Lecture Notes in Computer Science 7671

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

Venkat Venkatakrishnan
Diganta Goswami (Eds.)

Information Systems Security

8th International Conference, ICISS 2012
Guwahati, India, December 15-19, 2012
Proceedings

Springer

Volume Editors

Venkat Venkatakrishnan
University of Illinois at Chicago
Department of Computer Science
Chicago, IL 60607-7053, USA
E-mail: venkat@cs.uic.edu

Diganta Goswami
Indian Institute of Technology
Department of Computer Science and Engineering
Guwahati 781039, Assam, India
E-mail: dgoswami@iitg.ernet.in

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-35129-7 e-ISBN 978-3-642-35130-3
DOI 10.1007/978-3-642-35130-3
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012952156

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 2012
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)

Message from the General Chairs

Welcome to the Eighth International Conference on Information Systems Security (ICISS 2012), organized by the Indian Institute of Technology Guwahati under the aegis of the Society for Research in Information Security and Privacy (SRISP). Over the years, this conference has blossomed into an internationally renowned forum for interaction among representatives from academia and industry. Through technical sessions, tutorials, and invited talks, it aims to bring together participants wishing to present their latest thoughts and technologies.

The conference has been able to attract high profile invited speakers. This year we are fortunate to have Dr. Christopher Kruegel, the Eugene Aas Chair in Computer Science, Computer Science Department, University of California at Santa Barbara; Dr. Prasad Naldurg, Microsoft Research; and Dr. Lenore Zuck, Department of Computer Science, University of Illinois at Chicago.

A conference of this magnitude is the result of the tremendous collective effort of various chairs. With the help of the program committee members, the program co-chairs, Diganta Goswami and Venkat Venkatakrishnan, have produced a truly outstanding technical program. The tutorial co-chairs, Rajan Shankaran and Arijit Sur, have arranged six half-day tutorials by leading experts. ICISS also provides a platform for students and research scholars working in all areas of computer science and engineering, and communication and information technologies, to present their on-going research works and interact with peers. The student forum chair, Partha Sarathi Mandal, has done an excellent job in reviewing and selecting a good collection of student papers for presentation at this forum.

The publicity chairs, Shamik Sural, Claudio A. Ardagna, and Aryabartta Sahu, did a fantastic job in widely publicizing this conference. The publication chair, Samit Bhattacharya, was instrumental in putting together the proceedings and ensuring their high quality. Thanks are also due to the finance chair, Sanasam Ranbir Singh, for assuming the good financial health of the conference. Finally, our sincere thanks to the organizing co-chairs, J.K. Deka, Santosh Biswas, and their team, for their smooth management of the conference.

We are grateful to the Indian Institute of Technology Guwahati for extending logistics support. The steering-committee members, Gautam Barua, Chandan Mazumdar, Aditya Bagchi, Somesh Jha, Arun Kumar Majumdar, Anish Mathuria, Atul Prakash, Gulshan Rai, Sriram K. Rajamani, Pierangela Samarati, and Sushil Jajodia, provided the committee members with invaluable help, guidance, and support.

Last but not the least, we wish to sincerely thank all the authors, reviewers, program committee members, and participants for their continued support and

commitment to the success of this technical meeting. Once again, on behalf of the conference committee, we welcome you all to Guwahati, the Gateway to North-East India! We wish you a very pleasant stay in this beautiful city and hope you will find the ICISS 2012 experience a memorable one.

October 2012

Sukumar Nandi
R. Sekar

Message from the PC Chairs

This volume contains the papers selected for presentation at the Eighth International Conference on Information Systems Security (ICISS 2012) held during December 15–19, 2012 in Guwahati, India. ICISS is part of an effort to promote information security and privacy research in India. From its humble beginnings, it has grown to a conference of international repute with participation from several countries.

This year we received 72 submissions from 17 countries across the globe. Each submission was reviewed by about three program committee members. After a rigorous review process, the committee decided to accept 18 full-length papers and 3 short papers. Our special thanks goes to the program committee members and other external reviewers who generously offered their expertise and time to create the final program for the conference. We are also fortunate to have three invited talks from leading experts in the field of information security and privacy.

We thank the Steering Committee, and in particular Prof. Sushil Jajodia, whose counsel we frequently relied on. Profs. R. Sekar and Sukumar Nandi were of great assistance in matters related to conference organization.

We hope you will find the papers in this collection stimulating and rewarding.

December 2012

Venkat Venkatakrishnan
Diganta Goswami

Organizing Committee

General Co-chairs

R. Sekar	SUNY, Stonybrook, USA
Sukumar Nandi	IIT Guwahati, India

Program Co-chairs

Venkat Venkatakrishnan	University of Illinois, USA
Diganta Goswami	IIT Guwahati, India

Organizing Co-chairs

Jatindra Kumar Deka	IIT Guwahati, India
Santosh Biswas	IIT Guwahati, India

Publication Chair

Samit Bhattacharya	IIT Guwahati, India

Publicity Co-chairs

Shamik Sural	IIT Kharagpur, India
Claudio A. Ardagna	Università degli Studi di Milano, Italy
Aryabartta Sahu	IIT Guwahati, India

Tutorial Co-chairs

Rajan Shankaran	Macquarie University, Australia
Arijit Sur	IIT Guwahati, India

Finance Chair

Sanasam Ranbir Singh	IIT Guwahati, India

Students Forum Chair

Partha Sarathi Mandal	IIT Guwahati, IIndia

Steering Committee

Gautam Barua	IIT Guwahati, India
Chandan Mazumdar	Jadavpur University, India
Aditya Bagchi	ISI, Calcutta, India
Somesh Jha	University of Wisconsin, USA
Arun Kumar Majumdar	IIT Kharagpur, India
Anish Mathuria	DA-IICT, India
Atul Prakash	University of Michigan, USA
Gulshan Rai	DIT, Govt. of India, India
Sriram K. Rajamani	Microsoft Research, India
Pierangela Samarati	University of Milan, Italy
Sushil Jajodia	George Mason University, USA

Program Committee

Bruhadeshwar Bezawada	International Institute of Information Technology, Hyderabad, India
Sandeep Bhatkar	Symantec Research Labs, USA
Prithvi Bisht	University of Illinois at Chicago, USA
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Sanjit Chatterjee	Indian Institute of Science, India
Frédéric Cuppens	TELECOM Bretagne, France
Ashok Kumar Das	International Institute of Information Technology, Hyderabad, India
Anupam Datta	Carnegie Mellon University, USA
Meenakshi Dsouza	International Institute of Information Technology, Bangalore, India
William Enck	North Carolina State University, USA
Vinod Ganapathy	Rutgers University, USA
Diganta Goswami	Indian Institute of Technology, Guwahati, India (Co-chair)
Kevin Hamlen	University of Texas at Dallas, USA
Sebastian Hunt	City University, London, UK
Sushil Jajodia	George Mason University, USA
Somesh Jha	University of Wisconsin, USA
Aditya Kanade	Indian Institute of Science, Bangalore, India
Ram Krishnan	University of Texas at San Antonio, USA
Zhichun Li	NEC Laboratories America, USA
Zhenkai Liang	National University of Singapore, Singapore
Anish Mathuria	Dhirubhai Ambani Institute of Information and Communication Technology, India
Phu H. Phung	Chalmers Univ. of Technology, Sweden
Indranil Sengupta	Indian Institute of Technology, Kharagpur, India
Kapil Singh	IBM T.J. Watson Research Center, USA

Scott Stoller	Stony Brook University, USA
Mike Ter-Louw	LGS Innovations, USA
Alok Tongaonkar	Stony Brook University, USA
Mahesh Tripunitara	The University of Waterloo, Canada
Venkat Venkatakrishnan	University of Illinois at Chicago, USA (Co-chair)
Vinod Yegneswaran	SRI International, USA
Stefano Zanero	Politecnico di Milano, Italy

Additional Reviewers

Albanese, Massimiliano
Barenghi, Alessandro
Chabanne, Hervé
Chakraborty, Debrup
Davidson, Drew
De Benedictis, Alessandra
De Carli, Lorenzo
Fredrikson, Matt
Harris, William
Jayaraman, Karthick
Kamath, Chethan
Kumar, Vikas
Le, Meixing
Luchaup, Daniel
Mao, Jian
Qian, Zhiyun
Sisto, Alessandro
Sun, Kun
Thomson, Susan
Tschantz, Michael Carl
V N, Muralidhara
Vora, Poorvi
Wu, Zhenyu
Zhang, Lei

Table of Contents

Invited Talk I

Fighting Malicious Software 1
Christopher Kruegel

Technical Session I: Software Security

VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security 16
Chaitrali Amrutkar, Kapil Singh, Arunabh Verma, and Patrick Traynor

Security Assessment of Node.js Platform 35
Andres Ojamaa and Karl Düüna

Invited Talk II

Foundations of Dynamic Access Control 44
Prasad Naldurg

Technical Session II: Access Control

Risk-Aware RBAC Sessions 59
Khalid Zaman Bijon, Ram Krishnan, and Ravi Sandhu

A Cognitive Trust Model for Access Control Framework in MANET 75
Soumya Maity and Soumya K. Ghosh

TRUST-ORBAC: A Trust Access Control Model in Multi-Organization Environments 89
Khalifa Toumi, César Andrés, and Ana Cavalli

Invited Talk III

On Policies and Intents 104
Matthew L. Bolton, Celeste M. Wallace, and Lenore D. Zuck

Technical Session III: Covert Communications

ProtoLeaks: A Reliable and Protocol-Independent Network Covert Channel 119
Arne Swinnen, Raoul Strackx, Pieter Philippaerts, and Frank Piessens

Keyless Steganography in Spatial Domain Using *Energetic* Pixels 134
Goutam Paul, Ian Davidson, Imon Mukherjee, and S.S. Ravi

Fuzzy Inference Rule Based Reversible Watermarking for Digital Images 149
Ruchira Naskar and Rajat Subhra Chakraborty

Technical Session IV: Network Security I

Secure Trust Metadata Management for Mobile Ad-Hoc Networks 164
Vivek Natarajan, Yi Yang, and Sencun Zhu

Defence against Wormhole Attacks in Wireless Mesh Networks 181
Rakesh Matam and Somanath Tripathy

A Novel Key Update Protocol in Mobile Sensor Networks 194
Sarita Agrawal, Rodrigo Roman, Manik Lal Das, Anish Mathuria, and Javier Lopez

Autonomous Certification with List-Based Revocation for Secure V2V Communication 208
Anup Kumar Bhattacharya, Abhijit Das, Dipanwita Roychoudhury, Aravind Iyer, and Debojyoti Bhattacharya

Technical Session V: Database and Distributed Systems Security

Mitigating Insider Threat on Database Integrity 223
Weihan Li, Brajendra Panda, and Qussai Yaseen

Coercion Resistant MIX for Electronic Auction 238
Jaydeep Howlader, Jayanta Kar, and Ashis Kumar Mal

Verification of Money Atomicity in Digital Cash Based Payment System 249
Girish Chandra and Divakar Yadav

Technical Session VI: Network Security II

Cryptographic Analysis of a Type of Sequence Generators 265
Alberto Peinado and Amparo Fúster-Sabater

Certificate-Less On-Demand Public Key Management (CLPKM) for Self-organized MANETs 277
Soumyadev Maity and R.C. Hansdah

Computationally Efficient Secure Access Control for Vehicular Ad Hoc Networks 294
Y. Sreenivasa Rao and Ratna Dutta

Technical Session VII

Tracking Insecure Information Flows: A Prototype Evaluator in ASF+SDF 310
Doaa Hassan

Attacking Image Based CAPTCHAs Using Image Recognition Techniques 327
David Lorenzi, Jaideep Vaidya, Emre Uzun, Shamik Sural, and Vijayalakshmi Atluri

Correctness Verification in Database Outsourcing: A Trust-Based Fake Tuples Approach 343
Simin Ghasemi, Morteza Noferesti, Mohammad Ali Hadavi, Sadegh Dorri Nogoorani, and Rasool Jalili

Author Index 353