

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*New York University, NY, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

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

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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

[springeronline.com](http://springeronline.com)

©2005 IFIP International Federation for Information Processing, Hofstrasse 3, A-2361 Laxenburg, Austria  
Printed in Germany

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 Zatkó

# Table of Contents

## Applied Cryptography

Fast Contract Signing with Batch Oblivious Transfer <i>L'ubica Staneková, Martin Stanek</i> . . . . .	1
An Instruction Set Extension for Fast and Memory-Efficient AES Implementation <i>Stefan Tillich, Johann Großschädl, Alexander Szekeley</i> . . . . .	11
Self-Healing Key Distribution Schemes with Sponsorization <i>Germán Sáez</i> . . . . .	22

## DRM & E-Commerce

Effective Protection Against Phishing and Web Spoofing <i>Rolf Oppliger, Sebastian Gajek</i> . . . . .	32
Identity Based DRM: Personal Entertainment Domain <i>Paul Koster, Frank Kamperman, Peter Lenoir, Koen Vrieling</i> . . . . .	42
Rights and Trust in Multimedia Information Management <i>Jaime Delgado, Víctor Torres, Silvia Llorente, Eva Rodríguez</i> . . . . .	55
Signature Amortization Using Multiple Connected Chains <i>Qusai Abuein, Susumu Shibusawa</i> . . . . .	65

## Media Encryption

A Key Embedded Video Codec for Secure Video Multicast <i>Hao Yin, Chuang Lin, Feng Qiu, Xiaowen Chu, Geyong Min</i> . . . . .	77
Puzzle – A Novel Video Encryption Algorithm <i>Fuwen Liu, Hartmut Koenig</i> . . . . .	88
Selective Image Encryption Using JBIG <i>Roman Pfarrhofer, Andreas Uhl</i> . . . . .	98

## Multimedia Security

On Reversibility of Random Binning Techniques: Multimedia Perspectives <i>Sviatoslav Voloshynovskiy, Oleksiy Koval, Emre Topak, José Emilio Vila-Forcén, Pedro Comesaña Alfaro, Thierry Pun</i> . . . . .	108
A Graph-Theoretic Approach to Steganography <i>Stefan Hetzl, Petra Mutzel</i> . . . . .	119
Non-Interactive Watermark Detection for a Correlation-Based Watermarking Scheme <i>André Adelsbach, Markus Rohe, Ahmad-Reza Sadeghi</i> . . . . .	129

## Privacy

Video Surveillance: A Distributed Approach to Protect Privacy <i>Martin Schaffer, Peter Schartner</i> . . . . .	140
Privacy-Preserving Electronic Health Records <i>Liesje Demuyne, Bart De Decker</i> . . . . .	150
Using XACML for Privacy Control in SAML-Based Identity Federations <i>Wolfgang Hommel</i> . . . . .	160

## Biometrics & Access Control

Verifier-Tuple as a Classifier for Biometric Handwriting Authentication - Combination of Syntax and Semantics <i>Andrea Oermann, Jana Dittmann, Claus Viehauer</i> . . . . .	170
Decentralised Access Control in 802.11 Networks <i>Marco Domenico Aime, Antonio Liroy, Gianluca Ramunno</i> . . . . .	180
Multimodal Biometrics for Voice and Handwriting <i>Claus Viehauer, Tobias Scheidat</i> . . . . .	191

## Network Security

Compact Stimulation Mechanism for Routing Discovery Protocols in Civilian Ad-Hoc Networks <i>Huafei Zhu, Feng Bao, Tieyan Li</i> . . . . .	200
---	-----



Polymorphic Code Detection with GA Optimized Markov Models <i>Udo Payer, Stefan Kraußberger</i> .....	210
--	-----

A Secure Context Management for QoS-Aware Vertical Handovers in 4G Networks <i>Minsoo Lee, Sehyun Park</i> .....	220
--	-----

## Mobile Security

Security Analysis of the Secure Authentication Protocol by Means of Coloured Petri Nets <i>Wiebke Dresch</i> .....	230
--	-----

Assessment of Palm OS Susceptibility to Malicious Code Threats <i>Tom Goovaerts, Bart De Win, Bart De Decker, Wouter Joosen</i> .....	240
--	-----

Implementation of Credit-Control Authorization with Embedded Mobile IPv6 Authentication <i>HyunGon Kim, ByeongKyun Oh</i> .....	250
---	-----

## Work in Progress Track

Biometrics: Different Approaches for Using Gaussian Mixture Models in Handwriting <i>Sascha Schimke, Athanasios Valsamakis, Claus Vielhauer, Yannis Stylianou</i> .....	261
---	-----

INVUS: INtelligent VULnerability Scanner <i>Turker Akyuz, Ibrahim Sogukpinar</i> .....	264
---	-----

Personal Rights Management – Enabling Privacy Rights in Digital Online Content <i>Mina Deng, Lothar Fritsch, Klaus Kursawe</i> .....	266
--	-----

Flexible Traitor Tracing for Anonymous Attacks <i>Hongxia Jin, Jeffery Lotspiech</i> .....	269
---	-----

Efficient Key Distribution for Closed Meetings in the Internet <i>Fuwen Liu, Hartmut Koenig</i> .....	271
--	-----

Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics <i>Taras Holotyak, Jessica Fridrich, Sviatoslav Voloshynovskiy</i> .....	273
---	-----

Applying LR Cube Analysis to JSteg Detection  
*Kwangsoo Lee, Changho Jung, Sangjin Lee, HyungJun Kim, Jongin Lim* . . . . . 275

Digital Signatures Based on Invertible Watermarks for Video Authentication  
*Enrico Hauer, Jana Dittmann, Martin Steinebach* . . . . . 277

A Theoretical Framework for Data-Hiding in Digital and Printed Text Documents  
*Renato Villán, Sviatoslav Voloshynovskiy, Frédéric Deguillaume, Yuriy Rytsar, Oleksiy Koval, Emre Topak, Ernesto Rivera, Thierry Pun* . . . . . 280

Semantically Extended Digital Watermarking Model for Multimedia Content  
*Huajian Liu, Lucilla Croce Ferri, Martin Steinebach* . . . . . 282

An Architecture for Secure Policy Enforcement in E-Government Services Deployment  
*Nikolaos Oikonomidis, Sergiu Tcaciu, Christoph Ruland* . . . . . 284

Some Critical Aspects of the PKIX TSP  
*Cristian Marinescu, Nicolae Tapus* . . . . . 286

Motivations for a Theoretical Approach to WYSIWYS  
*Antonio Liroy, Gianluca Ramunno, Marco Domenico Aime, Massimiliano Pala* . . . . . 289

**Special Session: XML Security**

Secure XMaiL or How to Get Rid of Legacy Code in Secure E-Mail Applications  
*Lars Ewers, Wolfgang Kubbilun, Lijun Liao, Jörg Schwenk* . . . . . 291

Integrating XML Linked Time-Stamps in OASIS Digital Signature Services  
*Ana Isabel González-Tablas, Karel Wouters* . . . . . 301

Trustworthy Verification and Visualisation of Multiple XML-Signatures  
*Wolfgang Kubbilun, Sebastian Gajek, Michael Psarros, Jörg Schwenk* . . . . . 311

Experience XML Security – The XML-Security Plug-In for Eclipse  
*Dominik Schadow* . . . . . 321

How to Make a Federation Manageable <i>Christian Geuer-Pollmann</i> .....	330
XML Signatures in an Enterprise Service Bus Environment <i>Eckehard Hermann, Dieter Kessler</i> .....	339
Using the XML Key Management Specification (and Breaking X.509 Rules as You Go) <i>Stephen Farrell, José Kahan</i> .....	348
<b>Author Index</b> .....	359