Lecture Notes in Computer Science 7025

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

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

Springer

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

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)

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

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, BelSpo (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 Gambs	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

Multimedia Security

Network Security

Authentication

Part II: Work in Progress

Applicability and Interoperability

Architecture and Framework Security

Secure Hardware Platforms

Multimedia Security

Network Security

Authentication

Part III: Posters

Part IV: Keynotes