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

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

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

CONTENTS

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