

# **Communications and Multimedia Security II**

## **IFIP – The International Federation for Information Processing**

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- the IFIP World Computer Congress, held every second year;
- open conferences;
- working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

# Communications and Multimedia Security II

**Proceedings of the IFIP TC6/TC11 International Conference  
on Communications and Multimedia Security at  
Essen, Germany, 23rd – 24th September 1996**

Edited by

**Patrick Horster**

*University of Technology Chemnitz-Zwickau  
Germany*

Published by Chapman & Hall on behalf of the  
International Federation for Information Processing (IFIP)



**SPRINGER INTERNATIONAL PUBLISHING, CHAM**

First edition 1996

© 1996 IFIP International Federation for Information Processing

Originally published by Chapman & Hall in 1996

Softcover reprint of the hardcover 1st edition 1996

ISBN 978-1-5041-2931-2 ISBN 978-0-387-35083-7 (eBook)

DOI 10.1007/978-0-387-35083-7

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the UK Copyright Designs and Patents Act, 1988, this publication may not be reproduced, stored, or transmitted, in any form or by any means, without the prior permission in writing of the publishers, or in the case of reprographic reproduction only in accordance with the terms of the licences issued by the Copyright Licensing Agency in the UK, or in accordance with the terms of licences issued by the appropriate Reproduction Rights Organization outside the UK. Enquiries concerning reproduction outside the terms stated here should be sent to the publishers at the London address printed on this page.

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.

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

 Printed on permanent acid-free text paper, manufactured in accordance with ANSI/NISO Z39.48-1992 and ANSI/NISO Z39.48-1984 (Permanence of Paper).

## CONTENTS

---

|  |     |
|--|-----|
| <b>Preface</b>   | vii |
| 1 PLASMA Platform for secure multimedia applications<br><i>A. Krannig</i>  | 1   |
| 2 High-level security issues in multimedia/hypertext systems<br><i>E.B. Fernandez, K.R. Nair, M.M. Larrondo-Petrie and Y. Xu</i>           | 13  |
| 3 Approaches to security in healthcare multimedia systems<br><i>S.M. Furnell, N.J. Salmons, P.W. Sanders, C.T. Stockel and M.J. Warren</i> | 25  |
| 4 Security flows analysis of the ATM emulated LAN architecture<br><i>M. Laurent</i>  | 37  |
| 5 Cryptanalysis of a voting scheme<br><i>M. Michels and P. Horster</i>   | 53  |
| 6 Using workflow to enhance security in federated databases<br><i>M.S. Olivier</i>   | 60  |
| 7 Anonymous mobility management for third generation mobile networks<br><i>S. Hoff, K. Jakobs and D. Kesdogan</i>                          | 72  |
| 8 Security concepts for the WWW<br><i>P. Lipp and V. Hassler</i>   | 84  |
| 9 An integrated solution for secure communications over B-ISDN<br><i>J. Forné and J.L. Melús</i>   | 96  |
| 10 Network security in a telemedicine system<br><i>G. Vassilacopoulos, V. Chrissikopoulos and D. Peppes</i>                                | 108 |
| 11 On the application of image decomposition to image compression<br>and encryption<br><i>H. Cheng and X. Li</i>                           | 116 |
| 12 A new approach for delegation using hierarchical delegation tokens<br><i>Y. Ding, P. Horster and H. Petersen</i>                        | 128 |
| 13 BEAST: a fast block cipher for arbitrary block sizes<br><i>S. Lucks</i>   | 144 |
| 14 A WWW based certification infrastructure for secure open network transactions<br><i>T. Gustavsson</i>                                   | 154 |
| 15 Distributed registration and key distribution for online universities<br><i>R. Oppliger and M. Bracher</i>                              | 166 |
| 16 Establishing a key hierarchy for conditional access without encryption<br><i>J. Schwenk</i>   | 176 |
| 17 Cybermoney in the Internet: an overview over new payment systems<br>in the Internet<br><i>R. Grimm and K. Zangeneh</i>                  | 183 |

|    |   |     |
|----|---|-----|
| 18 | A restrictive blind signature scheme with applications to electronic cash<br><i>C. Radu, R. Govaerts and J. Vandewalle</i>                      | 196 |
| 19 | Secure billing – incontestable charging<br><i>S. Pütz</i>   | 208 |
| 20 | ISDN LAN access: remote access security and user profile management<br><i>R. Posch, H. Leitold and F. Pucher</i>                                | 222 |
| 21 | Secure World Wide Web access to server groups<br><i>A. Hutchison, M. Kaiserswerth and P. Trommler</i>   | 234 |
| 22 | Access control system using dynamic handwriting features<br><i>C. Schmidt</i>   | 244 |
| 23 | Is there a need for new information security models?<br><i>S.A. Kokolakis</i>   | 256 |
| 24 | Attack modelling in open network environments<br><i>S.K. Katsikas, D. Gritzalis and P. Spirakis</i>   | 268 |
| 25 | The intrusion detection system AID – architecture, and experiences<br>in automated audit analysis<br><i>M. Sobirey, B. Richter and H. König</i> | 278 |
| 26 | Defending networks: the expert system components of SECURENET<br><i>S.K. Katsikas and N. Theodoropoulos</i>                                     | 291 |
| 27 | Increasing firewall reliability by recording routes<br><i>P.M. Boshoff and M.S. Olivier</i>   | 303 |
|    | <b>Index of contributors</b>  | 315 |
|    | <b>Keyword index</b>  | 317 |

## Preface

This is the second working conference on Communications and Multimedia Security. After two security conferences held in Klagenfurt (A) in 1993, organized by Winfried Müller, and in Vienna (A) in 1994, organized by Günther Pernul, the name Communications and Multimedia Security was used for the first time in Graz (A) in 1995, created by Reinhard Posch.

This year, the conference will face a new challenge because the location has moved from Austria to Germany. The next Communication and Multimedia Security is scheduled to take place in Greece. This and the multinational program committee are clear indications that the disciplines we cover are of international interest.

As communication and multimedia are extremely important aspects for the information society, security is of vital interest. Therefore I think that this series of conferences will be quickly established as an important security event.

The program tracks have been established to serve a wide range of interests from highly technical R&D projects to user oriented management and administration topics. Clearly, network security is a high priority topic. Papers will address a broad spectrum of Communications and Multimedia Security related subjects including: basic concepts, multimedia and hypertext systems, attacks, dedicated solutions, healthcare and telemedicine, cryptographic techniques, security infrastructures, payment systems, access control, models and policies, auditing and firewalls.

I am very grateful to the members of the Program Committee

|                   |                       |                      |
|-------------------|-----------------------|----------------------|
| Eduardo Fernandez | Dirk Fox              | Dimitris Gritzalis   |
| Siegfried Herda   | Matthias Kaiserswerth | Dimitris Karagiannis |
| Sokratis Katsikas | Dipak Khakhar         | Peter Kraaibeek      |
| Markus Michels    | Winfried Müller       | Harald Niederreiter  |
| Günther Pernul    | Reinhard Posch        | Erwin Schoitsch      |
| Basie v. Solms    | Peter Sonntag         | Otto Spaniol         |
| Stephanie Teufel  | Gerhard Weck          | Louise Yngstrøm      |

for their hard work and the difficult selection of the submitted papers. In addition, we gratefully acknowledge the work of the conference organizers, especially Günther Pernul (local chair), Peter Kraaibeek, Konrad Schultz, Peter Sonntag and the local organizers. They all did an excellent job in preparing the conference. It is our pleasure to thank them for their essential work.

Finally we would like to thank those whose efforts are instrumental in making this conference a success, the authors who submitted papers and the participants who honour us with their presence.

Patrick Horster  
*pho@informatik.tu-chemnitz.de*