

# Computer Communications and Networks

---

Springer-Verlag London Ltd.

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

*Also in this series:*

**Multimedia Internet Broadcasting: Quality, Technology and Interface**

Andy Sloane and Dave Lawrence (Eds)

1-85233-283-2

**The Quintessential PIC Microcontroller**

Sid Katzen

1-85233-309-X

John M.D. Hunter

---

# **An Information Security Handbook**



Springer

John M.D. Hunter, BA (Hons), FBCS, CEng  
CISM Group, Cranfield University, RMCS, Shrivenham, Swindon SN6 8LA, UK

*Series editor*

Professor A.J. Sammes, BSc, MPhil, PhD, FBCS, CEng  
CISM Group, Cranfield University, RMCS, Shrivenham, Swindon SN6 8LA, UK

ISBN 978-1-85233-180-1

British Library Cataloguing in Publication Data

Hunter, John M.D.

An information security handbook. – (Computer communications and networks)

1. Computer security

I. Title

005.8

ISBN 978-1-85233-180-1

Library of Congress Cataloging-in-Publication Data

Hunter, John M.D., 1940-

An information security handbook. / John M.D. Hunter.

p. cm.

Includes bibliographical references and index.

ISBN 978-1-85233-180-1 ISBN 978-1-4471-0261-8 (eBook)

DOI 10.1007/978-1-4471-0261-8

1. Computer security – Handbooks, manuals etc. 2. Computers – Access control – Handbooks, manuals etc. I. Title.

QA76.9.A25 H87 2001

005.8 – dc21

00-066154

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

© Springer-Verlag London 2001

Originally published by Springer-Verlag London Berlin Heidelberg in 2001

The use of registered names, trademarks etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Typesetting: Electronic text files prepared by author

34/3830-54321 Printed on acid-free paper SPIN 10882470

*To Phillipa, Clare and Charlotte*

# Acknowledgements

I would like to thank all members of CISM Group at the Royal Military College of Science for their help, advice, general support and forbearance in connection with the preparation of this manuscript. Special thanks need to be given to Tony Sammes and Edna Day. Without them, this project would never have got off the ground. I would also like to acknowledge the helpful comments from the students of all the Design of Information MSc courses held at RMCS since 1990. Special thanks also need to go to the staff at Springer, London, for their truly professional assistance. Finally, a word of thanks must go to my family who have had to put up with the “grumpy lump” while this book has gone through its gestation.

# Contents

<b>1. Introduction</b> .....	1
1.1 Why a Book about Information Security? .....	1
1.2 Some Conventions .....	2
1.3 Risks .....	3
1.4 Information Sensitivity .....	4
1.5 Information Importance .....	5
1.6 Countermeasures .....	6
1.7 Information Warfare .....	7
1.8 Management .....	9
1.9 Summary .....	9
<b>2. Technology and Security</b> .....	11
2.1 Privilege and Machine Modes .....	11
2.2 System Configuration .....	13
2.3 Physical Aspects of Discs and Tapes .....	13
2.3.1 Hard Discs .....	14
2.3.2 CD-ROMs .....	18
2.3.3 Floppy Discs .....	19
2.3.4 Magnetic Tapes .....	20
2.4 Files and Access Control .....	21
2.4.1 File Access Controls .....	25
2.5 RAID Storage .....	26
2.6 Summary .....	27
<b>3. Physical Security</b> .....	29
3.1 The Security Domains .....	31
3.1.1 The Global Security Environment .....	32
3.1.2 The Local Security Environment .....	32
3.1.3 The Electronic Security Environment .....	33
3.2 Security Aspects of Layout .....	33
3.3 Summary .....	33

- 4. Personnel Security . . . . . 35
  - 4.1 Assessing Personnel Trustworthiness . . . . . 35
  - 4.2 Example and Leadership . . . . . 37
  - 4.3 Awareness . . . . . 38
  - 4.4 IT Staff . . . . . 38
  - 4.5 New Recruits and Leavers . . . . . 39
  - 4.6 General . . . . . 40
  - 4.7 Summary . . . . . 40
  
- 5. Communications Security . . . . . 41
  - 5.1 Encryption and Cryptanalysis . . . . . 42
    - 5.1.1 Crypto Administration . . . . . 43
    - 5.1.2 Encryption Weaknesses . . . . . 45
  - 5.2 Authentication Dialogues . . . . . 47
    - 5.2.1 Crypto Signatures . . . . . 48
    - 5.2.2 Summary . . . . . 48
  - 5.3 The Kerberos Authentication Dialogue . . . . . 49
  - 5.4 Hacking . . . . . 50
  - 5.5 Unix and the TCP/IP Family of Protocols . . . . . 53
  - 5.6 Firewalls and Gateways . . . . . 56
    - 5.6.1 One Way Filters and Related Systems . . . . . 60
  - 5.7 Communications Software Security Problems . . . . . 61
  - 5.8 Summary . . . . . 62
  
- 6. Unix Security . . . . . 63
  - 6.1 The Security Problems of Unix . . . . . 63
  - 6.2 Unix File Permissions . . . . . 64
  - 6.3 Executing as the Superuser . . . . . 64
  - 6.4 Password Security . . . . . 65
    - 6.4.1 Selecting Passwords . . . . . 65
    - 6.4.2 Password Policies . . . . . 67
    - 6.4.3 Checking Password Security . . . . . 67
    - 6.4.4 Password Ageing . . . . . 68
    - 6.4.5 Guest Accounts . . . . . 68
    - 6.4.6 Accounts Without Passwords . . . . . 68
    - 6.4.7 Group Accounts and Groups . . . . . 69
  - 6.5 Improving Unix Network Security . . . . . 69
    - 6.5.1 Trusted Hosts . . . . . 70
    - 6.5.2 The `rxxx` Utilities . . . . . 71
    - 6.5.3 The `finger` Utility . . . . . 71
    - 6.5.4 The `telnet` Utility . . . . . 71
    - 6.5.5 The `ftp` Utility . . . . . 72
    - 6.5.6 The `tftp` Utility . . . . . 72



6.5.7	The <code>http</code> Utility .....	73
6.5.8	The <code>nfs</code> Utility .....	73
6.5.9	E-mail .....	73
6.5.10	The X Windows System .....	74
6.5.11	Windows NT .....	74
<b>7.</b>	<b>Internet Security</b> .....	<b>77</b>
7.1	External Hazards .....	77
7.2	ISP Services .....	79
7.3	After an Attack .....	80
7.4	Summary .....	81
<b>8.</b>	<b>Radiation Security</b> .....	<b>83</b>
8.1	Equipment Layout .....	85
8.2	Maintenance .....	86
8.3	Summary .....	86
<b>9.</b>	<b>Procedural Security</b> .....	<b>87</b>
9.1	System Integrity .....	87
9.2	Magnetic Media .....	88
9.3	Denial of System Benefits to a Competitor .....	88
9.4	Disposal of Documents .....	89
9.4.1	Paper Documents .....	89
9.4.2	Magnetic Documents .....	90
9.5	Weeding and Downgrading .....	94
9.6	When It Starts to Go Wrong .....	95
9.7	Summary .....	96
<b>10.</b>	<b>Software Security</b> .....	<b>97</b>
10.1	Secure Computer Systems .....	100
10.2	Software Evaluation .....	101
10.3	Software Security Models .....	102
10.4	Other Software Security Issues .....	103
<b>11.</b>	<b>Some Notes on Static Analysis</b> .....	<b>105</b>
11.1	Introduction .....	105
11.1.1	Static Analysis .....	105
11.1.2	A Simple Example .....	106
11.2	Control Flow Analysis .....	106
11.3	Data Flow Analysis .....	110
11.4	Information Flow Analysis .....	111
11.5	Semantic Analysis .....	112
11.6	The Use of Static Analysis .....	113
11.7	Summary .....	114

<b>12. Computer Viruses</b> .....	115
12.1 Introduction .....	115
12.2 Viruses .....	118
12.2.1 Mechanisms .....	120
12.2.2 WORD Viruses .....	123
12.3 Virus Examples .....	125
12.3.1 The “Brain” virus .....	125
12.3.2 The “Lehigh” Virus .....	125
12.3.3 The “Jerusalem” Virus .....	125
12.3.4 The “CHRISTMA EXEC” .....	126
12.3.5 The “Love Letter” Worm .....	127
12.3.6 The “Nimda” Worm .....	127
12.4 Dealing with Viruses .....	128
12.4.1 Anti-Viral Software .....	128
12.4.2 Anti-Viral Precautions .....	129
12.4.3 Virus Decontamination .....	130
12.5 Java & Active-X .....	131
12.6 The “Millennium Bug” .....	132
12.7 Summary .....	134
<b>13. The UK Data Protection Acts</b> .....	135
13.1 Definitions .....	136
13.2 The Data Protection Principles .....	137
13.2.1 The First Principle .....	138
13.2.2 The Second Principle .....	138
13.2.3 The Third Principle .....	138
13.2.4 The Fourth Principle .....	138
13.2.5 The Fifth Principle .....	139
13.2.6 The Sixth Principle .....	139
13.2.7 The Seventh Principle .....	139
13.2.8 The Eighth Principle .....	139
13.3 Summary .....	139
<b>14. System Administration and Security</b> .....	141
14.1 The Procurement of Secure Information Systems .....	141
14.1.1 The Requirement .....	142
14.1.2 The Outline Security Policy .....	142
14.1.3 Hardware Selection .....	143
14.1.4 Software Selection .....	143
14.1.5 Certified Software .....	144
14.1.6 Summary .....	145
14.2 System and Data Backups .....	145
14.3 Resource Tracking and Management .....	147
14.4 System Testing and Probing .....	147

- 14.5 Configuration Management . . . . . 148
  - 14.5.1 System Change Control . . . . . 149
- 14.6 Database Maintenance . . . . . 149
  - 14.6.1 Database Monitoring and Culling . . . . . 150
  - 14.6.2 Legal Conformance . . . . . 150
  - 14.6.3 Database Integrity . . . . . 151
- 14.7 User Account Management . . . . . 151
- 14.8 Audit Trail Management . . . . . 152
- 14.9 Summary . . . . . 152
- 15. The Management of Security . . . . . 153**
  - 15.1 The Security Management Problem . . . . . 153
  - 15.2 A Security Management Methodology . . . . . 154
    - 15.2.1 Knowledge of the Information System . . . . . 154
    - 15.2.2 Threat Assessment . . . . . 155
    - 15.2.3 Risk Estimation . . . . . 155
    - 15.2.4 Choice of Mechanisms . . . . . 155
  - 15.3 System Security Policies . . . . . 156
  - 15.4 Summary . . . . . 157
- 16. Conclusions . . . . . 159**
  - 16.1 A Definition of Information System Security . . . . . 160
  - 16.2 The Security Problems of an Information System . . . . . 160
  - 16.3 Tailpiece . . . . . 161
- A. Unix Security Resources . . . . . 163**
  - A.1 Configuration Checkers . . . . . 164
  - A.2 Network Activity Monitors . . . . . 164
  - A.3 Intrusion Checkers . . . . . 165
  - A.4 Change Detectors . . . . . 165
  - A.5 Password Checkers . . . . . 166
  - A.6 Firewall Packages . . . . . 166
  - A.7 Security Documentation . . . . . 167
  - A.8 Other Secure Software . . . . . 167
- B. DoD Computer System Evaluation Criteria . . . . . 169**
- C. IT Security Evaluation Criteria (ITSEC) . . . . . 175**
- D. An Example System Security Policy . . . . . 183**
- E. System Threats and Countermeasures . . . . . 193**
  - E.1 Introduction . . . . . 193
  - E.2 Threats to the Level of Service . . . . . 193
    - E.2.1 Power Supplies . . . . . 195

- E.2.2 Hardware Faults ..... 196
- E.2.3 Software Crashes ..... 197
- E.2.4 Operator Errors ..... 198
- E.2.5 Computer Viruses ..... 198
- E.2.6 Environmental Disasters ..... 199
- E.3 Threats to the Information Base ..... 200
- E.4 Threats Leading to Information Leakage ..... 200
- E.5 Choice of Countermeasures ..... 201
- E.6 Summary ..... 202
- F. Example List of Security Countermeasures ..... 205**
  - F.1 Access Control ..... 205
    - F.1.1 Communications ..... 205
    - F.1.2 Covert Channel Control ..... 206
    - F.1.3 Discretionary Access Control ..... 206
    - F.1.4 Mandatory Access Control ..... 206
    - F.1.5 Physical Access Control ..... 207
  - F.2 Accountability ..... 207
    - F.2.1 Transactions ..... 207
    - F.2.2 Configuration ..... 207
  - F.3 Accuracy ..... 208
    - F.3.1 Communications ..... 208
    - F.3.2 Storage ..... 208
  - F.4 Availability ..... 208
    - F.4.1 Communications ..... 208
    - F.4.2 Logical Denial ..... 209
    - F.4.3 Personnel ..... 209
    - F.4.4 Physical Denial ..... 210
    - F.4.5 Environmental Damage ..... 210
  - F.5 Data Exchange ..... 210
    - F.5.1 Communications Security ..... 210
    - F.5.2 Covert Channel ..... 210
    - F.5.3 Radiation Security ..... 211
    - F.5.4 Transmission Security ..... 211
    - F.5.5 Traffic Flow Security ..... 211
  - F.6 Authentication ..... 212
  - F.7 Audit ..... 212
  - F.8 Personnel ..... 213
- G. Glossary of Information Security Terms ..... 215**
- H. References & Bibliography ..... 221**
- Index ..... 225**