

*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 for Informatics, Saarbruecken, Germany*

Sushil Jajodia Chandan Mazumdar (Eds.)

# Information Systems Security

7th International Conference, ICISS 2011  
Kolkata, India, December 15-19, 2011  
Proceedings



Springer

## Volume Editors

Sushil Jajodia

George Mason University, Center for Secure Information Systems

4400 University Drive, Fairfax, VA 22030-4422, USA

E-mail: jajodia@gmu.edu

Chandan Mazumdar

Jadavpur University, Center for Distributed Computing

Kolkata 7000032, India

E-mail: chandan.mazumdar@gmail.com

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-25559-5

e-ISBN 978-3-642-25560-1

DOI 10.1007/978-3-642-25560-1

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011941662

CR Subject Classification (1998): C.2.0, C.2, E.3, H.3, D.4.6, K.6.5, K.4.4, H.2.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

# Foreword from the General Chairs

It was a great pleasure for us to organize the 7th International Conference on Information Systems Security Conference (ICISS) during December 15–19, 2011, at Jadavpur University, Kolkata, at the same venue where ICISS began its journey in 2005. The conference has been held every year since then at different cities in India, the last one (ICISS 2010) was successfully held at Gandhinagar, Gujrat. We are also happy that this year ICISS was held under the aegis of the newly formed Society for Research in Information Security and Privacy (SRISP), which aims to promote research and development in this arena. In the span of the last 7 years, ICISS has followed a strict reviewing policy and the acceptance ratio on average has been 25%. This year, out of 105 submissions, the Program Committee selected 20 full papers and 4 short papers for presentation.

The Program Chairs, Sushil Jajodia and Chandan Mazumdar, with the help of committed Program Committee members and reviewers did an excellent job in completing the review process well within the deadline. They were also able to arrange keynote talks by eminent researchers and practitioners in this field. We would like to record our appreciation to the Program Committee members for their painstaking effort in drawing up a high-quality technical program. We are indebted to David Evans, William Enck, Anupam Dutta and Vipul Goyal for accepting our invitation to deliver keynote talks. The Tutorial Chair, Sarmistha Neogy, had to work hard to come up with four tutorial sessions which were of great help for students and researchers to learn about topics of contemporary interest in the information security field. We would like to thank the tutorial speakers, Bjornan Solhaug, Amiya Bhattacharya, Sourav Sengupta and Rajat Subhra Chakraborty, for agreeing to share their experience.

The Organizing Committee, chaired by Mridul Sankar Barik and Sanjoy Kumar Saha, and the Finance Chair, Anirban Sengupta, worked tirelessly to ensure that the conference can be conducted without any glitch. The effort made by the Publicity Chairs, Claudio Agostino Ardagna and Anil K. Kaushik, in promoting the conference in the international forum is appreciated. We also take this opportunity to thank our sponsors and the Industry Chair, Kushal Banerjee, for their contributions.

December 2011

Arun Kumar Majumdar  
Aditya Bagchi

# Foreword from the Technical Program Chairs

This volume contains the papers selected for presentation at the 7th International Conference on Information Systems Security (ICISS 2011) held December 15–19, 2011 in Kolkata, India. Although ICISS was started 7 years ago as an initiative to promote information security-related research in India, from the very beginning it was decidedly an international conference attracting strong participation from researchers from all corners of the globe.

This volume contains four invited papers and 20 long and four short refereed papers that were presented at the conference. The refereed papers, which were selected from the 105 submissions, were rigorously reviewed by the Program Committee members. The resulting volume provides researchers with a broad perspective of recent developments in information systems security.

A special note of thanks goes to the many volunteers whose efforts made this conference a success. We wish to thank Anupam Datta, David Evans, Vipul Goyal, and William Enck for agreeing to deliver the invited talks, the authors for their worthy contributions, and the referees for their time and effort in reviewing the papers. We are grateful to Aditya Bagchi and Arun Majumdar for serving as the General Chairs.

Last, but certainly not least, our thanks go to the members of the Steering Committee on whom we frequently relied upon for advice throughout the year and to Jadavpur University, Kolkata, for hosting the conference.

Finally, this was the first year this conference was held under the aegis of the newly formed Society for Research in Information Security and Privacy (<http://www.srisp.org.in/>). This is a necessary step to ensure that information systems security research continues to expand in India and that this conference brings together the best in security research from all over the world.

December 2011

Sushil Jajodia  
Chandan Mazumdar

# Conference Organization

## Steering Committee

Sushil Jajodia (Chair)

Chandan Mazumdar

(Convener)

Aditya Bagchi

Somesh Jha

Arun Kumar Majumdar

Anish Mathuria

Atul Prakash

Gulshan Rai

George Mason University, USA

Jadavpur University, Kolkata, India

Indian Statistical Institute, Kolkata, India

University of Wisconsin, USA

IIT Kharagpur, India

DA-IICT, India

University of Michigan, USA

Department of Information Technology,

Govt. of India

Microsoft Research, India

University of Milan, Italy

SUNY, Stonybrook, USA

Sriram K. Rajamani

Pierangela Samarati

R. Sekar

## General Chair

A. K. Majumdar

Aditya Bagchi

IIT, Kharagpur, India

ISI, Kolkata, India

## Program Chair

Sushil Jajodia

Chandan Mazumdar

George Mason University, USA

Jadavpur University, India

## Organizing Chair

Mridul S. Barik

Sanjay Kumar Saha

Jadavpur University, India

Jadavpur University, India

## Publicity Chair

Claudio Agostino Ardagna

Anil K. Kaushik

University of Milan, Italy

Department of Information Technology,

Govt. of India

## Tutorial Chair

Sarmistha Neogy

Jadavpur University, India

## Finance Chair

Anirban Sengupta

Jadavpur University, India

## Industry Chair

Kushal Banerjee

TCS, Kolkata, India

## Program Committee

Anish Mathuria

DA-IICT, Gandhinagar, India

Atul Prakash

University of Michigan, Ann Arbor, USA

Bezawada Bruhadeshwar

IIIT, Hyderabad, India

Fabio Massacci

University of Trento, Italy

Frédéric Cuppens

ENST, France

Goutam Kumar Paul

Jadavpur University, India

Guenter Karjoth

IBM Zurich Research Laboratory, Switzerland

Indrajit Ray

Colorado State University, USA

Indrakshi Ray

Colorado State University, USA

Indranil Sengupta

IIT, Kharagpur, India

Javier Lopez

University of Malaga, Spain

Jonathan Giffin

Georgia Tech University, USA

Michiharu Kudo

IBM TRL, Japan

Mihai Christodorescu

IBM T.J. Watson Research Center, USA

Nasir Memon

Polytechnic University, USA

Patrick McDaniel

Penn State University USA

Pierangela Samarati

University of Milan, Italy

R. Ramanujam

Institute of Mathematical Sciences, India

R. Sekar

SUNY, Stony Brook, USA

S.K. Gupta

IIT, Delhi, India

Sabrina De Capitani

di Vimercati

University of Milan, Italy

Samiran Chattopadhyay

Jadavpur University, India

Shamik Sural

IIT, Kharagpur, India

Shankardas Roy

Howard University, USA

Sharad Mehrotra

UC Irvine, USA

Shishir Nagaraja

IIIT Delhi, India

Shiuh-Pyng Shieh

NCTU, Taiwan

Somesh Jha

University of Wisconsin, Madison, USA

Steve Barker

King's College London, UK

Subhomoy Maitra

ISI Kolkata, India

Subrat Kumar Dash

LNMIIT, India

Sukumar Nandi

IIT, Guwahati, India

V.N. Venkatakrishnan  
Vijay Atluri  
Vijay Varadharajan  
Yingjiu Li  
Zutao Zhu

University of Illinois, Chicago, USA  
Rutgers University , USA  
Macquarie University, Australia  
SMU, Singapore  
Google Inc., USA

## External Reviewers

Ardagna, Claudio  
Barik, Mridul Sankar  
Baskar, A.  
Bayram, Sevinc  
Bedi, Harkeerat Singh  
Bisht, Prithvi  
Chakraborty, Sandip  
Chakraborty, Suchetana  
Cuppens-Boulahia, Nora  
Davidson, Drew  
De Carli, Lorenzo  
Devriese, Dominique  
Doudalis, Stelios  
Fredrikson, Matthew  
Garcia-Alfaro, Joaquin  
Gheorghe, Gabriela  
Gkoulalas-Divanis, Aris  
Harris, William  
Hore, Bijit  
Hsu, Chia-Wei

Jarecki, Stanislaw  
Khadilkar, Vaibhav  
Konidala, Divyan  
Lai, Junzuo  
Li, Bing-Han  
Li, Liyun  
Luchaup, Daniel  
Oktay, Kerim  
Paci, Federica  
Pelizzi, Riccardo  
Saha, Sudip  
Saidane, Ayda  
Sengupta, Anirban  
Shi, Jie  
Suresh, S. P.  
Tupakula, Uday  
Vhaduri, Sudip  
Wang, Chia-Wei  
Weinmann, Ralf-Philipp



# Table of Contents

## Invited Papers

Understanding and Protecting Privacy: Formal Semantics and Principled Audit Mechanisms .....	1
<i>Anupam Datta, Jeremiah Blocki, Nicolas Christin, Henry DeYoung, Deepak Garg, Limin Jia, Dilsun Kaynar, and Arunesh Sinha</i>	
Efficient Secure Computation with Garbled Circuits .....	28
<i>Yan Huang, Chih-hao Shen, David Evans, Jonathan Katz, and Abhi Shelat</i>	
Defending Users against Smartphone Apps: Techniques and Future Directions .....	49
<i>William Enck</i>	
Secure Composition of Cryptographic Protocols .....	71
<i>Vipul Goyal</i>	

## Regular Papers

Flow Based Interpretation of Access Control: Detection of Illegal Information Flows .....	72
<i>Mathieu Jaume, Valérie Viet Triem Tong, and Ludovic Mé</i>	
Consistency Policies for Dynamic Information Systems with Declassification Flows .....	87
<i>Julien A. Thomas, Frédéric Cuppens, and Nora Cuppens-Boulahia</i>	
Authorization Policy Specification and Enforcement for Group-Centric Secure Information Sharing .....	102
<i>Ram Krishnan and Ravi Sandhu</i>	
Abductive Analysis of Administrative Policies in Rule-Based Access Control .....	116
<i>Puneet Gupta, Scott D. Stoller, and Zhongyuan Xu</i>	
Towards Detection of Botnet Communication through Social Media by Monitoring User Activity .....	131
<i>Pieter Burghouwt, Marcel Spruit, and Henk Sips</i>	
Finding Non-trivial Malware Naming Inconsistencies .....	144
<i>Federico Maggi, Andrea Bellini, Guido Salvaneschi, and Stefano Zanero</i>	

Taint-Enhanced Anomaly Detection . . . . .	160
<i>Lorenzo Cavallaro and R. Sekar</i>	
Secured Cloud Storage Scheme Using ECC Based Key Management in User Hierarchy . . . . .	175
<i>Atanu Basu, Indranil Sengupta, and Jamuna Kanta Sing</i>	
Reversible Image Watermarking through Coordinate Logic Operation Based Prediction . . . . .	190
<i>Ruchira Naskar and Rajat Subhra Chakraborty</i>	
Some Combinatorial Results towards State Recovery Attack on RC4 . . .	204
<i>Apurba Das, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar</i>	
Distributed Signcryption from Pairings . . . . .	215
<i>Indivar Gupta and P.K. Saxena</i>	
Formal Privacy Analysis of Communication Protocols for Identity Management . . . . .	235
<i>Meilof Veeningen, Benne de Weger, and Nicola Zannone</i>	
Load Time Security Verification . . . . .	250
<i>Olga Gadyatskaya, Eduardo Lostal, and Fabio Massacci</i>	
Preserving Location Privacy for Continuous Queries on Known Route . . . . .	265
<i>Anuj S. Saxena, Mayank Pundir, Vikram Goyal, and Debajyoti Bera</i>	
A Data Mining Framework for Securing 3G Core Network from GTP Fuzzing Attacks . . . . .	280
<i>Faraz Ahmed, M. Zubair Rafique, and Muhammad Abulaish</i>	
An Efficient Decentralized Rekeying Scheme to Secure Hierarchical Geographic Multicast Routing in Wireless Sensor Networks . . . . .	294
<i>Prithu Banerjee, Mahasweta Mitra, Ferdous A. Barbhuiya, Sandip Chakraborty, and Sukumar Nandi</i>	
SecWEM: A Security Solution for Web Based E-mail . . . . .	309
<i>Ravi Shankar Yadav, Praveen Likhar, and M. Keshava Rao</i>	
A Multilayer Overlay Network Architecture for Enhancing IP Services Availability against DoS . . . . .	322
<i>Dimitris Geneiatakis, Georgios Portokalidis, and Angelos D. Keromytis</i>	
Mitigation of Malicious Modifications by Insiders in Databases . . . . .	337
<i>Harini Ragavan and Brajendra Panda</i>	
A Semantic Hierarchy for Erasure Policies . . . . .	352
<i>Filippo Del Tedesco, Sebastian Hunt, and David Sands</i>	

## Short Papers

A Universal Semantic Bridge for Virtual Machine Introspection . . . . .	370
<i>Christian Schneider, Jonas Pföh, and Claudia Eckert</i>	
A Signature-Based Approach of Correctness Assurance in Data Outsourcing Scenarios . . . . .	374
<i>Morteza Noferesti, Mohammad Ali Hadavi, and Rasool Jalili</i>	
Towards Access Control Model Engineering . . . . .	379
<i>Winfried E. Kühnhauser and Anja Pölck</i>	
IFrandbox - Client Side Protection from Malicious Injected Iframes . . . . .	383
<i>Tanusha S. Nadkarni, Radhesh Mohandas, and Alwyn R. Pais</i>	
<b>Author Index</b> . . . . .	387