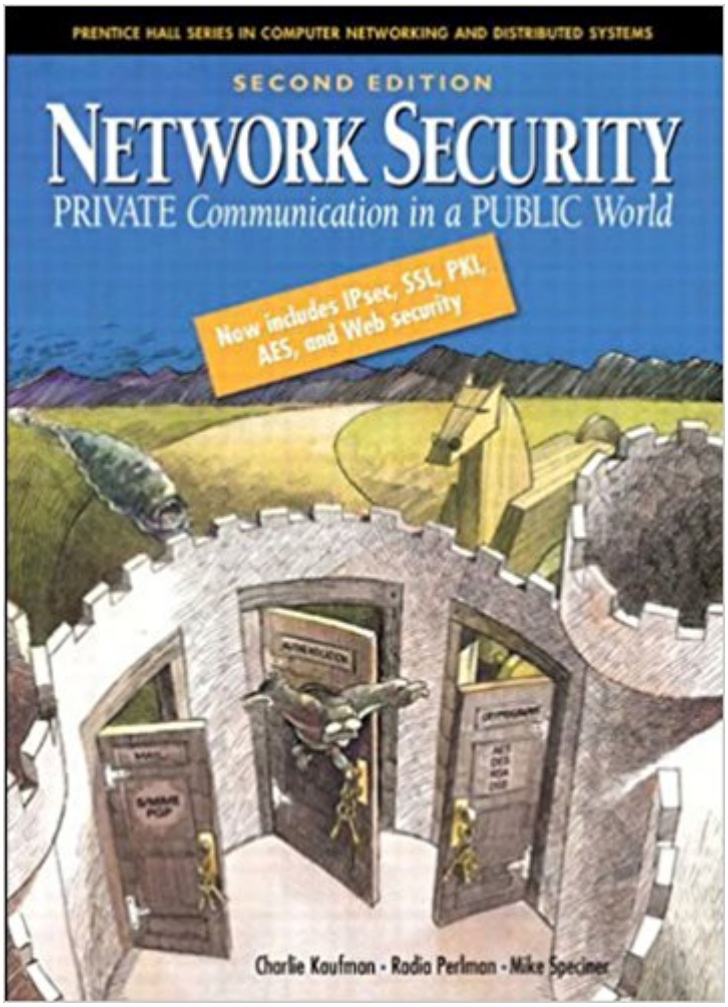
Network Security: Private Communications In A Public World (Radia Perlman Series In Computer Networking And Security)



Synopsis

The classic guide to network securityâ ”now fully updated!"Bob and Alice are back!" Â Widely regarded as the most comprehensive yet comprehensible guide to network security, the first edition of Network Security received critical acclaim for its lucid and witty explanations of the inner workings of network security protocols. In the second edition, this most distinguished of author teams draws on hard-won experience to explain the latest developments in this field that has become so critical to our global network-dependent society. Â Network Security, Second Edition brings together clear, insightful, and clever explanations of every key facet of information security, from the basics to advanced cryptography and authentication, secure Web and email services, and emerging security standards. Coverage includes: All-new discussions of the Advanced Encryption Standard (AES), IPsec, SSL, and Web security Cryptography: In-depth, exceptionally clear introductions to secret and public keys, hashes, message digests, and other crucial concepts Authentication: Proving identity across networks, common attacks against authentication systems, authenticating people, and avoiding the pitfalls of authentication handshakes Core Internet security standards: Kerberos 4/5, IPsec, SSL, PKIX, and X.509 Email security: Key elements of a secure email system-plus detailed coverage of PEM, S/MIME, and PGP Web security: Security issues associated with URLs, HTTP, HTML, and cookies Security implementations in diverse platforms, including Windows, NetWare, and Lotus Notes The authors go far beyond documenting standards and technology: They contrast competing schemes, explain strengths and weaknesses, and identify the crucial errors most likely to compromise secure systems. Network Security will appeal to a wide range of professionals, from those who design or evaluate security systems to system administrators and programmers who want a better understanding of this important field. It can also be used as a textbook at the graduate or advanced undergraduate level.

Book Information

File Size: 11089 KB

Print Length: 752 pages

Simultaneous Device Usage: Up to 5 simultaneous devices, per publisher limits

Publisher: Prentice Hall; 2 edition (April 22, 2002)

Publication Date: April 22, 2002

Sold by:Â Digital Services LLC

Language: English

ASIN: B001ADIWNI

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting: Enabled

Best Sellers Rank: #593,266 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #67 inÂ Books > Computers & Technology > Programming > Languages & Tools > Perl #223 inÂ Books > Computers & Technology > Certification > CompTIA #618 inÂ Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks

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 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 encylopedia 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. Its 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.

Networking Academy Program) (Cisco Networking Academy Program Series) The Linux TCP/IP Stack: Networking for Embedded Systems (Networking Series) Introduction to Network Security (Chapman & Hall/CRC Computer and Information Science Series) Millimeter Wave Wireless Communications (Prentice Hall Communications Engineering and Emerging Technologies Series from Ted Rappaport) Nessus Network Auditing: Jay Beale Open Source Security Series (Jay Beale's Open Source Security) Wireless Home Networking Simplified (Networking Technology)