Lecture Notes in Computer Science 7618

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

Tat Wing Chim  Tsz Hon Yuen (Eds.)

# Information and Communications Security

14th International Conference, ICICS 2012
Hong Kong, China, October 29-31, 2012
Proceedings

Springer

Volume Editors

Tat Wing Chim
The University of Hong Kong
Department of Computer Science
Room 519, 5/F, Haking Building, Pokfulam Road
852 Hong Kong, China
E-mail: twchim@cs.hku.hk

Tsz Hon Yuen
The University of Hong Kong
Department of Computer Science
Room 519, 5/F, Haking Wong Building, Pokfulam Road
852 Hong Kong, China
E-mail: thyuen@cs.hku.hk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-34128-1 e-ISBN 978-3-642-34129-8
DOI 10.1007/978-3-642-34129-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012948707

CR Subject Classification (1998): E.3, D.4.6, K.6.5, K.4.4, C.2, F.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

With the ever-increasing coverage of information technology in our daily lives, protecting confidentiality, integrity, and privacy of information via the usage of cryptography and other security technology will be an undeniable responsibility of researchers. The ICICS conference series is a well-established forum for researchers in universities, research institutes, and industry to get together to share the latest research results and exchange ideas in the areas of information and communications security. ICICS has taken place in a number of different countries including China (1997, 2001, 2003, 2005, 2007, 2009, 2011), Australia (1999), Singapore (2002), Spain (2004, 2010), USA (2006), and UK (2008). It was a memorable moment for the Center for Information Security and Cryptography (CISC), University of Hong Kong, to host the 14$^{\text{th}}$ International Conference on Information and Communication Security (ICICS 2012) in Hong Kong. This is because 2012 is the year that the University of Hong Kong started using the new Centennial Campus, which marks the 100$^{\text{th}}$ anniversary of HKU. Hosting ICICS, a renowned conference that had 13 successful past events, was a special tribute to the new campus. Participants of ICICS 2012 could use this event as a chance to visit this freshly launched new campus.

A more important attraction than visiting the new HKU Centennial Campus is to enjoy the strong technical program of ICICS. There were 101 submissions from 20 countries. A total of 23 regular papers and 26 short papers were accepted. The papers cover many important areas in information security such as privacy, security in mobile systems, software and network security, cryptanalysis, applied cryptography, as well as GPU-enabled computation. Each submission was anonymously reviewed by at least two reviewers. We would like to sincerely thank our 43 Program Committee members (from 16 countries) as well as all sub-reviewers and external referees who worked under a very tight review schedule, for their valuable time, effort, and contributions to the program.

The event of ICICS could only be made possible by the collaborating efforts of many other parties behind the scenes, including the Steering Committee Chair, local Organizing Committee members, Publication Chairs, and participants. Last, but not the least, we would like to thank also our co-organizers, the Institute of Software of Chinese Academy of Sciences (CAS), the Institute of Software and Microelectronics of Peking University, and the Information Security and Forensics Society (ISFS).

October 2012

K.P. Chow
Lucas C.K. Hui
S.H. Qing
S.M. Yiu

# Organization

## Conference Chairs

| | |
|---|---|
| K.P. Chow | The University of Hong Kong, Hong Kong |
| Lucas C.K. Hui | The University of Hong Kong, Hong Kong |

## Program Chairs

| | |
|---|---|
| S.H. Qing | Chinese Academy of Sciences and Peking University, China |
| S.M. Yiu | The University of Hong Kong, Hong Kong |

## Publication Chairs

| | |
|---|---|
| T.W. Chim | The University of Hong Kong, Hong Kong |
| T.H. Yuen | The University of Hong Kong, Hong Kong |

## Local Organizing Committee

| | |
|---|---|
| Catherine K.W. Chan | The University of Hong Kong, Hong Kong (Chair) |
| C.B. Chan | The University of Hong Kong, Hong Kong |
| P.F. Chan | The University of Hong Kong, Hong Kong |
| Y.H. Fung | The University of Hong Kong, Hong Kong |
| H. Xiong | The University of Hong Kong, Hong Kong |

## Program Committee

| | |
|---|---|
| Man Ho Au | University of Wollongong, Australia |
| Tuomas Aura | Aalto University, Finland |
| Feng Bao | Institute for Infocomm Research, Singapore |
| Alex Biryukov | University of Luxembourg, Luxembourg |
| Mike Burmester | Florida State University, USA |
| Zhenfu Cao | Shanghai Jiaotong University, China |
| Chin-Chen Chang | Feng Chia University, Taiwan |
| Xiaolin Chang | Beijing Jiaotong University, China |
| Zhong Chen | Peking University, China |
| T.W. Chim | The University of Hong Kong, Hong Kong |
| Sherman S.M. Chow | University of Waterloo, Canada / Chinese University of Hong Kong, Hong Kong |
| Cas Cremers | ETH Zurich, Switzerland |

| | |
|---|---|
| Junbin Fang | The University of Hong Kong, Hong Kong |
| Steven Furnell | University of Plymouth, UK |
| Dieter Gollmann | Hamburg University of Technology, Germany |
| Yong Guan | Iowa State University, USA |
| Shuhui Hou | University of Science and Technology, China |
| Kwangjo Kim | KAIST, Korea |
| Ming Li | Utah State University, USA |
| Joseph Liu | Institute for Infocomm Research, Singapore |
| Javier Lopez | University of Malaga, Spain |
| Di Ma | University of Michigan-Dearborn, USA |
| Mark Manulis | TU Darmstadt, Germany |
| Chris Mitchell | Royal Holloway, University of London, UK |
| Raphael Phan | Loughborough University, UK |
| Pierangela Samarati | Università degli Studi di Milano, Italy |
| Miguel Soriano | Universitat Politecnica de Catalunya, Spain |
| Willy Susilo | University of Wollongong, Australia |
| Tsuyoshi Takagi | Kyushu University, Japan |
| Wen-Guey Tzeng | National Chiao Tung University, Taiwan |
| Zhihui Wang | Dalian University of Technology, China |
| Andreas Wespi | IBM Zurich Research Laboratory, Switzerland |
| Duncan S. Wong | City University of Hong Kong, Hong Kong |
| Yang Xiang | Deakin University, Australia |
| Guomin Yang | University of Wollongong, Australia |
| Shucheng Yu | University of Arkansas at Little Rock, USA |
| T.H. Yuen | The University of Hong Kong, Hong Kong |
| Fangguo Zhang | Sun Yat-sen University, China |
| Wentao Zhang | Institute of Information Engineering, Chinese Academy of Sciences, China |
| Yuliang Zheng | University of North Carolina at Charlotte, USA |
| Jianying Zhou | Institute for Infocomm Research, Singapore |

## Additional Reviewers

| | |
|---|---|
| Duegi Aranha | Ravi Jhawar |
| Claudio Agostino Ardagna | Qingguang Ji |
| Roy Arnab | Grobschadl Johann |
| Ning Cao | Aapo Kalliola |
| Ching Bon Chan | Vadnala Praveen Kumar |
| Patrick P.F. Chan | Hyunrok Lee |
| Leurent Gaetan | Zhang Lei |
| Takuya Hayashi | Huang Lin |
| Yin Hu | Hsiao-Ying Lin |
| Xinyi Huang | Zhen Liu |
| Qiong Huang | Giovanni Livraga |
| Pustogarov Ivan | Xu Ma |

Thomas Martin
Kirill Morozov
Lan Nguyen
Takashi Nishide
Bertram Poettering
Anudath Krishna Prasad
Rodrigo Roman
Peter Schwabe
Lu Shi
Youngjoo Shin
Abdulhadi Shoufan
Xiao Tan
Boyang Wang
Weiping Wen
Jia Xu
Zhenyu Yang
Jiawei Yuan
Haibin Zhang
Mingwu Zhang
Wentao Zhang
Hui Zhang
Yao Zheng
Yan Zhu
Youwen Zhu

# Table of Contents

## Full Papers

## Applied Cryptography



## Cryptanalysis



## Network Security

## Optimization



## Privacy



## Protocols



## Security in Mobile Systems

## Multimedia Security and GPU-Enabled Computation



## Network Security



## Privacy

## Protocols



## Software Security