

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

Somesh Jha Anish Mathuria (Eds.)

Information Systems Security

6th International Conference, ICISS 2010
Gandhinagar, India, December 17-19, 2010
Proceedings



Springer

Volume Editors

Somesh Jha
University of Wisconsin
Computer Sciences Department
Madison, WI 53706, USA
E-mail: jha@cs.wisc.edu

Anish Mathuria
Dhirubhai Ambani Institute of Information
and Communication Technology
Gandhinagar 382007, Gujarat, India
E-mail: anish_mathuria@daiict.ac.in

Library of Congress Control Number: 2010940624

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-17713-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-17713-2 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 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Message from the General Chairs

It is our pleasure to welcome you to the proceedings of the 6th International Conference on Information Systems Security. ICISS was first held in 2005 in Kolkata, and has been successfully organized every year in different parts of India. Even within a short span of its life, the conference has left its mark in the field of information systems security.

There is a long list of people who have volunteered their time and energy to put together this conference and who deserve acknowledgement. Our thanks go to the Program Chairs, Somesh Jha and Anish Mathuria, along with the Program Committee members for an excellent job in completing a rigorous review process and selecting outstanding papers for presentation at the conference. We would also like to thank Jonathan Giffin, Andrew Myers, Sriram Rajamani, and V.N. Venkatakrisnan for accepting our invitation to deliver invited keynote talks at the conference. The effort made by the Tutorial Chair, Rakesh Verma, in selecting tutorial sessions on topics of contemporary interest in this field deserves special mention. We would also like to thank the Tutorial Speakers who kindly agreed to deliver their lectures.

We hope that you will find the proceedings of ICISS 2010 stimulating and a source of inspiration for future research.

December 2010

Sushil Jajodia
S.C. Sahasrabudhe

Message from the Technical Program Chairs

This volume contains the papers selected for presentation at the 6th International Conference on Information Systems Security (ICISS 2010) held during December 17–19, 2010 in Gandhinagar, India. ICISS is part of an effort started five years ago as an initiative to promote information security-related research in India. Held annually it now attracts strong participation from the international research community.

This year we received 51 papers from 19 countries all over the world. After a rigorous review process, the Program Committee selected 14 papers for presentation. Each paper was reviewed by at least three Program Committee members. All the Program Committee members discussed the reviews during a two-week on-line discussion phase. We would like to thank the authors of all the papers for submitting their quality research work to the conference. Our special thanks go to the Program Committee members and the external for sparing their time in carrying out the review process meticulously.

We were fortunate to have four eminent experts as invited keynote speakers. Their lectures provided fertile ground for stimulating discussions at the conference. As in previous years, the main conference was preceded by two days of tutorial presentations. We would like to thank the Tutorial Chair, Rakesh Verma, for arranging an excellent tutorial program. We would also like to thank the speakers who agreed to deliver tutorial lectures: Agostino Cortesi, Rop Gonggrijp, J. Alex Halderman, Alexander Malkis, Hari Prasad, Amitabh Saxena, and Poorvi Vora.

We would like to thank the General Chairs, Sushil Jajodia and S.C. Sahasrabudhe, members of the Steering Committee and previous PC Chair, Atul Prakash, on whom we frequently relied upon for advice throughout the year. We would also like to thank Drew Davidson for maintaining the conference website.

Finally, we would like to thank the conference publisher Springer for their co-operation. We hope that you will find the papers in this volume technically rewarding.

December 2010

Somesh Jha
Anish Mathuria

Conference Organization

Program Chairs

Somesh Jha
Anish Mathuria

University of Wisconsin, USA
DA-IICT, India

Program Committee

Claudio Agostino Ardagna
Bezawada Bruhadeshwar
Mihai Christodorescu
Cas Cremers
Naranker Dulay
Debin Gao
Jon Giffin
Sushil Jajodia
Gunter Karjoth
Zhenkai Liang
Javier Lopez
Keith Martin
Debdeep Mukhopadhyay
Srijith K. Nair
Karthik Pattabiraman
Gunther Pernul
Atul Prakash
Kouichi Sakurai
Nitesh Saxena

University of Milan, Italy
IIIT-Hyderabad, India
IBM T.J. Watson Research Center, USA
ETH Zurich, Switzerland
Imperial College London, UK
Singapore Management University, Singapore
Georgia Institute of Technology, USA
George Mason University, USA
IBM Zurich Research Laboratory, Switzerland
National University of Singapore, Singapore
University of Malaga, Spain
Royal Holloway University of London, UK
IIT-Kharagpur, India
British Telecom, UK
University of British Columbia, Canada
University of Regensburg, Germany
University of Michigan Ann Arbor, USA
Kyushu University, Japan
Polytechnic Institute of New York University,
USA

R. Sekar
Shamik Sural
S.P. Suresh
Vipin Swarup
Patrick Traynor
Venkat Venkatakrishnan
Rakesh Verma
Poorvi Vora
Guilin Wang

SUNY Stony Brook, USA
IIT-Kharagpur, India
Chennai Mathematical Institute, India
MITRE, USA
Georgia Institute of Technology, USA
University of Illinois Chicago, USA
University of Houston, USA
George Washington University, USA
University of Birmingham, UK

General Chairs

Sushil Jajodia George Mason University, USA
S.C. Sahasrabudhe DA-IICT, India

Tutorial Chairs

Chandan Mazumdar Jadavpur University, India
Rakesh Verma University of Houston, USA

Publicity Chair

Claudio Agostino Ardagna University of Milan, Italy

Finance Chair

Manik Lal Das DA-IICT, India

Steering Committee

Sushil Jajodia (Chair) George Mason University, USA
Aditya Bagchi Indian Statistical Institute, India
Somesh Jha University of Wisconsin, USA
Gargi Keeni Tata Consultancy Services, India
A.K. Majumdar IIT Kharagpur, India
Chandan Mazumdar Jadavpur University, India
Atul Prakash University of Michigan Ann Arbor, USA
Pierangela Samarati University of Milan, Italy
R. Sekar SUNY Stony Brook, USA
A.K. Kaushik Ministry of Communications and IT, Govt. of
India
Gulshan Rai Department of Information Technology, Govt.
of India

External Reviewers

A. Baskar
Abhijit Das
Adam Young
Andreas Reisser
Bailey Basile
Cheng-Kang Chu
Chester Rebeiro
Christian Broser
Christoph Fritsch
Chunhua Su
David Keppler
Isaac Agudo
Jingyu Hua
Jonathan Voris
Krishnaprasad Thirunarayan
Liang Zhao
Ludwig Fuchs
Mario Frank

Moritz Riesner
Oliver Gmelch
Pablo Najera
Qi Xie
Rajat Subhra Chakraborty
Rehana Yasmin
Rodrigo Roman
Ruben Rios
Sai Teja Peddinti
Shengdong Zhao
Shinsaku Kiyomoto
Stephanie Wehner
Steven Gianvecchio
Tzipora Halevi
Yanjiang Yang
Yizhi Ren
Yoshiaki Hori

Table of Contents

Invited Talks

Analyzing Explicit Information Flow	1
<i>Sriram K. Rajamani</i>	
WebAppArmor: A Framework for Robust Prevention of Attacks on Web Applications (Invited Paper)	3
<i>V.N. Venkatakrishnan, Prithvi Bisht, Mike Ter Louw, Michelle Zhou, Kalpana Gondi, and Karthik Thotta Ganesh</i>	
Toward Securely Programming the Internet	27
<i>Andrew C. Myers</i>	
Attribution of Malicious Behavior	28
<i>Jonathon Giffin and Abhinav Srivastava</i>	

Integrity and Verifiability

Unifying Facets of Information Integrity	48
<i>Arnar Birgisson, Alejandro Russo, and Andrei Sabelfeld</i>	
Determining the Integrity of Application Binaries on Unsecure Legacy Machines Using Software Based Remote Attestation	66
<i>Raghunathan Srinivasan, Partha Dasgupta, Tushar Gohad, and Amiya Bhattacharya</i>	
Stamp-It: A Method for Enhancing the Universal Verifiability of E2E Voting Systems	81
<i>Mridul Nandi, Stefan Popoveniuc, and Poorvi L. Vora</i>	

Web and Data Security

Strengthening XSRF Defenses for Legacy Web Applications Using Whitebox Analysis and Transformation	96
<i>Michelle Zhou, Prithvi Bisht, and V.N. Venkatakrishnan</i>	
Coverage Criteria for Automatic Security Testing of Web Applications	111
<i>Thanh Binh Dao and Etsuya Shibayama</i>	
A Practical Generic Privacy Language	125
<i>Moritz Y. Becker, Alexander Malkis, and Laurent Bussard</i>	

Efficient Detection of the Return-Oriented Programming Malicious Code	140
<i>Ping Chen, Xiao Xing, Hao Han, Bing Mao, and Li Xie</i>	
ValueGuard: Protection of Native Applications against Data-Only Buffer Overflows	156
<i>Steven Van Acker, Nick Nikiforakis, Pieter Philippaerts, Yves Younan, and Frank Piessens</i>	
Access Control and Auditing	
Mining RBAC Roles under Cardinality Constraint	171
<i>Ravi Kumar, Shamik Sural, and Arobinda Gupta</i>	
Specification of History Based Constraints for Access Control in Conceptual Level	186
<i>Fathiyeh Faghieh, Morteza Amini, and Rasool Jalili</i>	
Abstracting Audit Data for Lightweight Intrusion Detection	201
<i>Wei Wang, Xiangliang Zhang, and Georgios Pitsilis</i>	
System Security	
A Persistent Public Watermarking of Relational Databases	216
<i>Raju Halder and Agostino Cortesi</i>	
Security Rules <i>versus</i> Security Properties	231
<i>Mathieu Jaume</i>	
Protecting and Restraining the Third Party in RFID-Enabled 3PL Supply Chains	246
<i>Shaoying Cai, Chunhua Su, Yingjiu Li, Robert Deng, and Tieyan Li</i>	
Author Index	261