Lecture Notes in Computer Science 7644

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

Andrey Bogdanov Somitra Sanadhya (Eds.)

Security, Privacy, and Applied Cryptography Engineering

Second International Conference, SPACE 2012
Chennai, India, November 3-4, 2012
Proceedings

Springer

Volume Editors

Andrey Bogdanov
KU Leuven
ESAT/SCD/COSIC
Kasteelpart Arenberg 10
3001 Leuven-Heverlee, Belgium
E-mail: andrey.bogdanov@esat.kuleuven.be

Somitra Sanadhya
IIIT Delhi
Okhla Industrial Area, Phase III
New Delhi, India 110020
E-mail: somitra@iiitd.ac.in

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-34415-2 e-ISBN 978-3-642-34416-9
DOI 10.1007/978-3-642-34416-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012949648

CR Subject Classification (1998): E.3, C.2, K.6.5, D.4.6, J.1, G.2.1

LNCS Sublibrary: SL 4 – Security and Cryptology

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)

Preface

This volume contains the papers presented at SPACE 2012: the International Conference on Security, Privacy and Applied Cryptography Engineering held during November 2–3, 2012, in Chennai, India. This year's conference had a focus on the latter aspect—applied cryptography and cryptographic engineering. We believe that cryptology is an applied science in its essence which makes the areas in question most impactful.

We received 61 submissions. The Program Committee completed 203 reviews. Eleven papers were accepted for publication. We had four keynote talks on top of that, delivered by Thomas Peyrin, Bart Preneel, Pierangela Samarati and Berk Sunar, being top notch researchers in their respective domains.

The two core days of the conference were accompanied by four days of special-purpose tutorials. There were two days of pre-conference and two days of post-conference workshops. The workshops covered a wide array of topics ranging from mobile platform security, side channel attacks in cryptography to the provable security of cryptographic protocols. The speakers were eminent researchers from the world of industry and academia.

This was the second conference in the SPACE series. The first conference was named InfoSecHiComNet 2011 and its proceedings were published as LNCS volume 7011 in 2011. The Program Chairs of that conference—Marc Joye, Michael Tunstall, and Debdeep Mukhopadhyay—worked hard to start this series of conference. We are extremely thankful to these founders of the conference for establishing a solid platform for us, building on which has been easy.

SPACE 2012 was held in cooperation with the International Association for Cryptologic Research (IACR). We are extremely thankful to its current President, Bart Preneel, for awarding this status. This without doubt helped considerably to make this year's conference a success.

We would like to acknowledge the General Chairs Sanjay Burman and V. Kamakoti for the successful organization of the conference. They not only took pains to ensure the smooth running of the workshops and the conference, but also worked hard to get all the funding for the events. This event could not have been held without the energy and effort put in by the General Chairs. Special thanks go to Swarup Bhunia, who worked tirelessly as the Publicity Chair of the conference. Debdeep Mukhopadhyay was helpful at every stage of the conference organization. We would have found it hard to make it a successful event without the timely help of all of them.

The administration of IIT Madras was extremely positive and helpful in the organization of the conference. They warmly agreed to extend all support and facilities for SPACE 2012. Most of the speakers and guests of SPACE were housed in the excellent guest house of IIT Madras. The Society for Electronic Transactions and Security (SETS), Chennai, kindly provided their space and

resources for organizing the workshops. We are especially thankful to the director of SETS, R. Balasubramaniam, for all the help extended. SETS also provided us the formal legal umbrella under which we could apply to the IACR to hold this event.

We were lucky to find generous funding support from various agencies. We are particularly thankful to the Ministry of Information Technology, who funded us under the Information Security Education and Awareness (ISEA) scheme. We take this opportunity to warmly appreciate the funding support from the Defense Research and Development Organization (DRDO), Government of India and Center of Excellence in Cryptology (CoEC), Kolkata. Besides these, we also received industry funds. We would like to thank all our sponsors for the support they provided.

We thank all authors of submitted papers for considering SPACE 2012 to publish their work. Last but by no means least, we would like to thank the Program Committee members of SPACE 2012 for their numerous reviews and enlightening discussions that were a tremendous help in the challenging task of selecting papers for presentation.

September 2012

Andrey Bogdanov
Somitra Sanadhya

Organization

Program Committee

Rafael Accorsi	University of Freiburg, Germany
Toru Akishita	Sony Corporation, Japan
Elena Andreeva	COSIC, Katholieke Universiteit Leuven, Belgium
Andrey Bogdanov	COSIC, Katholieke Universiteit Leuven, Belgium
Rajat Subhra Chakraborty	IIT Kharagpur, India
Donghoon Chang	IIIT Delhi, India
Carlos Cid	Information Security Group, Royal Holloway, University of London, UK
Abhijit Das	IIT Kharagpur, India
Kris Gaj	George Mason University, USA
Craig Gentry	IBM, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Johann Johann Großschädl	University of Luxembourg, Luxembourg
Tim Gueneysu	Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany
Tibor Jager	Karlsruhe Institute of Technology, Germany
Marc Joye	Technicolor, France
Stefan Katzenbeisser	Technische Universität Darmstadt, Germany
Çetin Kaya Koç	University of California Santa Barbara, USA
Ilya Kizhvatov	Riscure, The Netherlands
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Gregor Leander	Technical University of Denmark, Denmark
Kerstin Lemke-Rust	Hochschule Bonn-Rhein-Sieg, Germany
Dongdai Lin	State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China
Keith Martin	Information Security Group, Royal Holloway, University of London, UK
Debdeep Mukhopadhyay	IIT Kharagpur, India
David Naccache	Ecole normale supérieure, France
Arpita Patra	ETH Zurich, Switzerland
Joachim Posegga	Institute for IT Security and Security Law (ISL) University of Passau, Germany
Bart Preneel	COSIC, Katholieke Universiteit Leuven, Belgium

Francesco Regazzoni	ALaRI Institute, University of Lugano, Switzerland
Vincent Rijmen	COSIC, Katholieke Universiteit Leuven, Belgium
Matt Robshaw	Orange Labs, France
Bimal Roy	Indian Statistical Institute, Kolkata, India
Pierangela Samarati	Università degli Studi di Milano, Italy
Somitra Sanadhya	IIIT Delhi, India
Sumanta Sarkar	University of Calgary, Canada
Martijn Stam	University of Bristol, UK
François-Xavier Standaert	UCL Crypto Group, Belgium
Berk Sunar	Worcester Polytechnic Institute (WPI), USA
Michael Tunstall	University of Bristol, UK
Gilles Van Assche	STMicroelectronics, Belgium
Bo-Yin Yang	Academia Sinica, Taiwan
Jianying Zhou	Institute for Infocomm Research, Singapore

Additional Reviewers

Aagren, Martin
Akdemir, Kahraman
Ali, Sk. Subidh
Ardagna, Claudio Agostino
Arnold, Michael
Bard, Gregory
Barenghi, Alessandro
Bartkewitz, Timo
Bernhard, David
Bilal, Zeeshan
Braun, Bastian
Buhan-Dulman, Ileana
Böhl, Florian
C. Ramanna, Somindu
Chen, Yu
Choudhury, Ashish
Chu, Cheng-Kang
Daemen, Joan
Delerablée, Cécile
Durvaux, David
El Aimani, Laila
Foresti, Sara
Gonzales Cerveron, Maria Teresa
Grosso, Vincent
Habib, Bilal
Hammouri, Ghaith
Hanley, Neil
Herrmann, Mathias
Herrmann, Michael
Hiwatari, Harunaga
Homsirikamol, Ekawat
Jacob, Nisha
Kamel, Dina
Karakoyunlu, Deniz
Kasem-Madani, Saffija
Kohlweiss, Markulf
Kusakawa, Masafumi
Lepoint, Tancrède
Liu, Peng
Maes, Roel
May, Alex
Mischke, Oliver
Naya-Plasencia, María
Nitaj, Abderrahmane
Oswald, David
Pandit, Tapas
Pashalidis, Andreas
Peeters, Michaël
Peters, Thomas
Poeppelmann, Thomas
Rebeiro, Chester
Ren, Kui

Rial, Alfredo
Rogawski, Marcin
Ruj, Sushmita
Schreckling, Daniel
Sen Gupta, Sourav
Shahid, Rabia
Sharif, Malik Umar
Striecks, Christoph
Tumeo, Antonino
Velegalati, Rajesh
Vercauteren, Frederik
von Maurich, Ingo
Witteman, Marc
Wojcik, Marcin
Xu, Jia
Xu, Zhiqian
Zhou, Yongbin