

*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*

Alfred Kobsa

*University of California, Irvine, CA, 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

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Bart De Decker    Jorn Lapon  
Vincent Naessens    Andreas Uhl    (Eds.)

# Communications and Multimedia Security

12th IFIP TC 6 / TC 11 International Conference, CMS 2011  
Ghent, Belgium, October 19-21, 2011  
Proceedings

## Volume Editors

Bart De Decker

K.U. Leuven, Department of Computer Science - DistriNet

Celestijnenlaan 200A, 3001 Leuven, Belgium

E-mail: bartde.decker@cs.kuleuven.be

Jorn Lapon

Vincent Naessens

KAHO Sint-Lieven - MSEC

Gebroeders De Smetstraat 1, 9000 Gent, Belgium

E-mail: {jorn.lapon,vincent.naessens}@kahosl.be

Andreas Uhl

University of Salzburg

Visual Computing and Multimedia

Jakob Haringer Str.2, A 5020 Salzburg, Austria

E-mail: uhl@cosy.sbg.ac.at

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-24711-8

e-ISBN 978-3-642-24712-5

DOI 10.1007/978-3-642-24712-5

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011937966

CR Subject Classification (1998): C.2, K.6.5, E.3, D.4.6, J.1, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© IFIP International Federation for Information Processing 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

*The original version of the book frontmatter was revised:  
The copyright line was incorrect. The Erratum  
to the book frontmatter is available at  
DOI: [10.1007/978-3-642-24712-5\\_30](https://doi.org/10.1007/978-3-642-24712-5_30)*

# Preface

It is with great pleasure that we present the proceedings of the 12th IFIP TC-6 and TC-11 Conference on Communications and Multimedia Security (CMS 2011), which was held in Ghent, Belgium on October 19–21, 2011. The meeting continued the tradition of previous CMS conferences which were held in Linz, Austria (2010) and Heraklion, Crete, Greece (2006).

The series of CMS meetings features an almost unique combined discussion of two specific topics in IT security which is hardly found elsewhere in the scientific community. At first sight communication and multimedia security does not seem to be highly related, but there are even applications where both aspects are obviously involved like streaming of secured video or privacy questions in social networks. On the one hand, there are specialized meetings on multimedia security like the ACM Multimedia and Security Workshop or the Information Hiding Conference, on the other hand there are specialized meetings on communication and network security like the ACM Computer and Communication Security Conference. The only meetings somewhat closer to CMS are the IFIP Information Security Conference (IFIP SEC), the Information Security Conference (ISC), and the Conference on Information and Communications Security (ICICS). However, the explicit focus on Multimedia Security is missing and usually, there are very few papers on this topic seen at those much more general conferences.

The program committee (PC) received 52 submissions out of which only 11 full papers were accepted. In this edition, we have included 10 short papers, which describe valuable work-in-progress. Also, five extended abstracts reflecting the posters discussed at the conference, complete these proceedings. We would like to thank all the authors who submitted papers. Each paper was anonymously reviewed by three to five reviewers. In addition to the PC Members, several external reviewers joined the review process in their particular areas of expertise. We are grateful for their sincere and hard work. We tried to compile a balanced program covering various topics of communications and multimedia security: cryptanalysis, covert channels, biometrics, watermarking, ... just to name a few.

We are also grateful to Moti Yung (Google Inc and Columbia University), Ronald Leenes (University of Tilburg), and Jaap-Henk Hoepman (TNO and Radboud University Nijmegen) for accepting our invitation to deliver keynote talks.

We appreciate the contributions of our sponsors: Luciad, IBM, Google, Bel-Spo (Belgian State, Belgian Science Policy). Without their financial support, it would not have been possible to organize this conference or to attract as many young researchers.

Finally, special thanks go to the organizing committee who handled all local organizational issues and provided us with a comfortable and inspiring location

and a terrific social program. For us, it was a distinct pleasure to serve as program chairs of CMS 2011.

We hope that you will enjoy reading these proceedings and that they may inspire you for future research in communications and multimedia security.

October 2011

Bart De Decker  
Andreas Uhl

# Organization

CMS 2011 was the 12th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security. It was organized by KAHO Sint-Lieven in cooperation with K.U.Leuven.

## Executive Committee

Conference Chair	Bart De Decker (K.U. Leuven, Belgium)
Program Co-chairs	Bart De Decker (K.U. Leuven, Belgium) Andreas Uhl (University of Salzburg, Austria)
Organizing Chair	Vincent Naessens (KAHO Sint-Lieven, Belgium)

## Program Committee

Anas Abou El Kalam	IRIT - INP, France
Partrick Bas	CNRS-Lagis, Lille, France
David W. Chadwick	University of Kent, UK
Howard Chivers	Cranfield University, UK
Isabelle Chrisment	LORIA-University of Nancy, France
Gabriela Cretu-Ciocarlie	Real-Time Innovations, Inc., USA
Frédéric Cuppens	Télécom Bretagne, France
Hervé Debar	Télécom SudParis, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Bart De Decker	K.U.Leuven, Belgium
Yvo G. Desmedt	University College London, UK
Lieven Desmet	K.U.Leuven, Belgium
Lieven De Strycker	KAHO Sint-Lieven, Belgium
Yves Deswarte	LAAS-CNRS, France
Jana Dittmann	University of Magdeburg, Germany
Stelios Dritsas	Athens University of Economics and Business, Greece
Taher Elgamal	Axway Inc., USA
Gerhard Eschelbeck	Webroot, USA
Simone Fischer-Hübner	Karlstad University, Sweden
Jürgen Fuß	Upper Austria University of Applied Sciences, Austria
Teddy Furon	INRIA Rennes - Bretagne Atlantique, France
Sébastien Gams	Université de Rennes 1 - INRIA / IRISA, France

Christian Geuer-Pollmann	Microsoft Research, Germany
Dieter Gollmann	Hamburg University of Technology, Germany
Mohamed Gouda	National Science Foundation, USA
Rüdiger Grimm	University of Koblenz, Germany
Jean Hennebert	University of Applied Sciences, HES-SO, Switzerland
Eckehard Hermann	Upper Austria University of Applied Sciences, Austria
Jaap-Henk Hoepman	TNO / Radboud University Nijmegen, The Netherlands
Andreas Humm	University of Fribourg, Switzerland
Edward Humphreys	XiSEC, UK
Christophe Huygens	K.U.Leuven, Belgium
Witold Jacak	Upper Austria University of Applied Sciences, Austria
Sushil Jajodia	George Mason University, USA
Lech Janczewski	University of Auckland, New Zealand
Günter Karjoth	IBM Research - Zurich, Switzerland
Stefan Katzenbeisser	TU Darmstadt, Germany
Markulf Kohlweiss	Microsoft Research Cambridge, UK
Herbert Leitold	Secure Information Technology Center (A-SIT), Austria
Javier Lopez	University of Malaga, Spain
Louis Marinos	ENISA, Greece
Keith Martin	Royal Holloway, University of London, UK
Fabio Massacci	University of Trento, Italy
Chris Mitchell	Royal Holloway, University of London, UK
Refik Molva	Eurécom, France
Jörg R. Mühlbacher	Johannes Kepler Universität Linz, Austria
Yuko Murayama	Iwate Prefectural University, Japan
Vincent Naessens	KAHO Sint-Lieven, Belgium
Chandrasekaran Pandurangan	Indian Institute of Technology, Madras, India
Günther Pernul	University of Regensburg, Germany
Alessandro Piva	University of Florence, Italy
Hartmut Pohl	University of Applied Sciences Bonn-Rhein-Sieg, Germany
Jean-Jacques Quisquater	Université catholique de Louvain, Belgium
Kai Rannenberg	Goethe University Frankfurt, Germany
Vincent Rijmen,	K.U.Leuven, Belgium and Graz University of Technology, Austria
Pierangela Samarati	Università degli Studi di Milano, Italy
Riccardo Scandariato	K.U.Leuven, Belgium
Ingrid Schaumüller-Bichl	Upper Austria University of Applied Sciences, Austria
Jörg Schwenk	Ruhr-Universität Bochum, Germany
Andreas Uhl	University of Salzburg, Austria



Umut Uludag	Scientific and Technological Research Council (TUBITAK), Turkey
Vijay Varadharajan	Macquarie University, Australia
Pedro Veiga	University of Lisbon, Portugal
Tatjana Welzer	University of Maribor, Slovenia
Andreas Westfeld	University of Applied Sciences, Dresden, Germany
Ted Wobber	Microsoft Research Silicon Valley, USA
Shouhuai Xu	University of Texas at San Antonio, USA
Moti Yung	Google & Columbia University, USA

## Referees

Gergely Alpár	University of Nijmegen, The Netherlands
Haitham Al-Sinani	Royal Holloway, University of London, UK
Goekhan Bal	Goethe University Frankfurt, Germany
Nataliia Bielova	University of Trento, Italy
Christian Broser	University of Regensburg, Germany
Gerardo Fernandez	University of Malaga, Spain
Christoph Fritsch	University of Regensburg, Germany
Joaquin Garcia-Alfaro	Télécom Bretagne, France
Mohamed Maachaoui	IRIT - INP, France
Jef Maerien	K.U.Leuven, Belgium
Sascha Müller	TU Darmstadt, Germany
Khalid Salih Nasr	IRIT - INP, France
Adam O'Neill	University of Texas, Austin, USA
Tobias Pulls	Karlstad University, Sweden
Andreas Reisser	University of Regensburg, Germany
Boyeon Song	National Institute for Mathematical Sciences, Daejeon, Korea
Borislav Tadic	Deutsche Telekom AG, Germany
Peter Teufl	IAIK, TU Graz, Austria
Marianthi Theoharidou	Athens University of Economics and Business, Greece
T.T. Tun	University of Trento, Italy
Subhashini Venugopalan	Indian Institute of Technology, Madras, India
Ge Zhang	Karlstad University, Sweden
Zhenxin Zhan	University of Texas at San Antonio, USA
Bernd Zwattendorfer	IAIK, TU Graz, Austria

## Sponsoring Institutions/Companies

Belgian State (Belgian Science Policy), IAP Programme, P6/26, "BCRYPT"  
 Luciad  
 IBM  
 Google

# Table of Contents

---

## Part I: Research Papers

---

### Applicability and Interoperability

Analysis of Revocation Strategies for Anonymous Idemix Credentials . . .	3
<i>Jorn Lapon, Markulf Kohlweiss, Bart De Decker, and Vincent Naessens</i>	

### Architecture and Framework Security

A Secure Key Management Framework for Heterogeneous Wireless Sensor Networks . . . . .	18
<i>Mahdi R. Alagheband and Mohammad Reza Aref</i>	
Twin Clouds: Secure Cloud Computing with Low Latency (Full Version) . . . . .	32
<i>Sven Bugiel, Stefan Nürnberger, Ahmad-Reza Sadeghi, and Thomas Schneider</i>	

### Secure Hardware Platforms

Implementation Aspects of Anonymous Credential Systems for Mobile Trusted Platforms . . . . .	45
<i>Kurt Dietrich, Johannes Winter, Granit Luzhnica, and Siegfried Podesser</i>	

### Biometrics

Approximation of a Mathematical Aging Function for Latent Fingerprint Traces Based on First Experiments Using a Chromatic White Light (CWL) Sensor and the Binary Pixel Aging Feature . . . . .	59
<i>Ronny Merkel, Jana Dittmann, and Claus Vielhauer</i>	
Two-Factor Biometric Recognition with Integrated Tamper-Protection Watermarking . . . . .	72
<i>Reinhard Huber, Herbert Stögner, and Andreas Uhl</i>	

Feature Selection by User Specific Feature Mask on a Biometric Hash Algorithm for Dynamic Handwriting .....	85
<i>Karl Kümmel, Tobias Scheidat, Christian Arndt, and Claus Vielhauer</i>	

## Multimedia Security

Dynamic Software Birthmark for Java Based on Heap Memory Analysis .....	94
<i>Patrick P.F. Chan, Lucas C.K. Hui, and S.M. Yiu</i>	
A Secure Perceptual Hash Algorithm for Image Content Authentication .....	108
<i>Li Weng and Bart Preneel</i>	

## Network Security

Low-Attention Forwarding for Mobile Network Covert Channels .....	122
<i>Steffen Wendzel and Jörg Keller</i>	

## Authentication

Cryptanalysis of a SIP Authentication Scheme .....	134
<i>Fuwen Liu and Hartmut Koenig</i>	

---

## Part II: Work in Progress

---

## Applicability and Interoperability

Mapping between Classical Risk Management and Game Theoretical Approaches .....	147
<i>Lisa Rajbhandari and Einar Arthur Snekkenes</i>	
Digital Signatures: How Close Is Europe to Truly Interoperable Solutions? .....	155
<i>Konstantinos Rantos</i>	

## Architecture and Framework Security

A Generic Architecture for Integrating Health Monitoring and Advanced Care Provisioning .....	163
<i>Koen Decroix, Milica Milutinovic, Bart De Decker, and Vincent Naessens</i>	

## Secure Hardware Platforms

A Modular Test Platform for Evaluation of Security Protocols in NFC Applications . . . . .	171
<i>Geoffrey Ottoy, Jeroen Martens, Nick Saeys, Bart Preneel, Lieven De Strycker, Jean-Pierre Goemaere, and Tom Hamelinckx</i>	
GPU-Assisted AES Encryption Using GCM . . . . .	178
<i>Georg Schönberger and Jürgen Fuß</i>	

## Multimedia Security

Radon Transform-Based Secure Image Hashing . . . . .	186
<i>Dung Q. Nguyen, Li Weng, and Bart Preneel</i>	

## Network Security

On Detecting Abrupt Changes in Network Entropy Time Series . . . . .	194
<i>Philipp Winter, Harald Lampesberger, Markus Zeilinger, and Eckehard Hermann</i>	
Motif-Based Attack Detection in Network Communication Graphs . . . . .	206
<i>Krzysztof Juszczyszyn and Grzegorz Kołaczek</i>	

## Authentication

Secure Negotiation for Manual Authentication Protocols . . . . .	214
<i>Milica Milutinovic, Roel Peeters, and Bart De Decker</i>	
A Secure One-Way Authentication Protocol in IMS Context . . . . .	222
<i>Mohamed Maachaoui, Anas Abou El Kalam, and Christian Fraboul</i>	

---

## Part III: Posters

---

High Capacity FFT-Based Audio Watermarking . . . . .	235
<i>Mehdi Fallahpour and David Megías</i>	
Efficient Prevention of Credit Card Leakage from Enterprise Networks . . . . .	238
<i>Matthew Hall, Reinoud Koornstra, and Miranda Mowbray</i>	
Security Warnings for Children's Smart Phones: A First Design Approach . . . . .	241
<i>Jana Fruth, Ronny Merkel, and Jana Dittmann</i>	

Ciphertext-Policy Attribute-Based Broadcast Encryption Scheme . . . . .	244
<i>Muhammad Asim, Luan Ibraimi, and Milan Petković</i>	
Anonymous Authentication from Public-Key Encryption Revisited (Extended Abstract) . . . . .	247
<i>Daniel Slamanig</i>	

## Part IV: Keynotes

Mobile Identity Management . . . . .	253
<i>Jaap-Henk Hoepman</i>	
Who Needs Facebook Anyway - Privacy and Sociality in Social Network Sites . . . . .	254
<i>Ronald E. Leenes</i>	
From Protecting a System to Protecting a Global Ecosystem . . . . .	255
<i>Moti Yung</i>	
Erratum to: Communications and Multimedia Security . . . . .	E1
<i>Bart De Decker, Jorn Lapon, Vincent Naessens, and Andreas Uhl</i>	
<b>Author Index</b> . . . . .	257