I believe The Craft of System Security is one of the best software security books on the market today. It has not only breadth, but depth, covering topics ranging from cryptography, networking, and operating systems--to the Web, computer-human interaction, and how to improve the security of software systems by improving hardware. Bottom line, this book should be required reading for all who plan to call themselves security practitioners, and an invaluable part of every university's computer science curriculum.

--Edward Bonver, CISSP, Senior Software QA Engineer, Product Security, Symantec Corporation

Heres to a fun, exciting read: a unique book chock-full of practical examples of the uses and the misuses of computer security. I expect that it will motivate a good number of college students to want to learn more about the field, at the same time that it will satisfy the more experienced professional.

--L. Felipe Perrone, Department of Computer Science, Bucknell University

Whether you're a security practitioner, developer, manager, or administrator, this book will give you the deep understanding necessary to meet today's security challenges--and anticipate tomorrows. Unlike most books, The Craft of System Security doesn't just review the modern security practitioners toolkit: It explains why each tool exists, and discusses how to use it to solve real problems.

After quickly reviewing the history of computer security, the authors move on to discuss the modern landscape, showing how security challenges and responses have evolved, and offering a coherent framework for understanding today's systems and vulnerabilities. Next, they systematically introduce the basic building blocks for securing
contemporary systems, apply those building blocks to today’s applications, and consider important emerging trends such as hardware-based security.

After reading this book, you will be able to

Understand the classic Orange Book approach to security, and its limitations
Use operating system security tools and structures—with examples from Windows, Linux, BSD, and Solaris
Learn how networking, the Web, and wireless technologies affect security
Identify software security defects, from buffer overflows to development process flaws
Understand cryptographic primitives and their use in secure systems
Use best practice techniques for authenticating people and computer systems in diverse settings
Use validation, standards, and testing to enhance confidence in a systems security
Discover the security, privacy, and trust issues arising from desktop productivity tools
Understand digital rights management, watermarking, information hiding, and policy expression
Learn principles of human-computer interaction (HCI) design for improved security
Understand the potential of emerging work in hardware-based security and trusted computing

My Personal Review:
The preface of the book says that the book grew from a college course to solve this problem: "to provide the right security education to students who may only ever take one security course and then move on toward a wide range of professional careers." Its nice when the authors put the goal of the book at the front, it makes reading it in the proper context much easier and reviewing the book (usually) much easier.

I think the authors met their goal of a book to give to people who may only read one security book in a college course and have it be readable and useful. It is written in an understandable manner and provides enough pictures and explanations for someone new to the subject who "has to take the class" and enough math and further reading for someone that wants to really delve into a subject to do so. Important words are in italics so if you wanted to or needed to look up the definitions to really understand the section you could, but there is enough information in the paragraphs to get by.

The book also has the added plus of being useful to someone studying for their CISSP (if they actually want to know the subjects). It explains topics that, in my opinion, are not explained very well in the study guides. Their discussion of the orange book was superb and I wish I had this book when I was trying to make sense of it when I was studying. The chapters on cryptography go beyond the typical Alice and Bob stuff you get in most books (Alice and Bob are still there) but they also get into examples of breaking cryptography and explaining how the attacks work and usually backing it up with the math involved. I really could say something good about every chapter in the book. Each chapter is laid out with a solid,
consistent road map, is full of quality readable content, and wraps it up with a "take home" message at the end.

The Table of Contents doesn't seem to be available on Amazon but if you are interested in the book, I'd recommend you take a look at it over at the InformIT site. It covers a lot of ground in its five parts of History, Security and the Modern Computing Landscape, Building Blocks for Secure Systems, Applications, and Emerging Tools. The book also comes with a huge list of references and a pretty good index for looking up topics.

I usually have my list of likes and dislikes for books. For this book I don't have any dislikes. The book is readable, well edited, a good font size, and I learned things from it. I've been actively recommending it to people at work, especially the guys working on their CISSP.

For More 5 Star Customer Reviews and Lowest Price: