

Lecture Notes in Computer Science

2727

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Rei Safavi-Naini Jennifer Seberry (Eds.)

Information Security and Privacy

8th Australasian Conference, ACISP 2003
Wollongong, Australia, July 9-11, 2003
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Rei Safavi-Naini
Jennifer Seberry
University of Wollongong
School of Information Technology and Computer Science
Wollongong, NSW 2522, Australia
E-mail: {rei,jennifer_seberry}@uow.edu.au

Cataloging-in-Publication Data applied for

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

ISSN 0302-9743

ISBN 3-540-40515-1 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH
Printed on acid-free paper SPIN: 10929049 06/3142 5 4 3 2 1 0

Preface

The 8th Australasian Conference on Information Security and Privacy (ACISP 2003) was held in Wollongong, 9–11 July, 2003. The conference was sponsored by the Australasian Computer Society, the School of Information Technology and Computer Science of the University of Wollongong, and the Smart Internet Technology Collaborative Research Centre. The conference was organized cooperatively with the IEEE-CS Task Force on Information Assurance.

The conference brought together researchers and practitioners, from academia, industry and government, with interests in information security and privacy. The conference program included 42 papers covering a wide range of topics including cryptography and cryptanalysis, network security and system security. The papers were selected from 158 submissions after an extensive and careful refereeing process in which each paper was reviewed by at least 3 members of the program committee. Of the accepted papers there were 11 from Korea, 9 from Japan, 6 from Australia, 3 from Taiwan, 2 each from Singapore and the USA, and 1 each from Canada, China, Denmark, France, Germany, India, Italy, Saudi Arabia, and Spain.

There were four invited speakers for the conference: Prof. Andrew Odlyzko (Digital Media Center, University of Minnesota, USA), Prof. Chris Mitchell (Information Security Group, Royal Holloway, University of London, UK), Dr. Li Gong (Sun Microsystems), and Prof. Gerard Milburn (University of Queensland, Australia).

We appreciate the diligence and hard work of the ACISP 2003 Program Committee. The committee benefited from the reviews and comments of many other experts: Aggelos Kiayias, Alex Dent, Alice Silverberg, Anand Desai, Andrew Clark, Atsuko Miyaji, Atsushi Fujioka, Beatrice Peirani, Bill Millan, Carine Boursier, Chi-Jen Lu, Chieng-Ning Chen, Chong Hee Kim, Christophe Tymen, Claude Carlet, Dae Hyun Yum, Darrel Hankerson, Dong Jin Park, Dong To, Drew Dean, Eiichiro Fujisaki, Eric Brier, Eric Chen, Fabienne Cathala, Gareth Brisbane, Gary Carter, Geraint Price, Gildas Avoine, Glenn Durfee, Gonzalvo Benoit, Greg Maitland, Hao-Chi Wong, Helena Handschu, Hsi-Chung Lin, Huaxiong Wang, Hung-Min Sun, In Kook Park, Jason Crampton, Jason Reid, Jean Monnerat, Jean-Sebastien Coron, Ji Hyun Jeong, John Proos, Jong Hoon Shin, Juan Manuel Gonzalez Nieto, Julien Bouchier, Kapali Viswanathan, Kazumaro Aoki, Khanh Nguyen, Koji Chida, Koji Chida, Koutarou Suzuki, Laurent Gauteron, Lionel Victor, Lu Yi, Ludovic Rousseau, Marc Joye, Mariusz Jakobowski, Mark Bauer, Mark Looi, Matt Henricksen, Min-Shiang Hwang, Nicholas Sheppard, Nicolas Courtois, Oleg Sheyner, Pascal Junod, Pascal Paillier, Philippe Oechslin, Pierre Girard, Ron Steinfeld, Sang Gyoo Sim, Sang Yun Han, Satomi Okazaki, Scarlet Schwiderski-Grosche, Shin'ichiro Matsuo, Simon Blackburn, Siu-Leung Chung, Svein Knapskog, Swee-Huay Heng, Takayuki Yamada, Teresa Lunt, Tetsu Iwata, Thomas Martin, Tung-Shou Chen, Wataru Kishimoto,

Willy Susilo, Xianmo Zhang, Xuli Wang, Yasuhiro Ohtaki, Yeon Hyeong Yang, Yi Lu, Yong Ho Hwang, and Zhi Guo.

The organizing committee was co-chaired by Dr. Willy Susilo and Prof. Jennifer Seberry. Special thanks to Takeyuki Uehara, Rongbo Du and Stephen Haynes for their technical support, to Takeyuki Uehara and Yejing Wang for their help with the local organization, and the following volunteers whose help allowed us to run the conference smoothly: Hartono Kurnio, Luke McAven, Nicholas Sheppard, Tianbing Xia, Nathan Curtis, David Haryanto, Yibing Kong, Gelareh Taban, and Rungrat Wiangsripanawan.

On behalf of all those involved in organizing the conference, we would like to thank the authors of all submitted papers, those who presented their work and those who participated in the conference: their work and contributions made the conference a great success.

July 2003

Rei Safavi-Naini

Australasian Conference on Information Security and Privacy ACISP 2003

Sponsored by
School of Information Technology and Computer Science of the
University of Wollongong
Australian Computer Society
Smart Internet Technology Cooperative Research Centre

In cooperation with
IEEE-CS Task Force on Information Assurance

General Chairs

Jennifer Seberry
Willy Susilo

University of Wollongong, Australia
University of Wollongong, Australia

Program Chair

Rei Safavi-Naini

University of Wollongong, Australia

Program Committee

Masayuki Abe
Lynn Batten
Colin Boyd
Ed Dawson
Dieter Gollmann
Jim Hughes
Kaoru Kurosawa
Kwok-Yan Lam
Chi-Sung Laih
Pil Joong Lee
Keith Martin
Mitsuru Matsui
Alfred Menezes
Yi Mu
David Naccache

NTT, Japan
Deakin University, Australia
Queensland University of Technology, Australia
Queensland University of Technology, Australia
Microsoft, UK
StorageTek, US
Ibaraki University, Japan
Tsinghua University, China
National Cheng Kung University, Taiwan
Pohang University of Science and Technology, Korea
Royal Holloway, University of London, UK
Mitsubishi Electric, Japan
University of Waterloo, Canada
University of Wollongong, Australia
Gemplus, France

VIII Program Committee

Dingyi Pei	<i>Chinese Academy of Sciences, China</i>
Josef Pieprzyk	<i>Macquarie University, Australia</i>
Pandu Rangan	<i>Indian Institute of Technology, Madras, India</i>
Greg Rose	<i>Qualcomm, Australia</i>
Jessica Staddon	<i>Palo Alto Research Center, US</i>
Vijay Varharadjan	<i>Macquarie University, Australia</i>
Serge Vaudeney	<i>EPFL (Swiss Fed. Inst. of Tech. Lausanne), Switzerland</i>
Eric Verheul	<i>PricewaterhouseCoopers, The Netherlands</i>
Chee Sun Won	<i>Dongguk University, Korea</i>
Sung-Ming Yen	<i>National Central University, Taiwan</i>
Moti Yung	<i>Columbia University, US</i>

Table of Contents

Privacy and Anonymity

Grouping Verifiable Content for Selective Disclosure	1
<i>Laurence Bull, David McG. Squire, Jan Newmarch, Yuliang Zheng</i>	
Evaluation of Anonymity of Practical Anonymous Communication Networks	13
<i>Shigeki Kitazawa, Masakazu Soshi, Atsuko Miyaji</i>	
An Anonymous Credential System and a Privacy-Aware PKI	27
<i>Pino Persiano, Ivan Visconti</i>	
Flaws in Some Robust Optimistic Mix-Nets	39
<i>Masayuki Abe, Hideki Imai</i>	

Invited Talk (I)

The Unsolvable Privacy Problem and Its Implications for Security Technologies	51
<i>Andrew Odlyzko</i>	

Elliptic Curves

The Security of Fixed versus Random Elliptic Curves in Cryptography ..	55
<i>Yvonne Hitchcock, Paul Montague, Gary Carter, Ed Dawson</i>	
Cryptanalysis of the Full Version Randomized Addition-Subtraction Chains	67
<i>Dong-Guk Han, Nam Su Chang, Seok Won Jung, Young-Ho Park, Chang Han Kim, Heuisu Ryu</i>	
Generic $GF(2^m)$ Arithmetic in Software and Its Application to ECC	79
<i>André Weimerskirch, Douglas Stebila, Sheueling Chang Shantz</i>	
An Addition Algorithm in Jacobian of C_{34} Curve	93
<i>Seigo Arita</i>	

Cryptanalysis (I)

Amplified Differential Power Cryptanalysis on Rijndael Implementations with Exponentially Fewer Power Traces	106
<i>Sung-Ming Yen</i>	

Differential Fault Analysis on AES Key Schedule and Some Countermeasures	118
<i>Chien-Ning Chen, Sung-Ming Yen</i>	
On the Pseudorandomness of KASUMI Type Permutations	130
<i>Tetsu Iwata, Tohru Yagi, Kaoru Kurosawa</i>	
Theoretical Analysis of χ^2 Attack on RC6	142
<i>Masahiko Takenaka, Takeshi Shimoyama, Takeshi Koshihara</i>	

Mobile and Network Security

A Typed Theory for Access Control and Information Flow Control in Mobile Systems	154
<i>Libin Wang, Kefei Chen</i>	
Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach	166
<i>Yiu Shing Terry Tin, Colin Boyd, Juan Manuel González Nieto</i>	
Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications	180
<i>Jabeom Gu, Sehyun Park, Ohyoung Song, Jaehil Lee, Jaehoon Nah, Sungwon Sohn</i>	
Practical Pay TV Schemes	192
<i>Arvind Narayanan, C. Pandu Rangan, Kwangjo Kim</i>	
Cooperative Routers against DoS Attacks	204
<i>Ha Yoon Song, Han-gyoo Kim</i>	
Detecting Distributed Denial of Service Attacks by Sharing Distributed Beliefs	214
<i>Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao</i>	
Malicious ICMP Tunneling: Defense against the Vulnerability.....	226
<i>Abhishek Singh, Ola Nordström, Chenghui Lu, Andre L.M. dos Santos</i>	
On Fair E-cash Systems Based on Group Signature Schemes	237
<i>Sébastien Canard, Jacques Traoré</i>	

Invited Talk (II)

A Taxonomy of Single Sign-On Systems	249
<i>Andreas Pashalidis, Chris J. Mitchell</i>	

Cryptanalysis (II)

Key Recovery Attacks on the RMAC, TMAC, and IACBC	265
<i>Jaechul Sung, Deukjo Hong, Sangjin Lee</i>	
Key Recovery Attacks on NTRU without Ciphertext Validation Routine	274
<i>Daewan Han, Jin Hong, Jae Woo Han, Daesung Kwon</i>	
Permanent Fault Attack on the Parameters of RSA with CRT	285
<i>Sung-Ming Yen, SangJae Moon, JaeCheol Ha</i>	
Backdoor Attacks on Black-Box Ciphers Exploiting Low-Entropy Plaintexts	297
<i>Adam Young, Moti Yung</i>	

Signature

Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings	312
<i>Fangguo Zhang, Kwangjo Kim</i>	
Digital Signature Schemes with Restriction on Signing Capability	324
<i>Jung Yeon Hwang, Hyun-Jeong Kim, Dong Hoon Lee, JongIn Lim</i>	
On the Exact Security of Multi-signature Schemes Based on RSA	336
<i>Kei Kawauchi, Mitsuru Tada</i>	

Cryptosystems (I)

A Length-Flexible Threshold Cryptosystem with Applications	350
<i>Ivan Damgård, Mads Jurik</i>	
Separating Encryption and Key Issuance in Digital Rights Management Systems	365
<i>Goichiro Hanaoka, Kazuto Ogawa, Itsuro Murota, Go Ohtake, Keigo Majima, Kimiyuki Oyamada, Seiichi Gohshi, Seiichi Namba, Hideki Imai</i>	
An Efficient Revocation Scheme with Minimal Message Length for Stateless Receivers	377
<i>Yong Ho Hwang, Chong Hee Kim, Pil Joong Lee</i>	
Parallel Authentication and Public-Key Encryption	387
<i>Josef Pieprzyk, David Pointcheval</i>	

Invited Talk (III)

Is Cross-Platform Security Possible?	402
<i>Li Gong</i>	

Cryptosystems (II)

A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems	403
<i>Jason Reid, Ian Cheong, Matthew Henricksen, Jason Smith</i>	
Cryptanalysis of a New Cellular Automata Cryptosystem	416
<i>Feng Bao</i>	
A CCA2 Secure Key Encapsulation Scheme Based on 3rd Order Shift Registers	428
<i>Chik How Tan, Xun Yi, Chee Kheong Siew</i>	
Clock-Controlled Shrinking Generator of Feedback Shift Registers	443
<i>Ali Kanso</i>	

Key Management

EPA: An Efficient Password-Based Protocol for Authenticated Key Exchange	452
<i>Yong Ho Hwang, Dae Hyun Yum, Pil Joong Lee</i>	
Constructing General Dynamic Group Key Distribution Schemes with Decentralized User Join	464
<i>Vanesa Daza, Javier Herranz, Germán Sáez</i>	
Robust Software Tokens – Yet Another Method for Securing User’s Digital Identity	476
<i>Taekyoung Kwon</i>	

Theory and Hash Functions

Public-Key Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders	488
<i>Hwankoo Kim, SangJae Moon</i>	
New Constructions for Resilient and Highly Nonlinear Boolean Functions	498
<i>Khoongming Khoo, Guang Gong</i>	
On Parallel Hash Functions Based on Block-Cipher	510
<i>Toshihiko Matsuo, Kaoru Kurosawa</i>	
Square Hash with a Small Key Size	522
<i>Swee-Huay Heng, Kaoru Kurosawa</i>	

Author Index	533
---------------------------	------------