

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zürich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

More information about this series at <http://www.springer.com/series/7410>

Yvo Desmedt (Ed.)

# Information Security

16th International Conference, ISC 2013  
Dallas, Texas, November 13–15, 2013  
Proceedings

*Editor*  
Yvo Desmedt  
The University of Texas at Dallas  
Richardson, TX  
USA

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-27658-8              ISBN 978-3-319-27659-5 (eBook)  
DOI 10.1007/978-3-319-27659-5

Library of Congress Control Number: 2015957049

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing Switzerland 2015

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.

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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by SpringerNature  
The registered company is Springer International Publishing AG Switzerland

# Preface

The Information Security Conference (ISC), which started as a workshop (ISW) in 1997, is an international conference organized yearly. It has been held in five different continents.

ISC 2013 was organized in cooperation with the International Association for Cryptologic Research, and the Department of Computer Science, The University of Texas at Dallas, USA.

There were 70 submitted papers, which were considered by the Program Committee. This is roughly the same as for ISC 2012, which took place in Passau, Germany, and had 72 submissions. Owing to the large number of submissions, some papers that contained new ideas had to be rejected. Priority was given to novel papers. Of the 70 submissions, 16 were selected, which is a 23 % acceptance rate. We also accepted 14 short papers. Each paper was sent to at least three members of the Program Committee for comments. Submissions to ISC 2013 were required to be anonymous. EasyChair was used for submissions, refereeing, etc.

Beside the accepted papers, two invited presentations were given. Michael Reiter (University of North Carolina at Chapel Hill) spoke about “How to Misuse, Use, and Mitigate Side Channels in Virtualized Environments.” G.R. Blakley (IACR Fellow) spoke about his joint work with Bob Blakley and Sean Blakley on “How to Draw Graphs: Seeing and Redrafting Large Networks in Security and Biology.”

The proceedings contain all the regular papers and short papers accepted, except for the paper “Formal Analysis of ECC-Based Direct Anonymous Attestation Schemes in Applied Pi Calculus,” by Li Xi, Yu Qin, and Dengguo Feng. Revisions of papers were not checked for correctness on their scientific aspects and the authors bear full responsibility for the content of their papers. Some of the papers may have been edited taking the comments of the Program Committee or external referees into account.

I am very grateful to the members of the Program Committee for their hard work and the difficult task of selecting the papers. The Program Committee appreciates the effort of the external referees who helped the Program Committee reach their decisions.

I thank the general chair, Bhavani Thuraisingham, and the local chair, Kevin Hamlen, for their help in organizing ISC 2013, and Stacy Morrison for some of the local organization aspects. Moreover, Julie Weekly helped with secretarial work and Jeyakesavan Veerasamy with the registration process.

Finally, I would like to thank everyone who submitted their work to ISC 2013.

# ISC 2013

The 15th Information Security Conference was held in in cooperation with the International Association for Cryptologic Research, and the Department of Computer Science, The University of Texas at Dallas.

## General Chair

Bhavani                      The University of Texas at Dallas, USA  
Thuraisingham

## Local Chair

Kevin Hamlen              The University of Texas at Dallas, USA

## Steering Committee Chair

Masahiro Mambo         Kanazawa University, Japan

## Program Chair

Yvo Desmedt                The University of Texas at Dallas, USA;  
and University College London, UK

## Local Organizing Committee

Yvo Desmedt  
Kevin Hamlen  
Stacy Morrison  
Bhavani Thuraisingham

## Program Committee

Alessandro Acquisti      Carnegie Mellon University, USA  
Elisa Bertino                Purdue University, USA  
Jean Camp                    Indiana University, USA  
K.P. Chow                    University of Hong Kong, SAR China  
Ed Dawson                    QUT, Australia  
Sabrina De Capitani        University of Milan, Italy  
Di Vimercati  
Yvo Desmedt                The University of Texas at Dallas, USA;  
(Chair)                        and University College London, UK  
Manuel Egele                Carnegie Mellon University, USA

Hanaoka Goichiro	AIST, Japan
Thomas Gross	University of Newcastle, UK
Yong Guan	Iowa State University, USA
Sushil Jajodia	George Mason University, USA
Audun Jøsang	University of Oslo, Norway
Guenter Karjoth	IBM Zurich, Switzerland
Brian King	Indiana University-Purdue University, Indianapolis, USA
Silvio Lattanzi	Google, USA
Benoit Libert	Technicolor, France
Helger Lipmaa	University of Tartu, Estonia
Javier Lopez	University of Malaga, Spain
Stephen McLaughlin	Pennsylvania State University, USA
Atsuko Miyaji	JAIST, Japan
David Naccache	University of Paris II, France
Tatsuaki Okamoto	NTT Labs, Japan
Giuseppe Persiano	University of Salerno, Italy
Josef Pieprzyk	Macquarie University, Australia
Bart Preneel	Catholic University of Leuven, Belgium
Rei Safavi-Naini	University of Calgary, Canada
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	University of Milan, Italy
Joshua Schiffman	AMD, USA
Gene Spafford	Purdue University, USA
John Steinberger	Tsinghua University, China
Ron Steinfeld	Monash University Australia
Tsuyoshi Takagi	Kyushu University, Japan
Catherine Tucker	MIT, USA
Vijay Varadharajan	Macquarie University, Australia
Meiqin Wang	Shandong University, China
Yongge Wang	University of North Carolina Charlotte, USA
Danfeng Yao	Virginia Tech, USA
John Zic	CSIRO, Australia

## Additional Reviewers

Albanese, Massimiliano  
Alcaraz, Cristina  
Alimomeni, Mohsen  
Balasch, Josep  
Bilgin, Begül  
Camp, Jean  
Chen, Jiageng  
Cheng, Shu  
Devigne, Julien  
Fong, Philip  
Futa, Yuichi  
Gierlichs, Benedikt  
Gupta, Aditi  
Hayashi, Takuya  
Hori, Yoshiaki  
Jiang, Shaoquan  
Kawai, Yutaka  
Kobayashi, Tetsutaro  
Liu, Zhenhua  
Livraga, Giovanni  
Min, Byungho  
Morozov, Kirill  
Ohata, Satsuya  
Persichetti, Edoardo

Sakai, Yusuke  
Sendrier, Nicolas  
Shebaro, Bilal  
Shin, Seonghan  
Shirase, Masaaki  
Sirvent, Thomas  
Su, Chunhua  
Sun, Kun  
Tibouchi, Mehdi  
Tupakula, Uday  
Van Herrewege, Anthony  
Varici, Kerem  
Wang, Haining  
Wang, Pengwei  
Wei, Puwen  
Xeng, Xifan  
Yanai, Naoto  
Yiu, Siu Ming  
Yoneyama, Kazuki  
Yoshino, Masayuki  
Zhang, Hui  
Zhang, Tongjie  
Zhao, Fangming  
Zhou, Lan



# Contents

## Security of Operating Systems

Integrity Checking of Function Pointers in Kernel Pools via Virtual Machine Introspection . . . . .	3
<i>Irfan Ahmed, Golden G. Richard III, Aleksandar Zoranic, and Vassil Roussev</i>	

Lightweight Attestation and Secure Code Update for Multiple Separated Microkernel Tasks. . . . .	20
<i>Steffen Wagner, Christoph Krauß, and Claudia Eckert</i>	

## Secret Sharing

The Security Defect of a Multi-pixel Encoding Method . . . . .	39
<i>Teng Guo, Feng Liu, ChuanKun Wu, YoungChang Hou, YaWei Ren, and Wen Wang</i>	

Encrypted Secret Sharing and Analysis by Plaintext Randomization . . . . .	49
<i>Stephen R. Tate, Roopa Vishwanathan, and Scott Weeks</i>	

## Encryption

Round-Efficient Private Stable Matching from Additive Homomorphic Encryption . . . . .	69
<i>Tadanori Teruya and Jun Sakuma</i>	

Efficient and Fully Secure Forward Secure Ciphertext-Policy Attribute-Based Encryption. . . . .	87
<i>Takashi Kitagawa, Hiroki Kojima, Nuttapon Attrapadung, and Hideki Imai</i>	

Reducing Public Key Sizes in Bounded CCA-Secure KEMs with Optimal Ciphertext Length . . . . .	100
<i>Takashi Yamakawa, Shota Yamada, Takahiro Matsuda, Goichiro Hanaoka, and Noboru Kunihiro</i>	

## Malware and Critical Infrastructures

4GMOP: Mopping Malware Initiated SMS Traffic in Mobile Networks . . . . .	113
<i>Marián Kühnel and Ulrike Meyer</i>	

Design and Analysis of a Sophisticated Malware Attack Against Smart Grid . . .	130
<i>Byungho Min and Vijay Varadharajan</i>	
Multi-round Attacks on Structural Controllability Properties for Non-complete Random Graphs . . . . .	140
<i>Cristina Alcaraz, Estefanía Etchevés Miciolino, and Stephen Wolthusen</i>	
<b>Cryptanalysis</b>	
Improved Meet-in-the-Middle Attacks on Round-Reduced ARIA . . . . .	155
<i>Dongxia Bai and Hongbo Yu</i>	
Establishing Equations: The Complexity of Algebraic and Fast Algebraic Attacks Revisited . . . . .	169
<i>Lin Jiao, Bin Zhang, and Mingsheng Wang</i>	
Factoring a Multiprime Modulus $N$ with Random Bits . . . . .	185
<i>Routo Terada and Reynaldo Cáceres Villena</i>	
<b>Block Ciphers and Stream Ciphers</b>	
Faster 128-EEA3 and 128-EIA3 Software . . . . .	199
<i>Roberto Avanzi and Billy Bob Brumley</i>	
Merging the Camellia, SMS4 and AES S-Boxes in a Single S-Box with Composite Bases. . . . .	209
<i>Alberto F. Martínez-Herrera, Carlos Mex-Perera, and Juan Nolasco-Flores</i>	
<b>Entity Authentication</b>	
Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards . . . . .	221
<i>Ding Wang and Ping Wang</i>	
Self-blindable Credential: Towards Anonymous Entity Authentication Upon Resource Constrained Devices . . . . .	238
<i>Yanjiang Yang, Xuhua Ding, Haibing Lu, Jian Weng, and Jianying Zhou</i>	
Practical and Provably Secure Distance-Bounding . . . . .	248
<i>Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay</i>	

**Usability and Risk Perception**

- On the Viability of CAPTCHAs for use in Telephony Systems: A Usability Field Study . . . . . 261  
*Niharika Sachdeva, Nitesh Saxena, and Ponnuram Kumaraguru*
- Cars, Condoms, and Facebook . . . . . 280  
*Vaibhav Garg and L. Jean Camp*

**Access Control**

- Achieving Revocable Fine-Grained Cryptographic Access Control over Cloud Data. . . . . 293  
*Yanjiang Yang, Xuhua Ding, Haibing Lu, Zhiguo Wan, and Jianying Zhou*
- Fine-Grained Access Control for HTML5-Based Mobile Applications in Android . . . . . 309  
*Xing Jin, Lusha Wang, Tongbo Luo, and Wenliang Du*

**Computer Security**

- CrowdFlow: Efficient Information Flow Security . . . . . 321  
*Christoph Kerschbaumer, Eric Hennigan, Per Larsen, Stefan Brunthaler, and Michael Franz*

**Privacy Attacks**

- DroidTest: Testing Android Applications for Leakage of Private Information . . . . . 341  
*Sarker T. Ahmed Rumeen and Donggang Liu*
- A Dangerous Mix: Large-Scale Analysis of Mixed-Content Websites . . . . . 354  
*Ping Chen, Nick Nikiforakis, Christophe Huygens, and Lieven Desmet*

**Cryptography**

- An Ordered Multisignature Scheme Under the CDH Assumption Without Random Oracles . . . . . 367  
*Naoto Yanai, Masahiro Mambo, and Eiji Okamoto*
- Human Assisted Randomness Generation Using Video Games . . . . . 378  
*Mohsen Alimomeni and Reihaneh Safavi-Naini*
- Security Ranking Among Assumptions Within the *Uber Assumption* Framework. . . . . 391  
*Antoine Joux and Antoine Rojat*

A Secure and Efficient Method for Scalar Multiplication on Supersingular  
Elliptic Curves over Binary Fields. . . . . 407  
*Matheus F. de Oliveira and Marco Aurélio Amaral Henriques*

**Author Index** . . . . . 417