

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 David W. Chadwick (Eds.)

Communications and Multimedia Security

13th IFIP TC 6/TC 11 International Conference, CMS 2012
Canterbury, UK, September 3-5, 2012
Proceedings



Springer

Volume Editors

Bart De Decker

K.U. Leuven, Department of Computer Science, IBBT-DistriNet
Celestijnenlaan 200A, 3001 Leuven, Belgium
E-mail: bart.dedecker@cs.kuleuven.be

David W. Chadwick

University of Kent, School of Computing
Canterbury, Kent, CT2 7NZ, UK
E-mail: d.w.chadwick@kent.ac.uk

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-32804-6

e-ISBN 978-3-642-32805-3

DOI 10.1007/978-3-642-32805-3

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012944644

CR Subject Classification (1998): K.4.4, E.3, C.2.0, C.2, K.6.5, J.1, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© IFIP International Federation for Information Processing 2012

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)

Preface

It is with great pleasure that we present the proceedings of the 13th IFIP TC-6 and TC-11 Conference on Communications and Multimedia Security (CMS 2012), which was held in Canterbury, UK, during September 3–5, 2012. The meeting continues the tradition of previous CMS conferences which were held in Ghent, Belgium (2011), and Linz, Austria (2010).

The Program Committee (PC) received 43 submissions, comprising 31 full papers, 9 short papers, and 3 extended abstracts, out of which only 6 full papers were accepted (19% acceptance rate). In this edition, we have included eight short papers, which describe valuable work-in-progress, as well as eight extended abstracts, which describe the posters that were discussed at the conference. Some of the latter two categories are shortened versions of original full or short paper submissions, respectively, which the PC judged to be valuable contributions but somewhat premature for submission under their original category.

We are also grateful to Siani Pearson (Cloud and Security Research Lab, HP Labs Bristol, UK) and Jon Crowcroft (University of Cambridge, UK) for accepting our invitations to deliver keynote addresses, which can be found at the end of these proceedings.

We would also like to say a word of appreciation to our sponsors: Google and HP. Without their financial support, it would not have been possible to attract as many young researchers or provide as rich a social program.

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 2012.

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

September 2012

David W. Chadwick
Bart De Decker

Organization

CMS 2012 was the 13th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security. It was organized by the University of Kent, UK.

Executive Committee

Conference Chair

Bart De Decker KU Leuven, Belgium

Program Co-chairs

David W. Chadwick
Bart De Decker

Organizing Chair

David W. Chadwick University of Kent, UK

Organizing Committee

David Chadwick
Angela Doe
Kaniz Fatema
James Lewis
Kristy Siu

Program Committee

Anas Abou El Kalam	UCA-ENSA of Marrakesh, Morocco
Patrick 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 F. Ciocarlie	Computer Science Lab, SRI International, 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	KU Leuven, Belgium
Lieven Desmet	KU Leuven, Belgium

VIII Organization

Lieven De Strycker	Katholieke Hogeschool Sint-Lieven, Belgium
Jana Dittmann	University of Magdeburg, Germany
Stelios Dritsas	Athens University of Economics and Business, Greece
Gerhard Eschelbeck	Sophos, USA
Simone Fischer-Hübner	Karlstad University, Sweden
Teddy Furon	INRIA Rennes - Bretagne Atlantique, France
Jürgen Fuß	University of Applied Sciences Upper Austria, Hagenberg, Austria
Sébastien Gambs	Université de Rennes 1 - INRIA / IRISA, France
Christian Geuer-Pollmann	Microsoft Research, Germany
Dieter Gollmann	Hamburg University of Technology, Germany
Rüdiger Grimm	University of Koblenz, Germany
Jean Hennebert	University of Applied Sciences, HES-SO, Switzerland
Eckehard Hermann	University of Applied Sciences Upper Austria, Austria
Jaap-Henk Hoepman	TNO / Radboud University Nijmegen, The Netherlands
Andreas Humm	University of Fribourg, Switzerland
Edward Humphreys	XiSEC, UK
Christophe Huygens	KU Leuven, Belgium
Witold Jacak	University of Applied Sciences Upper Austria, 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
Romain Laborde	Institut de Recherche en Informatique de Toulouse (IRIT), France
Jorn Lapon	Katholieke Hogeschool Sint-Lieven, Belgium
Herbert Leitold	Secure Information Technology Center (A-SIT), Austria
Javier Lopez	University of Malaga, Spain
Louis Marinou	European Network and Information Security Agency (ENISA), Greece
Keith Martin	Royal Holloway, University of London, UK
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	Katholieke Hogeschool Sint-Lieven, Belgium
Peter Neumann	Computer Science Lab, SRI International, USA
Nick Nikiforakis	KU Leuven, Belgium
Chandrasekaran Pandurangan	Indian Institute of Technology, Madras, India
Günther Pernul	University of Regensburg, Germany
Alessandro Piva	University of Florence, Italy
Bart Preneel	KU Leuven, Belgium
Jean-Jacques Quisquater	Université catholique de Louvain, Belgium
Kai Rannenber	Goethe University Frankfurt, Germany
Vincent Rijmen,	KU Leuven, Belgium
Pierangela Samarati	Università degli Studi di Milano, Italy
Riccardo Scandariato	KU Leuven, Belgium
Ingrid Schaumüller-Bichl	University of Applied Sciences Upper Austria, Austria
Jörg Schwenk	Ruhr-Universität Bochum, Germany
Einar Snekkenes	Gjovik University College, Norway
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
Claus Vielhauer	Brandenburg University of Applied Sciences, Germany
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 and Columbia University, USA
Gansen Zhao	South China Normal University, China

Reviewers

Christian Broser	University of Regensburg, Germany
Andrzej Drygajlo	École polytechnique fédérale de Lausanne EPFL, Switzerland
Joaquin Garcia-Alfaro	Télécom Bretagne, France
Sascha Koschinat	Goethe University Frankfurt, Germany
Andreas Leicher	Goethe University Frankfurt, Germany
Weiliang Luo	University of Texas at San Antonio, USA
Stefan Meier	University of Regensburg, Germany
Francisco Moyano	University of Malaga, Spain
Alexios Mylonas	Athens University of Economics and Business, Greece

Ahmad Sabouri	Goethe University Frankfurt, Germany
Peter Teuffl	Graz University of Technology, Austria
Lei Zang	Google, USA
Zhenxin Zhan	University of Texas at San Antonio, USA
Bernd Zwattendorfer	Graz University of Technology, Austria

Sponsoring Institutions/Companies

Google

HP

Table of Contents

Part I: Research Papers

Image and Handwriting Analysis

- Robust Resampling Detection in Digital Images 3
Hieu Cuong Nguyen and Stefan Katzenbeisser
- Feature Selection on Handwriting Biometrics: Security Aspects of
Artificial Forgeries 16
Karl Kümmel, Tobias Scheidat, Claus Vielhauer, and Jana Dittmann
- Security Analysis of Image-Based PUFs for Anti-counterfeiting 26
Salomeh Shariati, François Koeune, and François-Xavier Standaert

Authentication and Performance

- Document Authentication Using 2D Codes: Maximizing the Decoding
Performance Using Statistical Inference 39
Mouhamadou L. Diong, Patrick Bas, Chloé Pelle, and Wadih Sawaya
- Data-Minimizing Authentication Goes Mobile 55
*Patrik Bichsel, Jan Camenisch, Bart De Decker, Jorn Lapon,
Vincent Naessens, and Dieter Sommer*
- No Tradeoff between Confidentiality and Performance: An Analysis on
H.264/SVC Partial Encryption 72
Zhuo Wei, Xuhua Ding, Robert Huijie Deng, and Yongdong Wu

Part II: Work in Progress

Biometrics, Forensics and Watermarking

- Computer-Aided Contact-Less Localization of Latent Fingerprints in
Low-Resolution CWL Scans 89
*Andrey Makrushin, Tobias Kiertscher, Robert Fischer,
Stefan Gruhn, Claus Vielhauer, and Jana Dittmann*
- A Method for Reducing the Risk of Errors in Digital Forensic
Investigations 99
Graeme Horsman, Christopher Laing, and Paul Vickers

Short Term Template Aging Effects on Biometric Dynamic Handwriting Authentication Performance 107
Tobias Scheidat, Karl Kümmel, and Claus Vielhauer

A New Approach to Commutative Watermarking-Encryption 117
Roland Schmitz, Shujun Li, Christos Grecos, and Xinpeng Zhang

Communications Security

Systematic Engineering of Control Protocols for Covert Channels 131
Steffen Wendzel and Jörg Keller

Efficiency of Secure Network Coding Schemes 145
Elke Franz, Stefan Pfennig, and André Fischer

A New Approach for Private Searches on Public-Key Encrypted Data 160
Amar Siad

Multi-level Authentication Based Single Sign-On for IMS Services 174
Mohamed Maachaoui, Anas Abou El Kalam, Christian Fraboul, and Abdellah Ait Ouahman

Part III: Extended Abstracts

Are 128 Bits Long Keys Possible in Watermarking? 191
Patrick Bas and Teddy Furon

Predicate-Tree Based Pretty Good Privacy of Data 192
William Perrizo and Arjun G. Roy

OOXML File Analysis of the July 22nd Terrorist Manual 195
Hanno Langweg

Privacy-Preserving Scheduling Mechanism for eHealth Systems 198
Milica Milutinovic, Vincent Naessens, and Bart De Decker

Cuteforce Analyzer: Implementing a Heterogeneous Bruteforce Cluster with Specialized Coprocessors 201
Jürgen Fuß, Wolfgang Kastl, Robert Kolmhofer, Georg Schönberger, and Florian Wex

A Framework for Enforcing User-Based Authorization Policies on Packet Filter Firewalls 204
André Zúquete, Pedro Correia, and Miguel Rocha

From Biometrics to Forensics: A Feature Collection and First Feature Fusion Approaches for Latent Fingerprint Detection Using a Chromatic White Light (CWL) Sensor	207
<i>Robert Fischer, Tobias Kiertscher, Stefan Gruhn, Tobias Scheidat, and Claus Vielhauer</i>	
Practical Revocable Anonymous Credentials	211
<i>Jan Hajny and Lukas Malina</i>	

Part IV: Keynotes

Privacy Management in Global Organisations.	217
<i>Siani Pearson</i>	
From Panopticon to Fresnel, Dispelling a False Sense of Security	238
<i>Jon Crowcroft and Ian Brown</i>	
Author Index	243