

Editor-in-Chief

A. Joe Turner, Seneca, SC, USA

Editorial Board

Foundations of Computer Science

Jacques Sakarovitch, Télécom ParisTech, France

Software: Theory and Practice

Michael Goedicke, University of Duisburg-Essen, Germany

Education

Arthur Tatnall, Victoria University, Melbourne, Australia

Information Technology Applications

Erich J. Neuhold, University of Vienna, Austria

Communication Systems

Aiko Pras, University of Twente, Enschede, The Netherlands

System Modeling and Optimization

Fredi Tröltzsch, TU Berlin, Germany

Information Systems

Jan Pries-Heje, Roskilde University, Denmark

ICT and Society

Diane Whitehouse, The Castlegate Consultancy, Malton, UK

Computer Systems Technology

Ricardo Reis, Federal University of Rio Grande do Sul, Porto Alegre, Brazil

Security and Privacy Protection in Information Processing Systems

Yuko Murayama, Iwate Prefectural University, Japan

Artificial Intelligence

Tharam Dillon, Curtin University, Bentley, Australia

Human-Computer Interaction

Jan Gulliksen, KTH Royal Institute of Technology, Stockholm, Sweden

Entertainment Computing

Matthias Rauterberg, Eindhoven University of Technology, The Netherlands

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 also 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 about information processing 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.

Nora Cuppens-Boulahia Frédéric Cuppens
Sushil Jajodia Anas Abou El Kalam
Thierry Sans (Eds.)

ICT Systems Security and Privacy Protection

29th IFIP TC 11 International Conference, SEC 2014
Marrakech, Morocco, June 2-4, 2014
Proceedings



Springer

Volume Editors

Nora Cuppens-Boulahia
Frédéric Cuppens
Télécom Bretagne (Campus de Rennes)
2, rue de la Châtaigneraie, 35576 Cesson Sévigné Cedex, France
E-mail: {nora.cuppens, frederic.cuppens}@telecom-bretagne.eu

Sushil Jajodia
George Mason University
4400 University Drive, Fairfax, VA 22030-4422, USA
E-mail: jajodia@gmu.edu

Anas Abou El Kalam
Université Cadi Ayyad, École Nationale des Sciences Appliquées
Avenue Abdelkrim El Khattabi, 40000 Marrakech, Morocco
E-mail: elkalam@hotmail.fr

Thierry Sans
Carnegie Mellon University
Qatar Campus, Doha, Qatar
E-mail: tsans@cmu.edu

ISSN 1868-4238
ISBN 978-3-642-55414-8
DOI 10.1007/978-3-642-55415-5
Springer Heidelberg New York Dordrecht London

e-ISSN 1868-422X
e-ISBN 978-3-642-55415-5

Library of Congress Control Number: 2014937537

© IFIP International Federation for Information Processing 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, 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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

These proceedings contain the papers presented at the 29th IFIP International Information Security and Privacy Conference (SEC 2014). The conference, hosted for the first time in Marrakech, Morocco, June 2–4, 2014, offered outstanding research contributions to the field of security in Internet-related applications, networks, and systems.

In response to the call for papers, 151 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by four members of the Program Committee. The Program Committee meeting was held electronically with intensive discussion over a period of one week. Of the papers submitted, 27 full papers and 14 short papers were accepted for presentation at the conference. The conference program also included two invited talks by William Caelli Director at IISEC Pty Ltd, Brisbane, Australia, and V.S. Subrahmanian, Professor at University of Maryland, College Park, United States.

Several trends in computer security have become prominent since the beginning of the new century and are considered in the program. These include, the proliferation of intrusions that exploit new vulnerabilities, the necessity to respond to an increasing number of computer security incidents, the emergence of new security threats, and the need to adapt existing approaches, models, and metrics to handle these threats. Reflecting these trends, the conference includes sessions on intrusion detection, data security, privacy, mobile security, metrics and risk assessment, information flow control, identity management, identifiability and decision making, malicious behavior and fraud, organizational security.

The success of this conference was the result of the effort of many people who generously volunteered their time for the various organization tasks. It was a pleasure to work with such dedicated colleagues. We also thank our hosts, the staff from the ENSA Marrakesh and AMAN for their help in day-to-day running of the conference.

We gratefully acknowledge all authors who submitted papers for their efforts in continually enhancing the standards of this conference. It is also our pleasure to thank the members of the Program Committee and the external reviewers for their work and support.

Last but not least, thanks to all the attendees. We hope you will enjoy reading the proceedings.

March 2014

Nora Cuppens-Boulahia
Frédéric Cuppens
Sushil Jajodia

Organization

Program Committee

Anas Abou El Kalam	Cadi Ayyad University, ENSA of Marrakech, Morocco
Kamel Adi	University of Quebec in Outaouais, Canada
Vijay Atluri	Rutgers University, USA
Fabien Autrel	CNRS-LabSTICC, France
Richard Baskerville	Georgia State University, Atlanta, USA
Abdelmalek Benzekri	Université Toulouse 3 Paul Sabatier, France
Pierre Bieber	Onera, France
Joan Borrell	Universitat Autònoma de Barcelona, Spain
Adel Bouhoula	High School of Communication, Sup'Com, Tunisia
Dagmar Brechlerova	Euromise Prague, Czech Republic
Jonathan Butts	AFIT, USA
William Caelli	IISEC Pty Ltd., Australia
Jan Camenisch	IBM Research, Zurich Research Laboratory, Switzerland
Ana Cavalli	IMT- Telecom SudParis, France
Iliano Cervesato	Carnegie Mellon University, Qatar
Hakima Chaouchi	IMT-Telecom SudParis, France
Abdelghani Chibani	University of Paris Est Créteil, LISSI, France
Nathan Clarke	Plymouth University, UK
Gouenou Coatrieux	IMT-Telecom Bretagne, France
Bruno Crispo	University of Trento, Italy
Frédéric Cuppens	IMT-Telecom Bretagne, France
Nora Cuppens-Boulahia	IMT-Telecom Bretagne, France
Ernesto Damiani	University of Milan, Italy
Christian Damsgaard	Technical University of Denmark, Denmark
Sabrina De Capitani Di Vimercati	Università degli Studi di Milano, Italy
Bart De Decker	KU Leuven, Belgium
Hervé Debar	IMT-Telecom SudParis, France
Mourad Debbabi	Concordia University, Canada
Gurpreet Dhillon	Virginia Commonwealth University, USA
Theo Dimitrakos	British Telecommunications (BT) and University of Kent, UK
Ronald Dodge	United States Military Academy, USA
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Loic Duflo	ANSSI, France

VIII Organization

Hanan El Bakkali	Mohammed V- Souissi University, ENSIAS, Morocco
Said El Hajji	Med V. Agdal University Morocco
Driss El Ouadghiri	Moulay Ismail University, Morocco
David Espes	University of Brest, France
Simone Fischer-Hübner	Karlstad University, Sweden
William Michael Fitzgerald	EMC Information Systems International, Ireland
Caroline Fontaine	CNRS - LabSTICC, France
Sara Foresti	Università degli Studi di Milano, Italy
Steven Furnell	Plymouth University, UK
Alban Gabillon	University of Polynésie Française, France
Joaquin Garcia-Alfaro	IMT-Telecom SudParis, France
Dieter Gollmann	Hamburg University of Technology, Germany
Dimitris Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Sihem Guemara El Fatmi	High School of Communication, Sup'Com, Tunisia
Ahmed Hadj Kacem	ReDCAD-FSEG Sfax, Tunisia
Abdelkrim Haqiq	Hassan 1st University, Morocco
Jaap Henk Hoepman	Radboud University Nijmegen, The Netherlands
Labiod Houda	IMT-Telecom Paristech, France
Sushil Jajodia	George Mason University Fairfax
Lech Janczewski	University of Auckland, New Zealand
Lanet Jean-Louis	University of Limoges, France
Thomas Jensen	Inria Rennes, France
Wael Kanoun	Bell Labs, Alcatel-Lucent, France
Sokratis Katsikas	University of Piraeus, Greece
Nizar Kheir	Orange Labs, France
Valentin Kisimov	Applied Informatics and Statistics, Bulgaria
Zbigniew Kotulski	IPPT PAN, Poland
Ioannis Krontiris	Goethe University Frankfurt, Germany
Jean Leneutre	IMTTelecom ParisTech, France
Luigi Logrippo	Université du Québec en Outaouais, Canada
Javier Lopez	University of Malaga, Spain
Emil Lupu	Imperial College, UK
Heiko Mantel	TU Darmstadt, Germany
Jean-Yves Marion	Lorraine University, LORIA, France
Fabio Martinelli	IIT CNR, Italy
Hicham Medromi	ENSEM Casablanca, Morocco
Zbakh Mostapha	ENSIAS Rabat, Morocco
Yuko Murayama	Iwate Prefectural University, Japan

Jakob Illeborg Pagter	Centre for IT Security, Alexandra Institute Ltd., Denmark
Philippos Peleties	USB BANK PLC, Cyprus
Günther Pernul	Universität Regensburg, Germany
Nicolas Prigent	Supélec Rennes, France
Sihan Qing	School of Software and Microelectronics, China
Kai Rannenber	Goethe University Frankfurt, Germany
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Carlos Reider	Hochschule für Wirtschaft, Switzerland
Yves Roudier	EURECOM, France
Mark Ryan	University of Birmingham, UK
P.Y.A. Ryan	University of Luxembourg, Luxembourg
Pierangela Samarati	Università degli Studi di Milano, Italy
Thierry Sans	Carnegie Mellon University, Qatar
Claire Saurel	ONERA, France
Ingrid Schaumüller-Bichl	University of Applied Sciences Upper Austria, Austria
Anne Karen Seip	Finanstilsynet, Norway
Abderrahim Sekkaki	FS Casablanca, Morocco
Sujeet Sheno	University of Tulsa, USA
Radu State	University of Luxembourg, Luxembourg
Bhavani Thuraisingham	University of Texas at Dallas, USA
Pedro Veiga	University of Lisbon, Portugal
Rossouw Von Solms	Nelson Mandela Metropolitan University, South Africa
Jozef Vyskoc	VaF, Slovakia
Christian Weber	University of Applied Sciences, Germany

Additional Reviewers

Abbes, Tarek	Bkakria, Anis
Al Khalil, Firas	Blanco-Justicia, Alberto
Alcaraz, Cristina	Boukhtouta, Amine
Alpar, Gergely	Boulares, Sofiene
Ammar, Boulaiche	Boussi, Hanen
Armknecht, Frederik	Chen, Beijing
Asghar, Muhammad Rizwan	Damopoulos, Dimitrios
Ayachi, Mohamed Ali	Daniel, Joshua
Bal, Goekhan	de La Piedra, Antonio
Barbu, Guillaume	Diener, Michael
Batet, Montserrat	Doelitzscher, Frank
Ben Youssef Ben Souayah, Nihel	Dritsas, Stelios
Besson, Frederic	Drogkaris, Prokopios

Dubus, Samuel
 Ducatel, Gery
 Duquesne, Sylvain
 Farràs, Oriol
 Fernandez, Carmen
 Gaspar, Jaime
 Grewal, Gurchetan
 Grewe, Sylvia
 Hachem, Nabil
 Halbich, Cestmir
 Hamdi, Mohamed
 Hamouid, Khaled
 Hassan, Sabri
 Hillen, Christiaan
 Hu, Jinwei
 Idrees, Muhammad Sabir
 Jensen, Jonas Lindstrøm
 Ji, Qingguang
 Joaquim, Rui
 Kanoun, Waël
 Karyda, Maria
 Khambhammettu, Hemanth
 Klaoudatou, Eleni
 Kondratyeva, Olga
 Krasnova, Anna
 Kushik, Natalia
 Lancrenon, Jean
 Lapon, Jorn
 Lazouski, Aliaksandr
 Lemaire, Laurens
 Li, Fudong
 Liu, Jia
 Lortz, Steffen
 Lueks, Wouter
 Læssøe Mikkelsen, Gert
 Manso, Oscar
 Meharouech, Sourour
 Meier, Stefan
 Milutinovic, Milica
 Moataz, Tarik
 Mohamed, Aouadi

Moyano, Francisco
 Mukherjee, Subhojeet
 Mulamba, Dieudonne
 Mylonas, Alexios
 Netter, Michael
 Nielsen, Janus Dam
 Nordholt, Peter Sebastian
 Ordean, Mihai
 Pan, Wei
 Pawar, Pramod
 Peter, Andreas
 Phillips, Joshua
 Ray, Sujoy
 Rios, Ruben
 Rizomiliotis, Panagiotis
 Sabouri, Ahmad
 Samarji, Léa
 Sanchez, David
 Santos, Joao
 Saracino, Andrea
 Savary, Aymerick
 Schillinger, Rolf
 Sere, Ahmadou
 Sgandurra, Daniele
 Shen, Qingni
 Skjernaa, Berit
 Soeanu, Andrei
 Soupionis, Yannis
 Stergiopoulos, George
 Sängler, Johannes
 Tang, Qiang
 Tesfay, Welderufael
 Toumi, Khalifa
 Tschersich, Markus
 Tsohou, Aggeliki
 Veseli, Fatbardh
 Virvilis, Nick
 Vivas, José Luis
 Weber, Michael
 Yang, Shuzhe
 Yu, Jiangshan

Table of Contents

Intrusion Detection

Mentor: Positive DNS Reputation to Skim-Off Benign Domains in Botnet C&C Blacklists	1
<i>Nizar Kheir, Frédéric Tran, Pierre Caron, and Nicolas Deschamps</i>	
Game Theory Meets Information Security Management	15
<i>Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi</i>	
Model-Based Detection of CSRF	30
<i>Marco Rocchetto, Martín Ochoa, and Mohammad Torabi Dashti</i>	
Lightweight Resource Management for DDoS Traffic Isolation in a Cloud Environment	44
<i>Ibnu Mubarak, Kiryong Lee, Sihyung Lee, and Heejo Lee</i>	

Data Security

Multi-keyword Similarity Search over Encrypted Cloud Data	52
<i>Mikhail Strizhov and Indrajit Ray</i>	
Security of the Multiple-Key Blom's Key Agreement Scheme for Sensor Networks	66
<i>Mee Loong Yang, Adnan Al Anbuky, and William Liu</i>	
New Algorithmic Approaches to Point Constellation Recognition	80
<i>Thomas Bourgeat, Julien Bringer, Hervé Chabanne, Robin Champenois, Jérémie Clément, Houda Ferradi, Marc Heinrich, Paul Melotti, David Naccache, and Antoine Voizard</i>	
Protection Profile for PUF-Based Devices	91
<i>Andrea Kolberger, Ingrid Schaumüller-Bichl, Verena Brunner, and Martin Deutschmann</i>	

Mobile Security

Text-Based Active Authentication for Mobile Devices	99
<i>Hataichanok Saeveanee, Nathan Clarke, Steven Furnell, and Valerio Biscione</i>	
Styx: Design and Evaluation of a New Privacy Risk Communication Method for Smartphones	113
<i>Gökhan Bal, Kai Rannenberg, and Jason Hong</i>	

A Trusted UI for the Mobile Web 127
Bastian Braun, Johannes Koestler, Joachim Posegga, and Martin Johns

Detecting Code Reuse in Android Applications Using Component-Based Control Flow Graph 142
Xin Sun, Yibing Zhongyang, Zhi Xin, Bing Mao, and Li Xie

Privacy I

Privacy Risks from Public Data Sources 156
Zacharias Tzermias, Vassilis Prevelakis, and Sotiris Ioannidis

Security and Privacy in Video Surveillance: Requirements and Challenges 169
Qasim Mahmood Rajpoot and Christian Damsgaard Jensen

Playing Hide and Seek with Mobile Dating Applications 185
Guojun Qin, Constantinos Patsakis, and Mélanie Bourouche

Towards a Framework for Benchmarking Privacy-ABC Technologies 197
Fatbardh Veseli, Tsvetoslava Vateva-Gurova, Ioannis Krontiris, Kai Rannenber, and Neeraj Suri

Metrics and Risk Assessment

Evaluating the Security of a DNS Query Obfuscation Scheme for Private Web Surfing 205
Dominik Herrmann, Max Maaß, and Hannes Federrath

A Novel Metric for the Evaluation of IDSs Effectiveness 220
Khalid Nasr and Anas Abou El Kalam

How to Assess Confidentiality Requirements of Corporate Assets? 234
Gabriela Varona Cervantes and Stefan Fenz

Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks 242
Suhaila Ismail, Elena Sitnikova, and Jill Stay

Information Flow Control

Compatibility of Safety Properties and Possibilistic Information Flow Security in MAKS 250
Thomas Bauereiss and Dieter Hutter

Ghostrail: Ad Hoc Control-Flow Integrity for Web Applications	264
<i>Bastian Braun, Caspar Gries, Benedikt Petschkuhn, and Joachim Posegga</i>	

An Information Flow Monitor-Inlining Compiler for Securing a Core of JavaScript	278
<i>José Fragoso Santos and Tamara Rezk</i>	

Identity Management

Authenticated Dictionary Based on Frequency	293
<i>Kévin Atighehchi, Alexis Bonneau, and Traian Muntean</i>	

Géant-TrustBroker: Dynamic, Scalable Management of SAML-Based Inter-federation Authentication and Authorization Infrastructures	307
<i>Daniela Pöhn, Stefan Metzger, and Wolfgang Hommel</i>	

Efficient Identity-Based Signature from Lattices	321
<i>Miaomiao Tian and Liusheng Huang</i>	

Context-Aware Multifactor Authentication Based on Dynamic Pin	330
<i>Yair H. Diaz-Tellez, Eliane L. Bodanese, Theo Dimitrakos, and Michael Turner</i>	

Identifiability and Decision Making

Authorship Attribution for Forensic Investigation with Thousands of Authors	339
<i>Min Yang and Kam-Pui Chow</i>	

Detection and Labeling of Personal Identifiable Information in E-mails	351
<i>Christoph Bier and Jonas Prior</i>	

A Preliminary Study on User's Decision Making towards Retweet Messages	359
<i>Nor Athiyah Abdullah, Dai Nishioka, Yuko Tanaka, and Yuko Murayama</i>	

Malicious Behavior and Fraud

Behavior Analysis of Web Service Attacks	366
<i>Abdallah Ghourabi, Tarek Abbes, and Adel Bouhoula</i>	

BANKSEALER: An Online Banking Fraud Analysis and Decision Support System	380
<i>Michele Carminati, Roberto Caron, Federico Maggi, Ilenia Epifani, and Stefano Zanero</i>	

Security Assessment of Payment Systems under PCI DSS Incompatibilities 395
Şerif Bahtiyar, Gürkan Gür, and Levent Altay

Organizational Security

PriMan: Facilitating the Development of Secure and Privacy-Preserving Applications 403
Andreas Put, Italo Dacosta, Milica Milutinovic, and Bart De Decker

Managing Employee Security Behaviour in Organisations: The Role of Cultural Factors and Individual Values 417
Lena Connolly, Michael Lang, and Doug Tygar

Organizational Transformation and Information Security Culture: A Telecom Case Study 431
Gurpreet Dhillon, Romilla Chowdhuri, and Cristiane Pedron

A Holistic Approach for Cyber Assurance of Critical Infrastructure with the Viable System Model 438
Theodoros Spyridopoulos, Ioanna-Aikaterini Topa, Theo Tryfonas, and Maria Karyda

Privacy II

Privacy Design Strategies (Extended Abstract) 446
Jaap-Henk Hoepman

Distance Computation between Two Private Preference Functions 460
Alberto Blanco, Josep Domingo-Ferrer, Oriol Farràs, and David Sánchez

Privacy-Preserving Implicit Authentication 471
Nashad Ahmed Safa, Reihaneh Safavi-Naini, and Siamak F. Shahandashti

Trusted Computing to Increase Security and Privacy in eID Authentication 485
Jan Vossaert, Jorn Lapon, Bart De Decker, and Vincent Naessens

Author Index 493