

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

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 André Zúquete (Eds.)

Communications and Multimedia Security

15th IFIP TC 6/TC 11 International Conference, CMS 2014
Aveiro, Portugal, September 25-26, 2014
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

André Zúquete

University of Aveiro, DETI/IEETA

Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

E-mail: andre.zuquete@ua.pt

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-662-44884-7

e-ISBN 978-3-662-44885-4

DOI 10.1007/978-3-662-44885-4

Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014948333

LNCS Sublibrary: SL 4 – Security and Cryptology

© IFIP International Federation for Information Processing 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, 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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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 15th IFIP TC-6 and TC-11 Conference on Communications and Multimedia Security (CMS 2014), which was held in Aveiro, Portugal during September 25–26, 2014. The meeting continues the tradition of previous CMS conferences which were held in Magdeburg, Germany (2013), Canterbury, UK (2012), Ghent, Belgium (2011) and Linz, Austria (2010).

The Program Committee (PC) received 22 submissions, comprising 16 full papers, 3 short papers and 3 extended abstracts, out of which only 4 full papers were accepted (25% acceptance rate). In this edition, we have included 6 short papers, which describe valuable work-in-progress, as well as 3 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 Paulo Mateus, of the Instituto Superior Técnico/University of Lisbon and Rui Melo Biscaia, of Watchful Software, 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 sponsors, the Institute of Electronics and Telematics Engineering of Aveiro (IEETA) and the University of Aveiro, for hosting the conference and providing all the human and material support requested by the Organizing Committee.

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 interesting evening event. For us, it was a distinct pleasure to serve as program chairs of CMS 2014.

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

September 2014

Bart De Decker
André Zúquete

VIII Organization

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 Desmet	KU Leuven, Belgium
Lieven De Strycker	KU Leuven, Technology Campus Ghent, Belgium
Jana Dittmann	Otto-von-Guericke University Magdeburg, Germany
Stelios Dritsas	Athens University of Economics and Business, Greece
Gerhard Eschelbeck	Sophos, USA
Simone Fischer-Hübner	Karlstad University, Sweden
Steven Furnell	Plymouth University, UK
Jürgen Fuß	University of Applied Sciences Upper Austria, Austria
Sébastien Gambs	Université de Rennes 1 - Inria/IRISA, France
Dieter Gollmann	Hamburg University of Technology, Germany
Rüdiger Grimm	University of Koblenz, Germany
Eckehard Hermann	University of Applied Sciences Upper Austria, Austria
Jens Hermans	KU Leuven, Belgium
Alejandro Hevia	University of Chile, Chile
Andreas Humm	University of Fribourg, Switzerland
Christophe Huygens	KU Leuven, Belgium
Sushil Jajodia	George Mason University, USA
Günter Karjoth	Lucerne University of Applied Sciences and Arts, Switzerland
Stefan Katzenbeisser	TU Darmstadt, Germany
Ella Kolkowska	Swedish Business School, Örebro University, Sweden
Robert Kolmhofer	University of Applied Sciences Upper Austria, Austria
Christian Kraetzer	Otto-von-Guericke University Magdeburg, Germany
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
Keith Martin	Royal Holloway, University of London, UK
Chris Mitchell	Royal Holloway, University of London, UK
Yuko Murayama	Iwate Prefectural University, Japan
Vincent Naessens	KU Leuven, Technology Campus Ghent, Belgium
Eiji Okomoto	University of Tsukuba, Japan
Chandrasekaran Pandurangan	Indian Institute of Technology, 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 Rannenber	Goethe University Frankfurt, Germany
Carlos Ribeiro	Instituto Superior Técnico, Portugal
Sergi Robles	Universitat Autònoma de Barcelona, Spain
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 University Bochum, Germany
Stefaan Seys	KU Leuven, Belgium
Herman Sikora	Johannes Kepler University of Linz, Austria
Einar Snekkenes	Gjøvik University College, Norway
Andreas Uhl	University of Salzburg, Austria
Umut Uludag	Scientific and Technological Research Council (TUBITAK), Turkey
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
Gansen Zhao	South China Normal University, China
Ge Zhang	Karlstad University, Sweden
André Zúquete	IEETA, University of Aveiro, Portugal

Reviews

Cristina Alcaraz	University of Malaga, Spain
Philippe De Ryck	KU Leuven, Belgium
Michael Diener	University of Regensburg, Germany
Jingtao Li	Fudan University, China

Tarik Moataz

Télécom Bretagne, France

Roel Peeters

KU Leuven, Belgium

Sarah Louise Renwick

Royal Holloway, University of London, UK

Ahmad Sabouri

Goethe University Frankfurt, Germany

Thomas Zefferer

Graz University of Technology, Austria

Sponsoring Institutions

DETI / IEETA, University of Aveiro, Portugal.

Table of Contents

Part I: Research Papers

Malicious MPLS Policy Engine Reconnaissance	3
<i>Abdulrahman Al-Mutairi and Stephen Wolthusen</i>	
USB Connection Vulnerabilities on Android Smartphones: Default and Vendors' Customizations	19
<i>André Pereira, Manuel Correia, and Pedro Brandão</i>	
Free Typed Text Using Keystroke Dynamics for Continuous Authentication	33
<i>Paulo Pinto, Bernardo Patrão, and Henrique Santos</i>	
Secure Storage on Android with Context-Aware Access Control	46
<i>Faysal Boukayoua, Jorn Lapon, Bart De Decker, and Vincent Naessens</i>	

Part II: Work in Progress

A Study on Advanced Persistent Threats	63
<i>Ping Chen, Lieven Desmet, and Christophe Huygens</i>	
Dynamic Parameter Reconnaissance for Stealthy DoS Attack within Cloud Systems	73
<i>Suaad Alarifi and Stephen Wolthusen</i>	
Touchpad Input for Continuous Biometric Authentication	86
<i>Alexander Chan, Tzipora Halevi, and Nasir Memon</i>	
A Federated Cloud Identity Broker-Model for Enhanced Privacy via Proxy Re-Encryption	92
<i>Bernd Zwattendorfer, Daniel Slamanig, Klaus Stranacher, and Felix Hörandner</i>	
D-Shuffle for Prêt à Voter	104
<i>Dalia Khader</i>	
An Approach to Information Security Policy Modeling for Enterprise Networks	118
<i>Dmitry Chernyavskiy and Natalia Miloslavskaya</i>	

Part III: Extended Abstracts

Introduction to Attribute Based Searchable Encryption 131
Dalia Khader

Risk Analysis of Physically Unclonable Functions 136
*Andrea Kolberger, Ingrid Schaumüller-Bichl,
and Martin Deutschmann*

Decentralized Bootstrap for Social Overlay Networks 140
Rodolphe Marques and André Zúquete

Part IV: Keynotes

Enhancing Privacy with Quantum Networks 147
Paulo Mateus, Nikola Paunković, João Rodrigues, and André Souto

The Fundamental Principle of Breach Prevention 154
Rui Melo Biscaia

Author Index 157