Lecture Notes in Computer Science 6109

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

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

Springer

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

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 Gambs	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

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 Marinos	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 Rannenberg	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

Analysis and Detection of Malicious Code and Risk Management

VoIP Security

Biometrics

Applied Cryptography

Secure Communications