Lecture Notes in Computer Science 7232

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

Mark D. Ryan Ben Smyth Guilin Wang (Eds.)

Information Security Practice and Experience

8th International Conference, ISPEC 2012
Hangzhou, China, April 9-12, 2012
Proceedings

Springer

Volume Editors

Mark D. Ryan
University of Birmingham
School of Computer Science
Birmingham B15 2TT, UK
E-mail: mdr@cs.bham.ac.uk

Ben Smyth
Toshiba Corporation
1, Komukai-Toshiba-Cho, Saiwai-ku
Kawasaki 212-8582, Japan
E-mail: toshiba@bensmyth.com

Guilin Wang
University of Wollongong
School of Computer Science and Software Engineering
Wollongong NSW 2522, Australia
E-mail: guilin@uow.edu.au

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-29100-5 e-ISBN 978-3-642-29101-2
DOI 10.1007/978-3-642-29101-2
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.6, C.2.0, H.2.0, K.6.5, K.4.4, 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

The 8th International Conference on Information Security Practice and Experience (ISPEC 2012) was hosted by Hangzhou Normal University in Hangzhou, China, between 9–12 April 2012.

The ISPEC conference series is an established forum that brings together researchers and practitioners to provide a confluence of new information security technologies, including their applications and their integration with IT systems in various vertical sectors. In previous years, ISPEC has taken place in Singapore (2005), Hangzhou, China (2006), Hong Kong, China (2007), Sydney, Australia (2008), Xi'an, China (2009), Seoul, Korea (2010), and Guangzhou, China (2011). For all sessions, as this one, the conference proceedings were published by Springer in the *Lecture Notes in Computer Science* series.

In total, 109 papers from 20 countries were submitted to ISPEC 2012, and 27 were selected for inclusion in the proceedings (acceptance rate 25%), including 20 full papers and 7 works-in-progress. The accepted papers cover multiple topics of information security and applied cryptography. Each submission was anonymously reviewed by at least three reviewers and the majority of papers were reviewed by four reviewers. We are grateful to the Program Committee, which was composed of more than 53 well-known security experts from 16 countries; we heartily thank them as well as all external reviewers for their time and valued contributions to the tough and time-consuming reviewing process. In addition to the paper presentations, the program also featured three invited talks and we are grateful to each speaker for accepting our invitation to participate in the conference.

There are many people who contributed to the success of ISPEC 2012. We sincerely thank the Honorary Chair, Xiuyuan Yu, and the General Chairs, Robert H. Deng and Qi Xie, for their strong support. We also thank the Organizing Committee – namely, Xiumei Li, Wenhao Liu, Shengbao Wang, Xianqin Xiang, Mingrui Yu, and Zhenming Yuan – for dealing with local issues. We are grateful to the authors from around the world for submitting and presenting their papers. We are also deeply grateful to the Program Committee members for their fair review. It would have been impossible to organize ISPEC 2012 without the hard work of all our chairs and committees. Finally, we would like to thank all the participants for their contribution to ISPEC 2012.

April 2012

Mark D. Ryan
Ben Smyth
Guilin Wang

ISPEC 2012

8th International Conference on Information Security Practice and Experience

Hangzhou, China
April 9–12, 2012

Hosted by

Hangzhou Normal University, China

Honorary Chair

Xiuyuan Yu	Hangzhou Normal University, China

General Chairs

Robert H. Deng	Singapore Management University, Singapore
Qi Xie	Hangzhou Normal University, China

Program Chairs

Mark D. Ryan	University of Birmingham, UK
Guilin Wang	University of Wollongong, Australia

Program Committee

Moritz Becker	Microsoft, Cambridge, UK
Sergiu Bursuc	University of Birmingham, UK
Rohit Chadha	ENS Cachan, France
David Chadwick	University of Kent, UK
Kostas Chatzikokolakis	École Polytechnique, France
Kefei Chen	Shanghai Jiaotong University, China
Tom Chothia	University of Birmingham, UK
Sherman S.M. Chow	University of Waterloo, Canada
Richard Clayton	University of Cambridge, UK
Jason Crampton	Royal Holloway, University of London, UK
Cas Cremers	ETH Zürich, Switzerland
Stéphanie Delaune	ENS Cachan, France
Xuhua Ding	Singapore Management University, Singapore
Pooya Farshim	TU Darmstadt, Germany
Flavio D. Garcia	Radboud University Nijmegen, The Netherlands

Dawu Gu	Shanghai Jiaotong University, China
Gerhard Hancke	Royal Holloway, University of London, UK
James Heather	University of Surrey, UK
Matt Henricksen	Institute for Infocomm Research, Singapore
Dalia Khader	University of Luxembourg, Luxembourg
Boris Köpf	IMDEA Software Institute, Spain
Steve Kremer	INRIA Nancy, France
Tieyan Li	Irdeto (Cloakware), China
Dongdai Lin	Chinese Academy of Science, China
Peng Liu	Pennsylvania State University, USA
Subhamoy Maitra	Indian Statistical Institute, India
Andrew Martin	University of Oxford, UK
Kanta Matsuura	University of Tokyo, Japan
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Sebastian Mödersheim	DTU Informatics, Denmark
Yi Mu	University of Wollongong, Australia
Shishir Nagaraja	IIIT Delhi, India
Eiji Okamoto	University of Tsukuba, Japan
Alfredo Pironti	INRIA, France
Saša Radomirović	Université du Luxembourg, Luxembourg
Douglas S. Reeves	North Carolina State University, USA
Kouichi Sakurai	Kyushu University, Japan
Ben Smyth	Toshiba Corporation, Japan
Sriramkrishnan Srinivasan	University of Surrey, UK
Tomasz Truderung	University of Trier, Germany
Bogdan Warinschi	University of Bristol, UK
Jian Weng	Jinan University, China
Duncan S. Wong	City University of Hong Kong, China
Yongdong Wu	Institute for Infocomm Research, Singapore
Yang Xiang	Deakin University, Australia
Jeff Yan	Newcastle University, UK
Danfeng Yao	Virginia Tech, USA
Sung-Ming Yen	National Central University, Taiwan
Hongbo Yu	Tsinghua University, China
Yong Yu	University of Electronic Science and Technology of China, China
Zhenfeng Zhang	Chinese Academy of Science, China
Yunlei Zhao	Fudan University, China
Jianying Zhou	Institute for Infocomm Research, Singapore

Publication Chair

Ben Smyth	Toshiba Corporation, Japan

Organizing Committee

Xiumei Li	Hangzhou Normal University, China
Wenhao Liu	Hangzhou Normal University, China
Shengbao Wang	Hangzhou Normal University, China
Xianqin Xiang	Hangzhou Normal University, China
Mingrui Yu	Hangzhou Normal University, China
Zhenming Yuan	Hangzhou Normal University, China

External Reviewers

Shweta Agrawal
Toru Akishita
Man Ho Au
Matteo Avalle
Joonsang Baek
Subhadeep Banik
Gilles Barthe
Rana Barua
Joseph Bonneau
Sébastien Canard
Silvio Cesare
Shan Chen
Yu Chen
Kai-Yuen Cheong
Céline Chevalier
Cheng-Kang Chu
Ozgur Dagdelen
George Danezis
Prem Laxman Das
Angelo De Caro
Gerhard De Koning Gans
Ning Ding
Ehab Elsalamouny
Jia Fan
Daniel Fett
Pierre-Alain Fouque
Steven Galbraith
David Galindo
Sugata Gangopadhyay
Wei Gao
Thomas Gross
Haihua Gu
Hauhua Gu
Fuchun Guo
Satoshi Hada
Jinguang Han
Feng Hao
Julio Cesar Hernandez-Castro
Dennis Hofheinz
Xinyi Huang
Sorina Ionica
Vincenzo Iovino
Mahavir Jhawar
Dingding Jia
Jonathan Katz
Wei Ming Khoo
Markulf Kohlweiss
Yuichi Komano
Fabien Laguillaumie
Junzuo Lai
Jean Lancrenon
Fagen Li
Juanru Li
Zhenqi Li
Hongliang Liang
Kaitai Liang
Changlu Lin
Hsi-Chung Lin
Joseph Liu
Yamin Liu
Zhen Liu
Zhiqiang Liu
Zongbin Liu
Yu Long
Haining Lu
Jiqiang Lu
Xianhui Lu
Jiqiang Lv

Sergio Maffeis
Hamid Mala
Xianping Mao
Takahiro Matsuda
Murat Moran
Steven Murdoch
Sean Murphy
David Naccache
Takashi Nishide
Kazumasa Omote
Goutam Paul
Baodong Qin
Elizabeth A. Quaglia
Mohammad Reza Reyhanitabar
Alfredo Rial
Somitra Sanadhya
Santanu Sarkar
Patrick Schweitzer
Michael Scott
Sourav Sen Gupta
Taizo Shirai
Masaaki Shirase
Riccardo Sisto
Efstathios Stathakidis
Graham Steel
Koutarou Suzuki
Katsuyuki Takashima
Xiao Tan
Qiang Tang
Stefan Tillich
Jheng-Hong Tu
Max Tuengerthal
Joop Van De Pol
Roel Verdult
Andreas Vogt
Daoshun Wang
Jun Wang
Liangliang Wang
Yu Wang
Gaven J. Watson
Robert Watson
Lingbo Wei
Yongzhuang Wei
Sheng Wen
Gaoyao Xiao
Zhi Xin
Xi Xiong
Yanjiang Yang
Rehana Yasmin
Tomoko Yonemura
Ching-Hua Yu
S. Yu
Tsz Hon Yuen
Greg Zaverucha
Hailong Zhang
Jun Zhang
Shengzhi Zhang
Wei Zhang
Xusheng Zhang
Zongyang Zhang
Mingyi Zhao
Bin Zhu

Table of Contents

Digital Signatures

Public Key Cryptography

Cryptanalysis I: Differential Attacks

Applications I.i: Oblivious Transfer

Applications I.ii: Internet Security (Works-in-Progress)

Key Management

Applied Cryptography

Applications II.i: PINs

Applications II.ii: Fundamentals (Works-in-Progress)

Cryptanalysis II: Fault Attacks and Key Recovery

Cryptanalysis III: Key Recovery (Works-in-Progress)