Lecture Notes in Computer Science 8204

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

Benedikt Gierlichs Sylvain Guilley
Debdeep Mukhopadhyay (Eds.)

Security, Privacy, and Applied Cryptography Engineering

Third International Conference, SPACE 2013
Kharagpur, India, October 19-23, 2013
Proceedings

Springer

Volume Editors

Benedikt Gierlichs
KU Leuven, ESAT/COSIC
Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
E-mail: benedikt.gierlichs@esat.kuleuven.be

Sylvain Guilley
Institut MINES-TELECOM, TELECOM-ParisTech
CNRS LTCI (UMR 5141)
COMELEC Department, Crypto Group (SEN)
46 rue Barrault, 75013 Paris, France
E-mail: sylvain.guilley@telecom-paristech.fr

Debdeep Mukhopadhyay
Indian Institute of Technology
Department of Computer Science and Engineering
Kharagpur 721302, India
E-mail: debdeep@cse.iitkgp.ernet.in

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-41223-3 e-ISBN 978-3-642-41224-0
DOI 10.1007/978-3-642-41224-0
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013948608

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

We are glad to present the proceedings of the third International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2013 held during October 19–23, 2013 at the Indian Institute of Technology Kharagpur, West Bengal, India. The conference focuses on all aspects of applied cryptology attempting to make cryptographic engineering provide solutions for security and privacy. This is indeed a very challenging field, requiring the assembly of expertise from diverse domains.

In response to the call for papers, we received 39 submissions, out of which 8 submissions were accepted for presentation at the conference after a detailed review process. The submissions were evaluated on the basis of their significance, novelty, and technical quality. Most submissions were reviewed by three members of the Program Committee. The Program Committee was aided by 37 subreviewers. Reviewing was double-blind, meaning that the Program Committee was not able to see the names and affiliations of the authors, and the authors were not told which committee members reviewed their papers. The Program Committee meeting was held electronically, with intensive discussions over a period of almost seven days.

The program also included 9 invited talks and tutorials on several aspects of applied cryptology, delivered by prominent researchers in their respective fields: Elena Trichina, Simha Sethumadhavan, Patrick Schaumont, Michail (Mihalis) Maniatakos, Claude Carlet, Sanjay Burman, Anish Mathuria, Veezhinathan Kamakoti, and Srivaths Ravi.

SPACE 2013 was the third conference in the SPACE series. The two previous conferences provided the necessary platform, and the support of a strong Program Committee, which was very helpful in launching the third event. In this context we would like to express our gratitude to the previous years' Program Chairs, Michael Tunstall, Marc Joye, Andrey Bodganov, and Somitra Sanadhya for laying strong foundations.

SPACE 2013 was held in cooperation with the International Association for Cryptologic Research (IACR). We are extremely thankful to the IACR for awarding this status. It helped considerably to make the conference a success. We would like to extend our gratitude to Bimal Roy for his support through the aegis of the Cryptology Research Society of India (CRSI) to back the conference. We are also thankful to the Defence Institute of Advanced Technology (DIAT) for being in association with the conference.

The conference was sponsored by the Defence Research and Development Organisation (DRDO), the Ministry of Communication and Information Technology, and the Cryptology Research Society of India (CRSI). We would like to thank these organizations for their support, which has helped us to reduce registration fees and make the conference a success.

There is a long list of people who volunteered their time and energy to put together the conference and who deserve acknowledgment. Thanks to all the members of the Program Committee and the external reviewers for all their hard work in the evaluation of the submitted papers. Our hearty thanks to easychair for allowing us to use the conference management system, which was largely instrumental in the timely and smooth operation needed for hosting such an international event. We also thank Springer for agreeing to publish the proceedings as a volume in the Lecture Notes in Computer Science series. We are further very grateful to all the people who gave their assistance and ensured a smooth organization process: the Local Organizing Committee of the Indian Institute of the Technology. Special thanks to our General Chairs Dipanwita Roy Chowdhury and Anish Mathuria for being prime motivators. Also sincere gratitude to our Honorary General Chairs Bart Preneel and Indranil Sengupta for their advice and strong support of the event. We would also like to thank Abhijit Das, Rajesh Pillai, and Arun Mishra for their active involvement with SPACE 2013. We would like to thank Ramesh Karri for taking on the extremely important role of Publicity Chair. Sanjay Burman, Veezhinathan Kamakoti, Pramod Saxena, and Chandrasekhar Pandurangan have been backbones for this conference and their support and advice has been instrumental for the smooth running of the event. No words can express our sincere gratitude to Rajat Subhra Chakraborty, not only for his support in assembling a nice tutorial and workshop program, but also for his crucial help in managing local affairs. We thank Durga Prasad for maintaining the website for SPACE 2013.

Last, but certainly not least, our sincere thanks go to all the authors who submitted papers to SPACE 2013, and to all the attendees. We sincerely hope you find the program stimulating and inspiring.

October 2013

Benedikt Gierlichs
Sylvain Guilley
Debdeep Mukhopadhyay

Message from the General Chairs

We are pleased to extend a warm welcome to all participants of the Third International Conference on Security, Privacy, and Applied Cryptography Engineering. SPACE provides a major forum for researchers from academia, industry, and government to present and discuss ideas on challenging problems in the ever expanding field of security and cryptography. The third conference in this series is being held at IIT Kharagpur, India during October 19–23, 2013. The first meeting was named InfoSecHiComNet and held in Haldia, India in 2011. Its proceedings were published by Springer as LNCS 7011. The second event was renamed to SPACE and held in Chennai, India in 2012. Its proceedings were published by Springer as LNCS 7644. All instances of this conference series have been organized in cooperation with the International Association for Cryptologic Research (IACR).

The Program Chairs, Benedikt Gierlichs, Sylvain Guilley, and Debdeep Mukhopadhyay, deserve a special mention for their efforts in selecting an outstanding Program Committee and conducting a rigorous review process. Our sincere thanks go to the Program Committee members for their time and efforts in reviewing the submissions and selecting high-quality papers. The main technical program is accompanied by several tutorials, invited talks, and specialized workshops.

We are extremely grateful to DRDO, India and all the other sponsors for their financial support. The conference would not have been possible without their support. Last but not least our special thanks to the local host for making the smooth operation of the conference possible.

We hope you benefit from excellent technical and social interactions during the conference. Thank you for your participation, and have a wonderful time at the conference.

October 2013

Anish Mathuria
Dipanwita Roychowdhury

Organization

Program Chairs

Benedikt Gierlichs	KU Leuven, Belgium
Sylvain Guilley	Institut MINES-TELECOM, TELECOM-ParisTech; CNRS LTCI (UMR 5141), France
Debdeep Mukhopadhyay	IIT Kharagpur, India

Program Committee

Rafael Accorsi	University of Freiburg, Germany
Toru Akishita	University of Tokyo, Japan
Elena Andreeva	KU Leuven, Belgium
Josep Balasch	KU Leuven, Belgium
Bruhadeshwar Bezawada	International Institute of Information Technology, India
Shivam Bhasin	TELECOM ParisTech, France
Swarup Bhunia	Case Western Reserve University, USA
Andrey Bogdanov	Technical University of Denmark, Denmark
Rajat Subhra Chakraborty	IIT Kharagpur, India
Abhijit Das	IIT Kharagpur, India
Kris Gaj	George Mason University, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Tim Güneysu	Ruhr-University Bochum, Germany
Aniket Kate	Saarland University, Germany
Ilya Kizhvatov	Riscure, The Netherlands
Gregor Leander	Ruhr-University Bochum, Germany
Kerstin Lemke-Rust	University of Applied Sciences Bonn-Rhein-Sieg, Germany
Giovanni Livraga	Università degli Studi di Milano, Italy
Keith Martin	Royal Holloway, University of London, UK
David Naccache	Ecole normale supérieure, France
Chandrasekaran Pandu-Rangan	IIT Madras, India
Arpita Patra	University of Bristol, UK
Joachim Posegga	University of Passau, Germany
Bart Preneel	KU Leuven, Belgium
Francesco Regazzoni	ALaRI, Switzerland and TU Delft, The Netherlands
Vincent Rijmen	KU Leuven, Belgium

Matt Robshaw	Impinj, USA
Bimal Roy	Indian Statistical Institute, India
Kazuo Sakiyama	The University of Electro Communications, Japan
Somitra Sanadhya	Indraprastha Institute of Information Technology, India
Sumanta Sarkar	Indian Statistical Institute, India
Jörn-Marc Schmidt	Graz University of Technology, Austria
Berk Sunar	Worcester Polytechnic Institute, USA
Carmela Troncoso	Gradiant, Spain
Michael Tunstall	University of Bristol, UK
Gilles Van Assche	STMicroelectronics, Belgium
Bo-Yin Yang	Academia Sinica, Taiwan
Yongbin Zhou	Chinese Academy of Sciences, China

Additional Reviewers

Basak, Abhishek
Belgacem, Boutheyna
Bhattacherjee, Sanjay
Bilzhause, Arne
Choudhury, Ashish
Datta, Nilanjan
Delclef, Joris
Eisenbarth, Thomas
Fuchsbauer, Georg
Hermans, Jens
Heuser, Annelie
Hofheinz, Dennis
Karwe, Markus
Kawai, Yutaka
Khovratovich, Dmitry
Li, Yang
Majumdar, Bodhisatwa
Moradi, Amir
Palmieri, Paolo
Pandit, Tapas
Poeppelmann, Thomas
Qian, Wenchao
Reparaz, Oscar
Rial, Alfredo
Rothstein, Eric
S., Sree Vivek
Sasaki, Yu
Scholl, Peter
Schwabe, Peter
Sen Gupta, Sourav
Shibutani, Kyoji
Ullmann, Markus
Wang, Xinmu
Xu, Jing
Zhang, Bin

Thoughts on the Security Problem
(Invited Talk)

Sanjay Burman

Centre for Artificial Intelligence and Robotics,
C V Raman Nagar, Bangalore-560093, India
sanjayburman@gmail.com

Abstract. The spectacular failure of the system developers to deliver on the security requirements, with the simultaneous need to achieve security goals in an interconnected world that depends on information systems is astounding. Security vulnerabilities in the mainstream systems continue to be rampant. Commodity platforms for computing and for networking continue to leverage Moore's law to deliver on performance with increasing number of features or functionality. However, these systems deliver little or no security assurance. The *success* of the security industry in marketing such *no-assurance* products is primarily due to the cognitive limitation of humans in the context of security. The sheer lack of market incentive for delivering secure systems has led the system developers to ignore the significant body of knowledge already available for design of secure systems. This talk aims to explore the reasons for this state of (in)security, the gaps from theory to practice to deployment of *engineered secure systems.*

Table of Contents

Implementations and Protocols

Side Channel Attacks and Countermeasures

Identity-Based Identification Schemes

Signatures