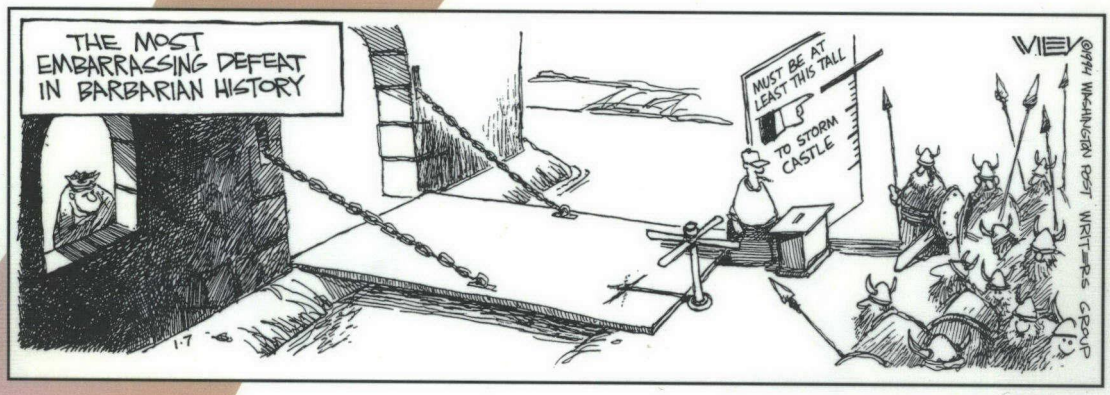
Firewalls and Internet Security

Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin



ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

IPR2023-00968
International Business Machines Corporation v. Digital Doors, Inc.
IBM's Exhibit 1025
Ex. 1025, Page 1

Firewalls and Internet Security

Cheswick
Bellovin

Addison
Wesley

63357

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

Copyright © 1994 by AT&T Bell Laboratories, Inc.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior consent of the publisher. Printed in the United States of America. Published simultaneously in Canada.

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

definition of acceptable input patterns. We have seen far too many programs crash when handed garbage that the author hadn't anticipated. An automated "syntax error" message is a much better outcome.

The next rule is *least privilege*. Do not give network daemons any more power than they need. Very few need to run as the superuser, especially on firewall machines. For example, some portion of a local mail delivery package needs special privileges, so that it can copy a message sent by one user into another's mailbox; a gateway's mailer, though, does nothing of the sort. Rather, it copies mail from one network port to another, and that is a horse of a different color entirely.

Even servers that *seem* to need privileges often don't, if structured properly. The UNIX FTP server, to cite one glaring example, uses *root* privileges to permit user logins and to be able to bind to port 20 for the data channel. The latter cannot be avoided completely—the protocol does, after all, require it—but there are several possible designs that would let a small, simple, and more obviously correct privileged program do that and only that. Similarly, the login problem could be handled by a front end that processes only the `USER` and `PASS` commands, sets up the proper environment, gives up its privileges, and then executes the *unprivileged* program that speaks the rest of the protocol. (See our design in Section 4.5.5.)

One final note: don't sacrifice correctness, and verifiable correctness at that, in search of "efficiency." If you think a program needs to be complex, tricky, privileged, or all of the above to save a few nanoseconds, you've probably designed it wrong. Besides, hardware is getting cheaper and faster; your time for cleaning up intrusions, and your users' time for putting up with loss of service, is expensive and getting more so.

9.4 Authentication Failures

Many of the attacks we have described derive from a failure of authentication mechanisms. By this we mean that a mechanism that might have sufficed has somehow been defeated. For example, source-address validation can work, under certain circumstances (i.e., if a firewall screens out forgeries), but hackers can use the *portmapper* to retransmit certain requests. In that case, the ultimate server has been fooled; the message as it appeared to them was indeed of local origin, but its ultimate provenance was elsewhere.

Address-based authentication also fails if the source machine is not trustworthy. PCs are the obvious example. A mechanism that was devised in the days when timesharing computers were the norm no longer works when individuals can control their own machines. Of course, the usual alternative—ordinary passwords—is no bargain either on a net filled with personal machines; password-sniffing is entirely too easy.

Sometimes authentication fails because the protocol doesn't carry the right information. Neither TCP nor IP ever identifies the sending user (if indeed such a concept exists on some hosts); protocols such as X11 and *rsh* must either obtain it on their own or do without (and if they can obtain it, they have to have some secure way of passing it over the network).

Even cryptographic authentication of the source host or user may not suffice. As mentioned earlier, a compromised host cannot do secure encryption.

The X11 protocol has more than its share of vulnerabilities. The normal mode of application

Networking/Security

Firewalls and Internet Security

"I wish that Cheswick and Bellovin had written this six years ago. I could have nailed down my system and avoided chasing a spy around the world."
—Cliff Stoll, author of *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*

As a user of the Internet, you are fortunate to be tied into the world's greatest communication and information exchange — but not without a price. As a result of this connection, your computer, your organization's network, and everywhere that network reaches are all vulnerable to potentially disastrous infiltration by hackers.

Written by the AT&T Bell Labs researchers who tracked the infamous "Berferd" hacker and also built the firewall gateway at Bell Labs, *Firewalls and Internet Security* gives you invaluable advice and practical tools for protecting your organization's computers from the very real threat of a hacker attack through the Internet. You will learn how to plan and execute a security strategy that will thwart the most determined and sophisticated of hackers — while still allowing you easy access to Internet services.

In particular, the authors show you a step-by-step plan for setting up a "firewall" gateway — a dedicated computer equipped with safeguards that acts as a single, more easily defended, Internet connection. They even include a description of their most recent gateway, the tools they used to build it, and the hacker attacks they devised to test it.

You wil t docu-
mented s creat-
ed havo nd vital
informat ers, and
the legal

With thi organi-
zation w

* Quantum Books *
Phone: 617-494-5042
4 Cambridge Center * Cambridge, MA 02142
e mail: quanbook@world.std.com
FIREWALLS INTERNET SECURITY 202
CHESWICK INTERNET ADDISO
$26.95 Special* $24.95 *** NC
0201633574

William R. Cheswick and **Steven M. Bellovin** are both senior researchers at AT&T Bell Laboratories, where they have designed and maintain AT&T's Internet gateway. They have published numerous papers in the field, which have established them as experts on the subject.

Cover illustration by Wiley Miller
♻ Text printed on recycled paper
Corporate & Professional Publishing Group
Addison-Wesley Publishing Company

90000
9 780201 633573
ISBN 0-201-63357-4