

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

Alfred Kobsa

University of California, Irvine, CA, 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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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 14th 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 100th 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 Politècnica 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

Audio Steganalysis Based on Lossless Data-Compression Techniques	1
<i>Fatiha Djebbar and Beghdad Ayad</i>	
Enhancing the Perceived Visual Quality of a Size Invariant Visual Cryptography Scheme	10
<i>Yang-Wai Chow, Willy Susilo, and Duncan S. Wong</i>	
Impact of the Revocation Service in PKI Prices	22
<i>Carlos Gañán, Jose L. Muñoz, Oscar Esparza, Jorge Mata-Díaz, and Juanjo Alins</i>	

Cryptanalysis

Cryptanalysis of Multi-Prime RSA with Small Prime Difference	33
<i>Hatem M. Bahig, Ashraf Bhery, and Dieaa I. Nassr</i>	
Implicit Polynomial Recovery and Cryptanalysis of a Combinatorial Key Cryptosystem	45
<i>Jun Xu, Lei Hu, and Siwei Sun</i>	
Improved Related-Key Differential Attacks on Reduced-Round LBlock	58
<i>Shusheng Liu, Zheng Gong, and Libin Wang</i>	

Network Security

Countermeasures on Application Level Low-Rate Denial-of-Service Attack	70
<i>Yajuan Tang</i>	
Firewall Packet Filtering Optimization Using Statistical Traffic Awareness Test	81
<i>Zouheir Trabelsi, Liren Zhang, and Safaa Zeidan</i>	
Group Behavior Metrics for P2P Botnet Detection	93
<i>John Felix, Charles Joseph, and Ali A. Ghorbani</i>	

Optimization

Hardware Performance Optimization and Evaluation of SM3 Hash Algorithm on FPGA	105
<i>Yuan Ma, Luning Xia, Jingqiang Lin, Jiwu Jing, Zongbin Liu, and Xingjie Yu</i>	

Privacy

Continual Leakage-Resilient Dynamic Secret Sharing in the Split-State Model	119
<i>Hao Xiong, Cong Zhang, Tsz Hon Yuen, Echo P. Zhang, Siu Ming Yiu, and Sihan Qing</i>	
Conversion of Real-Numbered Privacy-Preserving Problems into the Integer Domain	131
<i>Wilko Henecka, Nigel Bean, and Matthew Roughan</i>	
Perfect Ambiguous Optimistic Fair Exchange	142
<i>Yang Wang, Man Ho Au, and Willy Susilo</i>	
Privacy-Preserving Noisy Keyword Search in Cloud Computing	154
<i>Xiaoqiong Pang, Bo Yang, and Qiong Huang</i>	

Protocols

Forward Secure Attribute-Based Signatures	167
<i>Tsz Hon Yuen, Joseph K. Liu, Xinyi Huang, Man Ho Au, Willy Susilo, and Jianying Zhou</i>	
On Constant-Round Precise Zero-Knowledge	178
<i>Ning Ding and Dawu Gu</i>	
Outsourcing Encryption of Attribute-Based Encryption with MapReduce	191
<i>Jingwei Li, Chunfu Jia, Jin Li, and Xiaofeng Chen</i>	
Security Enhancement of Identity-Based Identification with Reversibility	202
<i>Atsushi Fujioka, Taiichi Saito, and Keita Xagawa</i>	

Security in Mobile Systems

Coopetitive Architecture to Support a Dynamic and Scalable NFC Based Mobile Services Architecture	214
<i>Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes</i>	

Permission-Based Abnormal Application Detection for Android	228
<i>Jiawei Zhu, Zhi Guan, Yang Yang, Liangwen Yu, Huiping Sun, and Zhong Chen</i>	

Symbian Smartphone Forensics and Security: Recovery of Privacy-Protected Deleted Data	240
<i>Vrizlynn L.L. Thing and Darell J.J. Tan</i>	

Software Security

Detecting Encryption Functions via Process Emulation and IL-Based Program Analysis	252
<i>Ruoxu Zhao, Dawu Gu, Juanru Li, and Hui Liu</i>	

Taint Analysis of Security Code in the KLEE Symbolic Execution Engine	264
<i>Ricardo Corin and Felipe Andrés Manzano</i>	

Short Papers

Authentication

A Generic Approach for Providing Revocation Support in Secret Handshake	276
<i>Yanjiang Yang, Haibing Lu, Jian Weng, Xuhua Ding, and Jianying Zhou</i>	

An Efficient Single-Slow-Phase Mutually Authenticated RFID Distance Bounding Protocol with Tag Privacy	285
<i>Anjia Yang, Yunhui Zhuang, and Duncan S. Wong</i>	

Exploring Mobile Proxies for Better Password Authentication	293
<i>Nitesh Saxena and Jonathan Voris</i>	

On Security of Universal Hash Function Based Multiple Authentication	303
<i>Aysajan Abidin</i>	

Cryptanalysis

A New Variant of Time Memory Trade-Off on the Improvement of Thing and Ying's Attack	311
<i>Zhenqi Li, Yao Lu, Wenhao Wang, Bin Zhang, and Dongdai Lin</i>	

Applying Time-Memory-Data Trade-Off to Plaintext Recovery Attack	321
<i>Zhenqi Li, Bin Zhang, Yao Lu, Jing Zou, and Dongdai Lin</i>	

Comparison between Side-Channel Analysis Distinguishers	331
<i>Houssein Maghrebi, Olivier Rioul, Sylvain Guilley, and Jean-Luc Danger</i>	

Multimedia Security and GPU-Enabled Computation

Acceleration of Composite Order Bilinear Pairing on Graphics Hardware	341
<i>Ye Zhang, Chun Jason Xue, Duncan S. Wong, Nikos Mamoulis, and Siu Ming Yiu</i>	

Evaluating the Effect of Tolerance on Click-Draw Based Graphical Password Scheme	349
<i>Yuxin Meng and Wenjuan Li</i>	

Robust Evidence Detection of Copy-Rotate-Move Forgery in Image Based on Singular Value Decomposition	357
<i>Liu Yong, Huang Meishan, and Lin Bogang</i>	

Network Security

Cookie-Proxy: A Scheme to Prevent SSLStrip Attack	365
<i>Sendong Zhao, Ding Wang, Sicheng Zhao, Wu Yang, and Chunguang Ma</i>	

Detecting and Preventing ActiveX API-Misuse Vulnerabilities in Internet Explorer	373
<i>Ting Dai, Sai Sathyanarayan, Roland H.C. Yap, and Zhenkai Liang</i>	

Endpoint Mitigation of DDoS Attacks Based on Dynamic Thresholding	381
<i>Daewon Kim, Byoungkoo Kim, Ikkyun Kim, Jeongnyeo Kim, and Hyunsook Cho</i>	

Parameter Pollution Vulnerabilities Detection Study Based on Tree Edit Distance	392
<i>Yan Cao, Qiang Wei, and Qingxian Wang</i>	

Privacy

A Privacy-Preserving Path-Checking Solution for RFID-Based Supply Chains	400
<i>Wei Xin, Huiping Sun, Tao Yang, Zhi Guan, and Zhong Chen</i>	

Efficient Attribute Proofs in Anonymous Credential Using Attribute-Based Cryptography	408
<i>Yan Zhang and Dengguo Feng</i>	

F ⁵ P ⁵ : Keyword Search over Encrypted Data with Five Functions and Five Privacy Assurances	416
<i>Huimin Shuai and Wen Tao Zhu</i>	
Location Privacy Policy Management System	427
<i>Arej Muhammed, Dan Lin, and Anna Squicciarini</i>	
Privacy Protection in Social Networks Using l -Diversity	435
<i>Liangwen Yu, Jiawei Zhu, Zhengang Wu, Tao Yang, Jianbin Hu, and Zhong Chen</i>	
Selling Power Back to the Grid in a Secure and Privacy-Preserving Manner	445
<i>Tat Wing Chim, Siu Ming Yiu, Lucas Chi Kwong Hui, Victor On Kwok Li, Tin Wing Mui, Yu Hin Tsang, Chun Kin Kwok, and Kwun Yin Yu</i>	

Protocols

A Key Sharing Fuzzy Vault Scheme	453
<i>Lin You, Mengsheng Fan, Jie Lu, Shengguo Wang, and Fenghai Li</i>	
A New Version of McEliece PKC Based on Convolutional Codes	461
<i>Carl Löndahl and Thomas Johansson</i>	
Flexible Attribute-Based Encryption	471
<i>Seiko Arita</i>	
Non-interactive Dynamic Identity-Based Broadcast Encryption without Random Oracles	479
<i>Yanli Ren, Shuozhong Wang, and Xinpeng Zhang</i>	

Software Security

A Comparative Study of Malware Family Classification	488
<i>Rafiqul Islam and Irfan Altas</i>	
A Fine-Grained Classification Approach for the Packed Malicious Code	497
<i>Shanqing Guo, Shuangshuang Li, Yan Yu, Anlei Hu, and Tao Ban</i>	
Author Index	505