Lecture Notes in Computer Science 4318

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

Helger Lipmaa Moti Yung
Dongdai Lin (Eds.)

Information Security and Cryptology

Second SKLOIS Conference, Inscrypt 2006
Beijing, China, November 29 - December 1, 2006
Proceedings

Springer

Volume Editors

Helger Lipmaa
Adastral Postgraduate Campus
University College
London, UK
E-mail: h.lipmaa@cs.ucl.ac.uk

Moti Yung
Computer Science Department
Columbia University
New York, USA
E-mail: moti@cs.columbia.edu

Dongdai Lin
SKLOIS, Institute of Software
Chinese Academy of Sciences
Beijing 100080, China
E-mail: ddlin@is.iscas.ac.cn

Library of Congress Control Number: 2006936729

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-49608-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49608-3 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 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11937807 06/3142 5 4 3 2 1 0

Preface

The second SKLOIS Conference on Information Security and Cryptology 2006 (Inscrypt, formerly CISC) was organized by the State Key Laboratory of Information Security of the Chinese Academy of Sciences. This international conference was held in Beijing, China and was sponsored by the Institute of Software, the Chinese Academy of Sciences, the Graduate University of Chinese Academy of Sciences and the National Natural Science Foundations of China. The conference proceedings, with contributed papers, are published by Springer in this volume of *Lecture Notes in Computer Science* (LNCS).

The research areas covered by Inscrypt have been gaining increased visibility recently since modern computing and communication infrastructures and applications require increased security, trust and safety. Indeed important fundamental, experimental and applied work has been done in wide areas of cryptography and information security research in recent years. Accordingly, the program of Inscrypt 2006 covered numerous fields of research within these areas.

The International Program Committee of the conference received a total of 225 submissions, from which only 23 submissions were selected for presentation at the regular papers track and are part of this volume. In addition to this track, the conference also hosted a short paper track of 13 presentations that were carefully selected as well. All anonymous submissions were reviewed by experts in the relevant areas and based on their ranking, technical remarks and strict selection criteria the papers were selected to the various tracks.

Many people and organizations helped in making the conference a reality. We would like to take this opportunity to thank the Program Committee members and the external experts for their invaluable help in producing the conference program. We would like to further thank the conference Organizing Committee. Special thanks are due to Dongdai Lin for his excellent help in organizing the conference and the proceedings. We wish to thank the various sponsors and, last but not least, we also express our thanks to all the authors who submitted papers to the conference, the invited speakers, the session chairs and all the conference attendees.

November 2006 Helger Lipmaa and Moti Yung

Inscrypt (formerly CISC) 2006

2nd SKLOIS Conference on Information Security and Cryptology

Beijing, China November 29 - December 1, 2006

Sponsored and organized by

State Key Laboratory of Information Security
(Chinese Academy of Sciences)

General Chair

Dengguo Feng	SKLOIS, Chinese Academy of Sciences, China

Program Co-chairs

Helger Lipmaa	University College London, UK
Moti Yung	RSA Labs and Columbia University, USA

Program Committee

N. Asokan	Nokia, Finland
Catharina Candolin	SET-Security Oy, Finland
Kefei Chen	Shanhai Jiaotong University, China
Ee Chien Chang	NUS, Singapore
Debra Cook	Bell Labs, USA
Claudia Diaz	K.U. Leuven, Belgium
Orr Dunkelman	Technion, Israel
Nelly Fazio	IBM Almaden, USA
Kris Gaj	George Mason University, USA
Juan Garay	Bell Labs, USA
Minaxi Gupta	Indiana University, USA
Florian Hess	TU Berlin, Germany
Yupu Hu	Xidian University, China
Tetsu Iwata	Nagoya University, Japan
Aggelos Kiayias	University of Connecticut, USA
Kaoru Kurosawa	Ibaraki University, Japan
Peeter Laud	University of Tartu, Estonia
Benoit Libert	UCL, Belgium

Dongdai Lin	SKLOIS, China
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	Tsukuba University, Japan
Wenbo Mao	HP Shanghai, China
Steven Myers	Indiana University, USA
Lan Nguyen	WinMagic Inc., Canada
Hieu Phan	UCL, UK
Raphael Phan	Swinburne University of Technology, Malaysia
Markku-Juhani O. Saarinen	Royal Holloway, UK
Palash Sarkar	ISI, India
Nitesh Saxena	Polytechnic University, USA
Katja Schmidt-Samoa	TU Darmstadt, Germany
Berry Schoenmakers	Eindhoven University of Technology, Netherlands
Yiannis Stamatiou	CTI, Greece
Rainer Steinwandt	FAU, USA
Ivan Visconti	University of Salerno, Italy
Guilin Wang	I2R, Singapore
Huaxiong Wang	Macquarie University, Australia
Xiaoyun Wang	Tsinghua University, China
Yunlei Zhao	Fudan University, China

Proceedings Co-editors

Helger Lipmaa	University College London, UK
Moti Yung	RSA Labs and Columbia University, USA
Dongdai Lin	Chinese Academy of Sciences, China

Organizing Committee

Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Jiwu Jing	SKLOIS, Chinese Academy of Sciences, China
Chuankun Wu	SKLOIS, Chinese Academy of Sciences, China
Wenling Wu	SKLOIS, Chinese Academy of Sciences, China
Zhenfeng Zhang	SKLOIS, Chinese Academy of Sciences, China

Secretary and Treasurer

Yi Qin	Chinese Academy of Sciences, China

Table of Contents

Digital Signature Schemes

Sequences and Stream Ciphers

Symmetric-Key Cryptography

Cryptographic Schemes

Network Security

Access Control

Computer and Applications Security

Web and Media Security