Foreword

Security incidents and vulnerabilities affecting networks, systems, and information are described frequently in technical journals and the popular press. Since the Morris worm incident in 1988, the number of incidents has more than doubled each year, growing in number as the Internet expands. These incidents include scans of entire networks for the purpose of identifying the network devices and services that are present on the network, directed attacks against vulnerabilities known to exist in these systems and services, and denial of service attacks designed to exhaust bandwidth, CPU, or other resources. The past year saw a number of serious worm attacks, including the well-publicized Code Red and Nimda worms. It is estimated that the impact of the Code Red worm was $2 billion and affected hundreds of thousands of hosts. These worms caused denial of service and also gave the attacker complete control of the victim systems. As it turns out, the vulnerability in Microsoft's Internet Information Service (IIS) was known, and a patch was available at the time of the attacks. Much of the impact of these worms could have been avoided had the vulnerable systems been patched in a timely fashion. More recently, a buffer overflow vulnerability was identified in Apache web servers, affecting nearly 50% of all web servers currently running on the Internet. How long will it take administrators to patch their systems? Will they do so before there is another attack of the magnitude of Code Red? The challenge to contain this trend, and even to reverse it, rests on both the technology vendors and the professionals who are designing, building, and maintaining today's sophisticated networks. Vendors must improve the quality of their products, and professionals responsible for systems and networks must consider security an important and integral component of their network infrastructures.

This book is a valuable asset to network operators and administrators who are tasked with securing these networks. Unlike books that focus on a single security technology, such as firewalls or intrusion detection systems, this book addresses the important task of knowing *when* and *where* to locate specific security technologies within a network. It then provides specific configuration information concerning these technologies. The author has made sure that the configurations are well-explained and tested, and case studies are used to put the theoretical knowledge in perspective. The book's focus provides an in-depth protocol-level understanding of the functioning of various security features. This is important, because it is nearly impossible to provide adequate security throughout your network if you have only a superficial understanding of the features and technologies available. All too often, network security is deployed as a collection of point solutions when what is really needed is a comprehensive, integrated approach. Such an approach is possible only when professionals have an in-depth understanding of how things work.

It's been my pleasure to know the author, Saadat Malik, for years. He is a talented and experienced networking professional who has experience in all the areas covered in the book. Saadat's involvement as the author of the CCIE Security lab exam gives him critical insight into the requirements of the CCIE Network Security certification. This insight and perspective make this book an invaluable asset to those working toward their CCIE Security certification. Furthermore, he has spent a number of years as a senior Technical Assistance Center engineer at Cisco, helping customers troubleshoot problems related to network security. He is the perfect author for this ultimate resource on network security. I highly recommend this book as a must-have for every networking professional working in the area of security.

Barbara Fraser

Co-chair, IP Security (IPsec) working group,The Internet Engineering Task Force (IETF)

Consulting Engineer, Chief Technology Office, Cisco Systems, Inc.