

*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*

Mike Burmester  
Gene Tsudik  
Spyros Magliveras  
Ivana Ilić (Eds.)

# Information Security

13th International Conference, ISC 2010  
Boca Raton, FL, USA, October 25-28, 2010  
Revised Selected Papers



Springer

## Volume Editors

Mike Burmester  
Department of Computer Science  
Florida State University  
Tallahassee, FL, 32306-4530, USA  
E-mail: burmester@cs.fsu.edu

Gene Tsudik  
Department of Computer Science  
University of California  
Irvine, CA, 92697-3425, USA  
E-mail: gts@ics.uci.edu

Spyros Magliveras  
Department of Mathematical Sciences  
Florida Atlantic University  
Boca Raton, FL, 33431-0991, USA  
E-mail: spyros@fau.edu

Ivana Ilić  
Department of Mathematical Sciences  
Florida Atlantic University  
Boca Raton, FL, 33431-0991, USA  
E-mail: iva\_ilic@yahoo.com

ISSN 0302-9743  
ISBN 978-3-642-18177-1  
DOI 10.1007/978-3-642-18178-8  
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349  
e-ISBN 978-3-642-18178-8

Library of Congress Control Number: 2010942728

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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)

# Preface

The 13<sup>th</sup> Information Security Conference (ISC 2010) was held at Deerfield Beach / Boca Raton, Florida, USA, during October 25–28, 2010. The conference was hosted by the Center for Cryptology and Information Security (CCIS) at the Mathematical Sciences Department of Florida Atlantic University in Boca Raton, Florida.

ISC is an annual international conference covering research in theory and applications of information security and aims to attract high quality-papers in all technical aspects of information security as well as to provide a forum for professionals from academia and industry to present their work and exchange ideas. We are very pleased with both the number and high quality of this year's submissions. The Program Committee received 117 submissions, and accepted 25 as full papers (acceptance rate 21%). The papers were selected after an extensive and careful refereeing process in which each paper was reviewed by at least three members of the Program Committee. A further 11 articles were selected as short papers because of their appropriateness and high quality. A new experimental format was adopted this year: pre-conference proceedings of all accepted papers were made available at the conference. This provided an additional opportunity for authors to solicit and obtain early feedback. The Springer proceedings were mailed to the authors after the conference.

Many people deserve our gratitude for their generous contributions to the success of this conference. We wish to thank all the members of the ISC 2010 Program Committee, as well as the external reviewers, for reviewing, deliberating and selecting (under severe time pressure and in the middle of summer) an excellent set of papers. Thanks are also due to Masahiro Mambo who, as our contact person on the ISC Steering Committee, helped maintain ISC traditions and provided guidance. Mega-kudos to Ivana Ilić for contributing a tremendous amount of work, much of it beyond the call of duty. Also, a great deal of thanks are due to: Emily Cimillo for helping with budgetary issues, Leanne Magliveras for keeping track of numerous organizational tasks, as well as Nidhi Singhi, Nikhil Singhi and Nicola Pace for invaluable assistance with various conference aspects.

We are delighted to acknowledge the sponsorship of CCIS; of the Center for Security and Assurance in IT (C-SAIT) of Florida State University; of the Charles E. Schmidt College of Science at Florida Atlantic University; and of the DATAMAXX group, the latter having provided support for the *Best Student Paper Awards* and additional funds for graduate student support.

Last but not least, on behalf of all those involved in organizing the conference we would like to thank all the authors who submitted papers to this conference. Without their submissions and support, ISC could not have been a success.

November 2010

Spyros Magliveras  
Mike Burmester  
Gene Tsudik

# Organization

## General Chair

Spyros Magliveras                      CCIS, Florida, USA

## Program Committee Co-chairs

Mike Burmester                      Florida State University, USA  
Gene Tsudik                          University of California, Irvine, USA

## Program Committee

Giuseppe Ateniese	Johns Hopkins University, USA
Elisa Bertino	Purdue University, USA
Simon Blackburn	Royal Holloway, UK
Ian Blake	University of Toronto, Canada
Marina Blanton	University of Notre Dame, USA
Carlo Blundo	Università di Salerno, Italy
Colin Boyd	Queensland University of Technology Australia
Levente Buttyan	Budapest University of Technology and Economics, Hungary
Cafer Caliskan	Michigan Technical University Michigan, USA
Claude Castelluccia	INRIA, France
David Chadwick	University of Kent, UK
Jung Hee Cheon	Seoul National University, Korea
Emiliano De Cristofaro	University of California, Irvine, USA
Vanesa Daza	Universitat Pompeu Fabra, Spain
Claudia Diaz	KU Leuven, Belgium
Roberto Di Pietro	Roma Tre University, Italy
Xuhua Ding	Singapore Management University, Singapore
Wenliang Du	Syracuse University, France
Thomas Eisenbarth	CCIS, Florida, USA
Eduardo Fernandez	Florida Atlantic University, USA
Juan Garay	ATT Research, USA
Madeline Gonzalez	Cybernetica AS, Estonia
Nick Hopper	University of Minnesota, USA
Ivana Ilić	CCIS, Florida, USA

## VIII Organization

Kwangjo Kim	KAIST, Korea
Yongdae Kim	University of Minnesota, USA
Panos Kotzanikolaou	University of Piraeus, Greece
Feifei Li	Florida State University, Florida, USA
Javier Lopez	University of Malaga, Spain
Di Ma	University of Michigan, Dearborn, USA
Masahiro Mambo	University of Tsukuba, Japan
Emmanouil Magkos	University of the Ionian, Greece
Mark Manulis	TU Darmstadt, Germany
Ken Matheis	CCIS, Florida, USA
Nasir Memon	New York Polytechnic, New York, USA
Alfred Menezes	University of Waterloo, Canada
Ron Mullin	University of Waterloo, Canada
Jorge Munilla	Universidad de Málaga, Spain
David Naccache	ENS and Université Paris II, France
Juan Gonzalez Nieto	Queensland University of Technology Australia
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Nitesh Saxena	CS Dept, Polytechnic Institute of NYU USA
Elaine Shi	PARC, USA
Radu Sion	Stony Brook University, USA
Nikhil Singhi	CCIS, Florida, USA
Nidhi Singhi	CCIS, Florida, USA
Claudio Soriente	Madrid Polytechnic, Spain
Michal Sramka	Universitat Rovira i Virgili, Spain
Rainer Steinwandt	CCIS, Florida, USA
Doug Stinson	University of Waterloo, Canada
Jonathan Trostle	Johns Hopkins University, USA
Patrick Traynor	Georgia Institute of Technology, USA
Tran van Trung	University of Essen-Duisburg, Germany
Ivan Visconti	Università di Salerno, Italy
Bogdan Warinschi	University of Bristol, UK
Shouhuai Xu	University of Texas at San Antonio USA
Sencun Zhu	Pennsylvania State University, USA

## External Reviewers

Gegerly Acs	Claudio A. Ardagna
Andrey Bogdanov	Eric Chan-Tin
Sanjit Chatterjee	Andrew Clark
Mauro Conti	Sabrina De Capitani di Vimercati
Elke De Mulder	Carmen Fernandez
Sara Foresti	Aurelien Francillon
Tim Gueneysu	Tzipora Halevi
Darrel Hankerson	Kristiyan Haralambiev
Jens Hermans	Javier Herranz
Seokhie Hong	Sebastiaan Indesteege
Vincenzo Iovino	Rob Jansen
Yoonchan Jhi	Seny Kamara
B. Hoon Kang	Jaehoon Kim
Jihye Kim	Taekyoung Kwon
Kerstin Lemke-Rust	Zi Lin
Gabriel Maganis	Joan Mir
Amir Moradi	Jose Morales
Franciso Moyano	Arvind Narayanan
Yuan Niu	Jose A. Onieva
Andrs Ortiz	Abhi Pandya
Sai Teja Peddinti	Daniele Perito
Benny Pinkas	Alessandra Scafuro
Stefan Schiffner	Max Schuchard
Gautham Sekar	Jae Hong Seo
Douglas Stebila	Dongdong Sun
Germn Sez	Anthony Van Herrewege
Nino V. Verde	Jose L. Vivas
Jonathan Voris	Qianhong Wu
Wei Xu	Li Xu
Aaram Yun	Zhenxin Zhan
Lei Zhang	



# Table of Contents

## Attacks and Analysis

Improved Collision Attacks on the Reduced-Round Grøstl Hash Function .....	1
<i>Kota Ideguchi, Elmar Tischhauser, and Bart Preneel</i>	
Improved Distinguishing Attack on Rabbit .....	17
<i>Yi Lu and Yvo Desmedt</i>	
Cryptanalysis of the Convex Hull Click Human Identification Protocol .....	24
<i>Hassan Jameel Asghar, Shujun Li, Josef Pieprzyk, and Huaxiong Wang</i>	
An Analysis of DepenDNS .....	31
<i>Nadhem J. AlFardan and Kenneth G. Paterson</i>	

## Analysis

Security Reductions of the Second Round SHA-3 Candidates .....	39
<i>Elena Andreeva, Bart Mennink, and Bart Preneel</i>	
Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents .....	54
<i>Özgür Dagdelen and Marc Fischlin</i>	
Revisiting the Security of the ALRED Design .....	69
<i>Marcos A. Simplicio Jr., Paulo S.L.M. Barreto, and Tereza C.M.B. Carvalho</i>	

## Authentication, PIR and Content Identification

Lightweight Anonymous Authentication with TLS and DAA for Embedded Mobile Devices .....	84
<i>Christian Wachsmann, Liqun Chen, Kurt Dietrich, Hans Löhr, Ahmad-Reza Sadeghi, and Johannes Winter</i>	
Implicit Authentication through Learning User Behavior .....	99
<i>Elaine Shi, Yuan Niu, Markus Jakobsson, and Richard Chow</i>	

Efficient Computationally Private Information Retrieval from Anonymity or Trapdoor Groups .....	114
<i>Jonathan Trostle and Andy Parrish</i>	

Video Streaming Forensic – Content Identification with Traffic Snooping .....	129
<i>Yali Liu, Ahmad-Reza Sadeghi, Dipak Ghosal, and Biswanath Mukherjee</i>	

## Privacy

Fair and Privacy-Preserving Multi-party Protocols for Reconciling Ordered Input Sets .....	136
<i>Georg Neugebauer, Ulrike Meyer, and Susanne Wetzel</i>	

Enhancing Security and Privacy in Certified Mail Systems Using Trust Domain Separation .....	152
<i>Arne Tauber and Thomas Rössler</i>	

Privacy-Preserving ECC-Based Grouping Proofs for RFID .....	159
<i>Lejla Batina, Yong Ki Lee, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede</i>	

## Malware, Crimeware and Code Injection

Artificial Malware Immunization Based on Dynamically Assigned Sense of Self .....	166
<i>Xinyuan Wang and Xuxian Jiang</i>	

Misleading Malware Similarities Analysis by Automatic Data Structure Obfuscation .....	181
<i>Zhi Xin, Huiyu Chen, Hao Han, Bing Mao, and Li Xie</i>	

Crimeware Swindling without Virtual Machines .....	196
<i>Vasilis Pappas, Brian M. Bowen, and Angelos D. Keromytis</i>	

An Architecture for Enforcing JavaScript Randomization in Web2.0 Applications .....	203
<i>Elias Athanasopoulos, Antonis Krithinakis, and Evangelos P. Markatos</i>	

## Intrusion Detection

Summary-Invisible Networking: Techniques and Defenses .....	210
<i>Lei Wei, Michael K. Reiter, and Ketan Mayer-Patel</i>	

Selective Regular Expression Matching .....	226
<i>Natalia Stakhanova, Hanli Ren, and Ali A. Ghorbani</i>	

Traceability of Executable Codes Using Neural Networks . . . . .	241
<i>Davidson R. Boccardo, Tiago M. Nascimento, Raphael C. Machado, Charles B. Prado, and Luiz F.R.C. Carmo</i>	

## Side Channels

On Side-Channel Resistant Block Cipher Usage . . . . .	254
<i>Jorge Guajardo and Bart Mennink</i>	
Security Implications of Crosstalk in Switching CMOS Gates . . . . .	269
<i>Geir Olav Dyrkolbotn, Knut Wold, and Einar Snekkenes</i>	
On Privacy Leakage through Silence Suppression . . . . .	276
<i>Ye Zhu</i>	

## Cryptography

One-Time Trapdoor One-Way Functions . . . . .	283
<i>Julien Cathalo and Christophe Petit</i>	
Public Key Encryption Schemes with Bounded CCA Security and Optimal Ciphertext Length Based on the CDH Assumption . . . . .	299
<i>Mayana Pereira, Rafael Dowsley, Goichiro Hanaoka, and Anderson C.A. Nascimento</i>	
A Short Signature Scheme from the RSA Family . . . . .	307
<i>Ping Yu and Rui Xue</i>	
Efficient Message Space Extension for Automorphic Signatures . . . . .	319
<i>Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo</i>	

## Smartphones

CRePE: Context-Related Policy Enforcement for Android . . . . .	331
<i>Mauro Conti, Vu Thien Nga Nguyen, and Bruno Crispo</i>	
Privilege Escalation Attacks on Android . . . . .	346
<i>Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, and Marcel Winandy</i>	

## Biometrics

Walk the Walk: Attacking Gait Biometrics by Imitation . . . . .	361
<i>Bendik B. Mjaaland, Patrick Bours, and Danilo Gligoroski</i>	

## Cryptography, Application

Efficient Multiplicative Homomorphic E-Voting . . . . .	381
<i>Kun Peng and Feng Bao</i>	
Double Spending Protection for E-Cash Based on Risk Management . . . .	394
<i>Patricia Everaere, Isabelle Simplot-Ryl, and Issa Traoré</i>	

## Buffer Overflow

Integrating Offline Analysis and Online Protection to Defeat Buffer Overflow Attacks . . . . .	409
<i>Donghai Tian, Xi Xiong, Changzhen Hu, and Peng Liu</i>	

## Cryptography, Theory

Deciding Recognizability under Dolev-Yao Intruder Model . . . . .	416
<i>Zhiwei Li and Weichao Wang</i>	
Indifferentiable Security Reconsidered: Role of Scheduling . . . . .	430
<i>Kazuki Yoneyama</i>	

<b>Author Index</b> . . . . .	445
-------------------------------	-----