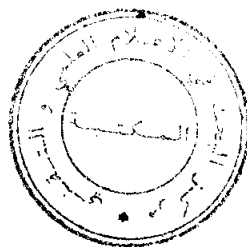


UNIX[®] installation security and integrity

David Ferbrache
Gavin Shearer

Blackwell Scientific Publications

UNIX[®] Installation Security and Integrity



David Ferbrache
Gavin Shearer

OXFORD
BLACKWELL SCIENTIFIC PUBLICATIONS
LONDON EDINBURGH BOSTON
MELBOURNE PARIS BERLIN VIENNA

Copyright © David Ferbrache and Gavin Shearer 1992

Blackwell Scientific Publications

Editorial Offices:

Osney Mead, Oxford OX2 0EL

25 John Street, London WC1N 2BL

23 Ainslie Place, Edinburgh EH3 6AJ

238 Main Street, Cambridge,

Massachusetts 02142, USA

54 University Street, Carlton

Victoria 3053, Australia

Other Editorial Offices:

Librairie Arnette SA

2, rue Casimir-Delavigne

75006 Paris

France

Blackwell Wissenschafts-Verlag

Meinekestrasse 4

D-1000 Berlin 15

Germany

Blackwell MZV

Feldgasse 13

A-1238 Wien

Austria

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 permission of the publisher.

First published 1992

Printed and bound in Great Britain
by Hartnolls Ltd, Bodmin, Cornwall

DISTRIBUTORS

Marston Book Services Ltd

PO Box 87

Oxford OX2 0DT

(Orders: Tel: 0865 791155

Fax: 0865 791927

Telex: 837515)

Australia

Blackwell Scientific Publications

(Australia) Pty Ltd

54 University Street

Carlton, Victoria 3053

(Orders: Tel: 03 347-0300)

British Library

Cataloguing in Publication Data

A catalogue record for this book
is available from the British Library.

ISBN 0-632-03134-4

Library of Congress Cataloging-in-
Publication Data

Ferbrache, David, 1965-

UNIX installation security and integrity/

David Ferbrache, Gavin Shearer

p. cm.

Includes bibliographical references and
index.

ISBN 0-632-03134-4

1. Operating systems (Computers)

2. UNIX (Computer file)

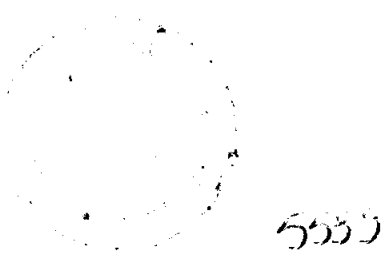
I. Shearer, Gavin. II. Title.

QA76.76.O63F46 1992

005.8—dc20

92-16278

CIP



Dedications

- To Allison, with love Gavin.**
- To Vi and Margaret, with best wishes Dave.**

BIBLIOTHEQUE DU CERIST

Contents

Dedications	v
Acknowledgements	xiii
Notes and conventions	xiv
Chapter 1 - Introduction	1
1.1 OVERVIEW	1
1.2 HISTORY OF UNIX	1
1.3 THE MAIN CAMPS	2
Chapter 2 - File System Security	5
2.1 INTRODUCTION	5
2.2 OVERVIEW OF THE UNIX FILE SYSTEM	5
2.3.1 User id	7
2.3.2 Group id	9
2.3.3 Discretionary access controls	10
2.3.4 Setuid	12
2.3.5 Setgid	14
2.3.6 Default permissions	14
2.3.7 Alteration times	15
2.3.8 Directory permissions	16
2.3.9 Hidden files	18
2.4 INTEGRITY	19
2.4.1 Backup	20
2.4.2 Dump and restore	23
2.5 FILE SYSTEMS	25
2.5.1 Mount annotations	27
2.5.2 Special file system mounts	28
2.5.3 Mounted directories	29
2.5.4 Unmounting	29
2.5.5 Deleting files	30
2.5.6 Quotas	31
2.5.7 Disk reserve	32
2.5.8 Consistency checking	33
2.5.9 Fsdb trapdoor mechanisms	35
2.6 SPECIAL DEVICES	38
Chapter 3 - Account Security	45

3.1 INTRODUCTION	45
3.2 PASSWORD FILE	45
3.3 GROUP FILE	46
3.4 ACCOUNT POLICY	48
3.5 THE LOGGING IN PROCEDURE	49
3.5.1 Penetrating the logging in procedure	50
3.6 RESTRICTED ENVIRONMENTS	52
3.6.1 Restricted shell	52
3.6.2 Changing root	54
3.6.3 Restricted logins	57
3.7 PASSWORD SECURITY	58
3.7.1 Preventing plaintext search	61
3.7.2 Trigram checking	63
3.7.3 Random password generation	64
3.7.4 Risks of random password	65
3.7.5 Shadow passwords	67
3.7.6 Password ageing	68
3.8 OTHER PASSWORD UTILITIES	71
3.8.1 Substitute user	71
3.8.2 Chsh (change shell)	72
3.8.3 Finger and GCOS	72
Chapter 4 - Process Security	77
4.1 INTRODUCTION	77
4.2 STRUCTURE OF PROCESSES	77
4.3 PROCESS CONTROL	78
4.3.1 Changing uid	82
4.3.2 Changing group ids	84
4.3.3 Signals and killing of processes	86
4.4 PROCESS RESOURCE MANAGEMENT	91
4.5 PROCESS PRIORITY	92
4.6 PROCESS TRACING AND DEBUGGING	93
4.6.1 Proc file system	94
4.6.2 Extended ptrace and system call trace	95
4.6.3 Core files	96
4.7 VIRUSES AND TROJAN HORSES	96
4.7.1 Trojan horses	96
4.7.2 Viruses	101
4.7.3 Identifying viruses	104
4.7.4 Viruses in perspective	107
4.8 SYSTEM INITIALISATION	107
4.8.1 SunOS 4.0	108
4.8.2 Ttytab and ttys files	111

4.8.3 Monitor ROMs	113
4.9 BATCH EXECUTION	114
4.10 DENIAL OF SERVICE	116
4.10.1 Kernel resources	117
4.10.2 Storage resources	119
4.10.3 Disk partitioning	120
4.10.4 Other devices	122
4.10.5 System crashes	122
Chapter 5 - Cryptography	125
5.1 CRYPT COMMAND	125
5.2 Data Encryption Standard	126
5.3 PASSWORD ENCRYPTION	128
5.4 PUBLIC KEY ENCRYPTION	129
5.5 DIGITAL SIGNATURES	131
5.6 NETWORK ENCRYPTION	131
5.7 PRIVACY ENHANCED MAIL (PEM)	132
Chapter 6 - Network Security	135
6.1 INTRODUCTION	135
6.2 TCP/IP PROTOCOLS	135
6.2.1 IP - Internet protocol	136
6.2.2 TCP - transmission control protocol	137
6.2.3 Inetd	138
6.2.4 FTP - file transfer protocol	139
6.2.5 TFTP - trivial file transfer protocol	139
6.2.6 SMTP - simple mail transfer protocol	140
6.2.7 Telnet	141
6.2.8 BOOTP	142
6.2.9 SNMP - simple network management	142
6.2.10 DNS - domain name system	143
6.3 UNIX-SPECIFIC PROTOCOLS	144
6.3.1 Trusted hosts	144
6.3.2 Trusted port	146
6.3.3 Other commands	147
6.4 RPC AND NFS PROTOCOLS	147
6.5 UUCP overview	151
6.5.1 Introduction	151
6.5.2 Password file	152
6.6 AT&T UUCP	153
6.6.1 USERFILE file	153
6.6.2 L.cmds file	154

6.6.3 L.sys and L.dialcodes files	154
6.6.4 Logging	154
6.6.5 Permissions	155
6.7 HONEYDANBER UUCP	155
6.7.1 Differences	155
6.7.2 Permissions file	156
6.7.3 Permissions file checking	158
6.7.4 System and dialcodes files	158
6.7.5 Logging	159
6.7.6 Permissions	159
6.8 NETWORK INTERFACE TAP	159
6.9 KERBEROS	160
6.9.1 How it works	160
6.9.2 Database	162
6.9.3 Using Kerberos	162
6.9.4 Limitations of Kerberos	163
6.10 FIREWALLS	164
Chapter 7 - Monitoring Security	165
7.1 FILE MONITORING	165
7.1.1 Find syntax	165
7.1.2 Find scripts	167
7.2 LOG FILE MONITORING	170
7.3 PASSWORD CHECKING	173
7.4 PROCESS MONITORING	174
7.5 SUN C2 SECURITY AUDIT TRAIL	175
Chapter 8 - Programming for Security	177
8.1 INTRODUCTION	177
8.2 VALIDATING THE USER	177
8.3 PASSWORD/GROUP FILE ACCESS	178
8.3.1 Password file	179
8.3.2 Group file	180
8.3.3 Checking passwords	180
8.4 FILE ACCESS CONTROLS	181
8.5 MOUNTING FILE SYSTEMS	183
8.6 HANDLING TEMPORARY FILES	184
8.7 PROCESS CONTROLS	185
8.7.1 Process signalling	185
8.7.2 Process resource control	185
8.7.3 Process tracing	186

8.7.4 Core file generation	187
8.8 SYSTEM LOGGING AND ACCOUNTING	187
8.9 RESTRICTED ENVIRONMENTS	189
8.10 COMMAND EXECUTION	189
8.11 KERNEL MEMORY ACCESS	193
8.12 INTEGRITY	195
8.13 QUEUES, SEMAPHORES, SHARED MEMORY	195
8.14 GENERAL PROGRAMMING NOTES	196
Chapter 9 - Trusted Systems	199
9.1 INTRODUCTION	199
9.2 ORANGE BOOK	201
9.2.1 Security policy	203
9.2.2 Accountability	204
9.2.3 Mandatory access	205
9.3 COVERT CHANNELS	209
9.4 ITSEC	212
9.5 DATA INTEGRITY	215
9.6 ENVIRONMENTAL FACTORS	216
9.7 COMPARTMENTED MODE WORKSTATION	219
Chapter 10 - Hardware Security Support	221
10.1 INTRODUCTION	221
10.2 SUPPORT FOR THE VIRTUAL MACHINE	222
10.3 CRYPTOGRAPHIC HARDWARE	226
10.4 AUTOMATIC FLOW VERIFICATION	228
10.5 DIAGNOSTIC COPROCESSORS	228
10.6 UPS	229
10.7 REDUNDANT SYSTEMS	229
10.8 TEMPEST	231
Chapter 11 - Standardisation	233
11.1 DE FACTO STANDARDS	233
11.2 DE JURE STANDARDS	235
11.3 GOVERNMENT STANDARDISATION	237
11.4 USER GROUPS	237
Chapter 12 - Common Sense	239

Appendices

Appendix A - The Internet Worm	241
Appendix B - COPS - a Security Checking Package	249
Appendix C - Other Public Domain Security Software	257
Appendix D - Forum for Incident Response Teams	259
Appendix E - CERT Advisories	263
Appendix F - CIAC Advisories	269
Appendix G - Sources of Patches	275
Appendix H - Security Alert and Information Lists	277
Appendix I - Restricted Chroot Environments	281
Appendix J - Requests For Comments	285
Appendix K - NCSC Documentation	287
Appendix L - References and Further Reading	289
Appendix M - Glossary	293
Appendix N - Contact Addresses	297
Index	299