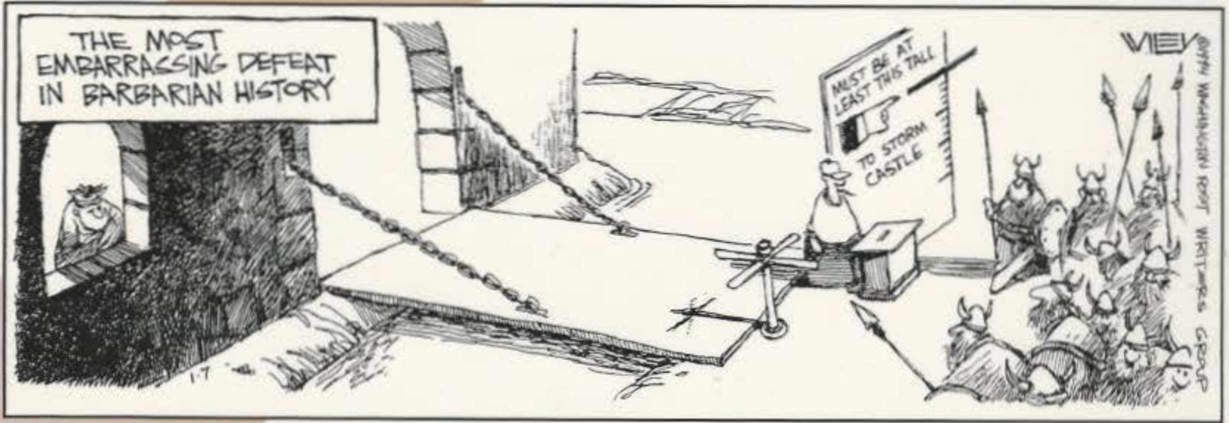
Firewalls and Internet Security

Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin


THE MOST EMBARRASSING DEFEAT IN BARBARIAN HISTORY
MUST BE AT LEAST THIS TALL
TO STORM CASTLE
VIEY
WASHINGTON POST WRITERS GROUP
1-7

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

RISC/os is a trademark of MIPS Computer Corporation. SunOS is a trademark of Sun Microsystems. RSAREF is a trademark of RSA Data Security, Inc. SPARCstation is a trademark of SPARC International, Inc. PostScript is a registered trademark of Adobe Systems, Inc. Ethernet is a trademark of Xerox Corporation. The X Window System and Kerberos are trademarks of the Massachusetts Institute of Technology. Datakit VCS is a registered trademark of AT&T. UNIX is a technology trademark of X/Open Company, Ltd. S/Key is a trademark of Bellcore.

The publisher offers discounts on this book when ordered in quantity for special sales. For more information please contact:

Corporate & Professional Publishing Group
Addison-Wesley Publishing Company
One Jacob Way
Reading, Massachusetts 01867

Library of Congress Cataloging-in-Publication Data
Cheswick, William R.
Firewalls and Internet Security : repelling the wily hacker /
William R. Cheswick, Steven M. Bellovin.
p. cm.
Includes bibliographical references and index.
ISBN 0-201-63357-4
1. Internet (Computer networks) 2. Computer networks--Security
measures. I. Bellovin, Steven M. II. Title.
TK5105.875.I57C44 1994
005.8--dc20 94-10747
CIP

This book was typeset by the authors in 10-point Times-Roman, Michael Urban's Tengwar font, and Joel Hoffman's Hclassic Hebrew font, using LaTeX, a fair amount of hacking, and a plethora of .sty files snarfed from the internet.

ISBN 0-201-63357-4

Text printed on recycled paper.
3 4 5 6 7 8 9 10-CRW-97969594
Third Printing July 1994

13

Secure Communications over Insecure Networks

13.1 An Introduction to Cryptography

It is sometimes necessary to communicate over insecure links without exposing one's systems. Cryptography—the art of secret writing—is the usual answer.

The most common use of cryptography is, of course, secrecy. A suitably encrypted packet is incomprehensible to attackers. In the context of the Internet, and in particular when protecting wide-area communications, secrecy is often secondary. Instead, we are often interested in the implied authentication provided by cryptography. That is, a packet that is not encrypted with the proper key will not decrypt to anything sensible. This considerably limits the ability of an attacker to inject false messages.

Before we discuss some actual uses for cryptography, we present a brief overview of the subject and build our cryptographic toolkit. It is of necessity sketchy; cryptography is a complex subject that cannot be covered fully here. Readers desiring a more complete treatment should consult any of a number of standard references, such as [Kahn, 1967], [Denning, 1982], [Davies and Price, 1989], or [Schneier, 1994].

We next discuss the Kerberos Authentication System, developed at MIT. Apart from its own likely utility—the code is widely available and Kerberos is being considered for adoption as an Internet standard—it makes an excellent case study, since it is a real design, not vaporware, and has been the subject of many papers and talks and a fair amount of experience.

Selecting an encryption system is comparatively easy; actually using one is less so. There are myriad choices to be made about exactly where and how it should be installed, with trade-offs in terms of economy, granularity of protection, and impact on existing system. Accordingly, Sections 13.3, 13.4, and 13.5 discuss the trade-offs and present some security systems in use today.

In the discussion that follows, we assume that the *cryptosystems* involved—that is, the cryptographic algorithm and the protocols that use it, but not necessarily the particular implementation—

are sufficiently strong, i.e., we discount almost completely the possibility of cryptanalytic attack. Cryptographic attacks are orthogonal to the types of attacks we describe elsewhere. (Strictly speaking, there are some other dangers here. While the cryptosystems themselves may be perfect, there are often dangers lurking in the cryptographic protocols used to control the encryption. See, for example, [Moore, 1988]. Some examples of this phenomenon are discussed in Section 13.2 and in the box on page 213.) A site facing a serious threat from a highly competent foe would need to deploy defenses against both cryptographic attacks and the more conventional attacks described elsewhere.

One more word of caution: in some countries the export, import, or even use of any form of cryptography may be regulated by the government. Additionally, many useful cryptosystems are protected by a variety of patents. It may be wise to seek competent legal advice.

13.1.1 Notation

Modern cryptosystems consist of an operation that maps a *plaintext* (P) and a *key* (K) to a *ciphertext* (C). We write this as

$$C \leftarrow K[P].$$

Usually, there is an inverse operation that maps a ciphertext and key K^{-1} to the original plaintext:

$$P \leftarrow K^{-1}[C].$$

The attacker's usual goal is to recover the keys K and K^{-1}. For a strong cipher, it should be impossible to recover them by any means short of trying all possible values. This should hold true no matter how much ciphertext and plaintext the enemy has captured.

It is generally accepted that one must assume that attackers are familiar with the encryption function; the security of the cryptosystem relies entirely on the secrecy of the keys. Protecting them is therefore of the greatest importance. In general, the more a key is used, the more vulnerable it is to compromise. Accordingly, separate keys, called *session keys*, are used for each job. Distributing session keys is a complex matter, about which we will say little; let it suffice to say that session keys are generally transmitted encrypted by a *master key*, and often come from a centralized *Key Distribution Center*.

13.1.2 Private-Key Cryptography

In conventional cryptosystems—sometimes known as secret-key or symmetric cryptosystems—there is only one key. That is,

$$K = K^{-1};$$

writing out K^{-1} is simply a notational convenience to indicate decryption. There are many different types of symmetric cryptosystems; here, we will concentrate on the *Data Encryption Standard* (*encryption, DES*) [NBS, 1977] and its standard modes of operation [NBS, 1980]. Note, though, that most things we say are applicable to other modern cipher systems, with the obvious exception of such parameters as encryption block size and key size.

Types of Attacks

Cryptographic systems are subject to a variety of attacks. It is impossible to give a complete taxonomy—but we discuss a few of the more important ones.

Cryptanalysis: Cryptanalysis is the science—or art—of reading encrypted traffic without prior knowledge of the key.

"Practical" cryptanalysis: "Practical" cryptanalysis is, in a sense, the converse. It refers to stealing a key, by any means necessary.

Known-plaintext attack: Often, an enemy will have one or more pairs of ciphertext and a known plaintext encrypted with the same key. These pairs, known as *cribs*, can be used to aid in cryptanalysis.

Chosen-plaintext: Attacks where you trick the enemy into encrypting your messages with the enemy's key. For example, if your opponent encrypts traffic to and from a file server, you can mail that person a message and watch the encrypted copy being delivered.

Exhaustive search: Trying every possible key. Also known as *brute force*

Passive eavesdropping: A passive attacker simply listens to traffic flowing by.

Active attack: In an active attack, the enemy can insert messages and—in some variants—delete or modify legitimate messages.

Man-in-the-middle: The enemy sits between you and the party with whom you wish to communicate, and impersonates each of you to the other.

Replay: Take a legitimate message and reinject it into the network at a later time.

Cut-and-paste: Given two messages encrypted with the same key, it is sometimes possible to combine portions of two or more messages to produce a new message. You may not know what it says, but you can use it to trick your enemy into doing something for you.

Time-resetting: In protocols that use the current time, try to confuse you about what the correct time is.

Birthday attack: An attack on hash functions where the goal is to find any two messages that yield the same value. If exhaustive search takes 2^n steps, a birthday attack would take only $2^{n/2}$ tries.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE