Lecture Notes in Computer Science 5352

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
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

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

R. Sekar Arun K. Pujari (Eds.)

Information Systems Security

4th International Conference, ICISS 2008
Hyderabad, India, December 16-20, 2008
Proceedings

Springer

Volume Editors

R. Sekar
Stony Brook University, Department of Computer Science
Stony Brook, NY 11794-4400, USA
E-mail: sekar@cs.sunysb.edu

Arun K. Pujari
University of Hyderabad, Department of Computer and Information Sciences
Hyderabad 500 046, India
E-mail: akpcs@uohyd.ernet.in

Library of Congress Control Number: 2008940485

CR Subject Classification (1998): C.2, E.3, D.4.6, K.6.5, K.4.4, H.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-89861-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-89861-0 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 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12577231 06/3180 5 4 3 2 1 0

Preface

The 4th International Conference on Information System Security (ICISS 2007) was held December 16–20, 2008 at the Jawaharlal Nehru Technological University (JNTU) in Hyderabad, India. Although this conference is held in India, it is a decidedly international conference, attracting papers from all around the world. This year, there were 81 submissions from 18 different countries. The final program contained papers from Australia, Austria, France, Germany, India, Poland, UK, and USA.

From the 81 submissions, the Program Committee accepted 15 full papers, 4 short papers, and 2 ongoing research reports. The accepted papers span a wide range of topics, including access control, cryptography, forensics, formal methods and language-based security, intrusion detection, malware defense, network and Web security, operating system security, and privacy.

The conference featured four keynote talks, with written papers accompanying most of them. We would like to thank the speakers Somesh Jha, Basant Rajan, Amit Sahai, and Dawn Song for accepting our invitation to deliver keynote talks at this year's conference. The conference was preceded by two days of tutorials.

We would like to thank JNTU for hosting the conference, and EasyChair (http://www.easychair.org/) for providing conference management services to handle the paper review and selection process. Lastly, we wish to express our deepest thanks to the members of the Program Committee who give their personal free time to perform the often thankless job of reviewing many papers under extremely short deadlines, and to the external reviewers, volunteers and local assistants who made this program a success.

December 2008

R. Sekar
Arun Pujari

Organization

Advisory Committee Chair	Sushil Jajodia George Mason University, USA
Program Co-chairs	Arun K. Pujari LNM IIT, India R. Sekar Stony Brook University, USA
Submissions and Website Co-chairs	Alok Tongaonkar Stony Brook University, USA Subrat Kumar Dash University of Hyderabad, India
Tutorial Co-chairs	Vineet P. Nair University of Hyderabad, India V.N. Venkatakrishnan University of Illinois at Chicago, USA
Organizing Chair	G. Vijaya Kumari JNTU, Hyderabad, India
Finance Chair	P. Radha Krishnan Infosys, Hyderabad, India

Steering Committee

Sushil Jajodia	George Mason University, USA, Chair
Vijay Atluri	Rutgers University, USA
Aditya Bagchi	Indian Statistical Institute, India
A.K. Chakrabarti	Dept. of IT, Govt. of India
Prem Chand	Mahindra British Telecom, India
Shyam K. Gupta	IIT Delhi, India
Arun K. Majumdar	IIT Kharagpur, India
Chandan Mazumdar	Jadavpur University, Kolkata, India
Patrick McDaniel	Pennsylvania State University, USA
Arun K. Pujari	LNMITT Jaipur, India
Pierangela Samarati	University of Milan, Italy
R. Sekar	Stony Brook University, USA
N. Sitaram	CAIR, India
Vijay Varadharajan	Maquarie University, Australia
N. Vijayaditya	Controller of Certifying Authorities, India

Program Committee

Vijay Atluri	Rutgers University, USA
Aditya Bagchi	Indian Statistical Institute, India
Kevin Butler	Pennsylvania State University, USA
Chakravarthy Bhagvat	University of Hyderabad, India
Lorenzo Cavallaro	University of California, Santa Barbara, USA
Hao Chen	University of California, Davis, USA
Shuo Chen	Microsoft Research, Redmond, USA
Marc Dacier	Symantec Research Labs Europe
Saumya Debray	University of Arizona, USA
Subrat Kumar Dash	University of Hyderabad, India
Vinod Ganapathy	Rutgers University, USA
Jonathon Giffin	Georgia Institute of Technology, USA
S.K. Gupta	Indian Institute of Technology, Delhi, India
Sushil Jajodia	George Mason University, USA
Somesh Jha	University of Wisconsin, Madison, USA
Shrikant Ojha	DRDO, Government of India, India
Engin Kirda	Technical University Vienna, Austria
P. Radha Krishna	Infosys Technologies Ltd., Hyderabad, India
G. Vijaya Kumari	JNTU, Hyderabad, India
Zhenkai Liang	National University of Singapore, Singapore
Arun K. Majumdar	Indian Institute of Technology, Kharagpur, India
Anish Mathuria	DA-IICT, Gandhinagar, India
Chandan Mazumdar	Jadhavpur University, Kolkata, India
Nasir Memon	Polytechnic University, Brooklyn, USA
Peng Ning	North Carolina State University, USA
Atul Prakash	University of Michigan, USA
R. Ramanujam	Institute of Mathematical Sciences, Chennai, India
Sanjay Rawat	Infosys Technologies Ltd., India
Pierangela Samarati	University of Milan, Italy
Amitabh Saxena	University of Trento, Italy
Radu Sion	Stony Brook University, USA
Anil Somayaji	Carleton University, Canada
Robin Sommer	ICSI/LBNL, USA
Gaurav Tandon	Florida Institute of Technology, USA
Vijay Varadharajan	Maquarie University, Australia
V.N. Venkatakrishnan	University of Illinois at Chicago, USA
Poorvi Vora	George Washington University, USA
Xiaofeng Wang	Indiana University
Wei Xu	VMWare, Inc., USA

External Reviewers

Rajesh Asthana
Giuseppe Ateniese
A. Baskar
Sevinc Bayram
Kevin Borders
Liang Cai
Manik Lal Das
Anupam Datta
Saumya Debray
Ahmet Dirik
William Enck
Laura Falk
Matt Fredrickson
Romesh Kumar Gambhir
Sanchit Gupta
Francis Hsu
Ken Ingham
Bharat Lal Jangid
Dr. Shri Kant
Stefan Katzenbeisser
Corrado Leita
Zhuowei Li
Subhamoy Maitra
Mandar Mitra
Thomas Moyer
Divya Muthukumaran
Anandrabratha Pal
Van Hau Pham
Stefan Popoveniuc
Arun Pujari
C.R. Ramakrishnan
A.V. Sarad
Amitabh Saxena
A. Prasad Sistla
Scott Stoller
S.P. Suresh
Yagiz Sutcu
Olivier Thonnard
Umut Topkara
Gene Tsudik
Uday Tupakula
Matthias Vallentin
Matthew Van Gundy
Kaushik Veeraraghavan
Rui Wang
Komminist Weldemariam
Haizhi Xu

Table of Contents

Keynote Address

BitBlaze: A New Approach to Computer Security via Binary Analysis 1
Dawn Song, David Brumley, Heng Yin, Juan Caballero, Ivan Jager, Min Gyung Kang, Zhenkai Liang, James Newsome, Pongsin Poosankam, and Prateek Saxena

Languages and Formal Methods

On the Decidability of Model-Checking Information Flow Properties 26
Deepak D'Souza, Raveendra Holla, Janardhan Kulkarni, Raghavendra K. Ramesh, and Barbara Sprick

Synthesizing Enforcement Monitors wrt. the Safety-Progress Classification of Properties 41
Yliès Falcone, Jean-Claude Fernandez, and Laurent Mounier

Implicit Flows: Can't Live with 'Em, Can't Live without 'Em 56
Dave King, Boniface Hicks, Michael Hicks, and Trent Jaeger

Protocols

A Robust Reputation Scheme for Decentralized Group Management Systems 71
Frédéric Cuppens, Nora Cuppens-Boulahia, and Julien A. Thomas

Complexity of Checking Freshness of Cryptographic Protocols 86
Zhiyao Liang and Rakesh M. Verma

Secure Internet Voting Based on Paper Ballots 102
Łukasz Nitschke

Short Papers

A Secure Round-Based Timestamping Scheme with Absolute Timestamps 116
Duc-Phong Le, Alexis Bonnecaze, and Alban Gabillon

A Framework for Trustworthy Service-Oriented Computing 124
Sasikanth Avancha

Revisiting Bluetooth Security 132
Manik Lal Das and Ravi Mukkamala

A Verification Framework for Temporal RBAC with Role Hierarchy 140
Samrat Mondal and Shamik Sural

Keynote Address

Computing on Encrypted Data (Extended Abstract) 148
Amit Sahai

Ongoing Research

Identification of Cryptographically Strong and Weak Pseudorandom Bit Generators 154
Neelam Verma, Prasanna R. Mishra, and Gireesh Pandey

Proxy Re-signature Schemes 156
N.R. Sunitha and B.B. Amberker

Keynote Address

Fast Signature Matching Using Extended Finite Automaton (XFA) 158
R. Smith, C. Estan, S. Jha, and I. Siahaan

Intrusion Detection

Real-Time Alert Correlation with Type Graphs 173
Gianni Tedesco and Uwe Aickelin

Incorporation of Application Layer Protocol Syntax into Anomaly Detection 188
Patrick Düssel, Christian Gehl, Pavel Laskov, and Konrad Rieck

A Parallel Architecture for Stateful, High-Speed Intrusion Detection 203
Luca Foschini, Ashish V. Thapliyal, Lorenzo Cavallaro, Christopher Kruegel, and Giovanni Vigna

Biometrics, Forensics and Steganography

Indexing Multimodal Biometric Databases Using Kd-Tree with Feature Level Fusion 221
Umarani Jayaraman, Surya Prakash, and Phalguni Gupta

Audio Watermarking Based on Quantization in Wavelet Domain 235
Vivekananda Bhat K., Indranil Sengupta, and Abhijit Das

Overwriting Hard Drive Data: The Great Wiping Controversy 243
Craig Wright, Dave Kleiman, and Shyaam Sundhar R.S.

Practical Applications

Optimizing the Block Cipher and Modes of Operations Overhead at the Link Layer Security Framework in the Wireless Sensor Networks ... 258
Devesh Jinwala, Dhiren Patel, and Kankar Dasgupta

Privacy Management for Facebook 273
Enkh-Amgalan Baatarjav, Ram Dantu, and Santi Phithakkitnukoon

HyDRo – Hybrid Development of Roles 287
Ludwig Fuchs and Günther Pernul

Keynote Address

The Enlightened Era of Enterprise Security 303
Basant Rajan

Author Index 307