Lecture Notes in Computer Science 4812

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Patrick McDaniel Shyam K. Gupta (Eds.)

Information Systems Security

Third International Conference, ICISS 2007
Delhi, India, December 16-20, 2007
Proceedings

Springer

Volume Editors

Patrick McDaniel
The Pennsylvania State University
360A IST/CSE Building, University Park, PA 16802, USA
E-mail: mcdaniel@cse.psu.edu

Shyam K. Gupta
Indian Institute of Technology Hauz Khas
Department of Computer Science and Engineering
New Delhi, 11016, India
E-mail: skg@cse.iitd.ernet.in

Library of Congress Control Number: 2007940398

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77085-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77085-5 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12199075 06/3180 5 4 3 2 1 0

Preface

The 3rd International Conference on Information System Security (ICISS 2007) was held from December 16–20, 2007 at the University of Delhi in Delhi, India. The conference was the third in the successful series of technical meetings of peer-reviewed research in information security hosted by Indian institutions. While held in India, the conference had a decidedly international flavor. This year's conference garnered submissions from all corners of the globe–the final program contains papers from the United States, India, China, Korea, Germany, France, Japan, Iran, and Italy. Support within the Indian academic community was also quite visible. The program included talks from a broad range of institutions spanning nearly the entirety of the Indian subcontinent. The broad demographic illustrated the truly exceptional growth of this relatively young conference.

This year's program contains 18 full papers, 5 short papers, and 4 keynote talk papers. The 78 papers submitted to the conference were as diverse as their authors. The submitted topics in cryptography, intrusion detection, network security, information flow systems, Web security, and many others offered a detailed view of the state of the art in information security. There were many more scientifically strong papers than could reasonably be accepted. This left the committee with a number of tough choices, but ultimately led to the technically strong and engaging program presented within these pages.

We are particularly grateful to Atul Prakash, Yves Deswarte, Sabrina de Capitani di Vimercati, and Kotagiri Rao for accepting our invitation to deliver invited talks at this year's conference. The conference was preceded by four tutorials held over the two days preceding the peer-reviewed technical content. We wish to thank the University of Delhi for providing the space to hold the conference.

We would like to acknowledge the exceptional effort by Kevin Butler in maintaining the website, marshaling the papers, and working with local organizers. He was essential to the success of this conference.

Lastly, we wish to express our deepest thanks to the members of the Program Committee, who gave their personal free time to perform the often thankless job of reviewing many papers under extremely short deadlines, and to the volunteers and local assistants who made this program a success.

December 2007

Patrick McDaniel
Shyam K. Gupta
Program Chairs

Organization

Patron	Deepak Pental Vice-Chancellor, University of Delhi, India
General Chair	N. Vijayaditya Controller of Certifying Authorities, India
Advisory Committee Chair	N. Vijayaditya Controller of Certifying Authorities, India
Program Co-chairs	Shyam K. Gupta IIT Delhi, India
	Patrick McDaniel Pennsylvania State University, USA
Submissions and Website Chair	Kevin Butler Pennsylvania State University,USA
Invited Talks Chair	Indrakshi Ray Colorado State University, USA
Tutorial Co-chairs	Vijay Atluri Rutgers University, USA
	Arun K. Pujari University of Hyderabad, India
Panel Chair	Rattan K. Datta SBBSIET, Jallandhar, India
Organizing Chair	Punam Bedi University of Delhi, India
Publicity Chairs	Chandan Majumdar Jadavpur University, India
	Marina Blanton University of Notre Dame, USA
Finance Chair	Shri Kant DRDO, India
Sponsorship Chair	Anuj Khare Appin Systems, India
Registration Co-chairs	Neelima Gupta University of Delhi, India
	Sameep Mehta IBM IRL, India
	D.V.L.N. Somayajulu NIT Warangal, 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	SUNY Stony Brook, USA
N. Sitaram	CAIR, India
Vijay Varadharajan	Macquarie University, Australia
N. Vijayaditya	Controller of Certifying Authorities, India

Program Committee

R.K. Agrawal	Jawaharlal University, India
Raj Bhatnagar	University of Cincinnati, USA
Vasudha Bhatnagar	University of Delhi, India
Joachim Biskup	University of Dortmund, Germany
Kevin Butler	Pennsylvania State University, USA
William Enck	Pennsylvania State University, USA
Deborah Frincke	Pacific Northwest National Laboratory, USA
Somnath Ghosh	University of Latrobe, Australia
Jonathan Giffin	Georgia Tech University, USA
Shantanu Godbole	IBM IRL, India
Qijun Gu	Texas State University, USA
Patrick C.K. Hung	University of Ontario Institute of Technology, Canada
Sushil Jajodia	George Mason University, USA
Karin Kalling	IBM Almaden Research Center, USA
Shri Kant	DRDO Delhi, India
Kamal Karlapalem	IIIT Hyderabad, India
Jun Li	University of Oregon, USA
Arun K. Majumdar	IIT Kharagpur, India
Chandan Mazumdar	University of Jadhavpur, India
Nasir Memon	Polytechnic University, USA
Ravi Mukkamala	Old Dominion University, USA
Lukasz Opyrchal	Miami University of Ohio, USA
Brajendra Panda	University of Arkansas, USA
Arun Pujari	University of Hyderabad, India

P. Radha Krishna	IDRBT Hyderabad, India
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
R. Sekar	SUNY Stony Brook, USA
Sumit Sarkar	University of Texas-Dallas, USA
S. Sudarshan	IIT Bombay, India
Jaideep Vaidya	Rutgers University, USA
Alec Yasinsac	Florida State University, USA

Advisory Committee

R.K. Arora	Ex-Professor, IIT Delhi, India
Rattan K. Datta	SBBSIET, Jallandhar, India
B.N. Jain	IIT Delhi, India
J.P. Gupta	JPIT, Noida, India
M.L. Goyal	CMC, New Delhi, India
Mukesh Mohania	IBM IRL, India
Y.K. Sharma	NIC, India
S.W. Wason	Jamia Milia University, India

Local Arrangments Committee

R.K. Agrawal	JNU Delhi, India
Abhay Bansal	ITS Gaziabad, India
M.P.S. Bhatia	NSIT Delhi, India
Vasudha Bhatnagar	University of Delhi, India
Anjana Choudhary	NIC, India
Sanjay Goel	JIIT, Noida, India
Anand Gupta	NSIT, Delhi, India
Neelima Gupta	University of Delhi, India
Rakesh Gupta	NIC, India
P.K. Hazra	University of Delhi, India
M.N. Hoda	Bharti Vidyapeeth, Delhi, India
Anil K. Kaushik	MCIT, Delhi, India
Rajeev Kumar	DCE, Delhi, India
Shobhit Mahajan	University of Delhi, India
Manohar Lal	IGNOU, Delhi, India
V. Kulkarni	University of Delhi, India
Rajeev Kumar	DCE, Delhi, India
S.K. Muttoo	University of Delhi, India
B.G. Prasad	EPCET, Bangalore, India
Sangeeta Sabharwal	NSIT, Delhi, India
Gaurav Saxena	Hans Raj College, Delhi, India
Neeraj Sharma	RLA College, Delhi, India

V.K. Singh	MSIT, Delhi, India
D.V.L.N. Somayajulu	NIT, Warangal, India
R.K. Vyas	University of Delhi, India

Sponsoring Institutions

University of Delhi, India
Center for Secure Information Systems, George Mason University, USA
Systems and Information Infrastructure Security Laboratory, Pennsylvania State University, USA

Table of Contents

Keynote Address

Network Security

Cryptography

Architectures and Systems

Cryptanalysis

Keynote Talk

Protocols

Keynote Talk

Short Papers

Detection and Recognition