Lecture Notes in Computer Science 7011

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

Marc Joye Debdeep Mukhopadhyay
Michael Tunstall (Eds.)

# Security Aspects in Information Technology

First International Conference
InfoSecHiComNet 2011
Haldia, India, October 19-22, 2011
Proceedings

Springer

Volume Editors

Marc Joye
Technicolor, Security and Content Protection Labs
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
E-mail: marc.joye@technicolor.com

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

Michael Tunstall
University of Bristol
Department of Computer Science
Merchant Venturers Building
Woodland Road
Bristol BS8 1UB, UK
E-mail: tunstall@cs.bris.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-24585-5 e-ISBN 978-3-642-24586-2
DOI 10.1007/978-3-642-24586-2
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011937700

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)

# Message from the General Chairs

We are happy to host the first International Conference on Security Aspects in Information Technology, High-Performance Computing and Networking, InfoSecHiComNet 2011, at Haldia Institute of Technology, Haldia, India, 19–22 October, 2011. This conference is being organized in cooperation with the International Association for Cryptographic Research (IACR) and in association with the Cryptology Research Society of India (CRSI).

As we are aware, different aspects of security, such as development of encryption algorithms and analysis of secrecy systems using high performance computing infrastructure, are of paramount importance for securing information. It is not only important to secure conventional electronic communication but security of networks is also emerging as a major thrust area of research in this age of digital communication. In this context, the present conference, InfoSecHiComNet 2011, is a very important event where the research community can deliberate upon different aspects of theoretical as well as application oriented work in the area of cryptology and information security. The conference has been divided into three tracks — Cryptography, Security Aspects in High Performance Computing, and Security Aspects in Networks.

It is expected that this conference will emerge as a powerful forum for researchers to interact and share their thoughts and their work with others, stimulating the growth of information and network security and cryptology research in the world, more specifically in India. The overwhelming response in quality submissions to the conference and transparent open review mechanism helped in keeping the standards high and also in encouraging researchers to participate in the conference and take up serious interest in pursuing research and development in this area. The presence of a large number of students indicates the growing interest in this area where achieving security and efficiency simultaneously in a network is a challenge.

The complete InfoSecHiComNet 2011 event spans over four days from 19 to 22 October 2011. The first day is totally dedicated to tutorials conducted by Michael Tunstall from the University of Bristol, UK and C. Pandurangan from IIT Madras, India. The main conference is held on the remaining three days with invited talks by experts from different parts of the world. Out of the 112 submitted papers, 14 papers have been selected through a transparent open review process and presented by the authors. The tutorials delivered by eminent speakers on areas covering recent developments in information security and cryptography provided insight to young researchers and also stimulated the thinking of others. We are thankful to all invited speakers who delivered stimulating talks and interesting tutorials on the subject.

A conference of this kind would not have been possible to organize without full support from different people across different committees. While all logistic and

general organizational aspects were looked after by the Organizing Committee teams headed by Prof. Debasis Giri, the coordination and selection of technical papers required dedicated and time-bound efforts by the Program Chairs. We are thankful to Marc Joye, Michael Tunstall, and Debdeep Mukhopadhyay for their efforts in bringing out such an excellent technical program for the participants. We are also thankful to all the Technical Program Committee members for thoroughly reviewing the papers submitted to the conference and sending constructive suggestions and comments within the deadlines.

We are indebted to our fellow Organizing Chair, Prof. Debasis Giri, and his team, who worked hard in making the stay of the participants comfortable and the event enjoyable. Thanks are also due to the Chairman and Director of Haldia Institute of Technology for providing the venue and infrastructure and agreeing to host the conference.

We express our heartfelt thanks to Intel, Neucleodyne, the Defence Research and Development Organization (DRDO), the Ministry of Communication and Information Technology (MCIT), and the Department of Science and Technology (DST) for sponsoring the event.

Last but not least, we extend our sincere thanks to all those who contributed to InfoSecHiComNet 2011 and especially to the researchers who are now authors in this prestigious LNCS series of conference proceedings, which has been brought out so nicely.

October 2011

P.K. Saxena
P.D. Srivastava

# Preface

We are glad to present the proceedings of the first International Conference on Security Aspects in Information Technology, High-Performance Computing and Networking (InfoSecHiComNet 2011), held October 19–22, 2011 in Haldia, West Bengal, India.

In response to the call for papers, 112 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the Program Committee. The Program Committee was aided by 13 sub-reviewers. 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 which papers. The Program Committee meeting was held electronically, with intensive discussions over a period of almost ten days. Of the papers submitted, 14 papers were selected for presentation at the conference. The program was completed with two instructive tutorials by C. Pandurangan (IIT Madras, India) and Michael Tunstall (University of Bristol, UK). Further, we had six invited talks by Ingrid Verbauwhede (Katholieke Universiteit Leuven, Belgium), Jörn-Marc Schmidt (IAIK, TUGraz, Austria), C.E. Venimadhavan (IISc, Bangalore,India), Benedikt Gierlichs (K.U.Leuven, Belgium), Palash Sarkar (ISI Kolkata,India), and Sanjay Burman (CAIR, India).

This conference was sponsored by Intel, Neucleodyne, the Defence Research and Development Organization, the Ministry of Communication and Information Technology, and the Department of Science and Technology, India. We would like to thank these organizations for their support, which helped us to reduce registration fees and make the conference a success.

InfoSecHiComNet 2011 was also organized in cooperation with the International Association for Cryptologic Research (IACR) and the Cryptology Research Society of India (CRSI). Their support has significantly contributed to raising the profile of the conference, which is reflected in the high quality of the submissions we received.

There is also 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 the makers of EasyChair for allowing us to use the conference management system, which was largely instrumental in the timely and smooth operation needed in 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 also very grateful to all the people who gave their assistance and ensured a smooth organization process: the local Organizing Committee of Haldia Institute of Technology. Special thanks to Dr. Debasis Giri, our Organizing Chair, for all his hard work, help and advice in initiating and making the conference a reality.

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

August 2011

Marc Joye
Debdeep Mukhopadhyay
Michael Tunstall

# InfoSecHiComNet 2011

## First International Conference on Security Aspects in Information Technology, High-Performance Computing and Networking

**Haldia, India**
**October 19–22, 2011**

### Patron

| | |
|---|---|
| Lakshman Seth | Haldia Institute of Technology, India |

### Honorary Chair

| | |
|---|---|
| C. Chang | Feng Chia University, Taiwan |

### Publication and Organizing Chair

| | |
|---|---|
| Debasis Giri | Haldia Institute of Technology, India |

### Program Chairs

| | |
|---|---|
| Marc Joye | Technicolor, France |
| Debdeep Mukhopadhyay | IIT Kharagpur, India |
| Michael Tunstall | University of Bristol, UK |

### Program Committee

| | |
|---|---|
| Anirban Banerjee | Indian Institute of Science, Education and Research – Kolkata, India |
| Ranieri Baraglia | ISTI-CNR, Italy |
| S.S. Bedi | SAG, Delhi, India |
| Sanjukta Bhowmick | University of Nebraska at Omaha, USA |
| Swarup Bhunia | Case Western Reserve Univ., USA |
| Santosh Biswas | IIT Guwahati, India |
| Bezawada Bruhadeshwar | IIIT Hyderabad, India |
| Sanjay Burman | CAIR Bangalore, India |
| Junwei Cao | Tsinghua University, China |
| Amlan Chakrabarti | Calcutta University, India |
| R.S. Chakraborty | IIT Kharagpur, India |
| C. Chang | Feng Chia University, Taiwan |
| Amit Chattopadhyay | Rijksuniversity of Groningen, The Netherlands |

| | |
|---|---|
| Tzungshi Chen | National University of Tainan, Taiwan |
| Peter Chong | Nanyang Technological University, Singapore |
| Abhijit Das | IIT Kharagpur, India |
| Ashok Kumar Das | IIIT, Hyderabad, India |
| Sajal Das | University of Texas at Arlington, USA |
| Ratna Dutta | IIT Kharagpur, India |
| Niloy Ganguly | IIT Kharagpur, India |
| Praveen Gauravaram | Technical University of Denmark, Denmark |
| S.K. Ghosh | IIT Kharagpur, India |
| Debasis Giri | Haldia Institute of Technology, India |
| Tiong Goh | Victoria University of Wellington, New Zealand |
| Guangjie Han | Hohai University, China |
| Jing He | Georgia State University, USA |
| Honggang Hu | University of Waterloo, Canada |
| Shaoquan Jiang | University of Electronic Science and Technology of China, China |
| Xiaohong Jiang | Tohoku University, Japan |
| Willem Jonker | EIT ICT Labs, The Netherlands |
| Marc Joye | Technicolor, France |
| Ramesh Karri | Polytechnic University, NY, USA |
| Chun-Ta Li | Tainan University of Technology, Taiwan |
| Jie Li | University of Tsukuba, Japan |
| Constandinos Mavromoustakis | University of Nicosia, Cyprus |
| Bivas Mitra | French National Centre for Scientific Research(CNRS), Paris |
| Animesh Mukherjee | ISI Foundation, Italy |
| Debdeep Mukhopadhyay | IIT Kharagpur, India |
| Sourav Mukhopadhyay | IIT Kharagpur, India |
| Sukumar Nandi | IIT Guwahati, India |
| Saibal Pal | SAG, Delhi, India |
| Subrat Panda | IBM, India |
| C. Pandu Rangan | Indian Institute of Technology, Madras, India |
| Goutam Paul | Jadavpur University, India |
| Rajesh Pillai | SAG, Delhi, India |
| Vincent Rijmen | IAIK, Graz University of Technology, Austria |
| Bimal Roy | Indian Statistical Institute, Kolkata, India |
| Romit Roychoudhury | Duke University, USA |
| Dipanwita Roychowdhury | IIT Kharagpur, India |
| Kouichi Sakurai | Kyushu University, Japan |
| Areejit Samal | Univ. Paris-Sud, France and Max Planck Institute for Mathematics in the Sciences, Germany |
| P. Saxena | SAG, India |
| Peter Schwabe | Academia Sinica, Institute of Information Science, Taiwan |
| Indranil Sengupta | IIT Kharagpur, India |

| | |
|---|---|
| P. Srivastava | IIT Kharagpur, India |
| Shamik Sural | IIT Kharagpur, India |
| Willy Susilo | University of Wollongong, Australia |
| Junko Takahashi | NTT Information Sharing Platform Laboratories, Japan |
| Sabu Thampi | Indian Institute of Information Technology and Management, India |
| Michael Tunstall | University of Bristol, UK |
| Athanasios Vasilakos | University of Western Macedonia, Greece |
| Kamakoti Veezhinathan | IIT Madras, India |
| Ramarathnam Venkatesan | Microsoft Research, USA |
| Michal Wozniak | Wroclaw University of Technology, Poland |
| Naixue Xiong | Georgia State University, USA |
| Eiko Yoneki | University of Cambridge, UK |
| Amr Youssef | Concordia University, Canada |

## External Reviewers

| | |
|---|---|
| Indivar Gupta | Rajesh Pillai |
| Arun Karthik Kanuparthi | Yizhi Ren |
| Aswin Krishna | Sharmila Deva Selvi |
| P.R. Mishra | Easter Selvan Suviseshamuthu |
| Seetharam Narasimhan | S.K. Tiwari |
| Ruchira Naskar | Mallapur Verraya Verraya |
| Takashi Nishide | Xinmu Wang |

## Local Organizing Committee

| | |
|---|---|
| M.M. Bag | Sourav Mandal |
| Subhabrata Barman | Anjan Mishra |
| Nandan Bhattacharyya | Apratim Mitra |
| Debdas Ganguly | Anupam Pattanayak |
| Tarun Kumar Ghosh | Soumen Paul |
| Subhankar Joardar | Palash Ray |
| Shyamalendu Kandar | Soumen Saha |
| Asish Lahiri | Sk. Sahnawaj |
| A.B. Maity | Kabita Thaoroijam |
| Susmit Maity | |

# Table of Contents


## Invited Talks

Engineering Trustworthy Systems . . . . . 1
*Sanjay Burman*

Secure Implementations for the Internet of Things . . . . . 2
*Jörn-Marc Schmidt*

## Embedded Security

Model Based Hybrid Approach to Prevent SQL Injection Attacks in PHP . . . . . 3
*Kunal Sadalkar, Radhesh Mohandas, and Alwyn R. Pais*

Security of Prime Field Pairing Cryptoprocessor against Differential Power Attack . . . . . 16
*Santosh Ghosh and Dipanwita Roychowdhury*

Embedded Software Security through Key-Based Control Flow Obfuscation . . . . . 30
*Rajat Subhra Chakraborty, Seetharam Narasimhan, and Swarup Bhunia*

## Digital Rights Management

Reversible Watermarking Using *Priority Embedding* through Repeated Application of *Integer Wavelet Transform* . . . . . 45
*Sambaran Bandyopadhyay, Ruchira Naskar, and Rajat Subhra Chakraborty*

Access Policy Based Key Management in Multi-level Multi-distributor DRM Architecture . . . . . 57
*Ratna Dutta, Dheerendra Mishra, and Sourav Mukhopadhyay*

Access Polynomial Based Self-healing Key Distribution with Improved Security and Performance . . . . . 72
*Ratna Dutta*

## Cryptographic Protocols

An ID-Based Proxy Multi Signature Scheme without Bilinear Pairings . . . . . 83
*Namita Tiwari and Sahadeo Padhye*

Distributed Signcryption Schemes with Formal Proof of Security ..... 93
*Indivar Gupta and P.K. Saxena*

Identity Based Online/Offline Encryption and Signcryption Schemes Revisited ..... 111
*S. Sharmila Deva Selvi, S. Sree Vivek, and C. Pandu Rangan*

## Cryptanalysis/Side Channel Attacks

"Rank Correction": A New Side-Channel Approach for Secret Key Recovery ..... 128
*Maxime Nassar, Youssef Souissi, Sylvain Guilley, and Jean-Luc Danger*

A Cache Trace Attack on CAMELLIA ..... 144
*Rishabh Poddar, Amit Datta, and Chester Rebeiro*

An Improvement of Linearization-Based Algebraic Attacks ..... 157
*Satrajit Ghosh and Abhijit Das*

## Cipher Primitives

Generalized Avalanche Test for Stream Cipher Analysis ..... 168
*P.R. Mishra, Indivar Gupta, and N.R. Pillai*

On Applications of Singular Matrices over Finite Fields in Cryptography ..... 181
*Dhirendra Singh Yadav, Rajendra K. Sharma, and Wagish Shukla*

**Author Index** ..... 187