

*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 of Computer Science, Saarbruecken, Germany*

Bart De Decker Ingrid Schaumüller-Bichl (Eds.)

# Communications and Multimedia Security

11th IFIP TC 6/TC 11 International Conference, CMS 2010  
Linz, Austria, May 31 – June 2, 2010  
Proceedings

## Volume Editors

Bart De Decker

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

Celestijnenlaan 200A, 3001 Leuven, Belgium

E-mail: bart.dedecker@cs.kuleuven.be

Ingrid Schaumüller-Bichl

Upper Austria University of Applied Sciences

School of Informatics, Communications and Media

Softwarepark 11, 4232 Hagenberg, Austria

E-mail: ingrid.schaumueller-bichl@fh-hagenberg.at

Library of Congress Control Number: 2010926923

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

ISSN 0302-9743

ISBN-10 3-642-13240-5 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-13240-7 Springer Berlin Heidelberg New York

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.

springer.com

© IFIP International Federation for Information Processing 2010

Printed in Germany

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

Printed on acid-free paper 06/3180

# Preface

Over the last decade, we have witnessed a growing dependency on information technology resulting in a wide range of new opportunities. Clearly, it has become almost impossible to imagine life without a personal computer or laptop, or without a cell phone. Social network sites (SNS) are competing with face-to-face encounters and may even oust them. Most SNS-adepts have hundreds of “friends”, happily sharing pictures and profiles and endless chitchat. We are on the threshold of the Internet of Things, where every object will have its RFID-tag. This will not only effect companies, who will be able to optimize their production and delivery processes, but also end users, who will be able to enjoy many new applications, ranging from smart shopping, and smart fridges to geo-localized services. In the near future, elderly people will be able to stay longer at home due to clever health monitoring systems. The sky seems to be the limit! However, we have also seen the other side of the coin: viruses, Trojan horses, breaches of privacy, identity theft, and other security threats. Our real and virtual worlds are becoming increasingly vulnerable to attack. In order to encourage security research by both academia and industry and to stimulate the dissemination of results, conferences need to be organized.

With the 11th edition of the joint IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2010), the organizers resumed the tradition of previous CMS conferences after a three-year recess. It is with great pleasure that we present the proceedings of CMS 2010, which was held in Linz, Austria on May 31 – June 2, 2010. The conference was organized by the Department of Secure Information Systems, Upper Austria University of Applied Sciences, School of Informatics, Communications, and Media, Hagenberg.

The program committee (PC) received 55 submissions out of which 23 papers were accepted. We would like to thank all the authors who submitted papers. Each paper was anonymously reviewed by three to four 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: VoIP, TLS, web services, watermarking, biometrics, risk management, just to name a few.

This year, the conference featured a poster session in which authors could present “work in progress”. We are grateful to Taher Elgamal (Axway Inc), Edward Humphreys (XiSEC) and Klaus Gheri (phion AG - a Barracuda Networks company) for accepting our invitation to deliver keynote speeches.

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

May 2010

Bart De Decker  
Ingrid Schaumüller-Bichl

# Organization

## General Chair

Ingrid Schaumüller-Bichl      Upper Austria University of Applied Sciences,  
Campus Hagenberg, Austria

## Program Chair

Bart De Decker      K.U.Leuven, Belgium

## Organizing Chair

Robert Kolmhofer      Upper Austria University of Applied Sciences,  
Campus Hagenberg, Austria

## Program Committee

Helen Armstrong	Curtin Business School, Australia
Wilhelm Burger	University of Applied Sciences, Hagenberg, Austria
Jan Camenisch	IBM Zurich Research Lab, Switzerland
David Chadwick	University of Kent, UK
Howard Chivers	Cranfield University, UK
Gabriela Cretu-Ciocarlie	Columbia University, USA
Frédéric Cuppens	ENST-Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Gerhard Eschelbeck	Webroot Software Inc., USA
Simone Fischer-Hübner	University of Karlstad, Sweden
Jürgen Fuß	University of Applied Sciences, Hagenberg, Austria
Sébastien Gambis	INRIA, France
Christian Geuer-Pollmann	EMIC, Germany
Dieter Gollmann	University of Hamburg, Germany
Rüdiger Grimm	University of Koblenz-Landau, Germany
Eckehard Hermann	University of Applied Sciences, Hagenberg, Austria
Jaap-Henk Hoepman	Radboud University Nijmegen, Netherlands
Russ Housley	Vigil Security, USA
Ted Humphreys	Xisec, UK
Witold Jacak	University of Applied Sciences, Hagenberg, Austria
Lech Janczewski	University of Auckland, New Zealand

## VIII Organization

Stefan Katzenbeisser	TU Darmstadt, Germany
Markulf Kohlweiss	K.U.Leuven, Belgium
Herbert Leitold	Technical University of Graz, Austria
Javier Lopez	University of Malaga, Spain
Louis Marinou	ENISA, Greece
Chris Mitchell	Royal Holloway, University of London, UK
Refik Molva	Institut Eurécom, France
Yoko Murayama	Iwate Prefectural University, Japan
Jörg R. Mühlbacher	Johannes Kepler University Linz, Austria
Vincent Naessens	Kath. Hogeschool Sint-Lieven, Gent, Belgium
Günther Pernul	University of Regensburg, Germany
Gerald Quirchmayr	University of Vienna, Austria
Jean-Jacques Quisquater	UCL, Belgium
Kai Rannenber	Goethe University Frankfurt, Germany
Vincent Rijmen	K.U.Leuven, Belgium & TU Graz, Austria
Pierangela Samarati	Università degli Studi di Milano, Italy
Riccardo Scandariato	K.U.Leuven, Belgium
Ingrid Schaumüller-Bichl	University of Applied Sciences, Hagenberg, Austria
Jörg Schwenk	Horst Görtz Institute, Germany
Hermann Sikora	GRZ IT Group, Austria
Leon Strous	De Nederlandsche Bank, Netherlands
Andreas Uhl	University of Salzburg, Austria
Rossouw von Solms	Nelson Mandela Metropolitan University, South-Africa
Tatjana Welzer	University of Maribor, Slovenia

## Local Organization

Department of Secure Information Systems, Upper Austria University of Applied Sciences, Campus Hagenberg, Austria

Robert Kolmhofer	Margit Lehner
Johannes Edler	Alexander Leitner
Jürgen Fuß	Anna Perschl
Eckehard Hermann	Dieter Vymazal
Yvonne Horner	Markus Zeilinger

## External Reviewers

Isaac Agudo	Matei Ciocarlie
Cristina Alcaraz	Gouenou Coatrieux
Claudio Agostino Ardagna	Nora Cuppens-Boulahia
Goekhan Bal	Leucio-Antonio Cutillo
Stefan Berthold	Stefan Dürbeck
Martin Centner	Kaoutar Elkhiyaoui

Christoph Fritsch  
Oliver Gmelch  
Hans Hedbom  
Marvin Hegen  
Stephan Heim  
Maarten Jacobs  
Tibor Jager  
Burt Kaliski  
Pablo Najera  
Michael Netter  
Anna Perschl  
Christian Rathgeb

Andreas Reisser  
Ruben Rios  
Sven Schäge  
Koen Simoens  
Peter Teufl  
Julien Thomas  
Dieter Vymazal  
Christian Weber  
Li Weng  
Lars Wolos  
Ge Zhang

# Table of Contents

Keynotes .....	1
<b>WiFi and RF Security</b>	
A Scalable Wireless Routing Protocol Secure against Route Truncation Attacks .....	4
<i>Amitabh Saxena and Ben Soh</i>	
Probabilistic Vehicular Trace Reconstruction Based on RF-Visual Data Fusion .....	16
<i>Saif Al-Kuwari and Stephen D. Wolthusen</i>	
<b>XML and Web Services Security</b>	
Throwing a MonkeyWrench into Web Attackers Plans .....	28
<i>Armin Büscher, Michael Meier, and Ralf Benzmüller</i>	
Security in OpenSocial-Instrumented Social Networking Services .....	40
<i>Matthias Häsel and Luigi Lo Iacono</i>	
Security for XML Data Binding .....	53
<i>Nils Gruschka and Luigi Lo Iacono</i>	
<b>Watermarking and Multimedia Security</b>	
Watermark Detection for Video Bookmarking Using Mobile Phone Camera .....	64
<i>Peter Meerwald and Andreas Uhl</i>	
Watermark-Based Authentication and Key Exchange in Teleconferencing Systems .....	75
<i>Ulrich Rüßmair, Stefan Katzenbeisser, Martin Steinebach, and Sascha Zmudzinski</i>	
Efficient Format-Compliant Encryption of Regular Languages: Block-Based Cycle-Walking .....	81
<i>Thomas Stütz and Andreas Uhl</i>	



## Analysis and Detection of Malicious Code and Risk Management

Statistical Detection of Malicious PE-Executables for Fast Offline Analysis .....	93
<i>Ronny Merkel, Tobias Hoppe, Christian Kraetzer, and Jana Dittmann</i>	
A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC) .....	106
<i>Nicolas Racz, Edgar Weippl, and Andreas Seufert</i>	
Business and IT Continuity Benchmarking .....	118
<i>Wolfgang Neudorfer, Louis Marinos, and Ingrid Schaumüller-Bichl</i>	

## VoIP Security

Peer-to-Peer VoIP Communications Using Anonymisation Overlay Networks .....	130
<i>Ge Zhang and Simone Fischer-Hübner</i>	
SIP Proxies: New Reflectors in the Internet .....	142
<i>Ge Zhang, Jordi Jaen Pallares, Yacine Rebahi, and Simone Fischer-Hübner</i>	
Analysis of Token and Ticket Based Mechanisms for Current VoIP Security Issues and Enhancement Proposal .....	154
<i>Patrick Battistello and Cyril Delétré</i>	

## Biometrics

Entropy of Graphical Passwords: Towards an Information-Theoretic Analysis of Face-Recognition Based Authentication .....	166
<i>Stefan Rass, David Schuller, and Christian Kollmitzer</i>	
Handwriting Biometric Hash Attack: A Genetic Algorithm with User Interaction for Raw Data Reconstruction .....	178
<i>Karl Kümmel, Claus Vielhauer, Tobias Scheidat, Dirk Franke, and Jana Dittmann</i>	
Privacy Preserving Key Generation for Iris Biometrics .....	191
<i>Christian Rathgeb and Andreas Uhl</i>	

## Applied Cryptography

Generalizations and Extensions of Redactable Signatures with Applications to Electronic Healthcare .....	201
<i>Daniel Slamanig and Stefan Rass</i>	

Chosen-Ciphertext Secure Certificateless Proxy Re-Encryption . . . . .	214
<i>Chul Sur, Chae Duk Jung, Youngho Park, and Kyung Hyune Rhee</i>	
Detecting Hidden Encrypted Volumes . . . . .	233
<i>Christopher Hargreaves and Howard Chivers</i>	
<b>Secure Communications</b>	
Tor HTTP Usage and Information Leakage . . . . .	245
<i>Markus Huber, Martin Mulazzani, and Edgar Weippl</i>	
Secure Communication Using Identity Based Encryption . . . . .	256
<i>Sebastian Roschke, Luan Ibraimi, Feng Cheng, and Christoph Meinel</i>	
Anonymous Client Authentication for Transport Layer Security . . . . .	268
<i>Kurt Dietrich</i>	
<b>Author Index</b> . . . . .	281