IFIP Advances in Information and Communication Technology 354

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 Simone Fischer-Hübner
Yuko Murayama Armand Portmann
Carlos Rieder (Eds.)

Future Challenges in Security and Privacy for Academia and Industry

26th IFIP TC 11 International
Information Security Conference, SEC 2011
Lucerne, Switzerland, June 7-9, 2011
Proceedings

Springer

Volume Editors

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

Simone Fischer-Hübner
Karlstad University, Department of Computer Science
Universitetsgatan 1, 65188 Karlstad, Sweden
E-mail: simone.fischer-huebner@kau.se

Yuko Murayama
Iwate Prefectural University, Faculty of Software and Information Science
152-52 Sugo, Takizawa, Takizawa-mura, Iwate 020-0193, Japan
E-mail: murayama@iwate-pu.ac.jp

Armand Portmann
Carlos Rieder
Lucerne University of Applied Sciences and Arts
Zentralstr. 9, 6002 Lucerne, Switzerland
E-mail: {armand.portmann, carlos.rieder}@hslu.ch

ISSN 1868-4238 e-ISSN 1868-422X
ISBN 978-3-642-21423-3 e-ISBN 978-3-642-21424-0
DOI 10.1007/978-3-642-21424-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011927858

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, H.4, J.1

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

This book contains the proceedings of the 26th IFIP TC-11 International Information Security Conference (IFIP/SEC 2011) on "Future Challenges in Security and Privacy for Academia and Industry" held during June 7–9, 2011, at the Lucerne University of Applied Sciences and Arts, Switzerland.

The SEC conferences are in a series of well-established international conferences on security and privacy organized annually by the Technical Committee 11 (TC-11) of IFIP (International Federation for Information Processing). IFIP SEC 2011 aimed at bringing together primarily researchers, but also practitioners from academia, industry and governmental institutions to elaborate and discuss the IT security and privacy challenges that we face today and in the future. Papers offering novel and mature research contributions, on any aspect of information security and privacy, were solicited for submission to the 26th IFIP TC-11 International Information Security Conference.

IFIP SEC 2011 received 100 submissions which were all reviewed by at least three members of the international Program Committee (PC). Based on an intensive discussion among the reviewers and other PC members, 24 papers were selected for presentation at the conference. Topics addressed by the accepted papers published in these proceedings include authentication, intrusion detection, malware, information flow and DoS attacks, network security and security protocols, policy compliance and obligations, privacy attacks and privacy-enhancing technologies, risk analysis and security metrics as well software security.

Further highlights of IFIP SEC 2011 were the three invited keynote presentations by high-ranked IT security and privacy experts: The recipient of the 2011 Kristian Beckman award granted by IFIP TC-11—Ann Cavoukian, Information and Privacy Commissioner (IPC) of Ontario, Canada, as well as Michael Waidner, Director of Fraunhofer SIT Darmstadt, Germany, and René Hüsler from the Lucerne University of Applied Sciences and Arts, Switzerland. The paper for the invited keynote by Ann Cavoukian is also included in these proceedings.

In addition to the invited keynote and accepted paper sessions, IFIP SEC 2011 also included an industrial track on "Research Meets Industry" as well as the following four workshops and sub-conferences: The workshops organized by the EU FP7 projects PrimeLife and PICOS, the iNetSec 2011 organized by IFIP Working Group 11.4, as well as the 7th World Conference on Information Security Education WISE7 organized by IFIP Working Group 11.8. WISE7 and iNetSec 2011 were organized autonomously by the respective IFIP Working Groups. They had their own Call for Papers and Program Committees and the accepted papers are published in their own proceedings.

IFIP SEC 2011 was organized by Lucerne University of Applied Sciences and Arts. We would like to thank UBS AG, Zurich/Switzerland, Crypto AG, Zug/Switzerland, Elsevier Limited, Oxford/UK and isec ag, Lucerne/Switzerland, for

sponsoring IFIP SEC 2011. Besides, we gratefully acknowledge all authors, members of the Program Committee and additional reviewers for their contributions to the scientific quality of this conference. Last but not least, we owe thanks to the Organizing Committee, and especially to its Chair Carlos Rieder, for all the efforts and dedication in preparing this conference.

June 2011

Jan Camenisch
Simone Fischer-Hübner
Yuko Murayama
Armand Portmann

Organization

Program Committee Chairs

Jan Camenisch	IBM Research - Zurich, Switzerland
Simone Fischer-Hübner	Karlstad University, Sweden
Yuko Murayama	Iwate Prefectural University, Japan

Publication Chair

Armand Portmann	Lucerne University of Applied Sciences and Arts, Switzerland

Program Committee Members

Ejaz Ahmed	Queensland University of Technology, Australia
Colin Armstrong	Gailaad Pty. Ltd., Australia
Vijay Atluri	Rutgers University, USA
Richard Baskerville	Georgia State University, USA
Bharat Bhargava	Purdue University, USA
Katrin Borcea-Pfitzmann	T.U. Dresden, Germany
Reinhardt Botha	NMMU, South Africa
David Chadwick	University of Kent, UK
Nathan Clarke	University of Plymouth, UK
Roger Clarke	Xamax Consultancy Pty. Ltd., ANU and UNSW, Australia
Nora Cuppens-Boulahia	TELECOM Bretagne, France
Ed Dawson	QUT, Australia
Sabrina de Capitani di Vimercati	Università degli Studi di Milano, Italy
Bart de Decker	K.U. Leuven, Belgium
Yves Deswarte	LAAS-CNRS, France
Ronald Dodge	U.S. Military Academy, USA
Jan Eloff	University of Pretoria, South Africa
Sarah Foresti	Università degli Studi di Milano, Italy
Felix Freiling	Mannheim University, Germany
Lothar Fritsch	Norwegian Computer Center, Norway
Steven Furnell	University of Plymouth, UK
Mark Gasson	University of Reading, UK

Dieter Gollmann	TU Hamburg-Harburg, Germany
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Marit Hansen	Independent Center for Privacy Protection, Germany
Alejandro Hevia	University of Chile, Chile
Jaap-Henk Hoepmann	University of Twente, The Netherlands
René Hüsler	Lucerne Univiversity of Applied Sciences and Arts, Switzerland
Cynthia Irvine	Naval Postgraduate School, Monterey, USA
Sushil Jajodia	George Mason University, USA
David-Olivier Jaquet-Chiffelle	Bern University of Applied Sciences, Switzerland
Lech Janczweski	University of Auckland, New Zealand
Dogan Kesdogan	University of Siegen, Germany
Valentin Kisimov	University of World and National Economy Sofia, Bulgaria
Stefan Köpsell	T.U. Dresden, Germany
Stewart Kowalski	DSV/Stockholm University (and Huawei), Sweden
Ioannis Krontiris	Goethe University Frankfurt, Germany
Lam-For Kwok	City University of Hong Kong, Hong Kong
Costas Lambrinoudakis	University of the Aegean, Greece
Carl E. Landwehr	University of Maryland, USA
Ronald Leenes	Tilburg University, The Netherlands
Herbert Leitold	Technical University of Graz, Austria
Stefan Lindskog	Karlstad University, Sweden
Javier López	Universidad de Malaga, Spain
Luigi Lo Iacono	EUFH Bruehl, Germany
Steve Marsh	Communications Research Center Canada, Canada
Fabio Martinelli	National Research Council, Italy
Leonardo Martucci	CASED, Germany
Václav Matyás	Masaryk University, Brno, Czech Republic
Carlos Maziero	University of Parana, Brazil
Natalia Miloslavskaya	MEPHI, Russia
Refik Molva	Institut Eurecom, France
Eiji Okamoto	University of Tsukuba, Japan
Rolf Oppliger	eSecurity, Switzerland
Jakob-Illeborg Pagter	Alexandra Instituttet AS, Denmark

George Pangalos	University of Thessaloniki, Greece
Jong-Hyuk Park	Kyungnam University, South Korea
Philippos Peleties	Universal Bank Ltd., Cyprus
Günther Pernul	University of Regensburg, Germany
Ulrich Pinsdorf	Microsoft EMIC, Germany
Hartmut Pohl	University of Applied Sciences Bonn-Rhein-Sieg, Germany
Roland Portmann	Lucerne University of Applied Sciences and Arts, Switzerland
Kai Rannenberg	Goethe University Frankfurt, Germany
Marc Rennhard	Zurich University of Applied Sciences, Switzerland
Carlos Rieder	Lucerne University of Applied Sciences and Arts, Switzerland
Rodrigo Roman	University of Malaga, Spain
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Pierangela Samarati	University of Milan, Italy
Ingrid Schaumüller-Bichl	Upper Austria University of Applied Sciences, Austria
Anne Karen Seip	Financial Supervisory Authority of Norway, Norway
Nahid Shahmehri	Linköping University, Sweden
Siraj Shaikh	Coventry University, UK
Einar Snekkenes	Gjøvik University College, Norway
Miquel Soriano	UPC, Spain
Sandra Steinbrecher	Technical University of Dresden, Germany
Rama Subramaniam	Valiant Technologies, India
Willy Susilo	University of Wollongong, Australia
Stephanie Teufel	University of Freiburg, Switzerland
Bill Tsoumas	Ernst & Young, Greece
Pedro-Manuel Veiga	Universidade de Lisboa, Portugal
Hein Venter	University of Pretoria, South Africa
Teemupekka Virtanen	Helsinki University of Technology, Finland
Melanie Volkamer	CASED, Germany
Rossouw von Solms	Nelson Mandela Metropolitan University, South Africa
Jozef Vyskoc	VaF, Slavak Republic
Christian Weber	Goethe University Frankfurt, Germany
Tatjana Welzer	University of Maribor, Slovenia
Rigo Wenning	W3C, France
Sven Wohlgemuth	National Institute of Informatics, Japan

Louise Yngström	University of Stockholm, Sweden
Jianying Zhou	I2R, Singapore

Additional Reviewers

Gergely Alpár
Gökhan Bal
Mohamed Bourimi
Christian Broser
Laurent Bussard
Sebastian Clauß
Denise Demirel
Anthony Dessiatnikoff
Andreas Dewald
Stelios Dritsas
Thomas Fielenbach
Christoph Fritsch
Viiveke Fåk
Dimitris Geneiatakis
Mariana Gerber
Shkodran Gerguri
Stephan Groß
Daniel Hedin
Stephan Heim
Christos Ilioudis
Maarten Jacobs
Thomas Jakobsen
Fatih Karatas
Jonathan Katz
Mohamed Kaâniche
Benjamin Kellermann
Nizar Kheir
Marc-Olivier Killijian
Leanid Krautsevich
Harsha Kumara
Jorn Lapon
Anja Lehmann
Dimitrios Lekkas
Jonas Magazinius
Ilaria Matteucci
Nasir Memon
Vincent Naessens
Michael Niedermeier
Janus Dam Nielsen
Alexandros Papanikolaou
Vinh Pham
Franz-Stefan Preiss
Klaus Rechert
Andreas Reisser
Moritz Riesner
Panagiotis Rizomiliotis
Jan Schlüter
Andriy Stetsko
Tim Storer
Petr Svenda
Marianthi Theoharidou
Aggeliki Tsohou
Pavel Tucek
Simeon Veloudis
Nikolaos Virvilis
Stefan Voemel
Carsten Willems
Lars Wolos
Hau-San Raymond Wong
Erik Wästlund
Thomas Zefferer
Bernd Zwattendorfer

Table of Contents

Software Security

Policy Compliance and Obligations

Privacy Attacks and Privacy-Enhancing Technologies

Risk Analysis and Security Metrics

Intrusion Detection

Appendix