

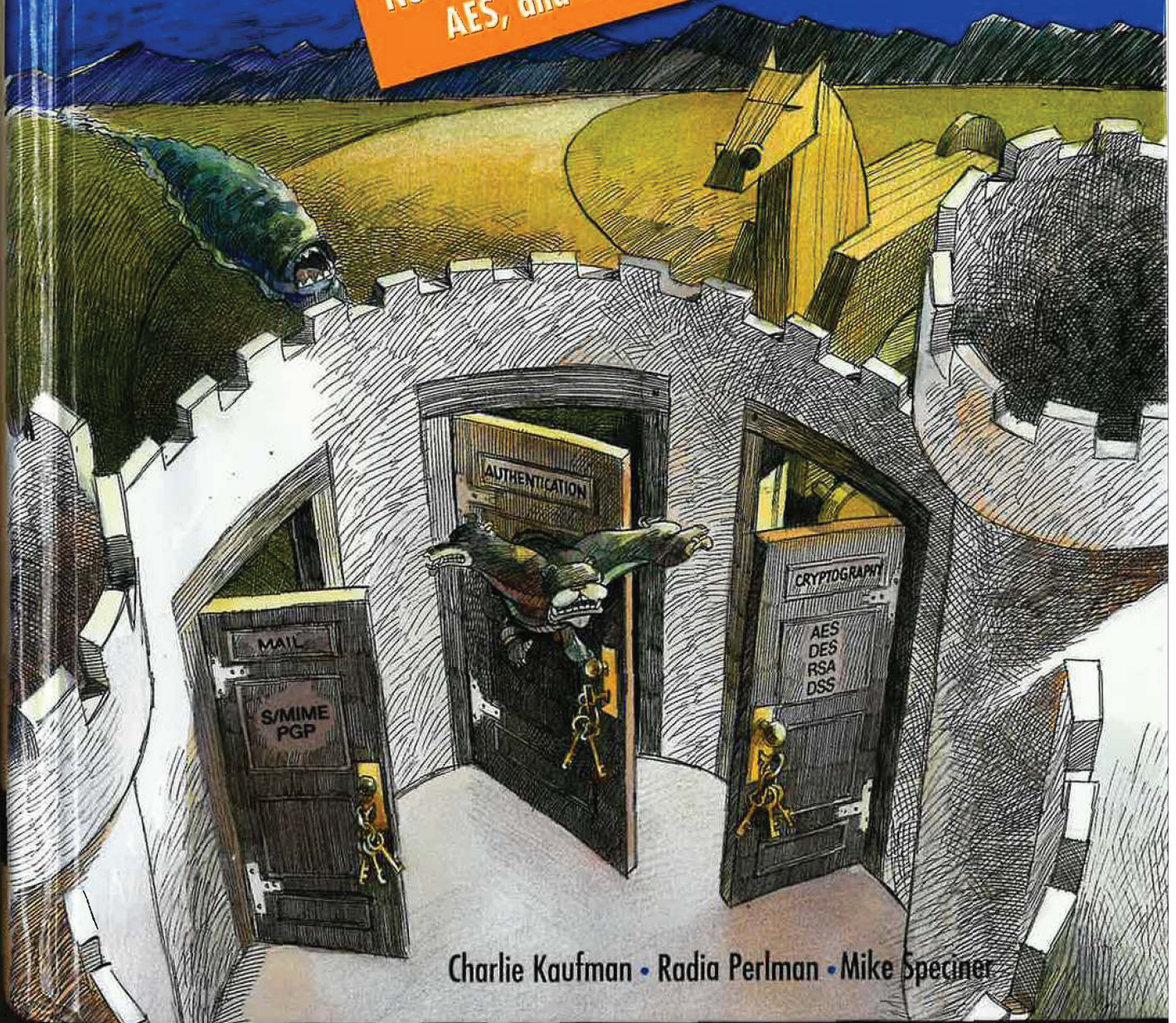
PRENTICE HALL SERIES IN COMPUTER NETWORKING AND DISTRIBUTED SYSTEMS

SECOND EDITION

NETWORK SECURITY

PRIVATE *Communication* in a PUBLIC World

Now includes IPsec, SSL, PKI,
AES, and Web security



Charlie Kaufman • Radia Perlman • Mike Speciner

NETWORK SECURITY

PRIVATE Communication in a PUBLIC World



The Radia Perlman Series in
Computer Networking and Security
Radia Perlman, Series Editor

Dusseault	<i>WebDAV: Next-Generation Collaborative Web Authoring</i>
Hellberg, Boyes, and Greene	<i>Broadband Network Architectures: Designing and Deploying Triple Play Services</i>
Kaufman, Perlman, and Speciner	<i>Network Security: Private Communication in a Public World, Second Edition</i>
Liska	<i>The Practice of Network Security: Deployment Strategies for Production Environments</i>
Mancill	<i>Linux Routers: A Primer for Network Administrators, Second Edition</i>
Maufer	<i>A Field Guide to Wireless LANs for Administrators and Power Users</i>
Mirkovic, Dietrich, Dittrich, and Reiher	<i>Internet Denial of Service: Attack and Defense Mechanisms</i>
Skoudis with Liston	<i>Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, Second Edition</i>
Skoudis with Zeltser	<i>Malware: Fighting Malicious Code</i>
Solomon	<i>Mobile IP: The Internet Unplugged</i>
Syme and Goldie	<i>Optimizing Network Performance with Content Switching: Server, Firewall, and Cache Load Balancing</i>
Tomsu and Schmutzter	<i>Next Generation Optical Networks</i>

NETWORK SECURITY

PRIVATE Communication in a PUBLIC World

CHARLIE KAUFMAN • RADIA PERLMAN • MIKE SPECINER



Prentice Hall PTR
Upper Saddle River, NJ 07458
www.phptr.com

Editorial/Production Supervision: Faye Gemmellaro
Executive Editor: Mary Franz
Editorial Assistant: Noreen Regina
Marketing Manager: Dan DePasquale
Manufacturing Buyer: Maura Zaldivar
Cover Illustration: Tom Post
Cover Design Director: Jerry Votta

© 2002 by Prentice Hall PTR
A division of Pearson Education, Inc.
Upper Saddle River, New Jersey 07458



Prentice Hall books are widely used by corporations and government agencies for training, marketing, and resale.

For information regarding corporate and government bulk discounts, please contact: Corporate and Government Sales, (800) 382-3419, or corpsales@pearsontechgroup.com

All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher. All trademarks mentioned herein are the properties of their respective owners.

ISBN 0-13-046019-2

Text printed in the United States on recycled paper at Courier Westford in Westford, Massachusetts.
11th Printing November 2007

Pearson Education Ltd.
Pearson Education Australia PTY, Ltd.
Pearson Education Singapore, Pte. Ltd.
Pearson Education North Asia Ltd.
Pearson Education Canada, Ltd.
Pearson Educación de México, S.A. de C.V.
Pearson Education—Japan
Pearson Education Malaysia, Pte. Ltd.

Si spy net work, big fedjaw iog link kyxogy

2.1.3 Secret Codes

We use the terms *secret code* and *cipher* interchangeably to mean any method of encrypting data. Some people draw a subtle distinction between these terms that we don't find useful.

The earliest documented cipher is attributed to Julius Caesar. The way the **Caesar cipher** would work if the message were in English is as follows. Substitute for each letter of the message, the letter which is 3 letters later in the alphabet (and wrap around to A from Z). Thus an A would become a D, and so forth. For instance, DOZEN would become GRCHO. Once you figure out what's going on, it is very easy to read messages encrypted this way (unless, of course, the original message was in Greek).

A slight enhancement to the Caesar cipher was distributed as a premium with Ovaltine in the 1940s as *Captain Midnight Secret Decoder rings*. (There were times when this might have been a violation of export controls for distributing cryptographic hardware!) The variant is to pick a secret number n between 1 and 25, instead of always using 3. Substitute for each letter of the message, the letter which is n higher (and wrap around to A from Z of course). Thus if the secret number was 1, an A would become a B, and so forth. For instance HAL would become IBM. If the secret number was 25, then IBM would become HAL. Regardless of the value of n , since there are only 26 possible letters to try, it is still very easy to break this cipher if you know it's being used and you can recognize a message once it's decrypted.

The next type of cryptographic system developed is known as a **monoalphabetic cipher**, which consists of an arbitrary mapping of one letter to another letter. There are $26!$ possible pairings of letters, which is approximately 4×10^{26} . [Remember, $n!$, which reads " n factorial", means $n(n-1)(n-2) \cdots 1$.] This might seem secure, because to try all possibilities, it took 1 microsecond to try each one, would take about 10 trillion years. However, by statistical analysis of language (knowing that certain letters and letter combinations are more common than others), it turns out to be fairly easy to break. For instance, many daily newspapers have a daily cryptogram, which is a monoalphabetic cipher, and can be broken by people who enjoy that sort of thing during their subway ride to work. An example is

Cf lq'xs xsnyclm n eqxqgsy lqul qf wdcq eqqh, erl lqrx qgt iqu!

Computers have made much more complex cryptographic schemes both necessary and possible. Necessary because computers can try keys at a rate that would exhaust an army of clerks; and possible because computers can execute the complex algorithms quickly and without errors.

2.2 BREAKING AN ENCRYPTION SCHEME

What do we mean when we speak of a bad guy Fred *breaking* an encryption scheme? The three basic attacks are known as **ciphertext only**, **known plaintext**, and **chosen plaintext**.

2.2.1 Ciphertext Only

In a ciphertext only attack, Fred has seen (and presumably stored) some ciphertext that he can analyze at leisure. Typically it is not difficult for a bad guy to obtain ciphertext. (If a bad guy can't access the encrypted data, then there would have been no need to encrypt the data in the first place!)

How can Fred figure out the plaintext if all he can see is the ciphertext? One possible strategy is to search through all the keys. Fred tries the decrypt operation with each key in turn. It is essential for this attack that Fred be able to recognize when he has succeeded. For instance, if the message was English text, then it is highly unlikely that a decryption operation with an incorrect key could produce something that looked like intelligible text. Because it is important for Fred to be able to differentiate plaintext from gibberish, this attack is sometimes known as a **recognizable plaintext** attack.

It is also essential that Fred have enough ciphertext. For instance, using the example of a monoalphabetic cipher, if the only ciphertext available to Fred were XYZ, then there is not enough information. There are many possible letter substitutions that would lead to a legal three-letter English word. There is no way for Fred to know whether the plaintext corresponding to XYZ is THE or CAT or HAT. As a matter of fact, in the following sentence, any of the words could be the plaintext for XYZ:

The hot cat was sad but you may now sit and use her big red pen.

[Don't worry—we've found a lovely sanatorium for the coauthor who wrote that.

—the other coauthors]

Often it isn't necessary to search through a lot of keys. For instance, the authentication scheme Kerberos (see §13.4 *Logging Into the Network*) assigns to user Alice a DES key derived from Alice's password according to a straightforward, published algorithm. If Alice chooses her password unwisely (say a word in the dictionary), then Fred does not need to search through all 2^{26} possible DES keys—instead he only needs to try the derived keys of the 10000 or so common English words.

A cryptographic algorithm has to be secure against a ciphertext only attack because of the accessibility of the ciphertext to cryptanalysts. But in many cases cryptanalysts can obtain additional information, so it is important to design cryptographic systems to withstand the next two attacks as well.



NETWORK SECURITY

PRIVATE Communication in a PUBLIC World

SECOND EDITION

The classic guide to network security—now fully updated!

"Bob and Alice are back!"

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.

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.

About the Authors

CHARLIE KAUFMAN is a Distinguished Engineer at IBM, where he is Chief Security Architect for Lotus Notes and Domino™. Previously, he was the Network Security Architect at Digital Equipment Corporation. He chaired the IETF's Web Transaction Security working group and currently serves on the IAB, the IETF's architecture board. RADIA PERLMAN, Distinguished Engineer at Sun Microsystems, is known worldwide for her contributions to bridging (spanning tree algorithm) and routing (link state routing) as well as security (sabotage-proof networks). Perlman is the author of *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*, and she is one of the 25 people whose work has most influenced the networking industry, according to *Data Communications Magazine*. MIKE SPECINER is a Senior Consulting Engineer at ThinkEngine Networks and is a recognized expert in mathematical algorithms and operating systems. Combined, this author team holds close to 100 patents.

PRENTICE HALL
Upper Saddle River, NJ 07458
www.phptr.com

\$69.99 U.S.
\$79.99 Canada

ISBN-13: 978-0-13-046019-6
ISBN-10: 0-13-046019-2



9 780130 460196

