COMPUTER SECURITY IN THE AGE OF INFORMATION

Proceedings of the Fifth IFIP International Conference on
Computer Security, IFIP/Sec '88
Gold Coast, Queensland, Australia, 19–21 May, 1988

Edited by

William J. CAELLI
Information Security Research Centre
Queensland University of Technology
Brisbane, Queensland

and

ERACOM Pty. Ltd.
Gold Coast, Queensland
Australia

1989

NORTH-HOLLAND
AMSTERDAM · NEW YORK · OXFORD · TOKYO

ELSEVIER SCIENCE PUBLISHERS B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

Distributors for the United States and Canada:
ELSEVIER SCIENCE PUBLISHING COMPANY INC.
655 Avenue of the Americas
New York, N.Y. 10010, U.S.A.

Library of Congress Cataloging-in-Publication Data

IFIP International Conference on Computer Security (5th : 1988 : Gold Coast, Qld.)
Computer security in the age of information : proceedings of the Fifth IFIP International Conference on Computer Security, IFIP/Sec '88, Gold Coast, Queensland, Australia, 19-21 May, 1988 / edited by William J. Caelli.
p. cm.
Includes bibliographical references.
ISBN 0-444-88324-X (U.S.)
1. Computers--Access control--Congresses. I. Caelli, William.
II. International Federation for Information Processing.
III. Title.
QA76.9.A25I45 1988
005.8--dc20 89-22974
CIP

ISBN: 0 444 88324 X

© IFIP, 1989
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 written permission of the publisher, Elsevier Science Publishers B.V./Physical Sciences and Engineering Division, P.O. Box 103, 1000 AC Amsterdam, The Netherlands.

Special regulations for readers in the U.S.A. – This publication has been registered with the Copyright Clearance Center Inc. (CCC), Salem, Massachusetts. Information can be obtained from the CCC about conditions under which photocopies of parts of this publication may be made in the U.S.A. All other copyright questions, including photocopying outside of the U.S.A., should be referred to the publisher, Elsevier Science Publishers B.V., unless otherwise specified.

No responsibility is assumed by the publisher or by IFIP for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

Pp. 31–38, 63–74, 223–234: copyright not transferred.

Printed in The Netherlands.

PREFACE

This volume contains 41 papers, which were presented at the IFIP/Sec'88 Conference in the Conrad International Hotel and Jupiters Casino, Gold Coast, Queensland, Australia from May 19- 21, 1988. IFIP/Sec'88 was the fifth international computer security conference sponsored by the International Federation for Information Processing (IFIP), under the auspices of IFIP's Technical Committee on Security and Protection in Information Processing Systems (TC11) and the Australian Computer Society Inc., a member society of IFIP. The conference was an endorsed activity of Australia's Bicentennary (1788-1988) and an associated activity of the Expo '88 World Exposition, Brisbane.

The theme of IFIP/Sec'88, "COMPUTER SECURITY IN THE AGE OF INFORMATION", was addressed by papers which covered all major aspects of Computer Security. The conference programme was divided into 21 technical sessions which included :

Cryptographic Systems (1, 2 and 3.),
Secure Data Bases,
EFTS and Banking,
Organisations and Education,
Computer Crime,
Office Automation,
Security Products and Systems,
Crypto-key Systems,
Secure/Trusted Systems (1 and 2),
Access/Authentication Control,
Auditing (1 and 2),
Document Interchange and Networks,
Networks / EFT,
Networks, PCs and Workstations, and
Authentication and Identification

together with 4 Plenary Sessions and a Public Forum. The Plenary Sessions were addressed by invited speakers, international experts in the field of computer security and banking, including:

Mr. J. Lobel, "Security and Management in the Space Age",
Dr. H. Highland, "Computer Viruses and the PC",
Dr. W. Ware, "Trusted Computer Base : What Have We Learned in 10 Years ?", and
Mr. G. Hogg, "EFT and Banking in the Year 2000".

The conference was officially opened by The Hon. Paul Clauson,M.L.A., Queensland State Minister for Justice and Attorney-General for the State of Queensland.

There is no doubt that the topic of security in computer and telecommunications systems has attracted worldwide attention in recent years. The creation and study of security systems for computers and their associated telecommunications networks has now firmly entered the mainstream of Computer Science and Computer Systems Engineering.

Research, development and educational activities in this emerging technology have now moved to the forefront in both academic and educational as well as industrial research organisations. Already research into computer architecture, operating systems, data base management systems, data communications protocols, standards, human interfaces and numerous other areas have been affected by the growing requirement for sufficiently developed security measures. Governmental responses to the problems of personal privacy, computer related criminal activity and so on have likewise been growing over the last two to three years and appear set to increase markedly in the near future

I would like to thank all who helped in making IFIP/Sec'88 a success and look forward to meeting again at IFIP/Sec'90, the Sixth International Conference on Computer Security, in Helsinki, Finland in May 1990.

William J. Caelli
Editor

Queensland University of Technology
and
ERACOM Pty. Ltd.
Australia.

ACKNOWLEDGEMENTS

IFIP/Sec'88 was held under the auspices of the International Federation for Information Processing's Technical Committee on Security and Protection in Information Processing Systems, through its Australian member, the Australian Computer Society Inc. The preparatory work was shared among the following volunteers and professional organising company :

ORGANISING COMMITTEE :

William J. Caelli (Chairman)
Alan Underwood
Graham Smith
John Heim

INTERNATIONAL PROGRAMME COMMITTEES :

William J. Caelli (General Chairman)
Per Hoving (Ex-Officio Member)

AUSTRALASIAN COMMITTEE

Dennis Longley
John Beatson

U.S.A. / CANADA COMMITTEE

Willis Ware
Jerome Lobel
Peter Kingston

EUROPEAN COMMITTEE

Klaus Dittrich
Juhani Saari
Andre Grissonanche

ORGANISING GROUP

Jetset Conventions
Mrs. Jane Prentice (Manager)

EDITOR'S NOTES

The papers contained in this volume represent the Proceedings of IFIP/Sec'88. As in previous volumes in this series the papers in this volume are ordered in the sequence they were presented under the various subject headings of the sessions. Papers from the addresses at a number of sessions are not included, particularly some of the review presentations of the plenary sessions. In these cases a formal paper was not available or not appropriate.

A subject index is included in this volume. This index only contains references to major topics addressed in the various papers. The page number referenced is that of the starting page for the referenced paper.

This manuscipt was prepared with the able assistance of Ms. Anne Hamburger, Secretary to the Information Security Research Centre (I.S.R.C.) at the Queensland University of Technology, to whom I extend my thanks and those of IFIP TC-11.

CONTENTS

Preface v
Acknowledgements vii
Editor's Notes ix

1. CRYPTOGRAPHIC SYSTEMS - I.

Generating Multiprecision Integers with Guaranteed Primality.
N. Demytko. 1

A Proposed Design for an Extended DES
L. Brown. 9

2. SECURE DATA BASES

AI and 4GL : Automated Detection and Investigation Tools.
W. Tener. 23

Sentinel : A Secure Relational Database.
G. Shore. 31

3. EFTS AND BANKING

The Practical Restraints and Solutions to Large Scale EFTPOS.
C. Reilly. 39

Security Aspects of Smart Cards.
S. Draper. 51

4. CRYPTOGRAPHIC SYSTEMS - II

Permutations that Maximise Non-Linearity and their Cryptographic Significance.
J. Pieprzyk and G. Finkelstein. 63

The Use of Automated Cryptographic Check-Sums.
H. Beker. 75

5. ORGANIZATIONS AND EDUCATION.

Getting Organizations Involved in Computer Security : The Role of Security Awareness.
E. Markey. 83

Experiences from a One-Year Academic Programme in Security Informatics.
L. Yngström. 87

6. COMPUTER CRIME

Computer Crime Legislation in Canada.
M. Kratz. 101

7. CRYPTOGRAPHIC SYSTEMS - III

Evaluating Cryptographic Strategies.
J. Carroll and M. Kantor. 119

A RSA Card for PC's.
M. Dupuy. 135

8. OFFICE AUTOMATION

Emerging Vulnerabilities in Office Automation Security.
T. Keenan. 139

Authorization and Access Control in the Office-Net System.
M. Fugini and R. Zicari. 147

9. SECURITY PRODUCTS AND SYSTEMS

Computer Security at Digital.
J. Derosier. 163

The Role of Classification of Information in Controlling Data Proliferation in End-User PC Environment.
J. Feuerlicht and P. Grattan. 167

10. CRYPTO-KEY SYSTEMS.

A Cryptographic Key Distribution Mechanism for Secret Communications.
T. Kobayashi. 177

11. SECURE / TRUSTED SYSTEMS.

A Manufacturer's Approach to the Security of Computer Systems.
C. Blatchford. 187

On the Suitability of Z for the Specification of Verifiably Secure Systems.
M. Henning and A. Rohde. 197

12. ACCESS / AUTHENTICATION CONTROL

Extended User Authentication : The Next Major Enhancement to Access Control Packages.
C. Cresson Wood. 223

Choosing a Logical Access Control Strategy.
K. Fitzgerald. 235

13. AUDITING

Considering Security when Auditing Applications Under Development.
R. Moeller. 245

Experiences of the Use of the SBA Vulnerability Analysis for Improving Computer Security in Finland.
R. Voutilainen. 263

14. SECURE / TRUSTED SYSTEMS - II

Rendering a Commercial Operating System Secure : A Case Study.
J. Legge. 273

Industrial Espionage and Theft of Information.
M. Kratz. 279

15. ACCESS / AUTHENTICATION CONTROL - II

Meeting Data Security Needs.
D. Ewing. 291

Experience of Using a Type Signature Password System for User Authentication in a Heavily Used Computing Environment.
M. Newberry and J. Seberry. 303

16. SECURE / TRUSTED SYSTEMS - III (KEYNOTE)

Perspectives on Trusted Computer Systems.
W. Ware. 309

17. DOCUMENT INTERCHANGE AND NETWORKS

Secure Electronic Data Interchange.
J. Snare. 331

The World Meganetwork and Terrorism.
C. Madsen. 343

18. NETWORKS / EFT

Securing the Micro-Mainframe Link.
R. Bosen. 351

Australian EFTPOS Security Standards.
R. Davids. 357

19. EFTS AND COST OF SECURITY

Security in Electronic Funds Transfer: Message Integrity in Money Transfer and Bond Settlements through GE Information Services Global Network.
M. Shain. 367

Computer Security : Operational or Investment Cost.
E. Orlandi. 381

20. AUDITING - II

Automation of Internal Control Evaluation.
W. Lee. 391

Auditing Changes to MVS.
M. Hahn. 407

21. NETWORKS, PCs AND WORKSTATIONS

The PC as a Secure Network Workstation.
I. Graham and S. Wieten. 425

A Framework for the Security, Control and Audit of Local Area Network Operations.
R. Jamieson and G. Low. 439

22. AUTHENTICATION AND IDENTIFICATION

Personal Authentication Devices - Data Security Applications.
J. Elsbury. 471

Use of Fingerprint as Identity Verification.
S. Duval, C. André, R. Collot and M. Achemlal. 479

AUTHOR INDEX 483

SUBJECT INDEX 485