Contents

Foreword

Introduction

Assessment Test

Chapter 1 WLAN Security Overview

WLAN Security Overview 1

Chapter 2 Legacy 802.11 Security

Legacy 802.11 Security 29
Summary 54
Exam Essentials 55
Review Questions 56

Chapter 3 Encryption Ciphers and Methods 61
Encryption Basics 62
- Symmetric and Asymmetric Algorithms 63
Stream and Block Ciphers 65
- RC4/ARC4 66
- RC5 66
- DES 66
- 3DES 67
- AES 67
WLAN Encryption Methods 68
- WEP 70
  - WEP MPDU 70
- TKIP 72
  - TKIP MPDU 72
- CCMP 73
  - CCMP MPDU 76
- WPA/WPA2 78
Future Encryption Methods 79
Proprietary Layer 2 Implementations 80
Summary 80
Exam Essentials 81
Review Questions 82

Chapter 4 802.1X/EAP Authentication 87
WLAN Authentication Overview 89
AAA 90
- Authentication 91
- Authorization 92
- Accounting 93
802.1X 95
- Supplicant 96
- Authenticator 99
- Authentication Server 102
Supplicant Credentials 106
- Usernames and Passwords 106
- Digital Certificates 107
- Protected Access Credentials (PACs) 109
- One-Time Passwords 109
- Smart Cards and USB Tokens 110
- Machine Authentication 112
802.1X/EAP and Certificates
  Server Certificates and Root CA Certificates 115
  Client Certificates 119
Shared Secret 120
Legacy Authentication Protocols
  PAP 121
  CHAP 121
  MS-CHAP 121
  MS-CHAPv2 121
EAP 122
  Weak EAP Protocols 125
  EAP-MD5 125
  EAP-LEAP 126
  Strong EAP Protocols 128
  EAP-PEAP 130
  EAP-TTLS 133
  EAP-TLS 134
  EAP-FAST 136
  Miscellaneous EAP Protocols 141
  EAP-SIM 141
  EAP-AKA 141
  EAP-TEAP 142
Summary 144
Exam Essentials 144
Review Questions 146

Chapter 5  802.11 Layer 2 Dynamic Encryption
Key Generation 151
Advantages of Dynamic Encryption 152
Robust Security Network (RSN) 156
  RSN Information Element 161
  Authentication and Key Management (AKM) 166
  RSNA Key Hierarchy 170
  4-Way Handshake 174
  Group Key Handshake 177
  PeerKey Handshake 179
  TDLS Peer Key Handshake 180
  RSNA Security Associations 181
  Passphrase-to-PSK Mapping 182
  Roaming and Dynamic Keys 183
Summary 184
Exam Essentials 184
Review Questions 186
Contents

Chapter 6  PSK Authentication  193
WPA/WPA2-Personal  194
  Preshared Keys (PSK) and Passphrases  195
  WPA/WPA2-Personal Risks  200
  Entropy  201
  Proprietary PSK  203
  Simultaneous Authentication of Equals (SAE)  205
Summary  208
Exam Essentials  208
Review Questions  209

Chapter 7  802.11 Fast Secure Roaming  215
History of 802.11 Roaming  216
  Client Roaming Thresholds  217
  AP-to-AP Handoff  218
RSNA  220
  PMKSA  221
  PMK Caching  224
  Preauthentication  225
Opportunistic Key Caching (OKC)  227
Proprietary FSR  230
Fast BSS Transition (FT)  231
  Information Elements  235
  FT Initial Mobility Domain Association  236
  Over-the-Air Fast BSS Transition  238
  Over-the-DS Fast BSS Transition  239
802.11k  243
802.11v  246
Voice Enterprise  247
Layer 3 Roaming  248
Troubleshooting  250
Summary  251
Exam Essentials  251
Review Questions  253

Chapter 8  WLAN Security Infrastructure  257
802.11 Services  258
  Integration Service (IS)  258
  Distribution System (DS)  259
Management, Control, and Data Planes  259
  Management Plane  260
  Control Plane  260
  Data Plane  261
WLAN Architecture .......................... 261
Autonomous WLAN Architecture .... 261
Centralized Network Management Systems .... 263
Cloud Networking .......................... 265
Centralized WLAN Architecture .... 265
Distributed WLAN Architecture .... 270
Unified WLAN Architecture .... 272
Hybrid Architectures ...................... 272
Enterprise WLAN Routers .......... 272
WLAN Mesh Access Points ........... 273
WLAN Bridging ........................ 274

VPN Wireless Security ................. 275
VPN 101 .................................. 275
Layer 3 VPNs ............................. 277
SSL VPN .................................. 278
VPN Deployment .......................... 278
Infrastructure Management ........... 279
Protocols for Management .......... 280
Summary .................................. 285
Exam Essentials .......................... 285
Review Questions ........................ 286

Chapter 9 RADIUS and LDAP .... 291

LDAP ....................................... 292
RADIUS ................................... 293
Authentication and Authorization .... 294
Accounting .................................. 295
RADIUS Configuration .................. 296
LDAP Proxy .................................. 298
RADIUS Deployment Models ........ 299
RADIUS Proxy ............................. 303
RADIUS Proxy and Realms .......... 304
RADIUS Failover ......................... 305
WLAN Devices as RADIUS Servers ... 306
Captive Web Portal and MAC Authentication ... 306
RadSec .................................... 307
Attribute-Value Pairs ................. 307
Vendor-Specific Attributes .......... 308
VLAN Assignment ...................... 309
Role-Based Access Control .......... 310
LDAP Attributes ......................... 311
Summary .................................. 311
Exam Essentials .......................... 311
Review Questions ........................ 313
# Chapter 10 Bring Your Own Device (BYOD) and Guest Access

Mobile Device Management 322
- Company-Issued Devices vs. Personal Devices 323
- MDM Architecture 324
- MDM Enrollment 325
- MDM Profiles 329
- MDM Agent Software 331
- Over-the-Air Management 332
- Application Management 335

Self-Service Device Onboarding for Employees 336
- Dual-SSID Onboarding 337
- Single-SSID Onboarding 338
- MDM vs. Self-Service Onboarding 339

Guest WLAN Access 339
- Guest SSID 340
- Guest VLAN 340
- Guest Firewall Policy 341
- Captive Web Portals 342
- Client Isolation, Rate Limiting, and Web Content Filtering 345
- Guest Management 345
- Guest Self-Registration 347
- Employee Sponsorship 348
- Social Login 349
- Encrypted Guest Access 351

Network Access Control (NAC) 352
- Posture 352
- OS Fingerprinting 353
- AAA 354
- RADIUS Change of Authorization 355
- Single Sign-On 356

Summary 358

Exam Essentials 359

Review Questions 360

# Chapter 11 Wireless Security Troubleshooting

Five Tenets of WLAN Troubleshooting 366
- Troubleshooting Best Practices 366
- Troubleshoot the OSI Model 369
- Most Wi-Fi Problems Are Client Issues 370
- Proper WLAN Design Reduces Problems 372
- WLAN Always Gets the Blame 372
- PSK Troubleshooting 372
Chapter 12 Wireless Security Risks

Unauthorized Rogue Access 398
  Rogue Devices 398
  Rogue Prevention 402
Eavesdropping 404
  Casual Eavesdropping 404
  Malicious Eavesdropping 406
  Eavesdropping Risks 407
  Eavesdropping Prevention 409
  Authentication Attacks 409
Denial-of-Service Attacks 411
  Layer 1 DoS Attacks 412
  Layer 2 DoS Attacks 416
  MAC Spoofing 420
  Wireless Hijacking 423
  Management Interface Exploits 427
  Vendor Proprietary Attacks 428
  Physical Damage and Theft 428
  Social Engineering 430
Guest Access and WLAN Hotspots 432
Summary 433
Exam Essentials 433
Review Questions 434

Chapter 13 Wireless LAN Security Auditing 439

WLAN Security Audit 440
  OSI Layer 1 Audit 442
  OSI Layer 2 Audit 447
  Penetration Testing 449
  Wired Infrastructure Audit 453
  Social Engineering Audit 453
Chapter 14  Wireless Security Monitoring 469

Wireless Intrusion Detection and Prevention Systems (WIDS and WIPS) 470
  WIDS/WIPS Infrastructure Components 471
  WIDS/WIPS Architecture Models 474
  Multiple Radio Sensors 478
  Sensor Placement 479
Proprietary WIPS 480
Device Classification 482
  Rogue Detection 484
  Rogue Mitigation 488
  Device Tracking 491
WIDS/WIPS Analysis 496
  Signature Analysis 496
  Behavioral Analysis 497
  Protocol Analysis 498
  Spectrum Analysis 500
  Forensic Analysis 501
  Performance Analysis 502
Monitoring 503
  Policy Enforcement 503
  Alarms and Notification 505
  False Positives 507
  Reports 508
802.11n/ac 508
802.11w 510
Summary 511
Exam Essentials 511
Review Questions 513

Chapter 15  Wireless Security Policies 517

General Policy 519
  Policy Creation 519
  Policy Management 522
Functional Policy 523
  Password Policy 524
  RBAC Policy 525
<table>
<thead>
<tr>
<th>Contents</th>
<th>xxi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Control Policy</td>
<td>526</td>
</tr>
<tr>
<td>Authentication and Encryption Policy</td>
<td>526</td>
</tr>
<tr>
<td>WLAN Monitoring Policy</td>
<td>527</td>
</tr>
<tr>
<td>Endpoint Policy</td>
<td>527</td>
</tr>
<tr>
<td>Acceptable Use Policy</td>
<td>528</td>
</tr>
<tr>
<td>Physical Security</td>
<td>529</td>
</tr>
<tr>
<td>Remote Office Policy</td>
<td>529</td>
</tr>
<tr>
<td>Government and Industry Regulations</td>
<td>530</td>
</tr>
<tr>
<td>The U.S. Department of Defense (DoD) Directive 8420.1</td>
<td>531</td>
</tr>
<tr>
<td>Federal Information Processing Standards (FIPS) 140-2</td>
<td>532</td>
</tr>
<tr>
<td>The Sarbanes-Oxley Act of 2002 (SOX)</td>
<td>534</td>
</tr>
<tr>
<td>Graham-Leach-Bliley Act (GLBA)</td>
<td>536</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>538</td>
</tr>
<tr>
<td>Payment Card Industry (PCI) Standard</td>
<td>540</td>
</tr>
<tr>
<td>Compliance Reports</td>
<td>543</td>
</tr>
<tr>
<td>802.11 WLAN Policy Recommendations</td>
<td>544</td>
</tr>
<tr>
<td>Summary</td>
<td>545</td>
</tr>
<tr>
<td>Exam Essentials</td>
<td>545</td>
</tr>
<tr>
<td>Review Questions</td>
<td>547</td>
</tr>
</tbody>
</table>

**Appendix A  Answers to Review Questions**  553

Chapter 1: WLAN Security Overview  554
Chapter 2: Legacy 802.11 Security  556
Chapter 3: Encryption Ciphers and Methods  558
Chapter 4: 802.1X/EAP Authentication  561
Chapter 5: 802.11 Layer 2 Dynamic Encryption Key Generation  563
Chapter 6: PSK Authentication  567
Chapter 7: 802.11 Fast Secure Roaming  570
Chapter 8: WLAN Security Infrastructure  573
Chapter 9: RADIUS and LDAP  576
Chapter 10: Bring Your Own Device (BYOD) and Guest Access  578
Chapter 11: Wireless Security Troubleshooting  581
Chapter 12: Wireless Security Risks  584
Chapter 13: Wireless LAN Security Auditing  587
Chapter 14: Wireless Security Monitoring  590
Chapter 15: Wireless Security Policies  594

**Appendix B  Abbreviations and Acronyms**  597

Certifications  598
Organizations and Regulations  598
Measurements  599
Technical Terms  599

Index  615
# Table of Exercises

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exercise 2.1</td>
<td>Viewing Open System and Shared Key Authentication Frames</td>
<td>34</td>
</tr>
<tr>
<td>Exercise 2.2</td>
<td>Viewing Encrypted MSDU Payload of 802.11 Data Frames</td>
<td>39</td>
</tr>
<tr>
<td>Exercise 2.3</td>
<td>TKIP-Encrypted Frames</td>
<td>44</td>
</tr>
<tr>
<td>Exercise 2.4</td>
<td>Viewing Hidden SSIDs</td>
<td>53</td>
</tr>
<tr>
<td>Exercise 3.1</td>
<td>CCMP Encrypted Frames</td>
<td>77</td>
</tr>
<tr>
<td>Exercise 4.1</td>
<td>802.1X/EAP Frame Exchanges</td>
<td>142</td>
</tr>
<tr>
<td>Exercise 5.1</td>
<td>Dynamic WEP</td>
<td>155</td>
</tr>
<tr>
<td>Exercise 5.2</td>
<td>Authentication and Key Management</td>
<td>170</td>
</tr>
<tr>
<td>Exercise 5.3</td>
<td>The 4-Way Handshake</td>
<td>177</td>
</tr>
<tr>
<td>Exercise 6.1</td>
<td>Passphrase-PSK Mapping</td>
<td>198</td>
</tr>
<tr>
<td>Exercise 7.1</td>
<td>FT Initial Mobility Domain Association</td>
<td>237</td>
</tr>
<tr>
<td>Exercise 7.2</td>
<td>Over-the-Air Fast BSS Transition</td>
<td>240</td>
</tr>
<tr>
<td>Exercise 7.3</td>
<td>Radio Resource Management and Neighbor Reports</td>
<td>245</td>
</tr>
</tbody>
</table>