Lecture Notes in Computer Science 8099

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

Editorial Board

Bart De Decker Jana Dittmann
Christian Kraetzer Claus Vielhauer (Eds.)

Communications and Multimedia Security

14th IFIP TC 6/TC 11 International Conference, CMS 2013
Magdeburg, Germany, September 25-26, 2013
Proceedings

Springer

Volume Editors

Bart De Decker
KU Leuven, Department of Computer Science, iMinds-DistriNet
Celestijnenlaan 200A, 3001 Leuven, Belgium
E-mail: bart.dedecker@cs.kuleuven.be

Jana Dittmann
Otto-von-Guericke-Universität Magdeburg
Universitätsplatz 2, 39106 Magdeburg, Germany
E-mail: jana.dittmann@iti.cs.uni-magdeburg.de

Christian Kraetzer
Otto-von-Guericke-Universität Magdeburg
Universitätsplatz 2, 39106 Magdeburg, Germany
E-mail: kraetzer@iti.cs.uni-magdeburg.de

Claus Vielhauer
Fachhochschule Brandenburg/Otto-von-Guericke-Universität Magdeburg
Magdeburger Str. 50, 14770 Brandenburg, Germany
E-mail: claus.vielhauer@fh-brandenburg.de

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-40778-9 e-ISBN 978-3-642-40779-6
DOI 10.1007/978-3-642-40779-6
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: : 2013946793

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

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 14th IFIP TC-6 and TC-11 Conference on Communications and Multimedia Security (CMS 2013), which was held in Magdeburg, Germany during September 25–26, 2013. The meeting continues the tradition of previous CMS conferences which were held in Canterbury, UK (2012), Ghent, Belgium (2011) and Linz, Austria (2010).

The Program Committee (PC) received 30 submissions, comprising 23 full papers, 6 short papers and 1 extended abstract, out of which only 5 full papers were accepted (22% acceptance rate). In this edition, we have included 11 short papers, which describe valuable work-in-progress, as well as 5 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 grateful to Prof. Sabah Jassim of the University of Buckingham, UK and Prof. Sachar Paulus of the Brandenburg University of Applied Sciences, Brandenburg, Germany for accepting our invitations to deliver keynote addresses, the abstracts of which can be found at the end of these proceedings.

We would also like to say a word of appreciation to our sponsor: The Advanced Multimedia and Security Lab (AMSL) of the Otto-von-Guericke University of Magdeburg. Without its financial support, it would not have been possible 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 an a interesting evening event. For us, it was a distinct pleasure to serve as program chairs of CMS 2013.

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

September 2013

Bart De Decker
Jana Dittmann
Claus Vielhauer

Organization

CMS 2013 is the 14th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security. It has been organized by the Otto-von-Guericke University of Magdeburg, Germany.

Executive Committee

Conference Chair

Claus Vielhauer	Brandenburg University of Applied Sciences, Germany

Program Co-Chairs

Bart De Decker	KU Leuven, Belgium
Jana Dittmann	Otto-von-Guericke University Magdeburg, Germany
Claus Vielhauer	

Organizing Chair

Jana Dittmann

Organizing Committee

Jana Dittmann
Christian Kraetzer
Silke Reifgerste

Program Committee

Anas Abou El Kalam	UCA-ENSA of Marrakesh, Morocco
Eric Alata	LAAS-CNRS, France
Patrick Bas	CNRS-Lagis, Lille, France
David W. Chadwick	University of Kent, UK
Howard Chivers	University of York, UK
Isabelle Chrisment	LORIA-University of Nancy, France
Gabriela F. Ciocarlie	Computer Science Lab, SRI International, USA
Frédéric Cuppens	Télécom Bretagne, France
Italo Dacosta	KU Leuven, Belgium
Hervé Debar	Télécom SudParis, France

Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Bart De Decker	KU Leuven, Belgium
Yvo Desmedt	University of Texas at Dallas, USA and University College London, UK
Lieven De Strycker	KU Leuven, Technology Campus Ghent, 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
Jean Hennebert	University of Applied Sciences, HES-SO, Switzerland
Eckehard Hermann	University of Applied Sciences Upper Austria, Hagenberg, Austria
Jens Hermans	KU Leuven, Belgium
Andreas Humm	University of Fribourg, Switzerland
Edward Humphreys	XiSEC, UK
Christophe Huygens	KU Leuven, Belgium
Witold Jacak	University of Applied Sciences Upper Austria, Hagenberg, Austria
Sushil Jajodia	George Mason University, USA
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	KU Leuven, Technology Campus Ghent, Belgium
Herbert Leitold	Secure Information Technology Center (A-SIT), Austria
Javier Lopez	University of Malaga, Spain
Louis Marinos	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
Yuko Murayama	Iwate Prefectural University, Japan
Vincent Naessens	KU Leuven, Technology Campus Ghent, Belgium
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
Franz-Stefan Preiss	IBM Research - Zurich, Switzerland
Jean-Jacques Quisquater	Université catholique de Louvain, Belgium
Kai Rannenberg	Goethe University Frankfurt, Germany
Pierangela Samarati	Università degli Studi di Milano, Italy
Riccardo Scandariato	KU Leuven, Belgium
Ingrid Schaumüller-Bichl	University of Applied Sciences Upper Austria, Hagenberg, Austria
Jörg Schwenk	Ruhr-Universität Bochum, Germany
Stefaan Seys	KU Leuven, Belgium
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	Dresden University of Applied Sciences, Germany
Ted Wobber	Microsoft Research Silicon Valley, USA
Shouhuai Xu	University of Texas at San Antonio, USA
Moti Yung	Google & Columbia University, USA
Gansen Zhao	South China Normal University, China
Ge Zhang	Karlstad University, Sweden

Reviewers

Filipe Beato	Microsoft Research, Cambridge, UK
Michael Diener	University of Regensburg, Germany
Jean-Luc Dugelay	Eurécom, France
Miltiadis Kandias	Athens University of Economics and Business, Greece

Andrea Melle	Eurécom, France
Aleksios Mylonas	Athens University of Economics and Business, Greece
Moritz Riesner	University of Regensburg, Germany
Ahmad Sabouri	Goethe University Frankfurt, Germany
Moustafa Saleh	University of Texas, San Antonio, USA
Dieter Sommer	IBM Research - Zurich, Switzerland
Fatbardh Veseli	Goethe University Frankfurt, Germany
Qingji Zheng	University of Texas, San Antonio, USA

Sponsoring Institutions

The Advanced Multimedia and Security Lab (AMSL) of the Otto-von-Guericke University of Magdeburg, Germany.

Table of Contents

Part I: Research Papers

Biometrics

Towards a Standardised Testsuite to Assess Fingerprint Matching Robustness: The StirMark Toolkit – Cross-Feature Type Comparisons 3
Jutta Hämmerle-Uhl, Michael Pober, and Andreas Uhl

Achieving Anonymity against Major Face Recognition Algorithms 18
Benedikt Driessen and Markus Dürmuth

Client-Side Biometric Verification Based on Trusted Computing 34
Jan Vossaert, Jorn Lapon, Bart De Decker, and Vincent Naessens

Applied Cryptography

Dedicated Hardware for Attribute-Based Credential Verification 50
Geoffrey Ottoy, Jorn Lapon, Vincent Naessens, Bart Preneel, and Lieven De Strycker

Decentralized Ciphertext-Policy Attribute-Based Encryption Scheme with Fast Decryption 66
Y. Sreenivasa Rao and Ratna Dutta

Part II: Work in Progress

Biometrics

Security of Features Describing the Visual Appearance of Handwriting Samples Using the Bio-hash Algorithm of Vielhauer against an Evolutionary Algorithm Attack 85
Andreas Hasselberg, Rene Zimmermann, Christian Kraetzer, Tobias Scheidat, Claus Vielhauer, and Karl Kümmel

Digital Watermarking, Steganography and Forensics

Video Watermarking Scheme with High Payload and Robustness against Geometric Distortion 95
Huajian Liu, Yiyao Li, and Martin Steinebach

Use of Linear Error-Correcting Subcodes in Flow Watermarking for Channels with Substitution and Deletion Errors 105
Boris Assanovich, William Puech, and Iuliia Tkachenko

Detecting Resized Double JPEG Compressed Images – Using Support Vector Machine 113
Hieu Cuong Nguyen and Stefan Katzenbeisser

Pit Stop for an Audio Steganography Algorithm 123
Andreas Westfeld, Jürgen Wurzer, Christian Fabian, and Ernst Piller

Robust Hash Algorithms for Text 135
Martin Steinebach, Peter Klöckner, Nils Reimers, Dominik Wienand, and Patrick Wolf

Hardware Based Security Enhanced Direct Memory Access 145
Marcel Eckert, Igor Podebrad, and Bernd Klauer

Social Network Privacy, Security and Authentication

Privacy Visor: Method for Preventing Face Image Detection by Using Differences in Human and Device Sensitivity 152
Takayuki Yamada, Seiichi Gohshi, and Isao Echizen

E-Learning of IT Security Threats: A Game Prototype for Children 162
Jana Fruth, Carsten Schulze, Marleen Rohde, and Jana Dittmann

Hiding Information in Social Networks from De-anonymization Attacks by Using Identity Separation 173
Gábor György Gulyás and Sándor Imre

An Equivalent Access Based Approach for Building Collaboration Model between Distinct Access Control Models 185
Xiaofeng Xia

Part III: Extended Abstracts

Authentication with Time Features for Keystroke Dynamics on Touchscreens 197
Matthias Trojahn, Florian Arndt, and Frank Ortmeier

Visibility Assessment of Latent Fingerprints on Challenging Substrates in Spectroscopic Scans 200
Mario Hildebrandt, Andrey Makrushin, Kun Qian, and Jana Dittmann

Creation of a Public Corpus of Contact-Less Acquired Latent Fingerprints without Privacy Implications 204
Mario Hildebrandt, Jennifer Sturm, Jana Dittmann, and Claus Vielhauer

SocACL: An ASP-Based Access Control Language for Online Social Networks 207
Edward Caprin and Yan Zhang

Watermark Resynchronization: An Efficient Approach Based on Eulerian Tours around a Robust Skeleton 211
Konstantinos Raftopoulos, Klimis Ntalianis, Paraskevi Tzouveli, Nicolas Tsapatsoulis, Aleatha Parker-Wood, and Marin Ferecatu

Part IV: Keynotes

Face Recognition from Degraded Images – Super Resolution Approach by Non-adaptive Image-Independent Compressive Sensing Dictionaries 217
Sabah A. Jassim

Trustworthy Software Development 233
Sachar Paulus, Nazila Gol Mohammadi, and Thorsten Weyer

Author Index 249