Lecture Notes in Computer Science 3677

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

Jana Dittmann Stefan Katzenbeisser
Andreas Uhl (Eds.)

# Communications and Multimedia Security

9th IFIP TC-6 TC-11 International Conference, CMS 2005
Salzburg, Austria, September 19 – 21, 2005
Proceedings

Volume Editors

Jana Dittmann
Otto-von-Guericke-Universität Magdeburg
Institut für Technische und Betriebliche Informationssysteme
Universitätsplatz 1, 39106 Magdeburg, Germany
E-mail: Jana.Dittmann@iti.cs.uni-magdeburg.de

Stefan Katzenbeisser
Technische Universität München
Institut für Informatik
Boltzmannstrasse 3, 85748 Garching, Germany
E-mail: katzenbe@in.tum.de

Andreas Uhl
Universität Salzburg
Department of Scientific Computing
Jakob Haringer Strasse 2, A-5020 Salzburg, Austria
E-mail: uhl@cosy.sbg.ac.at

Library of Congress Control Number: 2005931928

CR Subject Classification (1998): C.2, E.3, D.4.6, H.5.1, K.4.1, K.6.5, H.4

ISSN 0302-9743
ISBN-10 3-540-28791-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28791-9 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11552055 06/3142 5 4 3 2 1 0

# Preface

It is our great pleasure to present the proceedings of the 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2005), which was held in Salzburg on September 19–21, 2005. Continuing the tradition of previous CMS conferences, we sought a balanced program containing presentations on various aspects of secure communication and multimedia systems. Special emphasis was laid on papers with direct practical relevance for the construction of secure communication systems.

The selection of the program was a challenging task. In total, we received 143 submissions, from which 28 were selected for presentation as full papers. In addition to these regular presentations, the CMS conference featured for the first time a "work in progress track" that enabled authors to report preliminary results and ongoing work. These papers were presented in the form of a poster session during the conference; an extended abstract of the posters appears in this proceedings volume. From all papers submitted to the CMS conference, the program committee chose 13 submissions for inclusion in the work in progress track.

In addition to regular presentations, CMS 2005 featured a special session on XML security, containing both contributed and invited talks. This special session was jointly organized by Rüdiger Grimm (TU Ilmenau, Germany) and Jörg Schwenk (Ruhr-Universität Bochum, Germany). Their assistance in organizing CMS 2005 was greatly appreciated.

Besides the above mentioned presentations, the scientific program of CMS 2005 featured three invited speakers: Christian Cachin (IBM Zürich), with a talk about the cryptographic theory of steganography, Ton Kalker (HP Labs), with a survey talk on recent trends in the field of Digital Rights Management, and Ingemar Cox (University College London), with a talk about robust watermarking schemes.

We want to thank all contributors to CMS 2005. In particular, we are grateful to the authors and invited speakers for contributing their latest work to this conference, as well as to the PC members and external reviewers for their critical reviews of all submissions. Finally, special thanks go to the organizing committee who handled all local organizational issues and provided us with a comfortable location and a terrific social program. For us, it was a distinct pleasure to serve as program chairs of CMS 2005.

We hope that you will enjoy reading these proceedings and that they will be a catalyst for your future research in the area of multimedia security.

July 2005

Jana Dittmann
Stefan Katzenbeisser
Andreas Uhl

# 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security

## September 19–21, 2005, Salzburg (Austria)

### Program Chairs

Jana Dittmann, Otto-von-Guericke Universität Magdeburg, Germany
Stefan Katzenbeisser, Technische Universität München, Germany
Andreas Uhl, Universität Salzburg, Austria

### IFIP TC-6 TC-11 Chairs

Otto Spaniol, RWTH Aachen, Germany
Leon Strous, De Nederlandsche Bank, The Netherlands

### Program Committee

André Adelsbach, Ruhr-Universität Bochum, Germany
Elisa Bertino, University of Milan, Italy
Carlo Blundo, UNISA, Italy
Christian Cachin, IBM Zürich, Switzerland
Ingemar J. Cox, University College London, UK
David Chadwick, University of Kent, UK
Bart de Decker, KU Leuven, Belgium
Yves Deswarte, LAAS, France
Elke Franz, TU Dresden, Germany
Miroslav Goljan, SUNY Binghamton, USA
Patrick Horster, Universität Klagenfurt, Austria
Ton Kalker, HP Labs, USA
Stephen Kent, BBN Technologies, USA
Klaus Keus, BSI, Germany
Herbert Leitold, A-SIT, Austria
Nasir Memon, Polytechnic University, USA
Sead Muftic, Stockholm University, Sweden
Fernando Perez-Gonzalez, University of Vigo, Spain
Günter Pernul, Universität Regensburg, Germany
Reinhard Posch, Technische Universität Graz, Austria
Bart Preneel, KU Leuven, Belgium
Claus Vielhauer, Otto-von-Guericke University Magdeburg, Germany
Moti Young, Columbia University, USA

**Local Organization**

Dominik Engel
Roland Norcen
Helma Schöndorfer
Michael Tautschnig
Andreas Uhl

**External Reviewers**

Carlos Aguilar-Melchor
Felix Balado
Lejla Batina
Yannick Chevalier
Stelvio Cimato
Pedro Comesana
Peter Danner
Paolo D'Arco
Liesje Demuynck
Claudia Diaz
Kurt Dietrich
Wolfgang Dobmeier
Anas Abou El Kalam
Martin Feldhofer
Jessica Fridrich
Alban Gabillon
Sebastian Gajek
Steven Galbraith
Clemente Galdi
Jörg Gilberg
Ulrich Greveler
Hazem Hamed
Mark Hogan
Yongdae Kim
Franz Kollmann
Klaus Kursawe
Mario Lamberger
Peter Lipp
Mark Manulis
Björn Muschall
Vincent Naessens
Vincent Nicomette
Rodolphe Ortalo
Elisabeth Oswald
Federica Paci
Udo Payer
Luis Perez-Freire
Thomas Popp
Torsten Priebe
Markus Rohe
Thomas Rössler
Heiko Rossnagel
Martin Schaffer
Peter Schartner
Christian Schlaeger
Stefaan Seys
Dieter Sommer
Anna Squicciarini
Hung-Min Sun
Yagiz Sutcu
Ingrid Verbauwhede
Frederik Vercauteren
Tine Verhanneman
Kristof Verslype
Ivan Visconti
Ron Watro
Johannes Wolkerstorfer
Peiter Zatko

# Table of Contents

## Applied Cryptography



## DRM & E-Commerce



## Media Encryption

## Multimedia Security



## Privacy



## Biometrics & Access Control



## Network Security

## Mobile Security



## Work in Progress Track

## Special Session: XML Security