
      2.3.1.4 Customer Demands and Expectations
      2.3.1.5 Legal Liability
      2.3.1.6 Competition
      2.3.1.7 Terrorism and Cybercrime
   2.3.2 Business/Organizational Types
      2.3.2.1 Commercial
## FOUNDATION CONCEPTS

### 3.1 Security Concepts and Goals
- **3.1.1 Subjects and Objects**
- **3.1.2 What Is Trust?**
- **3.1.3 Domains, Security, and Trust**
- **3.1.4 Security Goals/Objectives**
- **3.1.5 X.800 Security Services**
  - 3.1.5.1 Authentication
  - 3.1.5.2 Access Control
  - 3.1.5.3 Confidentiality
  - 3.1.5.4 Data Integrity
  - 3.1.5.5 Non-Repudiation
- **3.1.6 A Modern Definition of Security Services**
  - 3.1.6.1 Authentication
  - 3.1.6.2 Authorization-Access Control
  - 3.1.6.3 Integrity
  - 3.1.6.4 Availability
  - 3.1.6.5 Accountability
  - 3.1.6.6 Privacy As a Security Service
  - 3.1.6.7 Service Mapping and Application of Services

### 3.2 Role of Cryptography in Information Security
- **3.2.1 Cryptographic Hash Algorithms**
  - 3.2.1.1 HMAC-MD5 and HMAC-SHA1
- **3.2.2 Encryption Algorithms**
  - 3.2.2.1 Symmetric Encryption
  - 3.2.2.2 Asymmetric Encryption
  - 3.2.2.3 Encryption Algorithm Performance
- **3.2.3 Cryptanalysis and Other Key Issues**
  - 3.2.3.1 Cryptanalysis
  - 3.2.3.2 Key Randomness
### Key Protection

3.2.3.3 Key Protection 106
3.2.3.4 Using Passwords with Cryptography 107
3.2.3.5 Using Passphrases with Cryptography 108

### Key Management

3.2.4 Key Management 108
3.2.4.1 Diffie–Hellmann Key Distribution 110

### Cryptographic Authentication

3.2.5 Cryptographic Authentication 112
3.2.5.1 Challenge–Response Technique 113
3.2.5.2 Message Authentication Code Technique 116
3.2.5.3 Digital Signature Authentication Technique 119

### Key Management Revisited

3.3 Key Management Revisited 120

### Chapter Summary

3.4 Chapter Summary 121

### Further Reading and Resources

3.5 Further Reading and Resources 122

---

### Authentication of Subjects

4 AUTHENTICATION OF SUBJECTS 123

#### Authentication Systems

4.1 Authentication Systems 123
4.1.1 Kerberos-Based Authentication 124
4.1.2 Public-Key Infrastructure 128
4.1.2.1 X.509 Digital Certificates 128
4.1.2.2 Certificate Authority Hierarchies 131
4.1.2.3 Certificate Generation Requests 136
4.1.2.4 PKI Component Deployment 139
4.1.2.5 Digital Certificate Revocation and Status Verification 141
4.1.2.6 Certificate Verification 143
4.1.3 Remote Authentication Dial-in User Service and EAP 144
4.1.4 Diameter 149
4.1.5 Secure Electronic Transactions (SET) 150
4.1.6 Authentication Systems Summary 154

#### Human Authentication

4.2 Human Authentication 154
4.2.1 What the Subject Has Factor 155
4.2.2 What the Subject Knows Factor 155
4.2.3 What the Subject Is Factor 156
4.2.4 Where the Subject Is Factor 157
4.2.5 Combinations of Factors 157
4.2.6 Rainbow Tables 158
4.2.7 Proxies for Humans 159
4.2.7.1 Operating Systems 159
5 SECURITY SYSTEMS ENGINEERING

5.1 Security Policy Development 170
5.2 Senior Management Oversight and Involvement 170
5.3 Security Process Management and Standards 170
5.3.1 ISO 27002 172
  5.3.1.1 Establishing Organizational Security Policy (Section 5) 172
  5.3.1.2 Organizational Security Infrastructure (Section 6) 173
  5.3.1.3 Asset Classification and Control (Section 7) 175
  5.3.1.4 Personnel Security (Section 8) 176
  5.3.1.5 Physical and Environmental Security (Section 9) 178
  5.3.1.6 Communications and Operations Management (Section 10) 179
  5.3.1.7 Access Controls (Section 11) 180
  5.3.1.8 Information Systems Acquisition, Development, and Maintenance (Section 12) 181
  5.3.1.9 Information Security Incident Management (Section 13) 182
  5.3.1.10 Business Continuity Management (Section 14) 182
  5.3.1.11 Compliance (Section 15) 183
  5.3.1.12 ISO 27002 Summary 185
5.3.2 ISO 27001 185
5.3.3 Policy Hierarchy 186
5.3.4 An Enterprise Security Policy Example 189
5.3.5 COBIT 189
5.3.6 Information Technology Infrastructure Library 194
5.3.7 Federal Information Security Management Act (FISMA) 196
5.4 Information Security Systems Engineering Methodology 199
5.4.1 Existing Asset Inventory and Classification 201
  5.4.1.1 Physical Assets 201
  5.4.1.2 Logical Assets 202
5.4.1.3 Conceptual Assets 202
5.4.2 Vulnerabilities, Threats, and Risk 203
5.4.2.1 Asset Vulnerabilities 204
5.4.2.2 Organization Threat Profile(s) 204
5.4.3 Dealing with Risk 224
5.4.3.1 ITU-T View of Risk Mitigation Approach 224
5.4.3.2 STRIDE Mitigation Approach 226
5.4.3.3 ISO 27005 Approach to Managing Risk 226
5.4.3.4 Common Criteria (CC) Mitigation Approach 227
5.4.3.5 ETSI Security-Related Vulnerability and Threat Analysis Efforts 230
5.4.4 Risk Management Framework 232
5.4.4.1 Impact Analysis 233
5.4.4.2 Risk Assessment Analysis 234
5.4.4.3 Risk Assessment—Asset Definition and Inventorying 236
5.4.4.4 Risk Assessment—Threats 237
5.4.5 Risk Assignment 240
5.5 Requirements Analysis and Decomposition 240
5.6 Access Control Concepts 244
5.6.1 Subjects, Objects, and Access Operations 245
5.6.2 Mandatory Access Control using a Matrix or Lattice Approach 246
5.6.3 Discretionary Access Control using an Access Control List Approach 246
5.6.4 Mandatory Access Control using a Capability List Approach 247
5.6.5 Administrative Tasks in Access Control Methods 248
5.6.5.1 Groups and Permissions 248
5.6.5.2 Protection Rings 249
5.6.6 Role-Based Access Control (RBAC) 249
5.7 Security Modeling and Security-Related Standards 251
5.7.1 Confidentiality Policies and Integrity Policies 252
5.7.2 Bell–LaPadula Model 253
5.7.3 Graham–Denning Confidentiality Model 254
5.7.4 Chinese Wall Multilateral Confidentiality Model 255
5.7.5 Biba Integrity Model 256
5.7.6 Clark–Wilson Model 256
5.7.7 Security Model Summary 258
5.7.8 Security Standards 259
6 TRADITIONAL NETWORK CONCEPTS

6.1 Networking Architectures
   6.1.1 OSI Network Model
   6.1.2 Internet Network Model

6.2 Types of Networks
   6.2.1 Local Area Network (LAN)
   6.2.2 Wireless LAN (WLAN)
   6.2.3 Metropolitan Area Networks (MAN)
   6.2.4 Wide Area Networks (WAN)
   6.2.5 The Internet
   6.2.6 Circuit Switched Networks
   6.2.7 Supervisory Control and Data Acquisition (SCADA) Systems
   6.2.8 Sensor Networks
   6.2.9 Clouds
      6.2.9.1 Hardware as a Service
      6.2.9.2 Infrastructure as a Service
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.9.3</td>
<td>Applications as a Service</td>
<td>292</td>
</tr>
<tr>
<td>6.2.9.4</td>
<td>Public versus Private Clouds</td>
<td>293</td>
</tr>
<tr>
<td>6.2.10</td>
<td>Cellular Networks</td>
<td>294</td>
</tr>
<tr>
<td>6.2.11</td>
<td>IEEE 802.16 Networks</td>
<td>295</td>
</tr>
<tr>
<td>6.2.12</td>
<td>Long-Term Evolution Networks</td>
<td>295</td>
</tr>
<tr>
<td>6.3</td>
<td>Network Protocols</td>
<td>295</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Layer 1—Physical</td>
<td>296</td>
</tr>
<tr>
<td>6.3.2</td>
<td>Layer 2—Data Link Protocols</td>
<td>296</td>
</tr>
<tr>
<td>6.3.2.1</td>
<td>Ethernet</td>
<td>297</td>
</tr>
<tr>
<td>6.3.2.2</td>
<td>Virtual Ethernets</td>
<td>299</td>
</tr>
<tr>
<td>6.3.2.3</td>
<td>Wireless Networking</td>
<td>300</td>
</tr>
<tr>
<td>6.3.2.4</td>
<td>MultiProtocol Label Switching</td>
<td>301</td>
</tr>
<tr>
<td>6.3.2.5</td>
<td>Asynchronous Transfer Mode and Frame Relay</td>
<td>304</td>
</tr>
<tr>
<td>6.3.2.6</td>
<td>Digital Subscriber Lines</td>
<td>304</td>
</tr>
<tr>
<td>6.3.2.7</td>
<td>Optical Networking</td>
<td>305</td>
</tr>
<tr>
<td>6.3.2.8</td>
<td>Security in Data Link Layer Protocols</td>
<td>310</td>
</tr>
<tr>
<td>6.3.3</td>
<td>Layer 3—Internetworking Layer Protocols</td>
<td>310</td>
</tr>
<tr>
<td>6.3.3.1</td>
<td>Address Resolution Protocol</td>
<td>310</td>
</tr>
<tr>
<td>6.3.3.2</td>
<td>IP Version 4</td>
<td>320</td>
</tr>
<tr>
<td>6.3.3.3</td>
<td>Internet Control Management Protocol</td>
<td>325</td>
</tr>
<tr>
<td>6.3.3.4</td>
<td>IPv4 Fragmentation and Related Attacks</td>
<td>327</td>
</tr>
<tr>
<td>6.3.3.5</td>
<td>IP Version 6</td>
<td>329</td>
</tr>
<tr>
<td>6.3.3.6</td>
<td>Security in Internetworking Layer Protocols</td>
<td>332</td>
</tr>
<tr>
<td>6.3.4</td>
<td>Layer 4—Transport</td>
<td>332</td>
</tr>
<tr>
<td>6.3.4.1</td>
<td>Transmission Control Protocol</td>
<td>334</td>
</tr>
<tr>
<td>6.3.4.2</td>
<td>User Datagram Protocol</td>
<td>338</td>
</tr>
<tr>
<td>6.3.4.3</td>
<td>Stream Control Transmission Protocol</td>
<td>339</td>
</tr>
<tr>
<td>6.3.4.4</td>
<td>Open Shortest Path First</td>
<td>340</td>
</tr>
<tr>
<td>6.3.4.5</td>
<td>Security in Transport Layer Protocols</td>
<td>342</td>
</tr>
<tr>
<td>6.3.5</td>
<td>Layer 5—User Application Protocols</td>
<td>342</td>
</tr>
<tr>
<td>6.3.5.1</td>
<td>Initial Internet User Application Protocols</td>
<td>344</td>
</tr>
<tr>
<td>6.3.5.2</td>
<td>HyperText Transfer Protocol</td>
<td>344</td>
</tr>
<tr>
<td>6.3.5.3</td>
<td>X Windows</td>
<td>346</td>
</tr>
<tr>
<td>6.3.5.4</td>
<td>eXtensible Markup Language</td>
<td>348</td>
</tr>
<tr>
<td>6.3.5.5</td>
<td>Security in User Application Protocols</td>
<td>349</td>
</tr>
<tr>
<td>6.3.6</td>
<td>Layer 5—Signaling and Control Application Protocols</td>
<td>349</td>
</tr>
<tr>
<td>6.3.6.1</td>
<td>MPLS Signaling Protocols</td>
<td>351</td>
</tr>
<tr>
<td>6.3.6.2</td>
<td>Border Gateway Protocol</td>
<td>352</td>
</tr>
</tbody>
</table>
7.6 Converged Network Management (TMN and eTOM) 393
7.7 General Network Security Architectures 401
  7.7.1 The ITU-T X.800 Generic Architecture 402
  7.7.2 The Security Frameworks (X.810–X.816) 402
  7.7.3 The ITU-T X.805 Approach to Security 403
7.8 Chapter Summary 405
7.9 Further Reading and Resources 405

8 GENERAL COMPUTER SECURITY ARCHITECTURE 409

8.1 The Hardware Protects the Software 410
  8.1.1 Processor States and Status 411
    8.1.1.1 Protection on the Motorola 68000 411
    8.1.1.2 Protection on the Intel 80386/80486 412
  8.1.2 Memory Management 412
    8.1.2.1 Fence 413
    8.1.2.2 Relocation 413
    8.1.2.3 Base/Bounds Registers 414
    8.1.2.4 Segmentation 416
    8.1.2.5 Paging 418
    8.1.2.6 Combining Segmentation and Paging (Virtual Memory) 419
  8.1.3 Interruption of Processor Activity 420
  8.1.4 Hardware Encryption 421
    8.1.4.1 Hardware Security Modules 421
    8.1.4.2 Hardware Acceleration Cards 422
    8.1.4.3 Hardware Acceleration USB Devices 422
    8.1.4.4 Smartcards 423

8.2 The Software Protects Information 424
8.3 Element Security Architecture Description 426
  8.3.1 The Kernel 429
  8.3.2 Security Contexts 430
  8.3.3 Security-Critical Functions 432
    8.3.3.1 Security Policy Decision Function (SPDF) 432
    8.3.3.2 Authentication Function 433
    8.3.3.3 Audit Function 433
    8.3.3.4 Process Scheduling Function 434
8.3.5 Device Management Functions and Device Controllers

8.3.6 Security-Related Functions

8.4 Operating System (OS) Structure

8.4.1 Security Management Function

8.4.2 Networking Subsystem Function

8.5 Security Mechanisms for Deployed Operating Systems (OSs)

8.5.1 General Purpose (GP) OSs

8.5.1.1 Hardware Mechanisms for GP OS Usage

8.5.1.2 Software Functional Entities for General Purpose (GP) OS Contexts

8.5.2 Minimized General Purpose Operating Systems

8.5.2.1 Hardware Mechanisms for Minimized GP OS Usage

8.5.2.2 Software Mechanisms for Minimized GP OS Usage

8.5.3 Embedded (“Real-Time”) Operating Systems

8.5.3.1 Hardware Mechanisms for Embedded OS Usage

8.5.3.2 Software Mechanisms for Embedded OS Usage

8.5.4 Basic Input–Output Systems (BIOS)

8.5.4.1 Hardware Mechanisms for BIOS Usage

8.5.4.2 Software Mechanisms for BIOS Usage

8.6 Chapter Summary

8.7 Further Reading and Resources

9 COMPUTER SOFTWARE SECURITY

9.1 Specific Operating Systems (OSs)

9.1.1 Unix and Linux Security

9.1.1.1 Login and User Accounts

9.1.1.2 Group Accounts

9.1.1.3 Set User ID (setuid) and Set Group ID (setgid)

9.1.1.4 Access Control

9.1.1.5 Audit Logs and Intrusion Detection

9.1.1.6 inetd and TCP Wrappers

9.1.1.7 Log Files and Unix Disk Partitions

9.1.2 Solaris Operating System and Role-Based Access Controls

9.1.3 Windows OSs
10 SECURITY SYSTEMS DESIGN—DESIGNING NETWORK SECURITY 517

10.1 Introduction 517
10.2 Security Design for Protocol Layer 1 520
   10.2.1 Wired and Optical Media 520
      10.2.1.1 Link-Bulk Encryption 520
      10.2.1.2 Dial-back Modems 522
   10.2.2 Wireless Media 522
      10.2.2.1 Fast Frequency Hopping 523
10.3 Layer 2—Data Link Security Mechanisms 524
   10.3.1 IEEE 802.1x 524
   10.3.2 IEEE 802.1ae 525
   10.3.3 IEEE 802.11 WPA and 802.11i 528
10.4 Security Design for Protocol Layer 3 530
   10.4.1 IP Security (IPsec) 530
      10.4.1.1 IPsec Architecture 531
      10.4.1.2 IPsec Key Management and Key Exchange 536
      10.4.1.3 IKE Operation 537
      10.4.1.4 IPsec Security Associations (SAs) 541
      10.4.1.5 Combining Security Associations 542
      10.4.1.6 IPsec Authentication Header (AH) Transform 544
      10.4.1.7 The IPsec Encapsulating Security Payload (ESP) Transform 545
      10.4.1.8 The Various ESP Transforms 545
      10.4.1.9 IPsec Processing 545
      10.4.1.10 IPsec Policy Management 547
      10.4.1.11 IPsec and Network Address Translation 549
      10.4.1.12 IPsec Implementation Availability 554
      10.4.1.13 IPsec and Fault-Tolerant Network Designs 554
      10.4.1.14 IPsec and PKI 556
      10.4.1.15 IPsec Summary and Observations 557
10.5 IP Packet Authorization and Access Control 558
   10.5.1 Network and Host Packet Filtering 559
   10.5.2 The Demilitarized Zone 563
   10.5.3 Application-Level Gateways 564
   10.5.4 Deep-Packet Inspection (DPI) 567
10.6 Chapter Summary 571
10.7 Further Reading and Resources 571
11 TRANSPORT AND APPLICATION SECURITY DESIGN AND USE  573

11.1 Layer 4—Transport Security Protocols  573
   11.1.1 TLS, DTLS, and SSL  574
      11.1.1.1 TLS Session Establishment  576
      11.1.1.2 TLS Operational Activities  579
      11.1.1.3 TLS and SSL Security Items  579
      11.1.1.4 SSL Virtual Private Networks  579
   11.1.2 Secure Shell (SSH)  581
   11.1.3 Comparison of SSL, TLS, DTLS, and IPsec  581

11.2 Layer 5—User Service Application Protocols  582
   11.2.1 Email  583
      11.2.1.1 Pretty Good Privacy (PGP)  583
      11.2.1.2 Secure/Multipurpose Internet Mail Extensions (S/MIME)  586
      11.2.1.3 S/MIME and OpenPGP Differences  587
      11.2.1.4 Email Attacks  587
   11.2.2 World Wide Web (Web) and Identity Management  589
      11.2.2.1 eXtensible Markup Language Security (XML)  589
      11.2.2.2 Service-Oriented Architecture (SOA)  590
      11.2.2.3 Web Services  593
      11.2.2.4 SOAP  593
      11.2.2.5 Security Assertion Markup Language (SAML)  594
   11.2.3 Voice over Internet Protocol (VoIP)  596
      11.2.3.1 VoIP Signaling Security  599
      11.2.3.2 Real-Time Protocol  599
      11.2.3.3 VoIP Media Security  601
      11.2.3.4 VoIP Session Border Control  602
      11.2.3.5 VoIP Device Security  602
      11.2.3.6 VoIP and NAT  604
   11.2.4 DNS Security Extensions  605
   11.2.5 Instant Messaging and Chat  608
   11.2.6 Peer-to-Peer Applications  615
   11.2.7 Ad hoc Networks  616
   11.2.8 Java  618
      11.2.8.1 Basic Concepts  619
      11.2.8.2 Java 2 Cryptographic Architecture  620
   11.2.9 .NET  622
12 SECURING MANAGEMENT AND MANAGING SECURITY 633

12.1 Securing Management Applications 633
  12.1.1 Management Roots 633
  12.1.2 The Telecommunications Management Network 634
    12.1.2.1 Telecommunications Management Network Structure 635
    12.1.2.2 Element, Network Management Systems, and Operations Systems 636
  12.1.3 TMN Security 640
  12.1.4 Management of Security Mechanisms 642
    12.1.4.1 EMS Security Needs 643
    12.1.4.2 NMS Security Additions 644
    12.1.4.3 Selected OSS/EMS Security Services 644
  12.1.5 A Security Management Framework 645

12.2 Operation, Administration, Maintenance, and Decommissioning 648
  12.2.1 Operational Security Mechanisms 649
    12.2.1.1 Separation of Duties and Roles 649
    12.2.1.2 Operational Guidelines and Procedures 650
    12.2.1.3 Independent Auditing and Review 651
    12.2.1.4 Human Resources and Legal Aspects 653
    12.2.1.5 Accountability 653
    12.2.1.6 Documentation 653
    12.2.1.7 Acceptance Testing, Field Testing, and Operational Readiness 653
  12.2.2 Operations Security 654
    12.2.2.1 Third-Party Access 655
    12.2.2.2 Security Event Response and Forensics 655