

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

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.jp

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

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.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

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

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

Intrusion Detection

Detecting System Emulators	1
<i>Thomas Raffetseder, Christopher Kruegel, and Engin Kirda</i>	
Features vs. Attacks: A Comprehensive Feature Selection Model for Network Based Intrusion Detection Systems	19
<i>Iosif-Viorel Onut and Ali A. Ghorbani</i>	
E-NIPS: An Event-Based Network Intrusion Prediction System	37
<i>Pradeep Kannadiga, Mohammad Zulkernine, and Anwar Haque</i>	

Digital Rights Management

Enabling Fairer Digital Rights Management with Trusted Computing...	53
<i>Ahmad-Reza Sadeghi, Marko Wolf, Christian Stübke, N. Asokan, and Jan-Erik Ekberg</i>	
Traitor Tracing with Optimal Transmission Rate	71
<i>Nelly Fazio, Antonio Nicolosi, and Duong Hieu Phan</i>	

Symmetric-Key Cryptography

The Security of Elastic Block Ciphers Against Key-Recovery Attacks ...	89
<i>Debra L. Cook, Moti Yung, and Angelos D. Keromytis</i>	
Impossible-Differential Attacks on Large-Block Rijndael	104
<i>Jorge Nakahara Jr. and Ivan Carlos Pavão</i>	
High-Speed Pipelined Hardware Architecture for Galois Counter Mode	118
<i>Akashi Satoh, Takeshi Sugawara, and Takafumi Aoki</i>	

Cryptographic Protocols and Schemes

Efficient Committed Oblivious Transfer of Bit Strings	130
<i>Mehmet S. Kiraz, Berry Schoenmakers, and José Villegas</i>	
An Efficient Certified Email Protocol	145
<i>Jun Shao, Min Feng, Bin Zhu, and Zhenfu Cao</i>	
Revisiting the Security Model for Timed-Release Encryption with Pre-open Capability	158
<i>Alexander W. Dent and Qiang Tang</i>	

On the Soundness of Restricted Universal Designated Verifier Signatures and Dedicated Signatures: How to Prove the Possession of an ElGamal/DSA Signature	175
<i>Fabien Laguillaumie and Damien Vergnaud</i>	

Identify-Based Cryptography

Identity-Based Proxy Re-encryption Without Random Oracles	189
<i>Cheng-Kang Chu and Wen-Guey Tzeng</i>	
Strongly-Secure Identity-Based Key Agreement and Anonymous Extension	203
<i>Sherman S.M. Chow and Kim-Kwang Raymond Choo</i>	

Cryptanalysis

Small Private-Exponent Attack on RSA with Primes Sharing Bits	221
<i>Yao-Dong Zhao and Wen-Feng Qi</i>	
Multiple Modular Additions and Crossword Puzzle Attack on NLSv2 . . .	230
<i>Joo Yeon Cho and Josef Pieprzyk</i>	
New Weaknesses in the Keystream Generation Algorithms of the Stream Ciphers TPy and Py	249
<i>Gautham Sekar, Souradyuti Paul, and Bart Preneel</i>	

Network Security

Queue Management as a DoS Counter-Measure?	263
<i>Daniel Boteanu, José M. Fernandez, John McHugh, and John Mullins</i>	

Software Obfuscation

On the Concept of Software Obfuscation in Computer Security	281
<i>Nikolay Kuzurin, Alexander Shokurov, Nikolay Varnovsky, and Vladimir Zakharov</i>	
Specifying Imperative Data Obfuscations	299
<i>Stephen Drape, Clark Thomborson, and Anirban Majumdar</i>	

Public-Key Cryptosystems

Token-Controlled Public Key Encryption in the Standard Model	315
<i>Sherman S.M. Chow</i>	

Trapdoor Permutation Polynomials of $\mathbb{Z}/n\mathbb{Z}$ and Public Key Cryptosystems	333
<i>Guilhem Castagnos and Damien Vergnaud</i>	
A Generalization and a Variant of Two Threshold Cryptosystems Based on Factoring	351
<i>Yvo Desmedt and Kaoru Kurosawa</i>	
Towards a DL-Based Additively Homomorphic Encryption Scheme	362
<i>Guilhem Castagnos and Benoît Chevallier-Mames</i>	
Elliptic Curves and Applications	
Differential Properties of Elliptic Curves and Blind Signatures	376
<i>Billy Bob Brumley and Kaisa Nyberg</i>	
Efficient Quintuple Formulas for Elliptic Curves and Efficient Scalar Multiplication Using Multibase Number Representation	390
<i>Pradeep Kumar Mishra and Vassil Dimitrov</i>	
Database Security and Privacy	
Enforcing Confidentiality in Relational Databases by Reducing Inference Control to Access Control	407
<i>Joachim Biskup and Jan-Hendrik Lochner</i>	
Efficient Negative Databases from Cryptographic Hash Functions	423
<i>George Danezis, Claudia Diaz, Sebastian Faust, Emilia Käsper, Carmela Troncoso, and Bart Preneel</i>	
Author Index	437