ADVANCED COMMUNICATIONS AND MULTIMEDIA SECURITY

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.

ADVANCED COMMUNICATIONS AND MULTIMEDIA SECURITY

IFIP TC6 / TC11 Sixth Joint Working Conference on Communications and Multimedia Security
September 26–27, 2002, Portorož, Slovenia

Edited by

Borka Jerman-Blažič
Tomaž Klobučar
Institut "Jožef Stefan"
Slovenia

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

ISBN 978-1-4757-4405-7 ISBN 978-0-387-35612-9 (eBook)
DOI 10.1007/978-0-387-35612-9

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available from the Library of Congress.

Advanced Communications and Multimedia Security
Edited by Borka Jerman-Blažič and Tomaž Klobučar
1-4020-7206-6

Originally published by Kluwer Academic Publishers in 2002

Printed on acid-free paper.

The original version of the book frontmatter was revised: The copyright line was incorrect. The Erratum to the book frontmatter is available at DOI: 10.1007/978-0-387-35612-9_23

Contents

COMMUNICATIONS SECURITY

DISTRIBUTED SYSTEMS SECURITY

Preface

Security, trust and confidence can certainly be considered as the most important parts of the Information society. Being protected when working, learning, shopping or doing any kind of e-commerce is of great value to citizens, students, business people, employees and employers. Commercial companies and their clients want to do business over Internet in a secure way, business managers when having meetings by videoconferencing tools require the exchanged information to be protected, publishing industry is concerned with the protection of copyright, hospital patients have a right to privacy etc. There is no area in the Information society that can proliferate without extensive use of services that provide satisfactory protection and privacy of data or personality.

In order to gather and present the latest development in the area of communications and multimedia security, and identify future security related research challenges, a Communications and Multimedia Security Conference (CMS 2002) was organised in Portorož, Slovenia, on 26th and 27th of September, 2002. CMS 2002 is the sixth IFIP working conference on communications and multimedia security since 1995. State-of-the-art issues as well as practical experiences and new trends in the areas were the topics of interest again, as proven by preceding conferences.

The book "Advanced Communications and Multimedia Security" contains 22 articles that were selected by the conference programme committee for presentation at CMS 2002. The articles address advanced concepts of communications and multimedia security, such as cryptography, applied

cryptography, biometry, communication systems security, multimedia security, digital watermarking, distributed systems security, applications security, and digital signatures. We would like to express our deep appreciation to all authors for their high-quality contributions. Special thanks also go to members of the programme committee:

- Augusto Casaca, INESC, chairman IFIP TC6, Portugal
- David Chadwick, University of Salford, UK
- Bart de Decker, Katholieke Universiteit Leuven, Belgium
- Yves Deswarte, LAAS CNRS, France
- Dieter Gollmann, Microsoft Research, UK
- Ruediger Grimm, TU Ilmenau, Germany
- Patrick Horster, Universitaet Klagenfurt, Austria
- Steve Kent, BBN, USA
- Klaus Keus, BSI, Germany
- Herbert Leitold, IAIK, Austria
- Peter Lipp, IAIK, Austria
- Antonio Lioy, Politecnico di Torino, Italy
- Guenther Pernul, University of Essen, Germany
- Bart Preneel, Katholieke Universiteit Leuven, Belgium
- Fabien A. P. Petitcolas, Microsoft Research, UK
- Wolfgang Schneider, SIT Fraunhofer Gesellschaft, Germany
- Leon Strous, De Nederlandsche Bank, chairman IFIP TC11, Netherlands

Borka Jerman-Blažič and Tomaž Klobučar