

Lecture Notes in Computer Science  
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2828

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Antonio Lioy Daniele Mazzocchi (Eds.)

# Communications and Multimedia Security

Advanced Techniques for Network and Data Protection

7th IFIP-TC6 TC11 International Conference, CMS 2003  
Torino, Italy, October 2-3, 2003  
Proceedings



Springer

## Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

## Volume Editors

Antonio Lioy  
Politecnico di Torino  
Dip. di Automatica e Informatica  
corso Duca degli Abruzzi, 24, 10129 Torino, Italy  
E-mail: lioy@polito.it

Daniele Mazzocchi  
Istituto Superiore Mario Boella  
corso Trento, 21, 10129 Torino, Italy  
E-mail: mazzocchi@ismb.it

## Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek  
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;  
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

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 3-540-20185-8 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

©IFIP International Federation for Information Processing, Hofstraße 3, A-2361 Laxenburg, Austria 2003  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH  
Printed on acid-free paper SPIN: 10959107 06/3142 5 4 3 2 1 0

# Preface

The Communications and Multimedia Security conference (CMS 2003) was organized in Torino, Italy, on October 2-3, 2003. CMS 2003 was the seventh IFIP working conference on communications and multimedia security since 1995. Research issues and practical experiences were the topics of interest, with a special focus on the security of advanced technologies, such as wireless and multimedia communications.

The book “Advanced Communications and Multimedia Security” contains the 21 articles that were selected by the conference program committee for presentation at CMS 2003. The articles address new ideas and experimental evaluation in several fields related to communications and multimedia security, such as cryptography, network security, multimedia data protection, application security, trust management and user privacy. We think that they will be of interest not only to the conference attendees but also to the general public of researchers in the security field.

We wish to thank all the participants, organizers, and contributors of the CMS 2003 conference for having made it a success.

October 2003

Antonio Lioy  
*General Chair of CMS 2003*

Daniele Mazzocchi  
*Program Chair of CMS 2003*

# Organization

CMS 2003 was organized by the TORSEC Computer and Network Security Group of the Dipartimento di Automatica ed Informatica at the Politecnico di Torino, in cooperation with the Istituto Superiore Mario Boella.

## Conference Committee

General Chair: Antonio Lioy (Politecnico di Torino, Italy)  
 Program Chair: Daniele Mazzocchi (Istituto Superiore Mario Boella, Italy)  
 Organizing Chair: Andrea S. Atzeni (Politecnico di Torino, Italy)

## Program Committee

F. Bergadano, Università di Torino  
 E. Bertino, Università di Milano  
 L. Breveglieri, Politecnico di Milano  
 A. Casaca, INESC, chairman IFIP TC6  
 M. Cremonini, Università di Milano  
 Y. Deswarte, LAAS-CNRS  
 M. G. Fugini, Politecnico di Milano  
 S. Furnell, University of Plymouth  
 R. Grimm, Technische Universität Ilmenau  
 B. Jerman-Blažič, Institut Jožef Stefan  
 S. Kent, BBN  
 T. Klobučar, Institut Jožef Stefan  
 A. Lioy, Politecnico di Torino  
 P. Lipp, IAIK  
 J. Lopez, Universidad de Málaga  
 F. Maino, CISCO  
 D. Mazzocchi, ISMB  
 S. Muftic, KTH  
 F. Piessens, Katholieke Universiteit Leuven  
 P. A. Samarati, Università di Milano  
 A. F. G. Skarmeta, Universidad de Murcia  
 L. Strous, De Nederlandsche Bank, chairman IFIP TC11  
 G. Tsudik, University of California at Irvine

# Organization

CMS 2003 was organized by the TORSEC Computer and Network Security Group of the Dipartimento di Automatica ed Informatica at the Politecnico di Torino, in cooperation with the Istituto Superiore Mario Boella.

## Conference Committee

General Chair: Antonio Lioy (Politecnico di Torino, Italy)  
Program Chair: Daniele Mazzocchi (Istituto Superiore Mario Boella, Italy)  
Organizing Chair: Andrea S. Atzeni (Politecnico di Torino, Italy)

## Program Committee

F. Bergadano, Università di Torino  
E. Bertino, Università di Milano  
L. Breveglieri, Politecnico di Milano  
A. Casaca, INESC, chairman IFIP TC6  
M. Cremonini, Università di Milano  
Y. Deswarte, LAAS-CNRS  
M. G. Fugini, Politecnico di Milano  
S. Furnell, University of Plymouth  
R. Grimm, Technische Universität Ilmenau  
B. Jerman-Blažič, Institut Jožef Stefan  
S. Kent, BBN  
T. Klobučar, Institut Jožef Stefan  
A. Lioy, Politecnico di Torino  
P. Lipp, IAIK  
J. Lopez, Universidad de Málaga  
F. Maino, CISCO  
D. Mazzocchi, ISMB  
S. Muftic, KTH  
F. Piessens, Katholieke Universiteit Leuven  
P. A. Samarati, Università di Milano  
A. F. G. Skarmeta, Universidad de Murcia  
L. Strous, De Nederlandsche Bank, chairman IFIP TC11  
G. Tsudik, University of California at Irvine

# Table of Contents

## Cryptography

Computation of Cryptographic Keys from Face Biometrics . . . . .	1
<i>Alwyn Goh, David C.L. Ngo</i>	
AUTHMAC_DH: A New Protocol for Authentication and Key Distribution . . . . .	14
<i>Heba K. Aslan</i>	
Multipoint-to-Multipoint Secure-Messaging with Threshold-Regulated Authorisation and Sabotage Detection . . . . .	27
<i>Alwyn Goh, David C.L. Ngo</i>	

## Network Security

Securing the Border Gateway Protocol: A Status Update . . . . .	40
<i>Stephen T. Kent</i>	
Towards an IPv6-Based Security Framework for Distributed Storage Resources . . . . .	54
<i>Alessandro Bassi, Julien Laganier</i>	
Operational Characteristics of an Automated Intrusion Response System . . . . .	65
<i>Maria Papadaki, Steven Furnell, Benn Lines, Paul Reynolds</i>	

## Mobile and Wireless Network Security

A Secure Multimedia System in Emerging Wireless Home Networks . . . . .	76
<i>Nut Taesombut, Richard Huang, Venkat P. Rangan</i>	
Java Obfuscation with a Theoretical Basis for Building Secure Mobile Agents . . . . .	89
<i>Yusuke Sakabe, Masakazu Soshi, Atsuko Miyaji</i>	
A Security Scheme for Mobile Agent Platforms in Large-Scale Systems . . . . .	104
<i>Michelle S. Wingham, Joni da Silva Fraga, Rafael R. Obelheiro</i>	

## Trust and Privacy

Privacy and Trust in Distributed Networks . . . . .	117
<i>Thomas Rössler, Arno Hollosi</i>	



Extending the SDSI / SPKI Model through Federation Webs .....	132
<i>Altair Olivo Santin, Joni da Silva Fraga, Carlos Maziero</i>	
Trust- $\mathcal{X}$ : An XML Framework for Trust Negotiations .....	146
<i>Elisa Bertino, Elena Ferrari, Anna C. Squicciarini</i>	
<b>Application Security</b>	
How to Specify Security Services: A Practical Approach .....	158
<i>Javier Lopez, Juan J. Ortega, Jose Vivas, Jose M. Troya</i>	
Application Level Smart Card Support through Networked Mobile Devices .....	172
<i>Pierpaolo Baglietto, Francesco Moggia, Nicola Zingirian, Massimo Maresca</i>	
Flexibly-Configurable and Computation-Efficient Digital Cash with Polynomial-Thresholded Coinage .....	181
<i>Alwyn Goh, Kuan W. Yip, David C.L. Ngo</i>	
<b>Multimedia Security</b>	
Selective Encryption of the JPEG2000 Bitstream .....	194
<i>Roland Norcen, Andreas Uhl</i>	
Robust Spatial Data Hiding for Color Images .....	205
<i>Xiaoqiang Li, Xiangyang Xue, Wei Li</i>	
Watermark Security via Secret Wavelet Packet Subband Structures .....	214
<i>Werner Dietl, Andreas Uhl</i>	
A Robust Audio Watermarking Scheme Based on MPEG 1 Layer 3 Compression .....	226
<i>David Megías, Jordi Herrera-Joancomartí, Julià Minguillón</i>	
Loss-Tolerant Stream Authentication via Configurable Integration of One-Time Signatures and Hash-Graphs .....	239
<i>Alwyn Goh, G.S. Poh, David C.L. Ngo</i>	
Confidential Transmission of Lossless Visual Data: Experimental Modelling and Optimization .....	252
<i>Bubi G. Flepp-Stars, Herbert Stögner, Andreas Uhl</i>	
<b>Author Index</b> .....	265