Lecture Notes in Computer Science 4779

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Juan A. Garay Arjen K. Lenstra
Masahiro Mambo René Peralta (Eds.)

Information Security

10th International Conference, ISC 2007
Valparaíso, Chile, October 9-12, 2007
Proceedings

Springer

Volume Editors

Juan A. Garay
Bell Labs
600 Mountain Ave., Murray Hill, NJ 07974, USA
E-mail: garay@research.bell-labs.com

Arjen K. Lenstra
EPFL IC LACAL
INJ 330, Station 14, CH-1015 Lausanne, Switzerland
E-mail: arjen.lenstra@epfl.ch

Masahiro Mambo
University of Tsukuba
1-1-1 Tennoudai, Tsukuba, Ibaraki, 305-8573, Japan
E-mail: mambo@cs.tsukuba.ac.ip

René Peralta
NIST, Security Division, Information Technology Laboratory
Gaithersburg, MD. 20899, USA
E-mail: rene.peralta@nist.gov

Library of Congress Control Number: 2007936070

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-75495-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-75495-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12170333 06/3180 5 4 3 2 1 0

Preface

The 10th Information Security Conference (ISC 2007) was held in Valparaíso, Chile, October 9–12, 2007. ISC is an annual international conference covering research in theory and applications of information security, aiming to attract high quality papers in all of its technical aspects. ISC was first initiated as a workshop (ISW) in Japan in 1997, ISW 1999 was held in Malaysia and ISW 2000 in Australia. The name was changed to the current one when the conference was held in Spain in 2001 (ISC 2001). The latest conferences were held in Brazil (ISC 2002), the UK (ISC 2003), the USA (ISC 2004), Singapore (ISC 2005), and Greece (ISC 2006). This year the event was sponsored by the Universidad Técnica Federico Santa María (Valparaíso, Chile), the Support Center for Advanced Telecommunications Technology Research, Foundation, SCAT(Tokyo, Japan), Microsoft Corporation, and Yahoo! Research.

Reflecting the conference's broad scope, this year's main Program Committee consisted of a relatively large number (49) of experts. Additionally, given the timely topic of cryptanalysis and design of hash functions and the NIST hash competition, the conference also featured a special Hash Subcommittee, chaired by Arjen Lenstra (EPFL and Bell Labs), as well as a panel on hashing, chaired by Bill Burr (NIST). The conference received 116 submissions, 29 of which were selected by the committee members for presentation at the conference, based on quality, originality and relevance. Each paper was anonymously reviewed by at least three committee members.

Extended abstracts of 28 of the selected papers (a decision was made that only papers whose authors could commit to presenting them at the conference would be published), many revised according to the reviewers' suggestions, appear in these proceedings. An important ISC interest is to encourage and promote student participation. In line with that interest, the ISC 2007 Program Committee had the pleasure of selecting three student-coauthored papers for the Best Student Paper award—one from each region ISC rotates among: Asia, Europe, and the Americas. The papers were, respectively, "Identity-Based Proxy Re-encryption Without Random Oracles," by Cheng-Kang Chu and Wen-Guey Tzeng (National Chiao Tung University, Taiwan), "Detecting System Emulators," by Thomas Raffetseder, Christopher Kruegel, and Engin Kirda (Technical University of Vienna, Austria), and "Impossible-Differential Attacks on Large-Block Rijndael," by Jorge Nakahara Jr. and Ivan Carlos Pavão (Catholic University of Santos, Brazil). The program also included invited lectures by Hugo Krawczyk (IBM's T.J. Watson Research Center, USA), and Brent Waters (SRI International, USA).

First and foremost, I am extremely grateful to the members of the Program Committee and Hash Subcommittee for their investment and effort in the

process—many times difficult and delicate—of paper review and selection, as well as to the large number of external reviewers for their valuable help.

Electronic submissions were made possible by the Web Submission and Review Software developed by Shai Halevi, which was hosted at the Universidad Técnica Federico Santa María. Many thanks to Raul Monge for making that possible—and for his perennial availability when problems arose, to Shai for his support, and to Debbie Cook and Marcos Kiwi for their help in the handling of the submissions.

Beyond the hosting of the submission software, Raúl Monge and his team did a magnificent job managing and taking care of all aspects of the local organization. I am also most grateful to the general chairs, Masahiro Mambo and René Peralta, for all their hard work, assistance and advice on a myriad of issues related to this conference.

Finally, I wish to thank all the authors for submitting their work to ISC 2007, and the authors of the accepted papers for their contribution to the high technical quality of the program. As technology evolves and means of communication and interaction become increasingly more complex and sophisticated, so does the need not only for guaranteeing their soundness and safety when run in adversarial settings, but also for novel techniques that actually make them possible. Without a doubt, the new notions, methods and designs presented in these proceedings constitute an important step in those directions.

August 2007 Juan A. Garay

ISC 2007

The 10th International Security Conference
Valparaíso, Chile, October 9–12, 2007

ISC Steering Committee

Ed Dawson	Queensland University of Technology, Australia
Sokratis K. Katsikas	University of the Aegean, Greece
Javier López	University of Málaga, Spain
Masahiro Mambo	University of Tsukuba, Japan
Eiji Okamoto	University of Tsukuba, Japan
René Peralta	NIST, USA
Rebecca Wright	Rutgers University, USA
Yuliang Zheng	University of North Carolina–Charlotte, USA

General Chairs

Masahiro Mambo	University of Tsukuba, Japan
René Peralta	NIST, USA

Program Chair

Juan A. Garay	Bell Labs, USA

Hash Subcommittee Chair

Arjen Lenstra	EPFL, Switzerland and Bell Labs, USA

Organizing Chair

Raúl Monge	Universidad Técnica Federico Santa María, Chile

Program Committee

Michel Abdalla	ENS, France
Mikhail Atallah	Purdue University, USA
Michael Backes	Saarland University, Germany
Feng Bao	Institute for Infocomm Research, Singapore
Paulo Barreto	University of Sao Paulo, Brazil

John Black	University of Colorado, USA
Debbie Cook	Bell Labs, USA
Claudia Diaz	K.U. Leuven, Belgium
Glenn Durfee	PARC, USA
Nelly Fazio	IBM Research, USA
Matthias Fitzi	ETH Zürich, Switzerland
Stuart Haber	HP Labs, USA
Shai Halevi	IBM Research, USA
Amir Herzberg	Bar-Ilan University, Israel
Alejandro Hevia	University of Chile, Chile
Trent Jaeger	Penn State University, USA
Stasio Jarecki	University of California-Irvine, USA
Angelos Keromytis	Columbia University, USA
Aggelos Kiayias	University of Connecticut, USA
Kwangjo Kim	Information and Comms. University, Korea
Marcos Kiwi	University of Chile, Chile
Steve Kremer	ENS Cachan, France
Dong Hoon Lee	Korea University, Korea
Helger Lipmaa	University College London, UK
Breno de Medeiros	Florida State University, USA
Atsuko Mijayi	JAIST, Japan
Fabian Monrose	Johns Hopkins University, USA
Gregory Neven	K.U. Leuven, Belgium
Kaisa Nyberg	Helsinki Univ. of Tech. and Nokia, Finland
Carles Padró	Polytechnic University of Catalonia, Spain
Sarvar Patel	Alcatel-Lucent, USA
Sihan Qing	Chinese Academy of Sciences, China
Greg Rose	Qualcomm, USA
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	University of Milan, Italy
Andre Scedrov	University of Pennsylvania, USA
Berry Schoenmakers	Technical University Eindhoven, Holland
Tom Shrimpton	Portland State University, USA
Michael Steiner	IBM Research, USA
Doug Tygar	University of California-Berkeley, USA
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Dominique Unruh	Saarland University, Germany
Ariel Waissbein	ITBA and Core Security, Argentina
Brent Waters	SRI International, USA
Susanne Wetzel	Stevens Institute of Technology, USA
Stephen Wolthusen	Royal Holloway University of London, UK
Moti Yung	Columbia University, USA
Xiaolan (Catherine) Zhang	IBM Research, USA

Hash Subcommittee

John Black	University of Colorado, USA
Shai Halevi	IBM Research, USA
Paul Hoffman	VPN Consortium, USA
John Kelsey	NIST, USA
Vlastimil Klima	Czech Republic
Stefan Lucks	Bauhaus-University Weimar, Germany
Tom Shrimpton	Portland State University, USA
Martijn Stam	EPFL, Switzerland
Ron Steinfeld	Macquarie University, Australia
Marc Stevens	Technical University Eindhoven, Holland

External Reviewers

Andre Adelsbach
Claudio Ardagna
Georges Baatz
Joonsang Baek
Billy Brumley
Matt Burnside
Reza Curtmola
George Danezis
Marie Duflot
Ratna Dutta
Sara Foresti
Ezequiel Gutesman
Martin Hirt
Susan Hohenberger
Bill Horne
Sotiris Ioannidis
Florent Jacquemard
Charanjit Jutla
Marcelo Kaihara
Darko Kirovski
Tetsutaro Kobayashi
Vladimir Kolesnikov
Yuichi Komano
Gaicheng Li
Hafiz Malik
Michael de Mare
Toshihiko Matsuo
Vishal Misra
Rossana Motta
Ginger Myles
Cedric Ng
Antonio Nicolosi
Prasad Rao
Mohammed-Reza Reyhanitabar
Mark Ryan
Siamak Shahandashti
Nicholas Sheppard
Seonghan Shin
Johan Sjoedin
Mitsuru Tada
Katsuyuki Takashima
Qiang Tang
Carmela Troncoso
Duc Liem Vo
Shabsi Walfish
Guilin Wang
Wendy Hui Wang
Qianhong Wu
Yongdong Wu
Angelika Zavou
Hong-Sheng Zhou

Sponsoring Institutions

Universidad Técnica Federico Santa María, Valparaíso, Chile
Support Center for Advanced Telecommunications Technology Research, Foundation, Japan
Microsoft Corporation
Yahoo! Research

Table of Contents

Identify-Based Cryptography

Cryptanalysis

Network Security

Software Obfuscation

Public-Key Cryptosystems

Elliptic Curves and Applications

Database Security and Privacy