

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

Dieter Gollmann Felix C. Freiling (Eds.)

Information Security

15th International Conference, ISC 2012
Passau, Germany, September 19-21, 2012
Proceedings



Springer

Volume Editors

Dieter Gollmann

Hamburg University of Technology, Institute for Security in Distributed Applications
Harburger Schlossstrasse 20, 21073, Hamburg, Germany

E-mail: diego@tu-harburg.de

Felix C. Freiling

Friedrich-Alexander-University, Department of Computer Science
Martenstrasse 3, 91058 Erlangen, Germany

E-mail: felix.freiling@cs.fau.de

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-33382-8

e-ISBN 978-3-642-33383-5

DOI 10.1007/978-3-642-33383-5

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012946460

CR Subject Classification (1998): E.3, E.4, D.4.6, K.6.5, C.2, J.1, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 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)

Foreword

Information security continues to be a topic of great relevance to society. The Information Security Conference (ISC) is an annual international conference dedicated to research on the theory and applications of information security. The 2012 conference was the 15th in the conference series that started as a workshop in 1997, changed to a conference in 2001, and has been held on five different continents since. Hosted by the University of Passau in Lower Bavaria, ISC 2012 was the first conference in this series to be held in Germany.

ISC 2012 attracted high-quality papers on all technical aspects of information security. We received 72 submissions, which were reviewed by at least three members of the program committee. We finally accepted 23 papers, which are collected in these proceedings. In addition, we invited Isabel Trancoso and her colleagues to speak on privacy issues in speech processing. A second keynote speech was given by Michael Waidner from Fraunhofer SIT and Technische Universität Darmstadt.

We wish to thank all the people who invested time and energy to make ISC 2012 a success: First and foremost come all the authors who submitted papers to ISC and presented them at the conference. The members of the program committee together with all the external reviewers worked hard in evaluating the submissions and, in some cases, in shepherding promising work. The ISC steering committee, in particular Masahiro Mambo, helped us graciously in all critical decisions. Thanks also go to the 2012 general chair Joachim Posegga and his team at Passau University for handling the local arrangements, to Eric Rothstein for maintaining the conference website, and to Isaac Agudo and Cheng-Kang Chu for their efforts as publicity chairs.

July 2012

Dieter Gollmann
Felix C. Freiling

Organization

General Chair

Joachim Posegga

University of Passau, Germany

Steering Committee Chair

Masahiro Mambo

Kanazawa University, Japan

Program Chairs

Dieter Gollmann

Hamburg University of Technology, Germany

Felix C. Freiling

Friedrich-Alexander-Universität, Erlangen,
Germany

Program Committee

Magnus Almgren

Chalmers University of Technology, Sweden

Tuomas Aura

Aalto University, Finland

Joonsang Baek

KUSTAR, UAE

Alex Biryukov

University of Luxembourg, Luxembourg

Sonja Buchegger

KTH Royal Institute of Technology, Sweden

Liqun Chen

HP Laboratories Bristol, UK

Xiaofeng Chen

Xidian University, P.R. China

Chen-Mou Cheng

National Taiwan University, Taiwan

Sherman S.M. Chow

University of Waterloo, Canada

Jorge Cuellar

Siemens, Germany

Vanesa Daza

Universitat Pompeu Fabra, Spain

Claudia Diaz

KU Leuven, Belgium

Roberto Di Pietro

Università degli Studi Roma Tre, Italy

Josep Domingo-Ferrer

Universitat Rovira i Virgili, Spain

Bao Feng

Institute for Infocomm Research, Singapore

Eduardo B. Fernandez

Florida Atlantic University, USA

Josep Ferrer

University of the Balearic Islands, Spain

Sara Foresti

Università degli Studi di Milano, Italy

Stefanos Gritzalis

University of the Aegean, Greece

Thorsten Holz

Ruhr-Universität Bochum, Germany

Martin Johns

SAP, Germany

Angelos Keromytis

Columbia University, USA

Igor Kotenko

Russian Academy of Sciences, Russia

Xuejia Lai

Shanghai Jiao Tong University, P.R. China

Zhenkai Liang	National University of Singapore, Singapore
Peng Liu	Pennsylvania State University, USA
Javier López	Universidad de Málaga, Spain
Masahiro Mambo	Kanazawa University, Japan
Mark Manulis	TU Darmstadt, Germany
Atsuko Miyaji	JAIST, Japan
Jose Morales	Carnegie Mellon University, USA
Raphael C.-W. Phan	Loughborough University, UK
Frank Piessens	KU Leuven, Belgium
Christian W. Probst	Technical University of Denmark, Denmark
Vincent Rijmen	KU Leuven, Belgium
Matt Robshaw	Orange Labs, France
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Jörg Schwenk	Ruhr-Universität Bochum, Germany
Jan Seedorf	NEC Laboratories Europe, Germany
Miguel Soriano	Universitat Politècnica de Catalunya, Spain
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Kyushu University, Japan
Lingyu Wang	Concordia University, Canada
Susanne Wetzel	Stevens Institute of Technology, USA
Duncan Wong	City University of Hong Kong, P.R. China
Jeff Yan	Newcastle University, UK
S.M. Yiu	University of Hong Kong, P.R. China
Jianying Zhou	Institute for Infocomm Research, Singapore
Alf Zugenmaier	Hochschule München, Germany

Additional Reviewers

Man Ho Au	Javier Herranz
Werner Backes	Jialin Huang
Oleksandr Bodriagov	Kangkook Jee
Andrey Chechulin	Christos Kalloniatis
Kai Yuen Cheong	Ergina Kavallieratou
Tat Wing Chim	Gunnar Kreitz
Cheng-Kang Chu	Po-Chun Kuo
Willem De Groef	Sebastian Lekies
Philippe De Ryck	Gaëtan Leurent
Xinshu Dong	Wei Li
Ming Duan	Yue-Hsun Lin
Sebastian Gajek	Flavio Lombardi
Wei Gao	Nikolaos Makriyannis
Stefano Guarino	Daniel A. Mayer
Seda Gurses	Kirill Morozov

Nick Nikiforakis
 Evgenia Novikova
 Kazumasa Omote
 Kailas Patil
 Constantinos Patsakis
 Alfredo Rial
 Panagiotis Rizomiliotis
 Santi Martinez Rodriguez
 Rodrigo Roman
 Arnab Roy
 Igor Saenko
 Bagus Santoso
 Theodoor Scholte
 Nicolas Sendrier
 Isamu Teranishi
 Elmar Tischhauser
 Aggeliki Tsochou

Frederik Vercauteren
 José Luis Vivas
 Huaqun Wang
 Baodian Wei
 Ralf-Philipp Weinmann
 Jia Xu
 Kenji Yasunaga
 Eunjung Yoon
 Bin Zhao
 Hang Zhao
 Yuanjie Zhao
 Hui Zhang
 Tao Zhang
 Yinghui Zhang
 Chen Zhong
 Youwen Zhu

Publicity Chairs

Isaac Agudo
 Cheng-Kang Chu

Universidad de Málaga, Spain
 National Chiao Tung University, Taiwan

Local Organization

Marita Güngerich, Siglinde Böck, Eric Rothstein

Table of Contents

Invited Paper

Privacy-Preserving Speaker Authentication	1
<i>Manas Pathak, Jose Portelo, Bhiksha Raj, and Isabel Trancoso</i>	

Cryptography and Cryptanalysis

Differential Attacks on Reduced RIPEMD-160	23
<i>Florian Mendel, Tomislav Nad, Stefan Scherz, and Martin Schl��ffer</i>	
Revisiting Difficulty Notions for Client Puzzles and DoS Resilience	39
<i>Bogdan Groza and Bogdan Warinschi</i>	
On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree	55
<i>Noboru Kunihiro</i>	

Mobility

Strong Authentication with Mobile Phone	70
<i>Sanna Suoranta, Andr�� Andrade, and Tuomas Aura</i>	
Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?	86
<i>Chaitrali Amrutkar, Patrick Traynor, and Paul C. van Oorschot</i>	

Cards and Sensors

Domain-Specific Pseudonymous Signatures for the German Identity Card	104
<i>Jens Bender, ��zg��r Dagdelen, Marc Fischlin, and Dennis K��gler</i>	
Solutions for the Storage Problem of McEliece Public and Private Keys on Memory-Constrained Platforms	120
<i>Falko Strenzke</i>	
100% Connectivity for Location Aware Code Based KPD in Clustered WSN: Merging Blocks	136
<i>Samiran Bag, Aritra Dhar, and Pinaki Sarkar</i>	

Software Security

Learning Fine-Grained Structured Input for Memory Corruption Detection	151
<i>Lei Zhao, Debin Gao, and Lina Wang</i>	
Dynamic Anomaly Detection for More Trustworthy Outsourced Computation	168
<i>Sami Alsouri, Jan Sinschek, Andreas Sewe, Eric Bodden, Mira Mezini, and Stefan Katzenbeisser</i>	
An Empirical Study of Dangerous Behaviors in Firefox Extensions	188
<i>Jiangang Wang, Xiaohong Li, Xuhui Liu, Xinshu Dong, Junjie Wang, Zhenkai Liang, and Zhiyong Feng</i>	

Processing Encrypted Data

Collaboration-Preserving Authenticated Encryption for Operational Transformation Systems	204
<i>Michael Clear, Karl Reid, Desmond Ennis, Arthur Hughes, and Hitesh Tewari</i>	
Selective Document Retrieval from Encrypted Database.....	224
<i>Christoph Bösch, Qiang Tang, Pieter Hartel, and Willem Jonker</i>	
Additively Homomorphic Encryption with a Double Decryption Mechanism, Revisited	242
<i>Andreas Peter, Max Kronberg, Wilke Trei, and Stefan Katzenbeisser</i>	

Authentication and Identification

Secure Hierarchical Identity-Based Identification without Random Oracles	258
<i>Atsushi Fujioka, Taiichi Saito, and Keita Xagawa</i>	
Efficient Two-Move Blind Signatures in the Common Reference String Model	274
<i>E. Ghadafi and N.P. Smart</i>	

New Directions in Access Control

Compliance Checking for Usage-Constrained Credentials in Trust Negotiation Systems.....	290
<i>Jinwei Hu, Khaled M. Khan, Yun Bai, and Yan Zhang</i>	
A Quantitative Approach for Inexact Enforcement of Security Policies	306
<i>Peter Drábik, Fabio Martinelli, and Charles Morisset</i>	

OSDM: An Organizational Supervised Delegation Model for RBAC	322
<i>Nezar Nassr, Nidal Aboudagga, and Eric Steegmans</i>	

GPU for Security

GPU-Acceleration of Block Ciphers in the OpenSSL Cryptographic Library	338
<i>Johannes Gilger, Johannes Barnickel, and Ulrike Meyer</i>	
A Highly-Efficient Memory-Compression Approach for GPU-Accelerated Virus Signature Matching	354
<i>Ciprian Pungila and Viorel Negru</i>	

Models for Risk and Revocation

Intended Actions: Risk Is Conflicting Incentives	370
<i>Lisa Rajbhandari and Einar Sneekenes</i>	
On the Self-similarity Nature of the Revocation Data	387
<i>Carlos Gañán, Jorge Mata-Díaz, Jose L. Muñoz, Oscar Esparza, and Juanjo Alins</i>	

Author Index	401
-------------------------------	-----