Wireless Security Architecture

Designing and Maintaining Secure Wireless for Enterprise

Jennifer (JJ) Minella
Foreword by Stephen Orr

WILEY

Table of Contents

List of Tables

List of Illustrations

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.