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

UNIVERSITÄTSBIBLIOTHEK
HANNOVER
TECHNISCHE
INFORMATIONSBIBLIOTHEK

1989

NORTH-HOLLAND
AMSTERDAM · NEW YORK · OXFORD · TOKYO

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