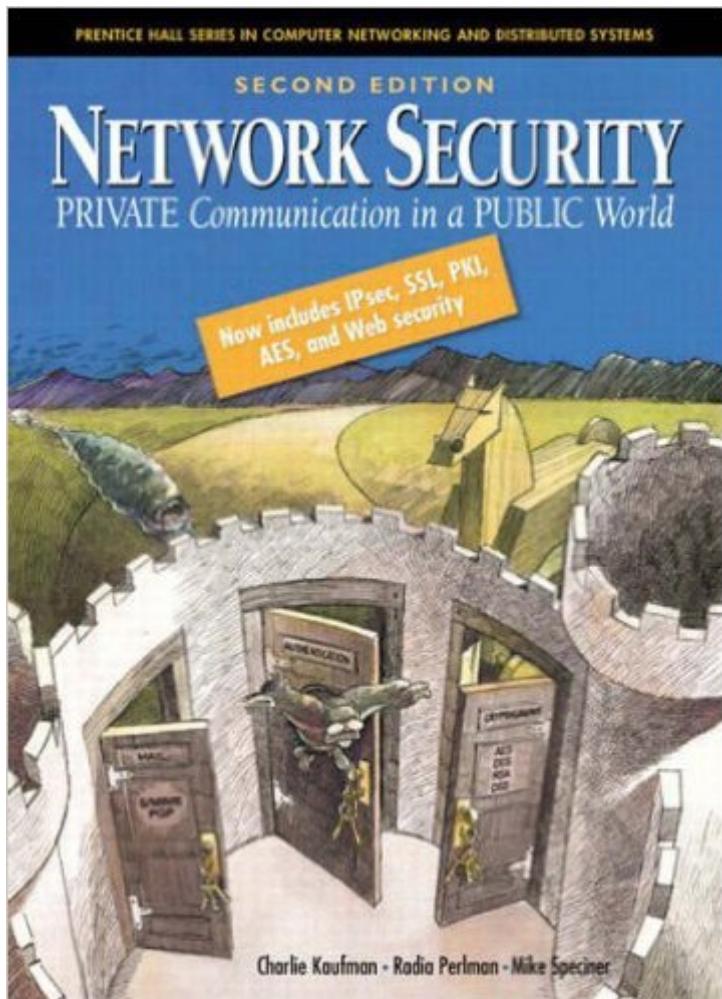


The book was found

# Network Security: Private Communication In A Public World (2nd Edition)



## Synopsis

The classic guide to network and Internet security has been thoroughly updated for today's latest security threats. In the second edition of Network Security, this most distinguished of author teams draws on hard-won experience to explain every facet of information security, from the basics to advanced cryptography and authentication; secure Web and email services; and emerging security standards. Highlights of the book's extensive new coverage include Advanced Encryption Standard (AES), IPsec, SSL, PKI Standards, and Web security.

## Book Information

Hardcover: 752 pages

Publisher: Prentice Hall; 2 edition (May 2, 2002)

Language: English

ISBN-10: 0130460192

ISBN-13: 978-0130460196

Product Dimensions: 7.3 x 1.1 x 9.5 inches

Shipping Weight: 2.9 pounds (View shipping rates and policies)

Average Customer Review: 4.3 out of 5 starsÂ  See all reviewsÂ  (30 customer reviews)

Best Sellers Rank: #223,874 in Books (See Top 100 in Books) #56 inÂ  Books > Computers & Technology > Certification > CompTIA #130 inÂ  Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks #200 inÂ  Books > Computers & Technology > Networking & Cloud Computing > Network Security

## Customer Reviews

I worked for 10 years in computer and network security, including many years as a cryptanalyst and a couple of years at a startup company. I now teach at San Jose State University, where I'm using this book as the primary textbook for a graduate class in computer security. The strengths of the book are its coverage of basic cryptography (chapters 2 thru 6), "security handshake pitfalls" (chapter 11) and "security folklore" (chapter 26). Chapter 11 alone is worth the (high) price of the book. It is absolutely the best introduction to the subtle issues that arise with network protocols you are likely to ever find. And Chapters 2 through 6 do a better job of covering cryptography (with particular emphasis on some of the not-so-obvious issues) than many books devoted solely to cryptography. And chapter 26 makes some nice points. One criticism I have is that--with few exceptions--the rest of the book does not come close to the standard achieved in the chapters mentioned above. The chapter on SSL/TLS is OK and the chapter on Kerberos is passable (if dull),

but the remaining chapters are relatively weak. Another criticism is that the title of the book is misleading. Outside of the cryptography chapters, the book is very narrowly focused on networking protocols. In my opinion, there is far more to network security than cryptography and protocols. Take a look at Ross Anderson's book, *Security Engineering*, to get a nice broad overview of security. Finally, the chapters related to IPsec are really poor. The author(s) seems to be so peeved with the standards committee for doing some stupid things that he/she/they do more carping than describing. In summary, I highly recommend chapters 2 thru 6, 11 and 26. But you'll need to look elsewhere if you want to learn about more than protocols and cryptography.

Who would have thought that a detailed technical book on network security would be fun to read? I wouldn't have, but this one is highly technical and also lots of fun to read. As the fundamental tenet of cryptography, instead of some abstract mathematical theorem about something or other being NP complete we get "If lots of smart people have failed to solve a problem, then it probably won't be solved (soon)". But don't get me wrong, this is not a content-free book for top management, it is highly technical, with long chapters on secret-key cryptography, hashes and message digests, public-key cryptography, number theory, authentication and much more. Unlike Bruce Schneier's book, *Applied Cryptography*, which is more like an encyclopedia than a book, this one is enjoyable to read while still carefully explaining state-of-the-art cryptographic protocols--not an easy feat to pull off. For anyone with a university degree in engineering, the sciences, or mathematics who wants to learn a lot about network security and be entertained while doing so, this book can't be beat.

I took this book along on a business trip with the expectation that it would work better than chamomile tea before bed -- instead it kept me up well into the night. It turns a, necessarily, tedious subject into compelling reading. A "must-read" and "must-have" reference for any person charged with managing a distributed computing environment.

The second edition of this witty and informative book on network security is even better than the first edition and is clearly the best book on the subject currently available. Secret and public key algorithms and protocols, message hashes, authentication, Kerberos, PKI, IPsec, SSL/TLS, and e-mail security are all explained at length. Chapter 26 on security folklore is a real gem. In security, the devil is in the details. For anyone planning to design a security system that is actually supposed to work, this chapter is must reading. The book is aimed at readers with a university degree in the sciences, engineering, or mathematics. If you want to learn everything there is to know about

network security, look no further.

Far and away the best book on network security and basic cryptography. This book is very well written and contains a number of simple examples to explain even the most complex theory. This is so far the only crypto book I've been able to read cover-to-cover more than once without pulling my hair out. It's not as deep on many topics as the Schneier or Stallings books. But if you buy one security/crypto book, buy this one.

This book has one of the most comprehensible explanations of network authentication protocols (including Kerberos V) that I've seen. The authors demonstrate intimate knowledge of the subject material, but they restrain themselves from simply performing a brain dump on the reader. Rather they include historical and personal footnotes that make the story witty and memorable, and give context to the topic at hand. Definitely add this book to your collection.

This book should appeal to both the beginner and the professional in network security. The book starts with very few assumptions about the existing security knowledge of the reader yet still manages to explain, in considerable depth, encryption and security protocols. Best of all, it's extremely well written, well illustrated and peppered with some good humour. A topic like this could be tedious to read, but this book isn't (although I have to admit, the chapter on Kerberos didn't quite spark me up the way the rest of it did!). The book has some excellent mathematical background for those who want to understand public key cryptography but aren't that familiar with modular exponentiation and the like. It also has detailed descriptions of a number of algorithms. In summary, an excellent all-rounder on this extremely important topic.

[Download to continue reading...](#)

Network Security: Private Communication in a Public World (2nd Edition) Network Security: Private Communications in a Public World (Radia Perlman Series in Computer Networking and Security)

Home Security: Top 10 Home Security Strategies to Protect Your House and Family Against Criminals and Break-ins (home security monitor, home security system diy, secure home network)

Monitor Your Home Network: A How-To Guide to Monitoring a Small, Private Network Extending Simple Network Management Protocol (SNMP) Beyond Network Management: A MIB Architecture for Network-Centric Services Network Security Assessment: Know Your Network CompTIA

Security+ Guide to Network Security Fundamentals Nessus Network Auditing: Jay Beale Open Source Security Series (Jay Beale's Open Source Security) Social Security: Time for a Life of

Leisure - The Guide of Secrets to Maximising Social Security Retirement Benefits and Planning Your Retirement (social ... disability, social security made simple) FBA: Beginner's Guide, Private Label & Launch Your Own Product (Private Label,How to Sell on ,Selling on ,Fulfillment By ,eBay,Etsy,Dropshipping) (Volume 1) Herbal Remedies: 30 Herbal Recipe Remedies From My Private Collection: Proven Herbal Recipes That Work! (Herbal Recipes Private Collection Book 1) Essential Oils: 50 Essential Oil Dog & Cat Recipes From My Essential Oil Private Collection: Proven Essential Oil Recipes That Work! (Essential Oil Pet Private Collection Book 1) Precontractual Liability in European Private Law (The Common Core of European Private Law) Free Books for Lovers of Private Letters, Diaries and Journals: Discover the Private Thoughts of Several Greats of the Past (Free Books For a Quick Download Book 4) The Manual to Online Public Records: The Researcher's Tool to Online Resources of Public Records and Public Information Descubra los secretos del network marketing: Redes de Mercadeo y Network marketing (Spanish Edition) How To Set Up a Home Network With Windows 7: Your Step-By-Step Guide To Setting Up a Home Network With Windows 7 Home Network Handbook: Learn how to set up your home network Network Programmability and Automation: Skills for the Next-Generation Network Engineer Effective TCP/IP Programming: 44 Tips to Improve Your Network Programs: 44 Tips to Improve Your Network Programs

[Dmca](#)