

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 Rannenber, 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.

Kai Rannenberg Vijay Varadharajan
Christian Weber (Eds.)

Security and Privacy – Silver Linings in the Cloud

25th IFIP TC 11 International Information
Security Conference, SEC 2010
Held as Part of WCC 2010
Brisbane, Australia, September 20-23, 2010
Proceedings

Volume Editors

Kai Rannenberg

Johann Wolfgang Goethe University Frankfurt
T-Mobile Chair of Mobile Business and Multilateral Security
Grüneburgplatz 1, 60629 Frankfurt, Germany
E-mail: kai.rannenberg@m-chair.net

Vijay Varadharajan

Macquarie University, Faculty of Science, Department of Computing
Science and Technology Building, E6A, Sydney 2109, Australia
E-mail: vijay.varadharajan@mq.edu.au

Christian Weber

Johann Wolfgang Goethe University Frankfurt
T-Mobile Chair of Mobile Business and Multilateral Security
Grüneburgplatz 1, 60629 Frankfurt, Germany
E-mail: christian.weber@m-chair.net

Library of Congress Control Number: 2010932410

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

ISSN 1868-4238
ISBN-10 3-642-15256-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-15256-6 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

© 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

IFIP World Computer Congress 2010 (WCC 2010)

Message from the Chairs

Every two years, the International Federation for Information Processing (IFIP) hosts a major event which showcases the scientific endeavors of its over one hundred technical committees and working groups. On the occasion of IFIP's 50th anniversary, 2010 saw the 21st IFIP World Computer Congress (WCC 2010) take place in Australia for the third time, at the Brisbane Convention and Exhibition Centre, Brisbane, Queensland, September 20–23, 2010.

The congress was hosted by the Australian Computer Society, ACS. It was run as a federation of co-located conferences offered by the different IFIP technical committees, working groups and special interest groups, under the coordination of the International Program Committee.

The event was larger than ever before, consisting of 17 parallel conferences, focusing on topics ranging from artificial intelligence to entertainment computing, human choice and computers, security, networks of the future and theoretical computer science. The conference History of Computing was a valuable contribution to IFIP's 50th anniversary, as it specifically addressed IT developments during those years. The conference e-Health was organized jointly with the International Medical Informatics Association (IMIA), which evolved from IFIP Technical Committee TC-4 "Medical Informatics".

Some of these were established conferences that run at regular intervals, e.g., annually, and some represented new, groundbreaking areas of computing. Each conference had a call for papers, an International Program Committee of experts and a thorough peer reviewing process of full papers. The congress received 642 papers for the 17 conferences, and selected 319 from those, representing an acceptance rate of 49.69% (averaged over all conferences). To support interoperability between events, conferences were grouped into 8 areas: Deliver IT, Govern IT, Learn IT, Play IT, Sustain IT, Treat IT, Trust IT, and Value IT.

This volume is one of 13 volumes associated with the 17 scientific conferences. Each volume covers a specific topic and separately or together they form a valuable record of the state of computing research in the world in 2010. Each volume was prepared for publication in the Springer IFIP Advances in Information and Communication Technology series by the conference's volume editors. The overall Publications Chair for all volumes published for this congress is Mike Hinchey.

For full details of the World Computer Congress, please refer to the webpage at <http://www.ifip.org>.

June 2010 Augusto Casaca, Portugal, Chair, International Program Committee
Phillip Nyssen, Australia, Co-chair, International Program Committee
Nick Tate, Australia, Chair, Organizing Committee
Mike Hinchey, Ireland, Publications Chair
Klaus Brunnstein, Germany, General Congress Chair

Preface

These proceedings contain the papers of IFIP/SEC 2010. It was a special honour and privilege to chair the Program Committee and prepare the proceedings for this conference, which is the 25th in a series of well-established international conferences on security and privacy organized annually by Technical Committee 11 (TC-11) of IFIP. Moreover, in 2010 it is part of the IFIP World Computer Congress 2010 celebrating both the Golden Jubilee of IFIP (founded in 1960) and the Silver Jubilee of the SEC conference in the exciting city of Brisbane, Australia, during September 20–23.

The call for papers went out with the challenging motto of “Security & Privacy – Silver Linings in the Cloud” building a bridge between the long standing issues of security and privacy and the most recent developments in information and communication technology. It attracted 102 submissions. All of them were evaluated on the basis of their significance, novelty, and technical quality by at least five member of the Program Committee. The Program Committee meeting was held electronically over a period of a week. Of the papers submitted, 25 were selected for presentation at the conference; the acceptance rate was therefore as low as 24.5% making SEC 2010 a highly competitive forum. One of those 25 submissions could unfortunately not be included in the proceedings, as none of its authors registered in time to present the paper at the conference.

In addition to sessions on important and timely subjects such as Security Management, Security Governance, Privacy, Network Security, Authentication, Intrusion Detection, Trust Management, Models, Software Security, Assurance, and Access Control SEC 2010 features a panel “Research Methodologies in Information Security Research: The Road Ahead”, whose introduction is also included in these proceedings.

SEC 2010 would not have been possible without the commitment of many people around the globe volunteering their competence and time. We would therefore like to express our sincere thanks to the members of the Program Committee (and especially to those who carried out shepherding tasks in a very competitive process), to the additional reviewers and last but not least to the authors who entrusted us with their works. Many thanks also go to all conference attendees, who are honouring the work of the authors and presenters.

Special thanks go to our distinguished keynote speaker Sebastiaan H. “Basie” von Solms, Academy for Information Technology, University of Johannesburg, South Africa, who is to receive the Kristian Beckman Award of IFIP TC-11 to honour his never tiring work towards broadening the meaning of Information Security in various aspects, e.g., by adding management aspects to the academic perception of information security and by creating the field of Security Governance. It is also to honour his work as Chair of TC-11, when he strongly demonstrated the importance of information security within IFIP and the entire field of information processing, and his various achievements in the area of IT Security Education on all levels.

Organization

Program Committee Chairs

Kai Rannenberg	Goethe University Frankfurt, Germany
Vijay Varadharajan	Macquarie University, Australia

Publication Chair

Christian Weber	Goethe University Frankfurt, Germany
-----------------	--------------------------------------

Program Committee Members

Alessandro Aldini	University of Urbino, Italy
Colin Armstrong	Curtin University, Australia
Vijay Atluri	Rutgers University, USA
Tuomas Aura	Microsoft Research, UK
Miguel Bañón	Epoche & Espri, Spain
Richard Baskerville	Georgia State University, USA
Josh Benaloh	Microsoft Research, USA
Christoph Benz Müller	Articulate Software, CA, USA
Joachim Biskup	T.U. Dortmund, Germany
Reinhardt Botha	NMMU, South Africa
Laurent Bussard	Microsoft EMIC, Germany
Jan Camenisch	IBM Research, Switzerland
Kim Cameron	Microsoft, France
Liqun Chen	Hewlett-Packard Labs, UK
Mihai Christodorescu	IBM T.J. Watson Research Center, USA
Roger Clarke	Xamax Consultancy Pty Ltd, Australia
Richard Clayton	University of Cambridge, UK
Cas Cremers	ETH Zurich, Switzerland
Malcolm Crompton	Information Integrity Solutions Pty Ltd, 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
Marijke de Soete	Security4Biz, Belgium
Yves Deswarte	LAAS-CNRS, France
Gurpreet Dhillon	Virginia Commonwealth University, USA
Theo Dimitrakos	BT Innovate & Design, UK
Ronald Dodge	U.S. Military Academy, USA
Jan Eloff	University of Pretoria & SAP, South Africa
Alberto Escudero-Pascual	it46.se, Sweden
Hannes Federrath	University of Regensburg, Germany
Stefan Fischer	University of Lübeck, Germany
Simone Fischer-Hübner	Karlstad University, Sweden
Ulrich Flegel	SAP AG, Germany
Simon Foley	University College Cork, Ireland
Felix Freiling	University of Mannheim, Germany
Andreas Fuchsberger	Microsoft Corp, Germany
Walter Fumy	Bundesdruckerei GmbH, Germany
Steven Furnell	University of Plymouth, UK
Mark Gasson	University of Reading, UK
Virgil Gligor	Carnegie Mellon University, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Rüdiger Grimm	University of Koblenz, Germany
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Marit Hansen	Independent Centre for Privacy Protection Schleswig-Holstein, Germany
Hans Hedbom	Karlstad Universitet, Sweden
Maritta Heisel	University of Duisburg-Essen, Germany
Udo Helmbrecht	ENISA, Greece
Peter Herrmann	NTNU, Norway
Alejandro Hevia	Universidad de Chile, Chile
Marko Hoelbl	University of Maribor, Slovenia
Jaap-Henk Hoepman	TNO and Radboud University Nijmegen, The Netherlands
Edward Humphreys	XISEC, UK
Jakob Illeborg Pagter	Alexandra Instituttet, Denmark
Cynthia Irvine	Naval Postgraduate School, USA
Sushil Jajodia	George Mason University, USA
Lech Janczewski	University of Auckland, New Zealand

David-Olivier Jaquet-Chiffelle	Bern University of Applied Sciences and University of Lausanne, Switzerland
Willem Jonker	Philips Research and Twente University, The Netherlands
Audun Jøsang	University of Oslo, Norway
Meng-Chow Kang	ISO/IEC JTC 1/SC 27/WG 4
Sokratis Katsikas	University of Piraeus, Greece
Dogan Kesdogan	University of Siegen, Germany
Hiroaki Kikuchi	Tokai University, Japan
Valentin Kisimov	University for World and National Economics, Bulgaria
Svein Knapskog	NTNU/Q2S, Norway
Klaus-Peter Kossakowski	PRESECURE Consulting GmbH, Germany
Ulrich Kühn	DZ BANK AG, Germany
Klaus Kursawe	Philips Research, The Netherlands
Brian LaMacchia	Microsoft Research, USA
Carl Landwehr	University of Maryland, USA
Pil Joong Lee	POSTECH, South Korea
Ronald Leenes	Tilburg University, The Netherlands
Herbert Leitold	A-SIT, Austria
Albert Levi	Sabancı University, Turkey
Timothy Levin	Naval Postgraduate School, USA
Kerry Long	US Army Research Laboratory, USA
Javier Lopez	University of Malaga, Spain
Volkmar Lotz	SAP Research, France
Norbert Luttenberger	Kiel University, Germany
Pedro Manuel Barbosa Veiga	Universidade de Lisboa, Portugal
Michael Marhöfer	Nokia Siemens Networks, Germany
Stephen Marsh	Communications Research Centre, Canada
Fabio Martinelli	National Research Council, Italy
Vaclav Matyas	Masaryk University Brno, Czech Republic
Sjouke Mauw	University of Luxembourg, Luxembourg
Carlos Maziero	PUCPR, Brazil
Catherine Meadows	Naval Research Laboratory, USA
Martin Meints	Dataport, Germany
Natalia G. Miloslavskaya	National Research Nuclear University MEPhI, Russia
Chris Mitchell	Royal Holloway, University of London, UK
Refik Molva	EURECOM, France

Günter Müller	Freiburg University, Germany
Yuko Murayama	Iwate Prefectural University, Japan
Mats Ohlin († in memoriam)	FMV, Sweden
Eiji Okamoto	University of Tsukuba, Japan
Rolf Oppliger	eSECURITY Technologies, Switzerland
Charles Palmer	IBM Research; Dartmouth College, USA
Aljosa Pasic	ATOS Origin, Spain
Philippos Peleties	USB BANK PLC, Cyprus
Günther Pernul	University of Regensburg, Germany
Gilbert Peterson	Air Force Institute of Technology, USA
Milan Petkovic	Philips Research / Eindhoven University of Technology, The Netherlands
Andreas Pfitzmann	Dresden University of Technology, Germany
Ulrich Pinsdorf	Microsoft EMIC, Germany
Hartmut Pohl	University of Applied Sciences Bonn-Rhein-Sieg, Germany
Mark Pollitt	University of Central Florida, USA
Reinhard Posch	TU Graz, Austria
Joachim Posegga	University of Passau, Germany
Bart Preneel	K. U. Leuven, Belgium
Geraint Price	Royal Holloway, University of London, UK
Christian Probst	Technical University of Denmark, Denmark
Sihan Qing	Chinese Academy of Sciences, China
Martin Reichenbach	Commerzbank, Germany
Carlos Rieder	Lucerne University of Applied Sciences and Arts, Switzerland
Michel Riguidel	ENST, France
Yves Roudier	EURECOM, France
Pierangela Samarati	Università degli Studi di Milano, Italy
Amardeo Sarma	NEC Laboratories Europe, Germany
Ryoichi Sasaki	Dendai University, Japan
Damien Sauveron	University of Limoges, France
Ingrid Schaumüller-Bichl	Upper Austria University of Applied Sciences, Austria
Annikken Bonnevie Seip	Finanstilsynet - The Financial Supervisory Authority of Norway, Norway
Sujeet Shenoj	University of Tulsa, USA
Einar Snekkenes	Gjøvik University College, Norway
Rossouw von Solms	NMMU, South Africa

Hans von Sommerfeld	Rohde & Schwarz SIT GmbH, Germany
Frank Stajano	University of Cambridge, UK
Sandra Steinbrecher	Dresden University of Technology, Germany
Rama Subramaniam	Valiant Technologies, India
Morton Swimmer	Trend Micro, USA
Paul Syverson	Naval Research Laboratory, USA
Kazuo Takaragi	Hitachi, Japan
Stephanie Teufel	University of Fribourg, Switzerland
Markus Ullmann	BSI & University of Applied Sciences Bonn-Rhein-Sieg, Germany
Teemupekka Virtanen	Helsinki University of Technology, Finland
Claire Vishik	Intel, UK
Jozef Vyskoc	VaF, Slovakia
Michael Waidner	IBM, USA
Colin Wallis	Department of Internal Affairs, New Zealand
Gerhard Weck	INFODAS GmbH, Germany
Nathalie Weiler	Sensaco, Switzerland
Stefan Weiss	KPMG AG Wirtschaftspruefungsgesellschaft, Germany
Tatjana Welzer	University of Maribor, Slovenia
Andreas Westfeld	University of Applied Sciences Dresden, Germany
Sven Wohlgenuth	National Institute of Informatics, Japan
Stephen Wolthusen	Royal Holloway, University of London, UK
Jianying Zhou	I2R, Singapore
Alf Zugenmaier	Munich University of Applied Sciences, Germany

Chair International Organizing Committee Chair

Nick Tate	Queensland University of Technology and Australian Research Collaboration Service (ARCS), Australia
-----------	---

Additional Reviewers

Farid Ahmed	Markus Karwe
Jonathan Anderson	Woo Chun Kim
Muhammad Asim	Yeonkyu Kim
Ulrich Bayer	Matthias Kirchner

Claudia Becker	Jan Kolter
Jens-Matthias Bohli	Stefan Köpsell
Mohamed Bourimi	Jiri Kur
Bastian Braun	Martin Mink
Ralph Breithaupt	Vinh Pham
Timm Busshaus	Jason Reid
Sebastian Clauss	Konrad Rieck
Janus DamNielsen	Peter Rothenpieler
Van Hai Dang	Winfried Schoech
Danny DeCock	Bernhard Sick
Aubrey Derrick-Schmidt	Koen Simoens
Claudia Diaz	Yannis Soupionis
Jaromir Dobias	Mark Stegelmann
Stelios Dritsas	Andriy Stetsko
Stefan Dürbeck	Ben Stock
Manuel Egele	Petr Svenda
Markus Engelberth	Wen TaoZhu
Sungwook Eom	Marianthi Theoharidou
Pooya Farshim	Philipp Trinius
William Fitzgerald	Carmela Troncoso
Ludwig Fuchs	Bill Tsoumas
Daniel Gille	Pavel Tucek
Jan Göbel	Li Weng
Christian Gorecki	Benedikt Westermann
Sebastian Indesteege	Christian Wieschebrink
Thomas Jakobsen	Ge Zhang
Aaron Johnson	

Table of Contents

Kristian Beckman Award Awardee Keynote

The 5 Waves of Information Security – From Kristian Beckman to the Present	1
<i>S.H. (Basie) von Solms</i>	

Security Management

A Business Continuity Management Simulator	9
<i>William J. Caelli, Lam-For Kwok, and Dennis Longley</i>	
Mining Business-Relevant RBAC States through Decomposition	19
<i>Alessandro Colantonio, Roberto Di Pietro, Alberto Ocello, and Nino Vincenzo Verde</i>	
Group Dynamics in a Security Risk Management Team Context: A Teaching Case Study	31
<i>Rostislav Barabanov and Stewart Kowalski</i>	

Security Management & Governance

Using Actor Network Theory to Understand Information Security Management	43
<i>Karin Hedström, Gurpreet Dhillon, and Fredrik Karlsson</i>	
Information Security Governance: When Compliance Becomes More Important than Security	55
<i>Terence C.C. Tan, Anthonie B. Ruighaver, and Atif Ahmad</i>	

Network Security & Authentication

Understanding Domain Registration Abuses	68
<i>Scott E. Coull, Andrew M. White, Ting-Fang Yen, Fabian Monrose, and Michael K. Reiter</i>	
Who on Earth Is “Mr. Cypher”: Automated Friend Injection Attacks on Social Networking Sites	80
<i>Markus Huber, Martin Mulazzani, and Edgar Weippl</i>	
Authentic Refinement of Semantically Enhanced Policies in Pervasive Systems	90
<i>Julian Schütte, Nicolai Kuntze, Andreas Fuchs, and Atta Badii</i>	

Qualified Mobile Server Signature 103
Clemens Orthacker, Martin Centner, and Christian Kittl

Intrusion Detection, Trust Management, and Models

Fraud Detection in ERP Systems Using Scenario Matching 112
*Asadul Khandoker Islam, Malcom Corney, George Mohay,
 Andrew Clark, Shane Bracher, Tobias Raub, and Ulrich Flegel*

Use of IP Addresses for High Rate Flooding Attack Detection 124
Ejaz Ahmed, George Mohay, Alan Tickle, and Sajal Bhatia

Augmenting Reputation-Based Trust Metrics with Rumor-Like
 Dissemination of Reputation Information 136
*Sascha Hauke, Martin Pyka, Markus Borschbach, and
 Dominik Heider*

Ex-SDF: An Extended Service Dependency Framework for Intrusion
 Impact Assessment 148
*Nizar Kheir, Nora Cuppens-Boulahia, Frédéric Cuppens, and
 Hervé Debar*

Software Security and Assurance

A Dynamic and Ubiquitous Smart Card Security Assurance and
 Validation Mechanism 161
Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes

On-the-fly Inlining of Dynamic Security Monitors 173
Jonas Magazinius, Alejandro Russo, and Andrei Sabelfeld

A Metric-Based Scheme for Evaluating Tamper Resistant Software
 Systems 187
Gideon Myles and Hongxia Jin

Evaluation of the Offensive Approach in Information Security
 Education 203
Martin Mink and Rainer Greifeneder

Panel

Research Methodologies in Information Security Research: The Road
 Ahead 215
Johan F. van Niekerk and Rossouw von Solms

Access Control and Privacy

Purpose-Based Access Control Policies and Conflicting Analysis	217
<i>Hua Wang, Lili Sun, and Vijay Varadharajan</i>	
Delegation in Predicate Encryption Supporting Disjunctive Queries	229
<i>Dongdong Sun, Colin Boyd, and Juan Manuel González Nieto</i>	
Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy	241
<i>Sven Wohlgemuth, Isao Echizen, Noboru Sonehara, and Günter Müller</i>	
k-Shares: A Privacy Preserving Reputation Protocol for Decentralized Environments	253
<i>Omar Hasan, Lionel Brunie, and Elisa Bertino</i>	

Privacy

Towards Fair Indictment for Data Collection with Self-Enforcing Privacy	265
<i>Mark Stegelmann</i>	
How to Enhance Privacy and Identity Management for Mobile Communities: Approach and User Driven Concepts of the PICOS Project	277
<i>Christian Kahl, Katja Böttcher, Markus Tschersich, Stephan Heim, and Kai Rannenberg</i>	
Performance Analysis of Accumulator-Based Revocation Mechanisms . . .	289
<i>Jorn Lapon, Markulf Kohlweiss, Bart De Decker, and Vincent Naessens</i>	

Appendix

IFIP Technical Committee 11 Security and Privacy Protection in Information Processing Systems	302
<i>Kai Rannenberg, S.H. (Basie) von Solms, and Leon Strous</i>	
Author Index	311