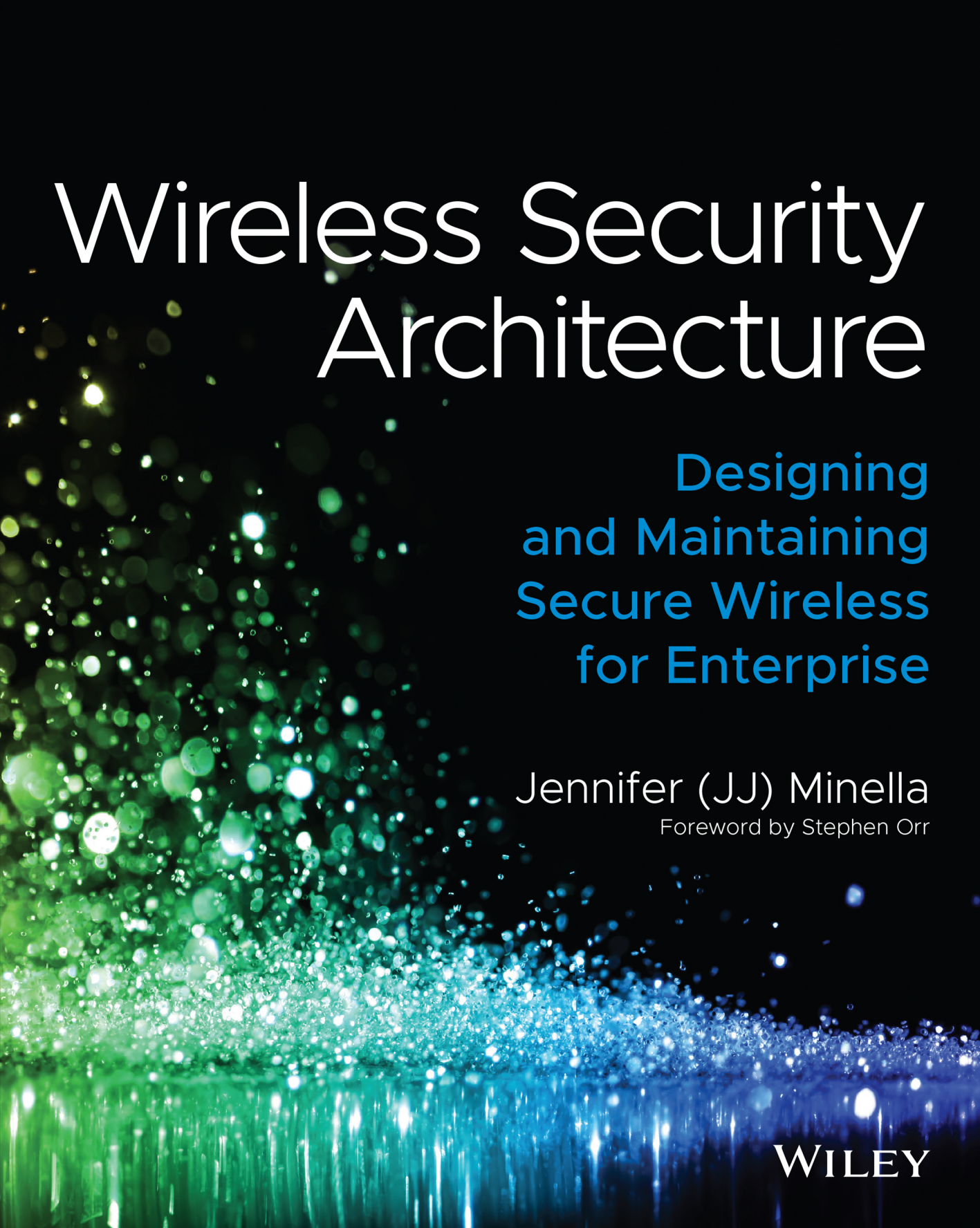
Wireless Security Architecture

Designing and Maintaining Secure Wireless for Enterprise

Jennifer (JJ) Minella
Foreword by Stephen Orr



WILEY

Wireless Security Architecture

Wireless Security Architecture

Designing and Maintaining Secure Wireless for Enterprise

Jennifer (JJ) Minella

WILEY

Copyright © 2022 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada and the United Kingdom.

978-1-119-88305-0
978-1-119-88306-7 (ebk.)
978-1-119-88307-4 (ebk.)

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permission.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware the Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2021952991

Trademarks: WILEY and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Cover images: © Leigh Prather/Adobe Stock Photos
Cover design: Wiley

This book is dedicated to my parents: to my Dad, who taught me to "follow the packet" and to my spunky Mom who we're told was the first woman in the world with a WLAN certification.

—Jennifer Minella

About the Author

Having begun working in the tech industry at the tender age of 14, **Jennifer (JJ) Minella** has spent the last 20 years helping security-conscious organizations solve network security challenges in meaningful ways.

Throughout that time, Jennifer has led strategic research and consulting for hundreds of organizations ranging from government, education, healthcare, and mid-market up to Fortune-5. This book is based on experience accumulated through the thousands of consulting and implementation engagements across these diverse environments. Jennifer holds, or has held, numerous technical certifications over the years ranging from switching and routing to firewalls, remote access, NAC, Wi-Fi, and IoT wireless, along with CISSP and other security certifications.

She's also a published author, internationally recognized speaker on network security and identity, analyst with IANS, member of Forbes Technology Council, and former chairperson of $(ISC)^2$. Combining master-level network architecture skills with CISO and compliance experience, she continues her mission of aligning security and networking as Founder and Principal Advisor of Viszen Security.

Jennifer is also known for introducing mindfulness-based leadership to individuals and organizations in infosec. And aside from meditation and security, she's a competitive powerlifter and dancer. It's also been reported that she loves Figment, the Imagination Dragon. For more information visit her company at `www.viszensecurity.com` or award-winning blog at `www.securityuncorked.com`.

About the Technical Editor

Stephen Orr is a twenty-three-year veteran of Cisco and serves as a Distinguished Architect for Cisco's Global Systems Engineering Organization. Stephen currently participates in multiple industry working groups such as the Wi-Fi Alliance where he is currently serving as the Chair for the Security Marketing and Security Technical Task Groups focusing on WPA3 as well as one of the Vice-Chairs for the IEEE 802.11TGbh Working Group (Operation with Randomized and Changing MAC Addresses).

Acknowledgments

They always say it takes a village to raise a child, and the creation of this book is no exception. Having worked in many areas of technology and information security for the last 20 years, the one thing I'm acutely aware of is exactly how much I *don't* know. It's a fool's errand to be the master of all technology in today's world. And while this book was based on my experiences with clients over the past twenty years, the depth of value in this content would not be made possible without the support of the communities.

First, Stephen Orr deserves a special callout; not only did he do exceptional work with the foreword and technical editing; he went above and beyond, helping me research and dig into complex topics, often sifting through lengthy documents to help aggregate data to be included here. As a Distinguished Cisco Engineer and leader of the Wi-Fi Alliance Security Task Group, I knew Stephen would ensure this text was accurate and inclusive and offer balance in many ways including supplementing my knowledge gaps.

We had a bit of a relay with some of the technical editing and I'm deeply appreciative of Adrian Sanabria, Mick Douglass, and Matthew Gast for their contributions throughout the book and for helping us stay on schedule. Their insights have been invaluable.

When certain topics of this book extended beyond my reach, the infosec and Wi-Fi communities were there. Instead of making educated guesses on the operation of certain technology, I solicited feedback from subject matter experts in addition to our dedicated technical editors. With that, additional thanks are sent to Peter Mackenzie, Troy Martin, Andrew von Nagy, Keith Parsons, Jonathan Davis, Sam Clements, and the lovely Tauni Odia. Additional thanks go to my infosec family, especially Chuck Kesler, Ryan Linn, my fellow IANS faculty, and friends at SecureIdeas.

This book wouldn't be possible without an introduction from none other than David Coleman to Wiley, and special thanks goes to Jim Minatel, Pete Gaughan, Tom Cirtin, and the editors at Wiley who indulged my completely ludicrous timeline to release this book.

Last but not least, special thanks are owed to my "work family" including Julie Allen, other colleagues from my twenty years with Carolina Advanced Digital, Inc., and amazing clients over the years who have trusted their infrastructures to me and let me into their lives and datacenters. You're the reason this book exists.

Contents at a Glance

Foreword		xxix
Preface		xxxi
Introduction		xxxv
Part I	**Technical Foundations**	**1**
Chapter 1	**Introduction to Concepts and Relationships**	**3**
Chapter 2	**Understanding Technical Elements**	**45**
Chapter 3	**Understanding Authentication and Authorization**	**101**
Chapter 4	**Understanding Domain and Wi-Fi Design Impacts**	**173**
Part II	**Putting It All Together**	**219**
Chapter 5	**Planning and Design for Secure Wireless**	**221**
Chapter 6	**Hardening the Wireless Infrastructure**	**281**
Part III	**Ongoing Maintenance and Beyond**	**365**
Chapter 7	**Monitoring and Maintenance of Wireless Networks**	**367**
Chapter 8	**Emergent Trends and Non-Wi-Fi Wireless**	**439**
Appendix A	**Notes on Configuring 802.1X with Microsoft NPS**	**513**
Appendix B	**Additional Resources**	**521**
Appendix C	**Sample Architectures**	**531**
Appendix D	**Parting Thoughts and Call to Action**	**559**
Index		567

Contents

Foreword		**xxix**
Preface		**xxxi**
Introduction		**xxxv**
Part I	**Technical Foundations**	**1**
Chapter 1	**Introduction to Concepts and Relationships**	**3**
	Roles and Responsibilities	4
	Network and Wireless Architects	4
	Security, Risk, and Compliance Roles	5
	Risk and Compliance Roles	5
	Chief Information Security Officer Roles	6
	Security Operations and Analyst Roles	7
	Identity and Access Management Roles	8
	Operations and Help Desk Roles	8
	Network Operations Teams	9
	Help Desk and End-User Support Roles	9
	External and Third Parties	9
	Technology Manufacturers and Integrators	10
	Vendor Management and Supply Chain Security Considerations	10
	Security Concepts for Wireless Architecture	11
	Security and IAC Triad in Wireless	11
	Integrity in Secure Wireless Architecture	12
	Availability in Secure Wireless Architecture	13
	Confidentiality in Secure Wireless Architecture	13
	Using the IAC Triad to Your Advantage	14
	Aligning Wireless Architecture Security to Organizational Risk	14
	Identifying Risk Tolerance	14

Factors Influencing Risk Tolerance 15
Assigning a Risk Tolerance Level 15
Considering Compliance and Regulatory Requirements 17
Compliance Regulations, Frameworks, and Audits 17
The Role of Policies, Standards, and Procedures 19
Policies 20
Standards 20
Procedures 20
Example with Wireless Security 21
Segmentation Concepts 22
Why and When to Segment Traffic 22
Methods to Enforce Segmentation 22
Authentication Concepts 23
Authentication of Users 24
Authentication of Devices 25
Authentication of Administrative Users 26
Authentication of the Servers (for Captive Portals and/or 802.1X RADIUS) 26
Authentication of the Wireless Infrastructure Components 26
Cryptography Concepts 27
Cryptographic Keys, Key Exchanges, and Key Rotation 27
Cryptographic Algorithms and Hashes 27
Tying It All Together 28
Wireless Concepts for Secure Wireless Architecture 30
Wireless Standards and Protocols 30
Wireless Standards and Technologies 30
Generations of 802.11 WLANs 32
NAC and IEEE 802.1X in Wireless 33
SSID Security Profiles 34
Open Wi-Fi Security 34
Personal (Passphrase) Wi-Fi Security 35
Enterprise (802.1X) Wi-Fi Security 35
Endpoint Devices 35
Form Factors 36
User-based vs. Headless 36
RF Capabilities 36
Security Capabilities 37
Ownership 37
Network Topology and Distribution of Users 37
Campus Environments 38
Remote Branch Environments 39
Remote Worker Environments 40
The Issue of Connectivity 41
Summary 43

Chapter 2 Understanding Technical Elements 45
Understanding Wireless Infrastructure and Operations 45
Management vs. Control vs. Data Planes 46

Management Plane 46
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

Legacy Open Authentication Networks 94
Wi-Fi Enhanced Open Networks 95
Summary 98

Chapter 3 Understanding Authentication and Authorization 101
The IEEE 802.1X Standard 102
Terminology in 802.1X 103
High-Level 802.1X Process in Wi-Fi Authentication 105
802.1X as the Iron Gate 106
RADIUS Servers, RADIUS Attributes, and VSAs 107
RADIUS Servers 107
RADIUS Servers and NAC Products 108
Relationship of RADIUS, EAP, and Infrastructure Devices 110
RADIUS Attributes 111
Common RADIUS Attributes 111
RADIUS Attributes for Dynamic VLANs 113
RADIUS Vendor-Specific Attributes 115
RADIUS Policies 116
RADIUS Servers, Clients and Shared Secrets 118
Specifying RADIUS Clients 118
RADIUS Shared Secrets 120
Other Requirements 121
User Directories 121
Server Certificate 121
Logging/Accounting 122
Additional Notes on RADIUS Accounting 122
Change of Authorization and Disconnect Messages 123
EAP Methods for Authentication 127
Outer EAP Tunnels 129
EAP-PEAP 129
EAP-TTLS 130
EAP-FAST 130
EAP-TEAP 131
Securing Tunneled EAP 132
Inner Authentication Methods 133
EAP-TLS 134
EAP-MSCHAPv2 135
EAP-GTC 135
EAP-POTP 136
Legacy and Unsecured EAP Methods 137
Recommended EAP Methods for Secure Wi-Fi 138
MAC-Based Authentications 140
MAC Authentication Bypass with RADIUS 140
Overview of Typical MAB Operations 142
Vendor Variations of MAC Operations 142
Security Considerations for MAB 143

Recommendations when Using MAB 145
MAC Authentication Without RADIUS 147
MAC Filtering and Denylisting 147
Certificates for Authentication and Captive Portals 148
RADIUS Server Certificates for 802.1X 148
Endpoint Device Certificates for 802.1X 151
Best Practices for Using Certificates for 802.1X 152
Never Use Wildcard Certificates 153
Never Use Self-Signed Certificates 153
Always Validate Server Certificates 154
Most Often, Use Domain-Issued Certificates for RADIUS Servers 154
Use Revocation Lists, Especially for Endpoint Certificates 157
Captive Portal Server Certificates 158
Best Practices for Using Certificates for Captive Portals 159
In Most Cases, Use a Public Root CA Signed Server Certificate 159
Understand the Impact of MAC Randomization on Captive Portals 159
Captive Portal Certificate Best Practices Recap 161
Summary 162
Captive Portal Security 163
Captive Portals for User or Guest Registration 163
Guest Self-Registration Without Verification 163
Guest Self-Registration with Verification 163
Guest Sponsored Registration 164
Guest Pre-Approved Registration 164
Guest Bulk Registration 164
Captive Portals for Acceptable Use Policies 165
Captive Portals for BYOD 166
Captive Portals for Payment Gateways 167
Security on Open vs. Enhanced Open Networks 167
Access Control for Captive Portal Processes 167
LDAP Authentication for Wi-Fi 168
The 4-Way Handshake in Wi-Fi 168
The 4-Way Handshake Operation 168
The 4-Way Handshake with WPA2-Personal and WPA3-Personal 170
The 4-Way Handshake with WPA2-Enterprise and WPA3-Enterprise 171
Summary 171

Chapter 4 Understanding Domain and Wi-Fi Design Impacts 173
Understanding Network Services for Wi-Fi 173
Time Sync Services 174
Time Sync Services and Servers 175
Time Sync Uses in Wi-Fi 175

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

Wireless Networks (SSIDs) 247
System Availability 249
Additional Software or Tools 249
Processes and Policy Updates 250
Infrastructure Hardening 251
Correlating Inputs to Outputs 252
Planning Processes and Templates 254
Requirements Discovery Template (Define and Characterize) 254
Sample Enterprise Requirements Discovery Template 255
Sample Healthcare Requirements Discovery Template 257
Defining BYOD in Your Organization 259
Sample Network Planning Template (SSID Planner) 261
Sample Access Rights Planning Templates 262
Sample Access Rights Planner for NAC 264
Sample Access Rights Planner for NAC in Higher Education 265
Sample Simplified Access Rights Planner 266
Notes for Technical and Executive Leadership 267
Planning and Budgeting for Wireless Projects 268
Involve Wireless Architects Early to Save Time and Money 268
Collaboration Is King for Zero Trust and Advanced Security Programs 268
Stop Planning 1:1 Replacements of APs 269
Penny Pinching on AP Quantities Sacrifices Security 269
Always Include Annual Budget for Training and Tools 270
Consultants and Third Parties Can Be Invaluable 271
Selecting Wireless Products and Technologies 271
Wi-Fi Isn't the Only Wireless Technology 272
The Product Your Peer Organization Uses May Not Work for You 273
Don't Buy Into Vendor or Analyst Hype 273
Interoperability Is More Important Now than Ever 274
Expectations for Wireless Security 275
Consider PSK Networks to Be the "New WEP" 275
You're Not as Secure as You Think 276
Get Control of Privileged Access, Especially Remote 277
Make Sure You've Addressed BYOD 278
Summary 279

Chapter 6 Hardening the Wireless Infrastructure 281
Securing Management Access 282
Enforcing Encrypted Management Protocols 283
Generating Keys and Certificates for Encrypted Management 283
Enabling HTTPS vs. HTTP 287
Enabling SSH vs. Telnet 289

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
Enforcing 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 UPnP 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

Security Event Logging 408
Security Event Correlation and Analysis 408
Wireless-Specific Tools 410
Handheld Testers 410
RF Design and Survey Software 412
Network Protocol Analyzers 415
Testing and Troubleshooting Applications 415
Logging, Alerting, and Reporting Best Practices 416
Events to Log for Forensics or Correlation 417
Secure Management Access 418
Infrastructure Integrity 418
Client Security and Other WIPS 418
Events to Alert on for Immediate Action 419
Secure Management Access 419
Infrastructure Integrity 420
Client Security and Other WIPS 421
Events to Report on for Analysis and Trending 422
Secure Management Access 423
Infrastructure Integrity 423
Client Security and Other WIPS 424
Troubleshooting Wi-Fi Security 424
Troubleshooting 802.1X/EAP and RADIUS 425
Things to Remember 425
Things to Troubleshoot 426
Troubleshooting MAC-based Authentication 428
MAC Address Formatting 429
MAC Authentication Bypass AAA Settings 429
Settings on the RADIUS and Directory Servers 430
Troubleshooting Portals, Onboarding, and Registration 431
Troubleshooting with Protected Management Frames Enabled 431
Training and Other Resources 432
Technology Training Courses and Providers 432
Wi-Fi Training and Certification 433
IoT Wireless Training and Certification 434
Network and Cyber Security Training 435
Vendor-Specific Training and Resources 435
Conferences and Community 436
Summary 437

Chapter 8 Emergent Trends and Non-Wi-Fi Wireless 439
Emergent Trends Impacting Wireless 440
Cloud-Managed Edge Architectures 440
Remote Workforce 441
Challenges Supporting Work from Home and Remote Users 442
Balancing Additional Work and the Tech Talent Shortage 443
Process Changes to Address Remote Work 443

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) 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 522
Navigating and Reading IEEE Standards 523
Helpful Links 523
IEEE 802.11 Standard 523
Wi-Fi Alliance 524
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 531
Architectures for Internal Access Networks 532
Managed User with Managed Device 533
Security Considerations 533
High-Security Architecture 534
Medium-Security Architecture 536
Low-Security Architecture 538
Headless/Non-User-Based Devices 539
Security Considerations 540
High-Security Architecture 540
Medium-Security Architecture 542
Low-Security Architecture 543
Contractors and Third Parties 544
Security Considerations 545
High-Security Architecture 545
Medium-Security Architecture 546
Low-Security Architecture 547
BYOD/Personal Devices with Internal Access 547
Security Considerations 547
High-Security Architecture 548
Medium-Security Architecture 548
Low-Security Architecture 549
Guidance on WPA2-Enterprise and WPA3-Enterprise 549
Migrating from WPA2-Enterprise to WPA3-Enterprise 549
Supporting WPA2-Enterprise with WPA3-Enterprise 550
Guidance on When to Separate SSIDs 550
Architectures for Guest/Internet-only Networks 551
Guest Networks 551
Security Considerations 551
High-Security Architecture 552
Medium-Security Architecture 552
Low-Security Architecture 553
BYOD/Personal Devices with Internet-only Access 553
Security Considerations 553
High-Security Architecture 554

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