Contents

Foreword xxi
Introduction xxvii
Assessment Test xlv

Chapter 1 Cryptographic Tools and Techniques 1

The History of Cryptography 2
Cryptographic Services 3
Cryptographic Goals 3
Cryptographic Terms 4
Cipher Types and Methods 6
Symmetric Encryption 8
Data Encryption Standard 10
Triple-DES 11
Advanced Encryption Standard 12
International Data Encryption Algorithm 12
Rivest Cipher Algorithms 13
Asymmetric Encryption 13
Diffie–Hellman 14
RSA 15
Elliptic Curve Cryptography 16
El Gamal 16
Merkle–Hellman Knapsack 16
Hybrid Encryption 16
Hashing 17
Hashing and Message Digests 17
MD Series 19
SHA 19
HAVAL 19
Message Authentication Code 20
HMAC 20
Digital Signatures 20
Public Key Infrastructure 22
Certificate Authority 22
Registration Authority 23
Certificate Revocation List 23
Digital Certificates 24
Certificate Distribution 26
The Client’s Role in PKI 26
Cryptographic Solutions 27
Application Layer Encryption 27
Transport Layer Encryption 28
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>2 Comprehensive Security Solutions</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Internet Layer Controls</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Physical Layer Controls</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Cryptographic Attacks</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Exam Essentials</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Review Questions</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Advanced Network Design</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Remote Access</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Placement of Security Devices</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>SCADA</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>VoIP</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>TCP/IP</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Network Interface Layer</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Internet Layer</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Transport Layer</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Application Layer</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Secure Communication Solutions</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Secure Facility Solutions</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>Building Layouts</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>Facilities Management</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>Secure Network Infrastructure Design</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>Router Configuration</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>Enterprise Service Bus</td>
<td>69</td>
</tr>
<tr>
<td></td>
<td>Web Services Security</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>Exam Essentials</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>Review Questions</td>
<td>73</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter</th>
<th>3 Securing Virtualized, Distributed, and Shared Computing</th>
<th>77</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enterprise Security</td>
<td>79</td>
</tr>
<tr>
<td></td>
<td>Cloud Computing</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>Cloud Computing Models</td>
<td>82</td>
</tr>
<tr>
<td></td>
<td>Cloud Computing Providers</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>Benefits of Cloud Computing</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>Security of Cloud Computing</td>
<td>86</td>
</tr>
<tr>
<td></td>
<td>Cloud Computing Vulnerabilities</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>Virtualization</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>Virtualized Servers</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>Virtual LANs</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Enterprise Storage</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>103</td>
</tr>
</tbody>
</table>
Exam Essentials 103
Review Questions 105

Chapter 4 Host Security 109
Firewalls and Access Control Lists 110
Host-Based Firewalls 114
Trusted Operating System 117
Endpoint Security Software 121
Anti-malware 124
  Antivirus 124
  Anti-spyware 126
  Spam Filters 128
Host Hardening 129
Asset Management 133
Data Exfiltration 134
Intrusion Detection and Prevention 135
Summary 139
Exam Essentials 139
Review Questions 141

Chapter 5 Application Security and Penetration Testing 145
Application Security 147
Specific Application Issues 149
  Cross-Site Scripting 150
  Clickjacking 151
  Session Management 151
  Input Validation 152
  SQL Injection 153
Application Sandboxing 154
Application Security Framework 154
Standard Libraries 155
Secure Coding Standards 156
Application Exploits 157
Escalation of Privilege 158
Improper Storage of Sensitive Data 159
Cookie Storage and Transmission 159
Process Handling at the Client and Server 160
  Ajax 161
  JavaScript 161
  Buffer Overflow 162
  Memory Leaks 163
  Integer Overflow 163
  Race Conditions (TOC/TOU) 163
  Resource Exhaustion 164
Security Assessments and Penetration Testing 165  
Test Methods 166  
Penetration Testing Steps 166  
Assessment Types 167  
Assessment Areas 168  
Security Assessment and Penetration Test Tools 170  
Summary 182  
Exam Essentials 182  
Review Questions 184

### Chapter 6 Risk Management 189

- Risk Terminology 191  
- Identifying Vulnerabilities 192  
- Operational Risks 195  
  - Risk in Business Models 195  
  - Risk in External and Internal Influences 201  
  - Risks with Data 204  
- The Risk Assessment Process 210  
  - Asset Identification 210  
  - Information Classification 212  
  - Risk Assessment 213  
  - Risk Analysis Options 217  
  - Implementing Controls 218  
  - Continuous Monitoring 219  
- Enterprise Security Architecture Frameworks 220  
- Best Practices for Risk Assessments 220  
- Summary 221  
- Exam Essentials 222  
- Review Questions 224

### Chapter 7 Policies, Procedures, and Incident Response 229

- A High-Level View of Documentation 231  
  - The Policy Development Process 232  
  - Policies and Procedures 233  
- Business Documents Used to Support Security 237  
- Documents and Controls Used for Sensitive Information 239  
  - Why Security? 240  
  - Personally Identifiable Information Controls 240  
  - Data Breach 242  
  - Policies Used to Manage Employees 243  
- Auditing Requirements and Frequency 247  
- The Incident Response Framework 248  
- Digital Forensics 250  
- The Role of Training and Employee Awareness 254
Chapter 8 Security Research and Analysis

Analyzing Industry Trends and Outlining Potential Impact 266
Performing Ongoing Research 266
Best Practices 270
New Technologies 273
Situational Awareness 281
Research Security Implications of New Business Tools 290
Global IA Industry Community 293
Research Security Requirements for Contracts 296
Carrying Out Relevant Analysis to Secure the Enterprise 298
Benchmarking 298
Prototyping and Testing Multiple Solutions 298
Cost-Benefit Analysis 299
Analyzing and Interpreting Trend Data to Anticipate Cyber Defense Aids 299
Reviewing Effectiveness of Existing Security 299
Reverse Engineering or Deconstructing Existing Solutions 301
Analyzing Security Solutions to Ensure They Meet Business Needs 301
Conducting a Lessons Learned/After-Action Review 302
Using Judgment to Solve Difficult Problems 303
Conducting Network Traffic Analysis 303
Summary 304
Exam Essentials 305
Review Questions 306

Chapter 9 Enterprise Security Integration

Integrate Enterprise Disciplines to Achieve Secure Solutions 313
The Role of Governance in Achieving Enterprise Security 315
Interpreting Security Requirements and Goals to Communicate with Other Disciplines 317
Guidance to Management 320
Establish Effective Collaboration within Teams to Implement Secure Solutions 322
Disciplines 325
Explain the Security Impact of Interorganizational Change 328
Security Concerns of Interconnecting Multiple Industries 330
Design Considerations During Mergers, Acquisitions, and De-mergers 331
## Contents

- Assuring Third-Party Products Only Introduce Acceptable Risk 332
- Network Secure Segmentation and Delegation 334
- Integration of Products and Services 336
- Summary 337
- Exam Essentials 338
- Review Questions 339

### Chapter 10 Security Controls for Communication and Collaboration 343

- Selecting and Distinguishing the Appropriate Security Controls 345
  - Unified Communication Security 345
  - VoIP Security 354
  - VoIP Implementation 356
  - Remote Access 357
  - Enterprise Configuration Management of Mobile Devices 358
  - Secure External Communications 359
  - Secure Implementation of Collaboration Platforms 360
  - Prioritizing Traffic with QoS 362
  - Mobile Devices 363
- Advanced Authentication Tools, Techniques, and Concepts 365
  - Federated Identity Management 365
  - XACML 366
  - SOAP 366
  - SSO 367
  - Service Provisioning Markup Language 368
  - Certificate-Based Authentication 369
- Carrying Out Security Activities across the Technology Life Cycle 370
  - End-to-End Solution Ownership 370
  - Understanding the Results of Solutions in Advance 371
  - Systems Development Life Cycle 373
  - Addressing Emerging Threats and Security Trends 375
  - Validating System Designs 376
- Summary 378
- Exam Essentials 378
- Review Questions 380

### Appendix A CASP Lab Manual 385

- What You’ll Need 386
- Lab A1: Download, Verify, and Install a Virtual Environment 389
- Lab A2: Explore Your Virtual Network 392
- Lab A3: Port Scanning 396
Contents xvii

Lab A4: Introduction to a Protocol Analyzer 400
Lab A5: Web Vulnerabilities 406
Lab A6: Introduction to the Nessus Vulnerability Scanner 408
Lab A7: Verify a Baseline Security Configuration 411
Lab A8: Basic Introduction to Windows Forensic Tools 413
Lab A9: Introduction to Helix 421
Lab A10: Introduction to Hashing 425
Lab A11: File Encryption 428
Lab A12: Cracking Encrypted Files 429
Lab A13: Intrusion Detection 431
Lab A14: An Introduction to Signature-Based Scanning 433
Lab A15: Rootkit Detection 437
Lab A16: Threat Modeling 440
Lab A17: Introduction to the Metasploit Framework 442
Lab A18: Social Engineering 445
Lab A19: Routing, Switching, and Security 449
Lab A20: Further Exploration 460

Appendix B Answers to Review Questions 463

Chapter 1: Cryptographic Tools and Techniques 464
Chapter 2: Comprehensive Security Solutions 465
Chapter 3: Securing Virtualized, Distributed, and Shared Computing 466
Chapter 4: Host Security 467
Chapter 5: Application Security and Penetration Testing 468
Chapter 6: Risk Management 469
Chapter 7: Policies, Procedures, and Incident Response 471
Chapter 8: Security Research and Analysis 472
Chapter 9: Enterprise Security Integration 473
Chapter 10: Security Controls for Communication and Collaboration 474

Appendix C About the Additional Study Tools 475

Additional Study Tools 476
Sybex Test Engine 476
Electronic Flashcards 476
PDF of Glossary of Terms 476
Adobe Reader 476
System Requirements 477
Using the Study Tools 477
Troubleshooting 477
Customer Care 478

Index 479