

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

Jan Camenisch Dogan Kesdogan (Eds.)

Open Problems in Network Security

IFIP WG 11.4 International Workshop, iNetSec 2011
Lucerne, Switzerland, June 9, 2011
Revised Selected Papers

Volume Editors

Jan Camenisch
IBM Research - Zurich
Säumerstrasse 4, 8803 Rüschlikon, Switzerland
E-mail: jca@zurich.ibm.com

Dogan Kesdogan
Universität Siegen
Institut für Wirtschaftsinformatik
Hölderlinstr. 3, 57068 Siegen, Germany
E-mail: kesdogan@fb5.uni-siegen.de

ISSN 0302-9743
ISBN 978-3-642-27584-5
DOI 10.1007/978-3-642-27585-2
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-27585-2

Library of Congress Control Number: 2011944283

CR Subject Classification (1998): K.6.5, K.4, C.2, E.3, D.4.6, H.3.4-5

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

The international workshop iNetSec 2011 – Open Problems in Network Security—is dedicated to open problem and research directions on all aspects related to network security. It is the main workshop of working group WG 11.4 of the IFIP. This year, iNetSec was co-located with IFIP SEC 2011 in Lucerne on June 9 and shared with it the keynote talk by the Kristian Beckman award-winner Ann Cavoukian.

Originally, iNetSec was run in the traditional format where research papers get submitted, peer-reviewed, and then presented at the workshop. Since 2009, the format was changed to discuss open research problems and directions in network security. To enable this open workshop style yet remain focused on particular topics, we called for two page abstracts in which the authors were asked to outline an open research problem or direction. This year, we received 28 short submissions. Each of them was independently reviewed by six Program Committee members with a focus on the relevance and suitability for discussion. After a round of discussion in the Program Committee, 12 papers were selected for presentation at the workshop. For these presentations almost the same time was given to discussions as for presentations. After the workshop, the authors submitted a full paper that also takes the discussion into account. These papers are in the proceedings you are now holding in your hands. We hope that they will serve as a source of inspiration for new research.

We thank the authors of all submissions for enabling the workshop and the presenters and all participants for making it a success with their lively contributions! We also thank the local organizers Carlos Rieder, Colette Hofer-Schürmann, and Fabia Bommers for making our stay in Lucerne such a pleasure.

September 2011

Jan Camenisch
Dogan Kesdogan

iNetSec 2011

Open Research Problems in Network Security

Lucerne University of Applied Sciences and Arts
June 9, 2011
Lucerne, Switzerland

Organized in cooperation with *IFIP WG 11.4*

Executive Committee

Program Chairs

Jan Camenisch	IBM Research – Zurich, Switzerland
Dogan Kesdogan	University of Siegen, Germany

Organizing Chair

Carlos Rieder	Lucerne University of Science & Arts, Switzerland
---------------	---

Program Committee

Endre Bangerter	Bern University of Applied Sciences, Switzerland
Jan Camenisch	IBM Research – Zurich, Switzerland
Hannes Federrath	University of Regensburg, Germany
Simone Fischer-Hübner	Karlstad University, Sweden
Virgil Gligor	Carnegie Mellon University, USA
Thomas Gross	IBM Research – Zurich, Switzerland
Dogan Kesdogan	University of Siegen, Germany
Engin Kirda	Northeastern University, Boston, USA
Albert Levi	Sabanci University, Turkey
Javier Lopez	University of Malaga, Spain
Ulrike Meyer	RWTH Aachen University, Germany
Refik Molva	Eurecom

Local Organizing Committee

Carlos Rieder	Lucerne University of Science and Arts
Colette Hofer-Schürmann	Lucerne University of Science and Arts
Fabia Bommers	Lucerne University of Science and Arts

Table of Contents

I Assisting Users

Evoking Comprehensive Mental Models of Anonymous Credentials	1
<i>Erik Wästlund, Julio Angulo, and Simone Fischer-Hübner</i>	
Towards Usable Interfaces for Proof Based Access Rights on Mobile Devices	15
<i>Marcel Heupel and Dogan Kesdogan</i>	
Commercial Home Assistance (eHealth) Services	28
<i>Milica Milutinovic, Koen Decroix, Vincent Naessens, and Bart De Decker</i>	

II Malware Detection

Detecting Computer Worms in the Cloud	43
<i>Sebastian Biedermann and Stefan Katzenbeisser</i>	
Efficient and Stealthy Instruction Tracing and Its Applications in Automated Malware Analysis: Open Problems and Challenges	55
<i>Endre Bangerter, Stefan Bühlmann, and Engin Kirda</i>	
Challenges for Dynamic Analysis of iOS Applications	65
<i>Martin Szydlowski, Manuel Egele, Christopher Kruegel, and Giovanni Vigna</i>	

III Saving Energy

Energy-Efficient Cryptographic Engineering Paradigm	78
<i>Marine Minier and Raphael C.-W. Phan</i>	

IV Policies

Towards a Similarity Metric for Comparing Machine-Readable Privacy Policies	89
<i>Inger Anne Tøndel and Åsmund Ahlmann Nyre</i>	
Abstract Privacy Policy Framework: Addressing Privacy Problems in SOA	104
<i>Laurent Bussard and Ulrich Pinsdorf</i>	
Flexible and Dynamic Consent-Capturing	119
<i>Muhammad Rizwan Asghar and Giovanni Russello</i>	

V Problems in the Cloud

Towards User Centric Data Governance and Control in the Cloud	132
<i>Stephan Groß and Alexander Schill</i>	
Securing Data Provenance in the Cloud	145
<i>Muhammad Rizwan Asghar, Mihaela Ion, Giovanni Russello, and Bruno Crispo</i>	
Author Index	161