

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 of Computer Science, Saarbruecken, Germany

Anupam Datta (Ed.)

Advances in Computer Science – ASIAN 2009

Information Security and Privacy

13th Asian Computing Science Conference
Seoul, Korea, December 14-16, 2009
Proceedings

Volume Editor

Anupam Datta
Carnegie Mellon University
5000 Forbes Ave
Pittsburgh, PA 15213, USA
E-mail: danupam@cmu.edu

Library of Congress Control Number: 2009939838

CR Subject Classification (1998): F.3, E.3, D.4.6, K.6.5, C.2, D.2.4, J.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN	0302-9743
ISBN-10	3-642-10621-8 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-10621-7 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.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12801756 06/3180 5 4 3 2 1 0

Preface

This volume contains the papers presented at the 13th Annual Asian Computing Science Conference (ASIAN 2009) held in Seoul, South Korea, December 14-16, 2009. The theme of this year's conference was "Information Security and Privacy: Theory and Practice." The series of annual Asian Computing Science Conferences (ASIAN) was initiated in 1995 by AIT, INRIA and UNU/IIST to provide a forum for researchers in computer science from the Asian continent and to promote interaction with researchers in other regions. Accordingly, the conference moves every year to a different center of research throughout Asia. This year ASIAN was co-located with the 7th Asian Symposium on Programming Languages and Systems (APLAS 2009).

We received 45 submissions. Each submission was carefully reviewed by the Program Committee. The committee decided to accept seven regular papers and three short papers, which are included in the proceedings. The program also included two invited talks by Jean Goubault-Larrecq (LSV, ENS Cachan, CNRS, INRIA Saclay) and Naoki Kobayashi (Tohoku University); the corresponding papers are also included in this volume. I would like to thank the Program Committee members and external reviewers for their work in selecting the contributed papers. I would also like to thank the Steering Committee for their timely advice, in particular, Kazunori Ueda and Iliano Cervesato. Finally, I would like to thank the Local Arrangements Chair, Gyesik Lee, for ensuring that the conference proceeded smoothly.

September 2009

Anupam Datta

Conference Organization

Steering Committee

Iliano Cervesato
Philippe Codognet
Joxan Jaffar

Mitsu Okada
R.K. Shyamasundar
Kazunori Ueda

Program Chair

Anupam Datta

Program Committee

Michael Backes
Adam Barth
Lujo Bauer
Bruno Blanchet
Iliano Cervesato
Stephen Chong
Hubert Comon-Lundh
Veronique Cortier
Yuxi Fu
Vinod Ganapathy
Masami Hagiya

Dilsun Kaynar
Steve Kremer
Ralf Kuesters
Sanjiva Prasad
R. Ramanujam
Andre Scedrov
Vitaly Shmatikov
Kazunori UEDA
Bogdan Warinschi
Yuqing Zhang
Liang Zhenkai

Local Arrangements Chair

Gyesik Lee

External Reviewers

Attrapadung, Nuttapong
Bursztein, Elie
Cai, Xiaojuan
Chadha, Rohit
Fuchsbauer, Georg
Hanaoka, Goichiro
Jayadeva, Jayadeva
Kalra, Prem
Long, Yu

Mitra, Niloy
O'Neal, Adam
Ota, Kazuo
Pereira, Olivier
Qi, Zhengwei
Rial, Alfredo
Sans, Thierry
Sarkar, Palash
Shi, Elaine

VIII Organization

Shin, SeongHan

Suresh, S.P.

Truderung, Tomasz

Tschantz, Michael Carl

Tsukada, Yasuyuki

Tuengerthal, Max

Umeno, Shinya

Vergnaud, Damien

Vogt, Andreas

Yang, Liu

Ying, Mingsheng

Zhang, Rui

Zhao, Jianjun

Table of Contents

“Logic Wins!”	1
<i>Jean Goubault-Larrecq</i>	
Higher-Order Program Verification and Language-Based Security (Extended Abstract)	17
<i>Naoki Kobayashi</i>	
Deducibility Constraints	24
<i>Sergiu Bursuc, Hubert Comon-Lundh, and Stéphanie Delaune</i>	
Automated Security Proof for Symmetric Encryption Modes.....	39
<i>Martin Gagné, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini</i>	
Noninterference with Dynamic Security Domains and Policies.....	54
<i>Robert Grabowski and Lennart Beringer</i>	
A Critique of Some Chaotic-Map and Cellular Automata-Based Stream Ciphers	69
<i>Matt Henricksen</i>	
A Logic for Formal Verification of Quantum Programs	79
<i>Yoshihiko Kakutani</i>	
Reducing Equational Theories for the Decision of Static Equivalence ...	94
<i>Steve Kremer, Antoine Mercier, and Ralf Treinen</i>	
A Simulation-Based Treatment of Authenticated Message Exchange	109
<i>Klaas Ole Kürtz, Henning Schnoor, and Thomas Wilke</i>	
Trusted Deployment of Virtual Execution Environment in Grid Systems	124
<i>Deqing Zou, Jinjiu Long, and Hai Jin</i>	
A Dolev-Yao Model for Zero Knowledge	137
<i>Anguraj Baskar, R. Ramanujam, and S.P. Suresh</i>	
A Special Proxy Signature Scheme with Multi-warrant.....	147
<i>Jianhong Zhang, Hua Chen, Shengnan Gao, and Yixian Yang</i>	
Author Index	159