Wireless Security Architecture

Preface

Part I Technical Foundations

Chapter 1 Introduction to Concepts and Relationships

Roles and Responsibilities

- Network and Wireless Architects
- Security, Risk, and Compliance Roles
- Risk and Compliance Roles
- Chief Information Security Officer Roles
- Security Operations and Analyst Roles
- Identity and Access Management Roles
- Operations and Help Desk Roles
- Network Operations Teams
- Help Desk and End-User Support Roles
- External and Third Parties
  - Technology Manufacturers and Integrators
  - Vendor Management and Supply Chain Security Considerations

Security Concepts for Wireless Architecture

- Security and IAC Triad in Wireless
- Integrity in Secure Wireless Architecture
- Availability in Secure Wireless Architecture
- Confidentiality in Secure Wireless Architecture
- Using the IAC Triad to Your Advantage

Aligning Wireless Architecture Security to

Organizational Risk
- Identifying Risk Tolerance
- Factors Influencing Risk Tolerance
- Assigning a Risk Tolerance Level

Link to Amazon
Contents

Control Plane 46
Data Plane 47
Cloud-Managed Wi-Fi and Gateways 48
  Today’s Cloud-Managed Benefits for Enterprise 48
  Architectures with Cloud Management 50
  The Role of Gateway Appliances with Cloud-Managed APs 51
Controller Managed Wi-Fi 52
Local Cluster Managed Wi-Fi 53
Remote APs 55
Summary 55
Understanding Data Paths 56
  Tunneled 58
  Bridged 59
    Considerations of Bridging Client Traffic 59
Hybrid and Other Data Path Models 61
Filtering and Segmentation of Traffic 62
  The Role of ACLs and VLANs in Segmentation 62
  Filtering Traffic within Wireless and Wired Infrastructures 63
  Filtering with Inter-Station Blocking on Wireless 64
  Filtering with SSIDs/VLANs on Wireless 65
  Filtering with ACLs on Wireless 65
  Controlling Guest Portals with DNS on Wireless 66
  Filtering with VLANs on Switches 67
  Filtering with ACLs on Routing Devices 68
  Filtering with Policies on Firewalls 70
  Filtering with Network Virtualization Overlay on Wired Infrastructure 71
Summary 71
Understanding Security Profiles for SSIDs 72
WPA2 and WPA3 Overview 73
  Security Benefits of Protected Management Frames 75
Transition Modes and Migration Strategies for Preserving Security 76
Enterprise Mode (802.1X) 77
  Planning Enterprise (802.1X) Secured SSIDs 77
  Untangling the Enterprise (802.1X) SSID Security Options 79
  Enhancements with WPA3-Enterprise 82
  WPA3-Enterprise 192-bit Mode 82
  Deciphering the Acronyms of 192-bit Mode 83
  WPA2 to WPA3-Enterprise Migration Recommendations 85
Personal Mode (Passphrase with PSK/SAE) 87
  Planning Personal/Passphrase-Secured SSIDs 87
  Enhancements with WPA3-Personal 88
  WPA2 to WPA3-Personal Migration Recommendations 92
Open Authentication Networks 94
## Chapter 3 Understanding Authentication and Authorization

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IEEE 802.1X Standard</td>
<td>102</td>
</tr>
<tr>
<td>Terminology in 802.1X</td>
<td>103</td>
</tr>
<tr>
<td>High-Level 802.1X Process in Wi-Fi Authentication</td>
<td>105</td>
</tr>
<tr>
<td>802.1X as the Iron Gate</td>
<td>106</td>
</tr>
<tr>
<td>RADIUS Servers, RADIUS Attributes, and VSAs</td>
<td>107</td>
</tr>
<tr>
<td>RADIUS Servers</td>
<td>107</td>
</tr>
<tr>
<td>RADIUS Servers and NAC Products</td>
<td>108</td>
</tr>
<tr>
<td>Relationship of RADIUS, EAP, and Infrastructure Devices</td>
<td>110</td>
</tr>
<tr>
<td>RADIUS Attributes</td>
<td>111</td>
</tr>
<tr>
<td>Common RADIUS Attributes</td>
<td>111</td>
</tr>
<tr>
<td>RADIUS Attributes for Dynamic VLANs</td>
<td>113</td>
</tr>
<tr>
<td>RADIUS Vendor-Specific Attributes</td>
<td>115</td>
</tr>
<tr>
<td>RADIUS Policies</td>
<td>116</td>
</tr>
<tr>
<td>RADIUS Servers, Clients and Shared Secrets</td>
<td>118</td>
</tr>
<tr>
<td>Specifying RADIUS Clients</td>
<td>118</td>
</tr>
<tr>
<td>RADIUS Shared Secrets</td>
<td>120</td>
</tr>
<tr>
<td>Other Requirements</td>
<td>121</td>
</tr>
<tr>
<td>User Directories</td>
<td>121</td>
</tr>
<tr>
<td>Server Certificate</td>
<td>121</td>
</tr>
<tr>
<td>Logging/Accounting</td>
<td>122</td>
</tr>
<tr>
<td>Additional Notes on RADIUS Accounting</td>
<td>122</td>
</tr>
<tr>
<td>Change of Authorization and Disconnect Messages</td>
<td>123</td>
</tr>
<tr>
<td>EAP Methods for Authentication</td>
<td>127</td>
</tr>
<tr>
<td>Outer EAP Tunnels</td>
<td>129</td>
</tr>
<tr>
<td>EAP-PEAP</td>
<td>129</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>130</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>130</td>
</tr>
<tr>
<td>EAP-TEAP</td>
<td>131</td>
</tr>
<tr>
<td>Securing Tunneled EAP</td>
<td>132</td>
</tr>
<tr>
<td>Inner Authentication Methods</td>
<td>133</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>134</td>
</tr>
<tr>
<td>EAP-MSCHAPv2</td>
<td>135</td>
</tr>
<tr>
<td>EAP-GTC</td>
<td>135</td>
</tr>
<tr>
<td>EAP-POTP</td>
<td>136</td>
</tr>
<tr>
<td>Legacy and Unsecured EAP Methods</td>
<td>137</td>
</tr>
<tr>
<td>Recommended EAP Methods for Secure Wi-Fi</td>
<td>138</td>
</tr>
<tr>
<td>MAC-Based Authentications</td>
<td>140</td>
</tr>
<tr>
<td>MAC Authentication Bypass with RADIUS</td>
<td>140</td>
</tr>
<tr>
<td>Overview of Typical MAB Operations</td>
<td>142</td>
</tr>
<tr>
<td>Vendor Variations of MAC Operations</td>
<td>142</td>
</tr>
<tr>
<td>Security Considerations for MAB</td>
<td>143</td>
</tr>
</tbody>
</table>
Contents

DNS Services 177
  DNS for Wi-Fi Clients and Captive Portals 177
  DNS for AP Provisioning 179
  DNS Security 179
DHCP Services 180
  DHCP for Wi-Fi Clients 181
  Planning DHCP for Wi-Fi Clients 184
  DHCP for AP Provisioning 185
Certificates 186
Understanding Wi-Fi Design Impacts on Security 187
Roaming Protocols’ Impact on Security 188
  Roaming Impact on Latency-Sensitive Applications 189
  Roaming and Key Exchanges on WPA-Personal Networks 190
  Roaming and Key Exchanges on WPA-Enterprise Networks 191
Fast Roaming Technologies 193
  Fast Reconnect 193
  PMK Caching (Roam-back) 194
  Opportunistic Key Caching 196
  Fast BSS Transition 197
  Summary of Fast Roaming Protocols 198
  Support for Fast Transition and Other Roaming 199
Changes in Roaming Facilitation with WPA3 and Enhanced Open Networks 200
  Recommendations for Fast Roaming in Secure Wi-Fi 201
System Availability and Resiliency 203
  Uptime, High Availability, and Scheduled Downtime 203
  Scheduled Maintenance and Testing 203
  AP Port Uplink Redundancy 204
RF Design Elements 205
  AP Placement, Channel, and Power Settings 205
  Wi-Fi 6E 207
  Rate Limiting Wi-Fi 208
Other Networking, Discovery, and Routing Elements 213
  Discovery Protocols 213
  Loop Protection 216
  Dynamic Routing Protocols 217
  Layer 3 Roaming Mobility Domains 217
Summary 217

Part II Putting It All Together 219

Chapter 5 Planning and Design for Secure Wireless 221
Planning and Design Methodology 222
  Discover Stage 223
    Phase 1: Define 223
    Phase 2: Characterize 224
Architect Stage 224
  Phase 3: Design 225
Iterate Stage 225
  Phase 4: Optimize 226
  Phase 5: Validate 227
Planning and Design Inputs (Define and Characterize) 227
  Scope of Work/Project 228
  Teams Involved 230
    CISO, Risk, or Compliance Officer 231
    Security Analyst or SOC 231
    Identity and Access Management Team 231
    Network Architect and Network Operations Team 232
    Domain Administrators 232
    Help Desk 232
    Other System or Application Owners 232
    Vendors, Integrators, and Other Contractors 233
  Organizational Security Requirements 233
  Current Security Policies 235
Endpoints 236
  Wireless Connection Type 236
  Form Factor 236
  Operating System 236
  Ownership 237
  Management 237
  Location 237
  User-Attached or Not 237
  Roaming Capabilities 238
  Security Capabilities 238
  Quantities 238
  Classification or Group 239
Users 239
System Security Requirements 239
Applications 240
Process Constraints 240
Wireless Management Architecture and Products 241
Planning and Design Outputs (Design, Optimize, and Validate) 241
  Wireless Connectivity Technology 241
  Endpoint Capability Requirements 242
  Wireless Management Model and Products 243
  RF Design and AP Placement 244
  Authentication 244
  Data Paths 245
  Wired Infrastructure Requirements 245
  Domain and Network Services 247
Chapter 6  Hardening the Wireless Infrastructure  281

Hardening the Wireless Infrastructure

Securing Management Access

Enforcing Encrypted Management Protocols

Generating Keys and Certificates for Encrypted Management

Enabling HTTPS vs. HTTP

Enabling SSH vs. Telnet
| Contents |
|------------------|------------------|
| Enabling Secure File Transfers | 291 |
| Enabling SNMPv3 vs. SNMPv2c | 291 |
| Eliminating Default Credentials and Passwords | 293 |
| Changing Default Credentials on Wireless Management | 293 |
| Changing Default Credentials on APs | 295 |
| Removing Default SNMP Strings | 296 |
| Controlling Administrative Access and Authentication | 296 |
| Enabling User-Based Logons | 297 |
| Creating a Management VLAN | 299 |
| Defining Allowed Management Networks | 301 |
| Securing Shared Credentials and Keys | 301 |
| Addressing Privileged Access | 303 |
| Securing Privileged Accounts and Credentials | 303 |
| Privileged Access Management | 305 |
| Privileged Remote Access | 306 |
| Additional Secure Management Considerations | 307 |
| Designing for Integrity of the Infrastructure | 308 |
| Managing Configurations, Change Management, and Backups | 309 |
| Configuration Change Management | 309 |
| Configuration Baselines | 312 |
| Configuration Backups and Rollback Support | 312 |
| Monitoring and Alerting for Unauthorized Changes | 313 |
| Configuring Logging, Reporting, Alerting, and Automated Responses | 313 |
| Verifying Software Integrity for Upgrades and Patches | 314 |
| Verifying Software Integrity | 314 |
| Upgrades and Security Patches | 315 |
| Working with 802.11w Protected Management Frames | 316 |
| Wi-Fi Management Frames | 317 |
| Unprotected Frame Types | 317 |
| Protected Frame Types | 318 |
| Validated vs. Encrypted | 319 |
| WPA3, Transition Modes, and 802.11w | 319 |
| Caveats and Considerations for 802.11w | 320 |
| Provisioning and Securing APs to Manager | 321 |
| Approving or Allowlisting APs | 322 |
| Using Certificates for APs | 324 |
| Enabling Secure Tunnels from APs to Controller or Tunnel Gateway | 324 |
| Addressing Default AP Behavior | 325 |
| Adding Wired Infrastructure Integrity | 325 |
| Authenticating APs to the Edge Switch | 326 |
| Specifying Edge Port VLANs | 329 |
| Planning Physical Security | 331 |
| Securing Access to Network Closets | 331 |
| Securing Access to APs and Edge Ports | 332 |
Locking Front Panel and Console Access on Infrastructure Devices 334
Disabling Unused Protocols 337
Controlling Peer-to-Peer and Bridged Communications 339
A Note on Consumer Products in the Enterprise 339
Blocking Ad-Hoc Networks 341
Blocking Wireless Bridging on Clients 342
Filtering Inter-Station Traffic, Multicast, and mDNS 344
SSID Inter-Station Blocking 344
Peer-Based Zero Configuration Networking 346
Disabling and Filtering Bonjour and mDNS Protocols 347
Disabling and Filtering UPrnP Protocols 350
A Message on mDNS and Zeroconf from a Pen Tester 351
Recommendations for Securing Against Zeroconf Networking 352
Best Practices for Tiered Hardening 353
Additional Security Configurations 354
Security Monitoring, Rogue Detection, and WIPS 355
Considerations for Hiding or Cloaking SSIDs 356
Requiring DHCP for Clients 359
Addressing Client Credential Sharing and Porting 360
Summary 362

Part III Ongoing Maintenance and Beyond 365
Chapter 7 Monitoring and Maintenance of Wireless Networks 367
Security Testing and Assessments of Wireless Networks 367
Security Audits 368
Vulnerability Assessments 370
Internal Vulnerability Assessment 372
External Vulnerability Assessment 373
Security Assessments 373
Penetration Testing 375
Ongoing Monitoring and Testing 376
Security Monitoring and Tools for Wireless 376
Wireless Intrusion Prevention Systems 377
WIDS vs. WIPS vs. Wired IPS 377
Requirements for WIPS 378
Integrated vs. Overlay vs. Dedicated 379
Attacks WIPS Can Detect and Prevent 384
Wireless Rogues and Neighbors 392
WIPS Mitigation and Containment 396
Legal Considerations of Over-the-Air Mitigation 398
Spectrum Analyzers and Special-Purpose Monitoring 400
Recommendations for WIPS 404
Synthetic Testing and Performance Monitoring 405
Security Logging and Analysis 407
Recommendations for Navigating a Remote Workforce 444
Bring Your Own Device 445
Stats on BYOD and Policies 445
Other Models for Ownership, Management, and Use 446
Further Defining BYOD in Your Organization 448
Legal Considerations for BYOD 449
Technical Considerations for Securing BYOD 451
Recommendations for Securing BYOD 452
Zero Trust Strategies 455
The Current State of Zero Trust 455
Zero Trust Language 456
Types of Zero Trust Products 457
Segmentation Enforcement Models 460
Zero Trust Strategy’s Impact on Wireless 462
Internet of Things 463
LAN-based IoT 463
Protocol-Translated IoT 465
Protocol-Routed IoT 465
Enterprise IoT Technologies and Non-802.11 Wireless 465
IoT Considerations 466
Technologies and Protocols by Use Case 467
LAN-based IoT 468
Bluetooth and BLE 470
Smart Building and Home Automation 475
Public Cellular for IoT 477
Private Cellular and Cellular LANs 481
Private WANs 499
Industrial Automation 501
Features and Characteristics Impact on Security 502
Physical Layer and RF Spectrums 503
Coverage 504
Edge IP Protocols 505
Topology and Connectivity 506
Other Considerations for Secure IoT Architecture 507
Final Thoughts from the Book 508

Appendix A Notes on Configuring 802.1X with Microsoft NPS 513
Wi-Fi Infrastructure That Supports Enterprise (802.1X) 513
SSID Security Profiles 513
Endpoints That Support 802.1X/EAP 514
A Way to Configure the Endpoints for the Specified Connectivity 515
An Authentication Server That Supports RADIUS 517

Appendix B Additional Resources 521
IETF RFCs 521
Navigating and Reading RFCs 521
Helpful RFCs and Links 522
## IEEE Standards and Documents

- Navigating and Reading IEEE Standards  
  523
- Helpful Links  
  523
- IEEE 802.11 Standard  
  523

## Wi-Fi Alliance

- Blog, Consulting, and Book Materials  
  524
- Compliance and Mappings  
  525
- NIST SP 800-53 and ISO 27001  
  525
- PCI Data Security Standards  
  528
- Cyber Insurance and Network Security  
  528

## Appendix C  Sample Architectures

### Architectures for Internal Access Networks

- Managed User with Managed Device
  - Security Considerations  
    533
  - High-Security Architecture  
    534
  - Medium-Security Architecture  
    536
  - Low-Security Architecture  
    538
- Headless/Non-User-Based Devices
  - Security Considerations  
    539
  - High-Security Architecture  
    540
  - Medium-Security Architecture  
    542
  - Low-Security Architecture  
    543
- Contractors and Third Parties
  - Security Considerations  
    544
  - High-Security Architecture  
    545
  - Medium-Security Architecture  
    546
  - Low-Security Architecture  
    547
- BYOD/Personal Devices with Internal Access
  - Security Considerations  
    547
  - High-Security Architecture  
    548
  - Medium-Security Architecture  
    548
  - Low-Security Architecture  
    549
- Guidance on WPA2-Enterprise and WPA3-Enterprise  
- Migrating from WPA2-Enterprise to WPA3-Enterprise  
- Supporting WPA2-Enterprise with WPA3-Enterprise  
- Guidance on When to Separate SSIDs  

### Architectures for Guest/Internet-only Networks

- Guest Networks
  - Security Considerations  
    551
  - High-Security Architecture  
    552
  - Medium-Security Architecture  
    552
  - Low-Security Architecture  
    553
- BYOD/Personal Devices with Internet-only Access
  - Security Considerations  
    553
  - High-Security Architecture  
    554
## Contents

- Medium-Security Architecture 555
- Low-Security Architecture 555
- Determining Length of a WPA3-Personal Passphrase 555
- Why Passphrase Length Matters 555
- Considerations for Passphrase Length 556
- Recommendations for Passphrase Lengths 557

## Appendix D Parting Thoughts and Call to Action 559

- The Future of Cellular and Wi-Fi 559
- Cellular Carrier Use of Unlicensed Spectrum 559
- Cellular Neutral Host Networks 560
- MAC Randomization 562
  - The Purpose of MAC Randomization 562
  - How MAC Randomization Works 562
  - The Future of Networking with MAC Randomization 563
  - Security, Industry, and The Great Compromise 564

Index 567