

Wireless Security Architecture

Designing
and Maintaining
Secure Wireless
for Enterprise

Jennifer (JJ) Minella
Foreword by Stephen Orr

WILEY

Table of Contents

[Cover](#)

[Title Page](#)

[Foreword](#)

[Preface](#)

[Who This Book Is For](#)

[Distinctive Features](#)

[Introduction](#)

[Overview of the Book and Technology](#)

[How This Book Is Organized](#)

[Why Read This Book](#)

[What's on the Website](#)

[Congratulations](#)

[Part I: Technical Foundations](#)

[CHAPTER 1: Introduction to Concepts and Relationships](#)

[Roles and Responsibilities](#)

[Security Concepts for Wireless Architecture](#)

[Wireless Concepts for Secure Wireless Architecture](#)

[Summary](#)

[CHAPTER 2: Understanding Technical Elements](#)

[Understanding Wireless Infrastructure and Operations](#)

[Understanding Data Paths](#)

[Understanding Security Profiles for SSIDs](#)

[Summary](#)

CHAPTER 3: Understanding Authentication and Authorization

The IEEE 802.1X Standard

RADIUS Servers, RADIUS Attributes, and VSAs

Change of Authorization and Disconnect Messages

EAP Methods for Authentication

MAC-Based Authentications

Certificates for Authentication and Captive Portals

Captive Portal Security

LDAP Authentication for Wi-Fi

The 4-Way Handshake in Wi-Fi

Summary

CHAPTER 4: Understanding Domain and Wi-Fi Design Impacts

Understanding Network Services for Wi-Fi

Understanding Wi-Fi Design Impacts on Security

Summary

Part II: Putting It All Together

CHAPTER 5: Planning and Design for Secure Wireless

Planning and Design Methodology

Planning and Design Inputs (Define and Characterize)

Planning and Design Outputs (Design, Optimize, and Validate)

Correlating Inputs to Outputs

Planning Processes and Templates

[Notes for Technical and Executive Leadership
Summary](#)

[CHAPTER 6: Hardening the Wireless Infrastructure](#)

[Securing Management Access](#)

[Designing for Integrity of the Infrastructure](#)

[Controlling Peer-to-Peer and Bridged
Communications](#)

[Best Practices for Tiered Hardening](#)

[Additional Security Configurations](#)

[Summary](#)

[Part III: Ongoing Maintenance and Beyond](#)

[CHAPTER 7: Monitoring and Maintenance of
Wireless Networks](#)

[Security Testing and Assessments of Wireless
Networks](#)

[Security Monitoring and Tools for Wireless](#)

[Logging, Alerting, and Reporting Best Practices](#)

[Troubleshooting Wi-Fi Security](#)

[Training and Other Resources](#)

[Summary](#)

[CHAPTER 8: Emergent Trends and Non-Wi-Fi
Wireless](#)

[Emergent Trends Impacting Wireless](#)

[Enterprise IoT Technologies and Non-802.11
Wireless](#)

[Final Thoughts from the Book](#)

[Appendix A: Notes on Configuring 802.1X with
Microsoft NPS](#)

[Wi-Fi Infrastructure That Supports Enterprise
\(802.1X\) SSID Security Profiles](#)

[Endpoints That Support 802.1X/EAP](#)

[A Way to Configure the Endpoints for the Specified Connectivity](#)

[An Authentication Server That Supports RADIUS](#)

[Appendix B: Additional Resources](#)

[IETF RFCs](#)

[IEEE Standards and Documents](#)

[Wi-Fi Alliance](#)

[Blog, Consulting, and Book Materials](#)

[Compliance and Mappings](#)

[Cyber Insurance and Network Security](#)

[Appendix C: Sample Architectures](#)

[Architectures for Internal Access Networks](#)

[Architectures for Guest/Internet-only Networks](#)

[Determining Length of a WPA3-Personal Passphrase](#)

[Appendix D: Parting Thoughts and Call to Action](#)

[The Future of Cellular and Wi-Fi](#)

[MAC Randomization](#)

[Security, Industry, and The Great Compromise](#)

[Index](#)

[Copyright](#)

[Dedication](#)

[About the Author](#)

[About the Technical Editor](#)

[Acknowledgments](#)

[End User License Agreement](#)

List of Tables

Chapter 2

[Table 2.1: Example of planes in wireless](#)

[Table 2.2: Cloud architecture and planes](#)

[Table 2.3: Current SSID security options in products](#)

[Table 2.4: WPA3-Enterprise cipher and AKM suites](#)

[Table 2.5: WPA3-Enterprise 192-bit TLS cipher suites](#)

Chapter 3

[Table 3.1: Examples of standard RADIUS attributes in Wi-Fi](#)

[Table 3.2: Standard RADIUS attributes and values for dynamic VLAN assignment...](#)

[Table 3.3: Examples of Vendor-Specific Attributes](#)

[Table 3.4: Sample list for planning RADIUS clients](#)

[Table 3.5: CoA and DM RADIUS code descriptions](#)

[Table 3.6: Comparison of EAP outer tunnels](#)

[Table 3.7: Comparison of EAP inner authentication methods for Wi-Fi](#)

[Table 3.8: Recommended EAP outer and inner combinations for enterprise Wi-Fi...](#)

[Table 3.9: Security differences in 802.1X vs. MAB](#)

[Table 3.10: Server certificate requirements for various EAP methods](#)

[Table 3.11: Summary of server certificate recommendations by use case](#)

Chapter 4

[Table 4.1: Summary of key exchanges with roaming facilitation](#)

Chapter 6

[Table 6.1: Overview of file transfer protocol security](#)

[Table 6.2: Summary of management protocols and recommended encrypted version...](#)

[Table 6.3: Comparing TACACS+ and RADIUS for management](#)

[Table 6.4: AP provisioning models supported](#)

[Table 6.5: Comparison of AP-to-switch authentication options](#)

Chapter 7

[Table 7.1: Comparison of common rogue classifications](#)

[Table 7.2: Summary of recommended logging, alerting, and reporting by type](#)

[Table 7.3: MAC address delimiter formats](#)

Chapter 8

[Table 8.1: Management and ownership models for devices](#)

[Table 8.2: Table of BYOD access planning](#)

[Table 8.3: Cellular generations and technologies](#)

[Table 8.4: Excerpt of 3GPP releases and IoT-friendly classes](#)

[Table 8.5: Private cellular vs. Wi-Fi](#)

Appendix B

[Table B.1 : NIST 800-53 control families](#)

[Table B.2 : Sample excerpt rows from NIST to ISO mapping](#)

Appendix C

[Table C.1 : WPA3-Personal passphrase length recommendations](#)

Appendix D

[Table D.1 : Overview of cellular, Wi-Fi, and MNO augmentation](#)

List of Illustrations

Chapter 1

[Figure 1.1: Elements of integrity, availability, and confidentiality are per...](#)

[Figure 1.2: As security requirements increase, risk tolerance decreases, and...](#)

[Figure 1.3: In the hierarchy of policies, standards, and procedures, one bro...](#)

[Figure 1.4: Recap of the intent and relationship of policies, standards, and...](#)

[Figure 1.5: Overview of the seven layers of the OSI model. Layer 2 is the MA...](#)

[Figure 1.6: A simplified view of public and private key use in public key cr...](#)

[Figure 1.7: A side-by-side comparison of pros and cons of symmetric and asym...](#)

[Figure 1.8: IEEE logo](#)

[Figure 1.9: The Wi-Fi Alliance manages the testing and certification of 802....](#)

[Figure 1.10: The IETF creates most of the world's Internet protocols in use ...](#)

[Figure 1.11: Summary of three classes of SSID security profiles with use cas...](#)

[Figure 1.12: In campus topologies, the users, infrastructure, and internal r...](#)

[Figure 1.13: With remote branch topologies, satellite locations are connecte...](#)

[Figure 1.14: In remote worker environments, the user either has a remote AP ...](#)

[Figure 1.15: Sample remote AP products from Aruba Networks and Juniper Mist...](#)

Chapter 2

[Figure 2.1: Management, control, and data planes](#)

[Figure 2.2: A sample architecture for bridged versus tunneled client data in...](#)

[Figure 2.3: Sample local cluster management architecture](#)

[Figure 2.4: Sample remote AP architecture](#)

[Figure 2.5: Comparison of tunneled \(left\) versus bridged \(right\) client traf...](#)

[Figure 2.6: A hybrid data path model using both tunneled and bridged traffic...](#)

[Figure 2.7: Sample overview of segmenting on the Wi-Fi infrastructure versus...](#)

[Figure 2.8: Comparison of the segmentation behavior of VLANs \(left\) versus V...](#)

[Figure 2.9: This endpoint's default gateway is on the wired network](#)

[Figure 2.10: Aruba Central's security profile options for the Enterprise cla...](#)

[Figure 2.11: High-level view of required components for 802.1X in secure Wi-...](#)

[Figure 2.12: Sample screenshots of 802.1X security options from Juniper Mist...](#)

[Figure 2.13: Screenshot from Aruba Central showing Personal network options...](#)

[Figure 2.14: Screenshot from a Fortinet FortiGate-managed AP showing Persona...](#)

[Figure 2.15: WPA2-Personal PSK versus WPA3-Personal SAE](#)

[Figure 2.16: This image demonstrates the exchanges during SAE and the deriva...](#)

[Figure 2.17: Adoption of encrypted Internet traffic from Google](#)

[Figure 2.18: The 802.11 Open System Authentication](#)

[Figure 2.19: Enhanced Open Transition Mode uses two SSIDs](#)

[Figure 2.20: Snapshot from NetAlly EtherScope nXG showing the two networks f...](#)

Chapter 3

[Figure 3.1: High-level view of 802.1X components](#)

[Figure 3.2: The use of EAPoL and RADIUS protocol during authentication Wi-Fi...](#)

[Figure 3.3: The two logical 802.1X port entities](#)

[Figure 3.4: Relationship between endpoints, Wi-Fi infrastructure, and the RA...](#)

[Figure 3.5: Sample attributes for dynamic VLAN assignment](#)

[Figure 3.6: Example of RADIUS policy conditions, constraints, and settings](#)

[Figure 3.7: RADIUS clients can be added by IP address, IP network, or hostna...](#)

[Figure 3.8: Microsoft NPS options for logging targets](#)

[Figure 3.9: Microsoft NPS options for level of logging detail and logging fa...](#)

[Figure 3.10: Markup of default Microsoft NPS text file log](#)

[Figure 3.11: View of CoA operations within 802.1X authentication](#)

[Figure 3.12: Comparison of CoA configurations](#)

[Figure 3.13: Conceptual representation of the EAP framework using an outer t...](#)

[Figure 3.14: A correct PEAP with MSCHAPv2 configuration on the top, and an i...](#)

[Figure 3.15: RSA SecureID USB token](#)

[Figure 3.16: MAB authentication process](#)

[Figure 3.17: Process of an endpoint validating a server's certificate](#)

[Figure 3.18: Microsoft Active Directory Group Policy options for validating ...](#)

[Figure 3.19: A Windows 10 device, showing MAC randomization options](#)

[Figure 3.20: An Apple iPhone private address \(MAC randomization\) settings...](#)

[Figure 3.21: An Android device MAC randomization settings](#)

[Figure 3.22: A view of the 4-way handshake between an endpoint \(defined as a...](#)

[Figure 3.23: The 4-way handshake after 802.1X authentication](#)

Chapter 4

[Figure 4.1: Machines and microservices use certificates, signatures, and tok...](#)

[Figure 4.2: DHCP request paths using proxy from wired and wireless infrastru...](#)

[Figure 4.3: Alternate configurations demonstrating ability of certain networ...](#)

[Figure 4.4: Windows ipconfig output showing the endpoint's default gateway o...](#)

[Figure 4.5: Exchanges required for a hard roam on a WPA2-Personal with PSK n...](#)

[Figure 4.6: Exchanges required for a hard roam on an 802.1X-secured network...](#)

[Figure 4.7: PMK derivation and key distribution for roaming facilitation](#)

[Figure 4.8: Conceptual view of Fast Reconnect](#)

[Figure 4.9: PMK caching, or roam back, offers benefits only in cases where a...](#)

[Figure 4.10: OKC eliminates the 802.1X re-authentication when roaming to nea...](#)

[Figure 4.11: An endpoint roaming on an 802.1X network with FT is faster than...](#)

[Figure 4.12: A high-level comparison of spectrum availability and channels i...](#)

[Figure 4.13: 6 GHz channel allocations in detail](#)

[Figure 4.14: In Wi-Fi, the white spaces are the only times the RF medium is ...](#)

[Figure 4.15: Sample rate limiting options on Juniper Mist](#)

[Figure 4.16: Sample output of CDP on the same AP and switch](#)

[Figure 4.17: Sample output of LLDP-MED of an AP connected to a switch](#)

[Figure 4.18: Sample output of LLDP-MED on a VoIP device](#)

Chapter 5

[Figure 5.1: The five phases of the planning and design methodology](#)

[Figure 5.2: Example of a simplified RACI matrix for a wireless project](#)

[Figure 5.3: Visualization of the relationship of inputs to outputs](#)

[Figure 5.4: Sample requirements discovery template for endpoints and users i...](#)

[Figure 5.5: Sample requirements discovery template populated with sample hea...](#)

[Figure 5.6: Sample planner template for controller and AP management network...](#)

[Figure 5.7: Sample planner to be used per SSID](#)

[Figure 5.8: An advanced access rights planner that factors ownership along w...](#)

[Figure 5.9: An advanced access rights planner for higher education](#)

[Figure 5.10: A simplified access rights form for wireless connections only,...](#)

Chapter 6

[Figure 6.1: Sample PEM certificate file format](#)

[Figure 6.2: Sample DER certificate file format](#)

[Figure 6.3: In most products you can enable HTTPS and disable HTTP in the we...](#)

[Figure 6.4: Creation of an ECDSA SSH key pair with PUTTYGEN](#)

[Figure 6.5: Many enterprise Wi-Fi products support public key authentication...](#)

[Figure 6.6: Where possible, always change the APs' default username and pass...](#)

[Figure 6.7: Figure 10 from the Verizon DBIR 2021 report, showing privilege a...](#)

[Figure 6.8: The report highlights credentials as top data varieties in breac...](#)

[Figure 6.9: Demonstrating three AP to switch authentication options](#)

[Figure 6.10: Example of a mounting enclosure with tamper-resistant screws \(u...](#)

[Figure 6.11: Example of a mounting enclosure with a key lock](#)

[Figure 6.12: An Aruba 7200 series Mobility Controller. Notice the console po...](#)

[Figure 6.13: Diagram of the front panel components of a Cisco 9800-80 Contro...](#)

[Figure 6.14: Image of an Aruba Networks 600 series AP with mini USB console...](#)

[Figure 6.15: An example of a tamper-evident label](#)

[Figure 6.16: Peer communication through an enterprise AP vs. ad-hoc networks...](#)

[Figure 6.17: On most devices, it's trivial for a user to share network conne...](#)

[Figure 6.18: Juniper Mist options for inter-station blocking and multicast c...](#)

[Figure 6.19: Aruba Networks Central Cloud SSID configuration](#)

[Figure 6.20: Excerpt from Trustwave's post on the security vulnerabilities o...](#)

[Figure 6.21: Tiered guidance for securing management access for low, medium,...](#)

[Figure 6.22: Tiered guidance for designing for integrity in low, medium, and...](#)

[Figure 6.23: Tiered guidance for controlling peer-to-peer and bridged commun...](#)

[Figure 6.24: Conceptual comparison of connecting to a hidden SSID versus a b...](#)

[Figure 6.25: A Windows configuration option to connect to an SSID even if it...](#)

[Figure 6.26: The Hide SSID option in Juniper Mist](#)

[Figure 6.27: The Hide SSID option of Aruba Networks Central Cloud platform](#)

[Figure 6.28: The option to share a passphrase credential via QR code from an...](#)

[Figure 6.29: Screenshot from Apple on sharing network passwords](#)

Chapter 7

[Figure 7.1: Sample data from vulnerability scanning in a lab environment](#)

[Figure 7.2: CVE-2020-26140 was one of many vulnerabilities exploited in Frag...](#)

[Figure 7.3: The level of touch varies from audits and assessments to penetra...](#)

[Figure 7.4: Visibility of WIPS vs. wired IPS](#)

[Figure 7.5: For any given radio, an AP also serving as a WIPS sensor will sp...](#)

[Figure 7.6: Juniper Mist has limited WIPS configuration in the web UI.](#)

[Figure 7.7: WIPS configuration options on Aruba Central cloud](#)

[Figure 7.8: In AP impersonation \(top\), an AP is advertising the same network...](#)

[Figure 7.9: Image from a Cisco article detailing how to identify randomized ...](#)

[Figure 7.10: In request-to-send \(RTS\) and clear-to-send \(CTS\) attacks, airt...](#)

[Figure 7.11: Screenshot from a Windows laptop showing the option for a user ...](#)

[Figure 7.12: After configuring the bridged interface, an end user can specif...](#)

[Figure 7.13: In a client misassociation, an enterprise client associates wit...](#)

[Figure 7.14: APs are commonly classified a few ways.](#)

[Figure 7.15: Over-the-air mitigation by a WIPS using spoofed broadcast and u...](#)

[Figure 7.16: The cover of a nine-page order issued by the FCC to Marriott re...](#)

[Figure 7.17: Spectrum analyzers, protocol analyzers, and packet analyzers op...](#)

[Figure 7.18: Visualization of spectrum analysis overlaid with Wi-Fi channel ...](#)

[Figure 7.19: NetAlly's AirMagnet Spectrum XT software](#)

[Figure 7.20: NetAlly dual band USB spectrum analyzer](#)

[Figure 7.21: Vendor 7Signal offers an app-based agent and hardware sensors i...](#)

[Figure 7.22: The NetAlly EtherScope nXG is a great handheld tool for testing...](#)

[Figure 7.23: Heatmap output from a live RF survey.](#)

[Figure 7.24: A Wireshark Wi-Fi packet capture can parse from layers 2 and hi...](#)

[Figure 7.25: Connected components with numbers designating each troubleshoot...](#)

[Figure 7.26: Sample port-level configuration of a switch using 802.1X with M...](#)

Chapter 8

[Figure 8.1: Gartner's predictive analysis shows a continued increase in remo...](#)

[Figure 8.2: Zero trust terminology is just an upcycle of NAC](#)

[Figure 8.3: Simplified view of cloud-routed versus direct-routed zero trust ...](#)

[Figure 8.4: LAN-based IoT vs. protocol-translated IoT vs. protocol-routed Io...](#)

[Figure 8.5: Comparison of power consumption and range for common IoT technol...](#)

[Figure 8.6: Visual map of IoT technologies, their topologies, coverage areas...](#)

[Figure 8.7: Excerpt table from a network connectivity datasheet for a Wi-Fi-...](#)

[Figure 8.8: The Bluetooth-enabled Azure Medtronic pacemaker was just one of ...](#)

[Figure 8.9: Visualizing the ratio of IPv4 to IPv6 addresses \(top\) and 802.15...](#)

[Figure 8.10: The Thread communication stack](#)

[Figure 8.11: 5G network slices can divvy up airtime and bandwidth to meet va...](#)

[Figure 8.12: Cellular LANs are deployed much like Wi-Fi.](#)

[Figure 8.13: Cellular LANs can be integrated into the enterprise LAN several...](#)

[Figure 8.14: As an example of the coverage capabilities, this vendor's rough...](#)

[Figure 8.15: Comparison of roaming decisions on Wi-Fi \(left\) versus cellular...](#)

[Figure 8.16: Cellular nodes \(or cellular APs\) look and operate very much lik...](#)

[Figure 8.17: Sigfox adoption is focused in about a dozen European countries ...](#)

[Figure 8.18: Diagram of WirelessHART architecture](#)

[Figure 8.19: ISA100.11a sample architecture](#)

Appendix A

[Figure A.1: Most non-standard endpoints such as network printers and VoIP ph...](#)

[Figure A.2: Microsoft NPS can be instructed to forward or proxy RADIUS reque...](#)

[Figure A.3: The Network Policies of Microsoft NPS, which set the criteria fo...](#)

[Figure A.4: This view shows the details of a policy specifying Microsoft PEA...](#)

[Figure A.5: Network Policy configuration showing the attributes for dynamic ...](#)

Appendix B

[Figure B.1: Sample IETF RFC header](#)

Appendix C

[Figure C.1: Architecture summary for internal access by managed users with m...](#)

[Figure C.2: Architecture summary for internal access by headless devices](#)



Wireless Security Architecture

**Designing and Maintaining Secure
Wireless for Enterprise**

Jennifer (JJ) Minella

WILEY

Foreword

With all the innovations and alphabet soup of the different 802.11 standards, Wi-Fi security is one of those functions at the core of all modern protocol development. We are in an age of ensuring that we protect not only the information in transit, but also the identity of the user and device, and we need to balance this with protecting the access to personal and corporate resources. Modern-day security development and deployment for Wi-Fi is a delicate balancing act where all these nuances must be considered. If you make security too difficult to use/deploy, people will bypass it or turn it off; if it's not secure enough, you will surely make the headlines.

Full disclosure, Wi-Fi security is a topic near and dear, so I am slightly biased to its importance. My journey started by asking a simple question: how is Wi-Fi Protected Access different than WEP and could this be deployed for use in government agencies? Years later this continued interest in Wi-Fi security led to an opportunity to participate in the Wi-Fi Alliance Security Working Groups, where I was introduced to a talented group of individuals focused on advancing wireless security capabilities. Fast forward 10+ years and this group has addressed vulnerabilities in Wi-Fi Certified WPA2, launched Wi-Fi Certified WPA3 (multiple releases), addressed the challenges of Open networks with Wi-Fi Certified Enhanced Open, and finally, set a new bar for wireless security by eliminating WPA2 and Open networks in new MAC/PHY bands starting with 6 GHz. Introducing new security requirements is hard and not always fast. Status quo is easy and change is difficult specifically with security, but sometimes ripping the bandage off may need to be done because the major

headlines get made when there is an issue with Wi-Fi security.

When asked to write the foreword for JJ's book on Wireless Security Architecture, I needed to think about how to frame the journey readers will take because the context of the title is important. The topic isn't securing wireless—it's wireless security architectures, which is an overarching defense-in-depth approach to creating an architecture that meets your business objectives, starting at the wireless access layer with security at the forefront and continuing that into the enterprise network. Most don't look past the 802.11 layer when we talk about Wi-Fi security, however 802.11 is now the dominant access layer and care must be taken on its integration into your enterprise.

Entire books have been written on the intricacies, nuances, and in-depth protocol discussions of 802.11 security. They have done so from the point of view of the interpretation of the standards bodies (IEEE 802.11) or the certification organizations such as the Wi-Fi Alliance, but not from the perspective of the CXO, network operator, network architect, or the user. Where this book is different is that it is all about context. JJ takes a unique approach to making wireless security relevant and peels back the complexities to show how security at the wireless access layer should be integrated as part of your overall architecture design and strategy, as opposed to bolted on as an independent afterthought. Additionally, the discussions and insights on how compliance will cause decisions to be made and impact architecture designs are invaluable for those dealing with customers that must meet requirements set forth by PCI, HIPAA, NIST, etc.

I hope you enjoy reading the book as much as I did, and I will leave everyone with a few final thoughts.

Security is a continual process; requirements and designs must always be reevaluated. What was good three years ago may not provide the same security levels that you need today; “good enough” security is never “good enough.”

Raise the bar. Security can and should be at the forefront of the discussions with your vendors, consultants, and architects during the acquisition process, not after.

Certifications are critical to the security conversation—not only do they define interoperability, but they ensure conformance. You shouldn't fall back to compromising your network because the latest security standards are not supported (remember you will make the news, not them).

Ensure your use cases are driving development by asking questions, contributing to forums, and getting involved.

Stephen Orr

Preface

This book was envisioned with the goal of empowering a broad category of network and security professionals to design and maintain secure wireless networks in enterprise environments.

It focuses on the most current and relevant details and offers appropriate background information and explanations that will persist for years, even as technology evolves. This book teaches network, wireless, and security architects “how to fish” and make ongoing decisions about how best to secure networks.

Wi-Fi-connected devices alone have tripled in the past six years, surpassing 20 billion in 2021. That growth, coupled with the projected 75 billion connected IoT devices by 2025 means network and security teams will be faced with new challenges securely connecting all of these “things” and protecting enterprise assets from the ones that introduce risk. With wireless connections growing exponentially, security threats increasing, ransomware rampant, and new initiatives like zero trust strategies and digital transformation, yesterday's technologies and techniques aren't sufficient to secure tomorrow's enterprise. And in fact, they're not even adequate to protect us today.

Plus, these new initiatives necessitate tighter integration between network and security disciplines. Cross-functional teams mean greater communication and knowledge sharing, and this book bridges the divide between risk management and network architecture.

This book merges the concepts of enterprise security architecture with wireless networking and teaches professionals how to design, implement, and maintain

secure enterprise wireless networks. It covers everything a technology professional needs to know to make sure the organization's wireless matches the organization's risk models and compliance requirements.

Who This Book Is For

The reader is assumed to be an IT or infosec professional with basic networking knowledge (in line with Network+ or Cisco CCNA). Wi-Fi experience, while helpful, is not required. There are portions of the book written for technical and non-technical leadership, summarizing more complex technical recommendations into business requirements.

For organization size, this book is appropriate for security-conscious organizations of all sizes and industries from small schools to universities, healthcare systems, state and local government, commercial enterprise, and even federal agencies. The only requirement being that this content is most relevant for environments using fully managed switches.

Wireless, and especially Wi-Fi, touches so many aspects of the enterprise network, from wired infrastructure to authentication servers, endpoint management, and security monitoring. This book is for you if you are:

- Network, wireless, and security architects responsible for designing secure network and wireless infrastructures. You're the primary audience for the book.
- IT professionals, network engineers, and system admins interested in learning more about securing wireless. Even if your role isn't architecting, you'll learn a lot about supporting and maintaining secure wireless systems, devices, and users.
- Technical leaders with strategic responsibility for network security and security controls compliance. While you may prefer to skip some of the more technical minutia, this book provides valuable insight

into what's possible, what's practical, and the complexity of meeting stringent security postures.

- Non-technical executive leadership and boards with oversight of risk management. Only portions of this book are appropriate for non-technical audiences, but they provide valuable actionable business-level guidance.

While the vast majority of my own experience has been with clients in the United States, this book addresses the variations in policies and compliance requirements across the globe, and the standards and technologies used are applicable in all parts of the world, with slight variations in implementation such as the RF frequencies, which are localized.

I truly hope this book will spark conversations in the networking and infosec communities, and that each professional will take aspects of this content, make it their own, and further expand the reach of not only the book, but of their own experiences and contributions.

As always, we have done our best to be as complete and accurate as possible, but alas we are human, and errors are to be expected. Although I had amazing technical editors, I accept full responsibility for any errors or omissions, and graciously appreciate any feedback including corrections. If you come across an error, please email wileysupport@wiley.com with the subject line "Possible Book Errata Submission." For other feedback you can contact me on LinkedIn or at info@viszensecurity.com.

Distinctive Features

This book separates itself from others in many ways. While other books, authors, and publishers of network security

topics add valuable content and context, this book offers these unique features:

- This book is vendor-neutral, but references vendor-specific features and documentation where applicable to ensure guidance is actionable. Many vendors call the same feature by different names, and that's addressed throughout the book.
- Advice throughout this book is based on hundreds of real-world implementations, not academic or theoretical research.
- This book addresses current and, at times, relevant future technologies, and anticipated changes.
- While other books focus on technical standards and specifications, this book provides an applied how-to approach to use that knowledge in practice.
- Unlike many training programs and books, this book seamlessly merges security, risk, and compliance considerations with network architecture at each step.
- This book prepares professionals for successfully executing their work, not merely for passing a certification test.
- The content is presented in a casual and conversational tone, making it accessible to a wide audience by not relying on niche terminology and acronyms.

Introduction

In business environments, wireless and especially Wi-Fi networks are configured and maintained by a breadth of technology professionals—from Wi-Fi specialists to the sole IT professional left to juggle everything from networking to managing endpoints, applications, and servers. This book brings deep technical details to the seasoned wireless professional and summarizes best practices in easy-to-follow advice for those wearing many hats.

After fifteen years of stale Wi-Fi security suites and a limited focus on IoT security, the world of wireless is finally putting the spotlight on security. But designing secure wireless networks isn't nearly as straightforward as it seems. The newest WPA3 security suite greatly enhances security, but also introduces complexity as organizations move from legacy security to the latest standards.

This book reframes and redefines architecting secure wireless, opposing outdated guidance in favor of more robust security practices meant to address today's and tomorrow's evolving wireless networks. Its contents walk professionals through the decision-making steps of architecting secure networks, starting from risk and compliance considerations to detailed technical configurations. Along the way, it offers practical guidance, best practices, and specific recommendations for a variety of environments, vendor implementations, and security needs.