preface

Wireless LANs are becoming ubiquitous. From hotel lobbies to Starbucks coffee shops, to airports and offices, it is difficult not to be able to pick up a wireless LAN signal. Accompanying the growth in the use of wireless LANs is a recognition that as initially designed they are not secure.

The focus of this book is upon wireless LAN security. In this book we will examine how wireless LANs operate, with special attention focused upon the manner in which security occurs under the IEEE 802.11 wireless LAN standard and its extensions, and why the standard and its extensions are weak. We will use this information to note many vulnerabilities associated with the use of wireless LANs and the security risks that can occur via an over-the-air transmission method. Because network managers and LAN administrators, as well as small business and home users of wireless LANs, need to know how to overcome the security limitations of wireless LANs, several chapters in this book are devoted to security enhancement techniques. One chapter is focused upon vendor-specific solutions, while a second chapter examines the use of existing and evolving standards that can be employed to literally harden your wireless LAN.

Throughout this book we will note via the use of vendor products the reason why, as designed, wireless LANs are insecure. This information will enable us to observe how easy it was for two men in a van, who moved from parking lot to parking lot in Silicon Valley, to obtain information about the use of wireless LANs from people operating equipment within the buildings the men focused their antennas upon. Although several news articles about the exploits of these two men appeared in major newspapers, what was significantly lacking was an explanation concerning why they were able to easily understand what was being transmitted and how this third party activity could be prevented, topics that I will discuss in this book.

While the primary focus of this book is upon technical issues, upon occasion we will also focus upon common sense items. For example, by understanding the default settings of IEEE 802.11 wireless LAN functions and simply changing a few settings, it becomes possible to make it more difficult for a third party to both monitor and understand data being transmitted over-the-air. As another example of applying common sense to security, the positioning of

equipment and the use of shielding can be employed to block signals. Thus, if a third party cannot receive a signal, they obviously cannot intercept or alter the signal.

Although there are several common sense approaches to securing a wireless LAN, unfortunately we need more than common sense to make wireless LANs secure. Thus, we will examine a number of techniques that can be employed to literally harden our wireless communication. Through the use of a number of computer screen captures I will illustrate tools and techniques you can consider to secure your wireless communications.

As a professional author I look forward to any comments you may have concerning the material presented in this book. Please feel free to contact me directly or via my publisher, whose address is contained on the copyright page of this book. Let me know if I omitted an item of interest, if I spent too many pages on a particular topic, or any other comments you wish to share with me. You can contact me directly via email at gil_held@yahoo.com.

Gilbert Held
Macon, GA