

*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*

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

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Iliano Cervesato (Ed.)

# Advances in Computer Science – ASIAN 2007

Computer and Network Security

12th Asian Computing Science Conference  
Doha, Qatar, December 9-11, 2007  
Proceedings



Springer

Volume Editor

Iliano Cervesato  
Carnegie Mellon University  
Doha, Qatar  
E-mail: [iliano@cmu.edu](mailto:iliano@cmu.edu)

Library of Congress Control Number: 2007939450

CR Subject Classification (1998): F.3, E.3, D.2.4, D.4.6-7, K.6.5, C.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743  
ISBN-10 3-540-76927-7 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-76927-9 Springer Berlin Heidelberg New York

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.

Springer is a part of Springer Science+Business Media

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2007  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12195626 06/3180 5 4 3 2 1 0

# Preface

The ASIAN conference series provides a forum for researchers throughout Asia to present cutting-edge results in yearly-themed areas of computer science, to discuss advances in these fields, and to promote interaction with researchers from other continents. Accordingly, the conference moves every year to a different center of research throughout Asia: previous editions were held in Tokyo, Kunming (China), Bangkok, Mumbai, Hanoi, Penang (Malaysia), Phuket (Thailand), Manila, Kathmandu, Singapore, and Pathumthani (Thailand) where ASIAN was initiated by AIT, INRIA and UNU/IIST in 1995. The 12th edition took place in Doha, Qatar, during December 9–11, 2007.

Each year, the conference focuses on a different theme at the cutting edge of computer science research. The theme of ASIAN 2007 was “Computer and Network Security”. It has been a tradition of ASIAN to invite three of the most influential researchers in the focus area, one from Asia, one from Europe and one from the Americas, to discuss their work and their vision for the field. This year’s distinguished speakers were Andrei Sabelfeld (Chalmers University, Sweden), Joshua Guttman (MITRE, USA) and Kazuhiko Kato (University of Tsukuba, Japan).

Following the call for paper, ASIAN 2007 received 112 submissions, of which 65 were eventually reviewed. Of these, the Program Committee selected 15 regular papers and 10 short papers. This volume contains the abstracts of the invited talks and the revised versions of the regular papers and the short papers. I wish to thank the members of the Program Committee and the external reviewers for doing an excellent job at selecting the contributed papers under severe time pressure. *EasyChair* proved an egregious platform for smoothly carrying out all aspects of the program selection and finalization.

The conference was held in Doha, Qatar, where Carnegie Mellon University recently established a branch campus with the goal of promoting the same high standards of research and education for which its original campus in Pittsburgh, USA, is internationally recognized. Carnegie Mellon Qatar is located in Education City, a 2,500-acre campus which provides state-of-the-art research and teaching facilities to branches of five of the world’s leading universities. It is part of an unprecedented commitment of resources made by the Qatari leadership to position Qatar as a world-class center of education and research.

Many people were involved in the organization of this conference. In particular, I wish to thank the General Chair, Kazunori Ueda, for his support, and the Steering Committee for endorsing the candidacy of Doha for this year’s edition of ASIAN. This conference would not have been possible without the hard work of the many people who relentlessly handled the local arrangements, especially Thierry Sans and Kara Nesimiuk. We greatly appreciate the generous support

of our sponsors, Carnegie Mellon University in Qatar and QCERT. Finally we are grateful to the authors, the invited speakers and the attendees who made this conference an enjoyable and fruitful event.

September 2007

Iliano Cervesato

# Conference Organization

## Steering Committee

Philippe Codognet (French Embassy, Japan)  
Joxan Jaffar (National University, Singapore)  
Mitsu Okada (Keio University, Japan)  
R.K. Shyamasundar (Tata Institute of Fundamental Research, India)  
Kazunori Ueda (Waseda University, Japan)

## General Chair

Kazunori Ueda (Waseda University, Japan)

## Program Chair

Iliano Cervesato (Carnegie Mellon University, Qatar)

## Program Committee

Michael Backes (Saarland University, Germany)  
Anupam Datta (Stanford University, USA)  
Mourad Debbabi (Concordia University, Canada)  
Sven Dietrich (CERT, USA)  
Masami Hagiya (University of Tokyo, Japan)  
Yassine Lakhnech (VERIMAG, France)  
Ninghui Li (Purdue University, USA)  
Catherine Meadows (Naval Research Lab, USA)  
R. Ramanujam (Institute of Mathematical Sciences, India)  
Takamichi Saito (Meiji University, Japan)  
Dheeraj Sanghi (IIT Kanpur, India)  
Thierry Sans (Carnegie Mellon University, Qatar)  
Andre Scedrov (University of Pennsylvania, USA)  
Vitaly Shmatikov (University of Texas-Austin, USA)  
Duminda Wijesekera (George Mason University, USA)  
Yuqing Zhang (Chinese Academy of Sciences, China)  
Jianying Zhou (Institute for Infocomm Research, Singapore)

## Local Organization

Thierry Sans (Carnegie Mellon University, Qatar)

## External Reviewers

Kumar Avijit  
Vishwas B.C.  
Adam Barth  
A. Baskar  
Justin Brickell  
Judicaël Courant  
Shruti Dubey  
Markus Dürmuth  
Jason Franklin  
Yoshinobu Kawabe  
Dilsun Kaynar  
Ken Mano  
Azzam Mourad  
Hadi Otrok  
Iosif Radu  
Arun Raghavan  
Arnab Roy  
Hideki Sakurada  
Mohamed Saleh  
Satyam Sharma  
S.P. Suresh  
Yasuyuki Tsukada

# Table of Contents

## Invited Speaker: Andrei Sabelfeld

Dimensions of Declassification in Theory and Practice (Invited Talk) ... <i>Andrei Sabelfeld</i>	1
---	---

## Session 1: Program Security

A Static Birthmark of Binary Executables Based on API Call Structure .....	2
<i>Seokwoo Choi, Heewan Park, Hyun-il Lim, and Taisook Han</i>	
Compiling C Programs into a Strongly Typed Assembly Language .....	17
<i>Takahiro Kosakai, Toshiyuki Maeda, and Akinori Yonezawa</i>	
Information Flow Testing: The Third Path Towards Confidentiality Guarantee .....	33
<i>Gurvan Le Guernic</i>	

## Session 2: Short Papers on Computer Security

Large Scale Simulation of Tor: Modelling a Global Passive Adversary ... <i>Gavin O’Gorman and Stephen Blott</i>	48
Privacy Enhancing Credentials .....	55
<i>Junji Nakazato, Lihua Wang, and Akihiro Yamamura</i>	
Browser Based Agile E-Voting System .....	62
<i>Sriperumbuduru Kandala Simhalu and Keiji Takeda</i>	
Risk Balance in Exchange Protocols .....	70
<i>Mohammad Torabi Dashti and Yanjing Wang</i>	
Scalable DRM System for Media Portability .....	78
<i>Hyoungshick Kim</i>	
Computational Semantics for Basic Protocol Logic – A Stochastic Approach .....	86
<i>Gergei Bana, Koji Hasebe, and Mitsuhiro Okada</i>	

## Session 3: Access Control

Management Advantages of Object Classification in Role-Based Access Control (RBAC) .....	95
<i>Mohammad Jafari and Mohammad Fathian</i>	



An Integrated Model for Access Control and Information Flow Requirements..... 111  
*Samih Aged, Nora Cuppens-Boulahia, and Frédéric Cuppens*

Digital Rights Management Using a Master Control Device..... 126  
*Imad M. Abbadi*

**Invited Speaker: Joshua Guttman**

How to do Things with Cryptographic Protocols (Invited Talk) ..... 142  
*Joshua D. Guttman*

**Session 4: Protocols**

A Formal Analysis for Capturing Replay Attacks in Cryptographic Protocols ..... 150  
*Han Gao, Chiara Bodei, Pierpaolo Degano, and Hanne Riis Nielson*

An Abstraction and Refinement Framework for Verifying Security Protocols Based on Logic Programming..... 166  
*MengJun Li, Ti Zhou, ZhouJun Li, and HuoWang Chen*

Secure Verification of Location Claims with Simultaneous Distance Modification ..... 181  
*Vitaly Shmatikov and Ming-Hsiu Wang*

**Invited Speaker: Kazuhiko Kato**

Modeling and Virtualization for Secure Computing Environments (Invited Talk) ..... 196  
*Kazuhiko Kato*

**Session 5: Intrusion Detection**

Empirical Study of the Impact of Metasploit-Related Attacks in 4 Years of Attack Traces..... 198  
*E. Ramirez-Silva and M. Dacier*

A Logical Framework for Evaluating Network Resilience Against Faults and Attacks ..... 212  
*Elie Bursztein and Jean Goubault-Larrecq*

Masquerade Detection Based Upon GUI User Profiling in Linux Systems..... 228  
*Wilson Naik Bhukya, Suneel Kumar Kommuru, and Atul Negi*

## Session 6: Short Papers on Network Security

One-Time Receiver Address in IPv6 for Protecting Unlinkability . . . . .	240
<i>Atsushi Sakurai, Takashi Minohara, Ryota Sato, and Keisuke Mizutani</i>	
A Comprehensive Approach to Detect Unknown Attacks Via Intrusion Detection Alerts . . . . .	247
<i>Jungsuk Song, Hayato Ohba, Hiroki Takakura, Yasuo Okabe, Kenji Ohira, and Yongjin Kwon</i>	
Combining Heterogeneous Classifiers for Network Intrusion Detection . . .	254
<i>Ali Borji</i>	
Managing Uncertainty in Access Control Decisions in Distributed Autonomous Collaborative Environments . . . . .	261
<i>Petros Belsis, Stefanos Gritzalis, Christos Skourlas, and Vassilis Tsoukalas</i>	

## Session 7: Safe Execution

On Run-Time Enforcement of Policies . . . . .	268
<i>Harshit Shah and R.K. Shyamasundar</i>	
Static vs Dynamic Typing for Access Control in Pi-Calculus . . . . .	282
<i>Michele Bugliesi, Damiano Macedonio, and Sabina Rossi</i>	
A Sandbox with a Dynamic Policy Based on Execution Contexts of Applications . . . . .	297
<i>Tomohiro Shioya, Yoshihiro Oyama, and Hideya Iwasaki</i>	
<b>Author Index</b> . . . . .	313