IFIP Advances in Information and Communication Technology 309

Editor-in-Chief

A. Joe Turner, Seneca, SC, USA

Editorial Board

Foundations of Computer Science
Mike Hinchey, Lero, Limerick, Ireland

Software: Theory and Practice
Bertrand Meyer, ETH Zurich, Switzerland

Education
Bernard Cornu, CNED-EIFAD, Poitiers, France

Information Technology Applications
Ronald Waxman, EDA Standards Consulting, Beachwood, OH, USA

Communication Systems
Guy Leduc, Université de Liège, Belgium

System Modeling and Optimization
Jacques Henry, Université de Bordeaux, France

Information Systems
Barbara Pernici, Politecnico di Milano, Italy

Relationship between Computers and Society
Chrisanthi Avgerou, London School of Economics, UK

Computer Systems Technology
Paolo Prinetto, Politecnico di Torino, Italy

Security and Privacy Protection in Information Processing Systems
Kai Rannenberg, Goethe University Frankfurt, Germany

Artificial Intelligence
Max A. Bramer, University of Portsmouth, UK

Human-Computer Interaction
Annelise Mark Pejtersen, Center of Cognitive Systems Engineering, Denmark

Entertainment Computing
Ryohei Nakatsu, National University of Singapore

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

> *IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.*

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

Jan Camenisch Dogan Kesdogan (Eds.)

iNetSec 2009 – Open Research Problems in Network Security

IFIP WG 11.4 International Workshop
Zurich, Switzerland, April 23-24, 2009
Revised Selected Papers

Springer

Volume Editors

Jan Camenisch
IBM Research - Zurich
Säumerstr. 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

Library of Congress Control Number: 2009937722

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

ISSN 1868-4238
ISBN-10 3-642-05436-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-05436-5 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 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12780877 06/3180 5 4 3 2 1 0

Preface

The working group WG 11.4 of IFIP ran an iNetSec conference a few times in the past, sometimes together with IFIP security conference, sometimes as a stand-alone workshop with a program selected from peer-reviewed submissions. When we were elected to chair WG 11.4 we asked ourselves whether the security and also the computer science community at large benefits from this workshop. In particular, as there are many (too many?) security conferences, it has become difficult to keep up with the field. After having talked to many colleagues, far too many to list all of them here, we decided to try a different kind of workshop: one where people would attend to discuss open research topics in our field, as typically only happens during the coffee breaks of ordinary conferences.

To enable this we called for abstracts of 2 pages where the authors outline the open problems that they would like to discuss at the workshop, the intent being that the author would be given 15 minutes to present the topic and another 15 minutes for discussion. These abstracts were then read by all members of the Program Committee and ranked by them according to whether they thought this would lead to an interesting talk and discussion. We then simply selected the abstracts that got the best rankings.

We were happy to see this result in many really interesting talks and discussions in the course of the workshop. Of course, these lively and direct discussions are almost impossible to achieve in a printed text. Still, we asked the authors to distill the essence of these discussions into full papers. The results are in your hands.

The participants' feedback to the workshop was very positive, and consequently the next iNetSec workshop will be held in March 2010 in Sofia, Bulgaria.

We thank Helga Steimann and Hanni Rüesch for the excellent local organization and IBM Research – Zurich for hosting the conference. We are grateful to Franz-Stefan Preiss for compiling these proceedings and running after all the files needed for this.

August 2009

Jan Camenisch
Dogan Kesdogan

iNetSec 2009

Open Research Problems in Network Security

IBM Research, Zurich, Switzerland
April 23–24, 2009

Organized in cooperation with *IFIP WG 11.4*

Program and General Chair

Jan Camenisch	IBM Research
Dogan Kesdogan	University of Siegen

Program Committee

David Basin	ETH Zurich
Jan Camenisch	IBM Research
George Danezis	Microsoft Research
Stefan Fischer	University Lübeck
Simone Fischer-Hübner	Karlstad University
Felix Freiling	Universität Mannheim
Virgil Gligor	Carnegie Mellon Univsersity
Jean-Pierre Hubaux	EPF Lausanne
Dogan Kesdogan	University of Siegen
Albert Levi	Sabanci University
Javier Lopez	University of Malaga
Refik Molva	Eurecom
Victor Shoup	New York University
Gene Tsudik	UC Irvine

External Reviewers

Claudia Becker	Daniela Krüger	Axel Wegener
Carsten Buschmann	Dennis Pfisterer	Berrin Yanikoglu
Maick Danckwardt	Stefan Ransom	Maick Danckwardt
Nils Glombitza	Peter Rothenpieler	

Table of Contents

Involving Humans

On the Design of *Forgiving* Biometric Security Systems 1
Raphael C.-W. Phan, John N. Whitley, and David J. Parish

Remotely Telling Humans and Computers Apart: An Unsolved Problem 9
Carlos Javier Hernandez-Castro and Arturo Ribagorda

Web 2.0

Leveraging Social Links for Trust and Privacy in Networks 27
Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe

Open Problems in Web 2.0 User Content Sharing 37
San-Tsai Sun and Konstantin Beznosov

Protecting Resources

Mitigating Drive-By Download Attacks: Challenges and Open Problems 52
Manuel Egele, Engin Kirda, and Christopher Kruegel

Context-Dependent Authentication and Access Control 63
Michael Kirkpatrick and Elisa Bertino

Pervasive Devices

New Directions in RFID Security 76
Erik-Oliver Blass and Refik Molva

Tailored Security and Safety for Pervasive Computing 85
Erik-Oliver Blass and Martina Zitterbart

Protocol Security

Rational Protocols 93
Christian Cachin

Security Issues for P2P-Based Voice- and Video-Streaming Applications 95
Jan Seedorf

Threshold Things That Think: Authorisation for Resharing 111
Roel Peeters, Markulf Kohlweiss, and Bart Preneel

Privacy

Privacy Policies, Tools and Mechanisms of the Future 125
Vincent Naessens, Mehmet Tahir Sandikkaya, Jorn Lapon, Kristof Verslype, Pieter Verhaeghe, Girma Nigusse, and Bart De Decker

Security and Privacy Preservation in Human-Involved Networks..... 139
Craig Asher, Jean-Philippe Aumasson, and Raphael C.-W. Phan

Discussing Anonymity Metrics for Mix Based Anonymity Approaches... 149
Dang Vinh Pham and Joss Wright

Author Index 169