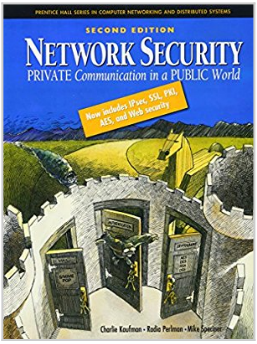

Network Security: Private Communication in a Public World (2nd Edition)

By Charlie Kaufman, Radia Perlman, Mike Speciner

Network Security: Private Communication in a Public World (2nd Edition)
By Charlie Kaufman, Radia Perlman, Mike Speciner

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.

Network Security: Private Communication in a Public World (2nd Edition)

By Charlie Kaufman, Radia Perlman, Mike Speciner

Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner

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.

Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner Bibliography

- Sales Rank: #329678 in Books
- Published on: 2002-05-02
- Original language: English
- Number of items: 1
- Dimensions: 9.53" h x 1.13" w x 7.30" l, 2.71 pounds
- Binding: Hardcover
- 752 pages

Editorial Review

From Library Journal
The authors offer a meaty survey of computer security in three broad sections. Opening with cryptography, they describe the meaning of keys and algorithms-a difficult task, requiring a bit of math that may frighten novices. The second part deals with authentication, or proof of identity on a network. The benefits and pitfalls of different schemes are discussed in a lively and engaging way and are spiced with appropriate quotes throughout. In the final section, E-mail-for some the most chaotic risk of all-is examined. Terms are defined well even for beginners, and exercises at the end of each chapter allow you to test your comprehension of a given set of concepts. But the authors use a notation system (discussed in the introduction) that you'll need to understand to follow some of the examples and arguments. Clearly, this thought-provoking book was designed for serious students of computers and their networks, but even a newbie will find entertaining and useful tidbits.

From the Publisher
A comprehensive yet comprehensible and witty guide to the latest advances in computer network security protocols. In this book the authors go beyond documenting standards and technology; they contrast competing schemes, explain weaknesses and strengths, and describe common mistakes people make when intending to design secure systems.

From the Inside Flap
It was a dark and stormy night. Somewhere in the distance a dog howled. A shiny object caught Alice's eye. A diamond cufflink! Only one person in the household could afford diamond cufflinks! So it was the butler, after all! Alice had to warn Bob. But how could she get a message to him without alerting the butler? If she phoned Bob, the butler might listen on an extension. If she sent a carrier pigeon out the window with the message taped to its feet, how would Bob know it was Alice that was sending the message and not Trudy attempting to frame the butler because he spurned her advances? That's what this book is about. Not much character development for Alice and Bob, we're afraid, nor do we really get to know the butler. But we do discuss how to communicate securely over an insecure medium.

What do we mean by communicating securely? Alice should be able to send a message to Bob that only Bob can understand, even though Alice can't avoid having others see what she sends. When Bob receives a message, he should be able to know for certain that it was Alice who sent the message, and that nobody tampered with the contents of the message in the time between when Alice launched the message and Bob received it.

What do we mean by an insecure medium? Well, in some dictionary or another, under the definition of "insecure medium" should be a picture of the Internet. The world is evolving towards interconnecting every computer, and people talk about connecting household appliances as well, all into some wonderful global internetwork. How wonderful! You'd be able to send electronic mail to anyone in the world.

You'd also be able to control your nuclear power plant with simple commands sent across the network while you were vacationing in Fiji. Or sunny Libya. Or historic Iraq. Inside the network the world is scary. There are links that eavesdroppers can listen in on. Information needs to be forwarded through packet switches, and these switches can be reprogrammed to listen to or modify data in transit. The situation might seem hopeless, but we may yet be saved by the magic of mathematics, and in particular cryptography, which can take a message and transform it into a bunch of numbers known as ciphertext. The ciphertext is unintelligible gibberish except to someone who knows the secret to reversing the transformation. Cryptography allows us to disguise our data so that eavesdroppers gain no information from listening to the information as transmitted.

Cryptography also allows us to create an unforgeable message and protect it from being modified in transit. One method of accomplishing this is with a digital signature, a number associated with a message and its sender that can be verified as authentic by others, but can only be generated by the sender. This should seem astonishing. How can there be a number which you can verify but not generate? A person's handwritten signature can (more or less) only be generated by that person, though it can be verified by others. But it would seem as if a number shouldn't be hard to generate, especially if it can be verified. Theoretically you could generate someone's signature by trying lots of numbers and testing each one until one passed the verification test. But with the size of the numbers used, it would take too much compute time (for instance, several universe lifetimes) to generate the signature that way. So a digital signature has the same property as a handwritten signature, in that it can only be generated by one person. But a digital signature does more than a handwritten signature.

Since the digital signature depends on the contents of the message, if someone alters the message the signature will no longer be correct and the tampering will be detected. This will all become clear if you read Chapter 2 Introduction to Cryptography.

Cryptography is a major theme in this book, not because cryptography is intrinsically interesting (which it is), but because the security features people want in a computer network can best be provided through cryptography.

1.1. Roadmap to the Book The book is divided into three main sections.

Cryptography.

Chapter 2 Introduction to Cryptography is the only part of the cryptography section of the book essential for understanding the rest of the book, since it explains the generic properties of secret key, message digest, and public key algorithms, and how each is used. We've tried our best to make the descriptions of the actual cryptographic algorithms nonthreatening yet thorough, and to give intuition into why they work. It's intended to be readable by anyone, not just graduate students in mathematics. Never once do we use the term lemma. We do hope you read.

Chapter 3 Secret Key Cryptography, Chapter 4 Hashes and Message Digests, and Chapter 5 Public Key Algorithms which give the details of the popular standards, but it's also OK to skip them and save them for later, or just for reference. For you math types who would have noticed that we skipped a number if we didn't mention it, Chapter 6 Number Theory gives a deeper treatment of the mathematics behind the cryptography.

Authentication.

Chapter 7 Authentication Systems introduces the general issues involved in proving your identity across a network.

Chapter 8 Authentication of People deals with the special circumstances when the device proving its identity is a human being.

Chapter 9 Security Handshake Pitfalls deals with the details of authentication handshakes. There are many security flaws that keep getting designed into protocols. This chapter attempts to describe variations of authentication handshakes and their relative security and performance strengths. We end the chapter with a checklist of security attacks, so that someone designing a protocol can specifically check their protocol for these flaws.

Chapter 10 Kerberos V4 and Chapter 11 Kerberos V5 describe the details of those authentication systems. Secure electronic mail. Chapter 12 Electronic Mail Security describes the various types of security features one might want, and how they might be provided. Chapter 13 Privacy Enhanced Mail (PEM), Chapter 14 PGP (Pretty Good Privacy), and Chapter 15 X.400 describe three mail standards which are compared in Chapter 16 A Comparison of PEM, PGP, and X.400. There are two chapters that aren't in any of the three main sections. The first chapter (the one you're reading now) gives a whirlwind tour of computer networking and computer security to set the stage for the main focus of the book-computer network security. The final chapter, Chapter 17 More Security Systems, describes a variety of security systems, including Novell NetWare (Versions 3 and 4), Lotus Notes, DCE, KryptoKnight/NetSP, Clipper, SNMP, DASS/SPX, and sabotage-proof routing protocols.

1.2. What type of book is this?

We believe the reason most computer science is hard to understand is because of jargon and irrelevant details. When people work with something long enough they invent their own language, come up with some meta-architectural framework or other, and forget that the rest of the world doesn't talk or think that way. We intend this book to be reader-friendly. We try to extract the concepts and ignore the meta-architectural framework, since whatever a meta-architectural framework is, it's irrelevant to what something does and how it works.

We believe someone who is a relative novice to the field ought to be able to read this book. But readability doesn't mean "lack of technical depth". We try to go beyond the information one might find in specifications. The goal is not just to describe exactly how the various standards and de facto standards work, but to explain why they are the way they are, why some protocols designed for similar purposes are different, and the implications of the design decisions. Sometimes engineering tradeoffs were made.

Sometimes the designers could have made better choices (they are human after all), in which case we explain how the protocol could have been better. This analysis should make it easier to understand the current protocols, and aid in design of future protocols.

The primary audience for this book is engineers, especially those who might need to evaluate the security of or add security features to a distributed system, but the book is also intended to be useable as a textbook, either on the advanced undergraduate or graduate level. Most of the chapters have homework problems at the end.

1.3. Terminology

Any field with science in its name isn't.

Tony Lauck

Computer science is filled with ill-defined terminology used by different authors in conflicting ways, often by the same author in conflicting ways. We apologize in advance for probably being guilty sometimes ourselves. Some people take terminology very seriously, and once they start to use a certain word in a certain way, are extremely offended if the rest of the world does not follow.

When I use a word, it means j

Users Review

From reader reviews:

Sharon Bedgood:

This Network Security: Private Communication in a Public World (2nd Edition) book is not ordinary book, you have after that it the world is in your hands. The benefit you have by reading this book is actually information inside this publication incredible fresh, you will get details which is getting deeper anyone read a lot of information you will get. That Network Security: Private Communication in a Public World (2nd Edition) without we realize teach the one who reading through it become critical in pondering and analyzing. Don't always be worry Network Security: Private Communication in a Public World (2nd Edition) can bring if you are and not make your bag space or bookshelves' become full because you can have it with your lovely laptop even mobile phone. This Network Security: Private Communication in a Public World (2nd Edition) having great arrangement in word and layout, so you will not truly feel uninterested in reading.

Ann Mickey:

Information is provisions for those to get better life, information these days can get by anyone in everywhere. The information can be a knowledge or any news even an issue. What people must be consider while those information which is within the former life are challenging be find than now is taking seriously which one is appropriate to believe or which one the particular resource are convinced. If you find the unstable resource then you obtain it as your main information it will have huge disadvantage for you. All those possibilities will not happen within you if you take Network Security: Private Communication in a Public World (2nd Edition) as the daily resource information.

Miguel Penix:

Reading can called mind hangout, why? Because if you are reading a book mainly book entitled Network Security: Private Communication in a Public World (2nd Edition) your mind will drift away trough every dimension, wandering in each and every aspect that maybe unfamiliar for but surely will become your mind friends. Imaging just about every word written in a guide then become one web form conclusion and explanation this maybe you never get before. The Network Security: Private Communication in a Public World (2nd Edition) giving you yet another experience more than blown away your brain but also giving you useful info for your better life on this era. So now let us show you the relaxing pattern is your body and mind will probably be pleased when you are finished reading it, like winning a. Do you want to try this extraordinary spending spare time activity?

Sabrina Crockett:

This Network Security: Private Communication in a Public World (2nd Edition) is new way for you who has curiosity to look for some information as it relief your hunger of information. Getting deeper you on it getting knowledge more you know otherwise you who still having small amount of digest in reading this Network Security: Private Communication in a Public World (2nd Edition) can be the light food in your case because the information inside this book is easy to get simply by anyone. These books produce itself in the form which is reachable by anyone, yeah I mean in the e-book application form. People who think that in publication form make them feel drowsy even dizzy this book is the answer. So there is absolutely no in reading a publication especially this one. You can find what you are looking for. It should be here for anyone. So , don't miss the item! Just read this e-book type for your better life in addition to knowledge.

Download and Read Online Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner #GIEHX6OP27J

Read Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner for online ebook

Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner books to read online.

Online Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner ebook PDF download

Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner Doc

Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner Mobipocket

Network Security: Private Communication in a Public World (2nd Edition) By Charlie Kaufman, Radia Perlman, Mike Speciner EPub