

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

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

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Yi Mu Willy Susilo Jennifer Seberry (Eds.)

Information Security and Privacy

13th Australasian Conference, ACISP 2008
Wollongong, Australia, July 7-9, 2008
Proceedings



Springer

Volume Editors

Yi Mu

Willy Susilo

Jennifer Seberry

University of Wollongong

School of Computer Science and Software Engineering

Northfields Avenue, Wollongong, NSW 2522, Australia

E-mail: {ymu, wsusilo, jennie}@uow.edu.au

Library of Congress Control Number: Applied for

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-69971-6 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-69971-2 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

© Springer-Verlag Berlin Heidelberg 2008

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12322725 06/3180 5 4 3 2 1 0

Preface

The 13th Australasian Conference on Information Security and Privacy (ACISP 2008) was held at Wollongong, Australia, during July 7–9, 2008. The conference was sponsored by the Centre for Computer and Information Security of the University of Wollongong and the Research Network for a Secure Australia. The submission and review process was run using the iChair software, written by Thomas Baigneres and Matthieu Finiasz from EPFL, LASEC, Switzerland. We would like to thank them for letting us use their iChair software.

The conference received 111 submissions, out of which the Program Committee selected 33 papers for presentation at the conference after a rigorous review process. These papers are included in the proceedings. The accepted papers cover a range of topics in information security, including authentication, key management, public key cryptography, privacy, anonymity, secure communication, ciphers, network security, elliptic curves, hash functions, and database security. The conference proceedings contain revised versions of the selected papers. Since some of them were not checked again for correctness before publication, the authors bear full responsibility for the contents of their papers. We would like to thank the authors of all papers for submitting their papers to the conference.

In addition to the contributed papers, the program comprised three invited talks. The invited speakers were Xavier Boyen (Voltage, USA), Josef Pieprzyk (Macquarie University, Australia) and Nigel Phair (Australian High Tech Crime Centre). We would like to express our thanks to them.

As in previous years, we selected a “best student paper.” To be eligible for selection, a paper has to be co-authored by a postgraduate student, whose contribution was more than 50%. The winner was Risto Hakala from Helsinki University of Technology, Finland, for the paper “Linear Distinguishing Attack on Shannon.”

We would like to thank all the people who helped with the conference program and organization. In particular, we heartily thank the Program Committee and the sub-reviewers listed on the following pages for the effort and time they contributed to the review process. We would like to express our thanks to Springer for continuing to support the ACISP conference and for help in the conference proceedings production.

Finally, we would like to thank the Organizing Committee for their excellent contribution to the conference.

July 2008

Yi Mu
Willy Susilo
Jennifer Seberry

The 13th Australasian Conference on Information Security and Privacy (ACISP 2008)

Sponsored by

Centre for Computer and Information Security Research,
University of Wollongong, Australia

Research Network for a Secure Australia

General Chair

Jennifer Seberry University of Wollongong, Australia

Program Chairs

Yi Mu University of Wollongong, Australia

Willy Susilo University of Wollongong, Australia

Program Committee

Michel Abdalla	ENS, Paris, France
Masayuki Abe	NTT, Japan
Colin Boyd	QUT, Australia
Feng Bao	Institute for Infocomm Research, Singapore
Lynn Batten	Deakin University, Australia
Ed Dawson	QUT, Australia
Dieter Gollmann	TU Hamburg, Germany
Aggelos Kiayias	University of Connecticut, USA
Kwangjo Kim	ICU, Korea
Tanja Lange	Technische Universiteit Eindhoven, Netherlands
Pil Joong Lee	Pohang University of Science and Technology, Korea
Benoit Libert	UCL, Belgium
Javier Lopez	University of Malaga, Spain
Chris Mitchell	RHUL, UK
Yi Mu	University of Wollongong, Australia
Kaisa Nyberg	Helsinki University of Technology, Finland
Eiji Okamoto	Tsukuba University, Japan
Josef Pieprzyk	Macquarie University, Australia
Sihan Qing	Chinese Academy of Sciences, China
Jean-Jacques Quisquater	UCL, Belgium
Rei Safavi-Naini	University of Calgary, Canada

Jennifer Seberry	University of Wollongong, Australia
Ron Steinfeld	Macquarie University, Australia
Douglas Stinson	University of Waterloo, Canada
Willy Susilo	University of Wollongong, Australia
C. Pandu Rangan	Indian Institute of Technology, India
Tsuyoshi Takagi	Future University, Japan
Vijay Varadharajan	Macquarie University, Australia
Sabrina De Capitani di Vimercati	University of Milan, Italy
Huaxiong Wang	Nanyang Technological University, Singapore
Duncan S. Wong	City University of Hong Kong, China
Fangguo Zhang	Sun Yat-Sen University, China
Ning Zhang	University of Manchester, UK
Jianying Zhou	Institute for Infocomm Research, Singapore

Organizing Committee

Man Ho Au	University of Wollongong, Australia
Xinyi Huang	University of Wollongong, Australia
Shams Ud Din Qazi	University of Wollongong, Australia
Mohammad Reza Reyhanitabar	University of Wollongong, Australia
Siamak Fayyaz	
Shahandashti	University of Wollongong, Australia
Pairat Thorncharoensri	University of Wollongong, Australia
Wei Wu	University of Wollongong, Australia
Tsz Hon Yuen	University of Wollongong, Australia

External Referees

Isaac Agudo	Reza Rezaeian Farashahi	Jang Seong Kim
Hadi Ahmadi	Gerardo Fernandez	Sun Young Kim
K. Ambika	Carmen Fernandez-Gago	Young Mok Kim
Venkat Balakrishnan	Georg Fuchsbaue	Varad Kirthane
Daniel J. Bernstein	Juan Garay	Hoi Le
Jean-Luc Beuchet	Praveen Gauravaram	Fagen Li
Peter Birkner	Juan Gonzalez	Jin Li
Billy Bob Brumley	Satoshi Hada	Vo Duc Liem
S. Chandrasekar	Risto Hakala	Peter van Liesdonk
Joo Yeon Cho	Kevin Henry	Joseph K. Liu
Sherman Chow	Matt Henricksen	Jiqiang Lu
Baudoin Collard	Jason Hinek	Mark Manulis
Alex Dent	Michael Hitchens	Krystian Matusiewicz
Dang Nguyen Duc	Qiong Huang	Antonina Mitrofanova
Sung Wook Eom	Shaoquan Jiang	Cameron McDonald

Pablo Najera	Igor Shparlinski	Jiang Wu
Miyako Ohkubo	Leonie Simpson	Guomin Yang
Vijayakrishnan P.	Michal Sramka	Yanjiang Yang
Arpita Patra	Jerry Sui	Yeon-Hyeong Yang
Angela Piper	Christophe Tartary	Chan Yeob Yeun
M.R. Reyhanitabar	Ronghua Tian	Hongbo Yu
Rodrigo Roman	Tomas Toft	Yu Yu
Chun Ruan	Mohammed A.A. Tuhin	Janson Zhang
Palash Sarkar	Udaya Kiran Tupakula	Chang-An Zhao
Sharmila Devi Selvi	Damien Vergnaud	Weiliang Zhao
Jae Woo Seo	José Villegas	Hong-Sheng Zhou
Siamak Shahandashti	Jose L. Vivas	Huafei Zhu
Hongsong Shi	Yongge Wang	Sebastien Zimmer
Jong Hoon Shin	Baodian Wei	
Masaaki Shirase	Kenneth Wong	

Table of Contents

New Paradigms for Password Security: Abstract from the Keynote Lecture	1
<i>Xavier Boyen</i>	
Enforcing User-Aware Browser-Based Mutual Authentication with Strong Locked Same Origin Policy	6
<i>Sebastian Gajek, Mark Manulis, and Jörg Schwenk</i>	
Secure Biometric Authentication with Improved Accuracy	21
<i>Manuel Barbosa, Thierry Brouard, Stéphane Cauchie, and Simão Melo de Sousa</i>	
A Critical Analysis and Improvement of AACS Drive-Host Authentication	37
<i>Jiayuan Sui and Douglas R. Stinson</i>	
Comparing the Pre- and Post-specified Peer Models for Key Agreement	53
<i>Alfred Menezes and Berkant Ustaoglu</i>	
Efficient One-Round Key Exchange in the Standard Model	69
<i>Colin Boyd, Yvonne Cliff, Juan Gonzalez Nieto, and Kenneth G. Paterson</i>	
On the Improvement of the BDF Attack on LSBS-RSA	84
<i>Hung-Min Sun, Mu-En Wu, Huaxiong Wang, and Jian Guo</i>	
Public-Key Cryptosystems with Primitive Power Roots of Unity	98
<i>Takato Hirano, Koichiro Wada, and Keisuke Tanaka</i>	
Relationship between Two Approaches for Defining the Standard Model PA-ness	113
<i>Isamu Teranishi and Wakaha Ogata</i>	
Distributed Verification of Mixing - Local Forking Proofs Model	128
<i>Jacek Cichoń, Marek Klonowski, and Mirosław Kutylowski</i>	
Fully-Simulatable Oblivious Set Transfer	141
<i>Huafei Zhu</i>	
Efficient Disjointness Tests for Private Datasets	155
<i>Qingsong Ye, Huaxiong Wang, Josef Pieprzyk, and Xian-Mo Zhang</i>	

Efficient Perfectly Reliable and Secure Message Transmission Tolerating Mobile Adversary	170
<i>Arpita Patra, Ashish Choudhary, Madhu Vaidyanathan, and C. Pandu Rangan</i>	
Methods for Linear and Differential Cryptanalysis of Elastic Block Ciphers	187
<i>Debra L. Cook, Moti Yung, and Angelos D. Keromytis</i>	
Multidimensional Linear Cryptanalysis of Reduced Round Serpent	203
<i>Mia Hermelin, Joo Yeon Cho, and Kaisa Nyberg</i>	
Cryptanalysis of Reduced-Round SMS4 Block Cipher	216
<i>Lei Zhang, Wentao Zhang, and Wenling Wu</i>	
On the Unprovable Security of 2-Key XCBC	230
<i>Peng Wang, Dengguo Feng, Wenling Wu, and Liting Zhang</i>	
Looking Back at a New Hash Function	239
<i>Olivier Billet, Matthew J.B. Robshaw, Yannick Seurin, and Yiqun Lisa Yin</i>	
Non-linear Reduced Round Attacks against SHA-2 Hash Family	254
<i>Somitra Kumar Sanadhya and Palash Sarkar</i>	
Collisions for Round-Reduced LAKE	267
<i>Florian Mendel and Martin Schl��ffer</i>	
Preimage Attacks on Step-Reduced MD5.....	282
<i>Yu Sasaki and Kazumaro Aoki</i>	
Linear Distinguishing Attack on Shannon	297
<i>Risto M. Hakala and Kaisa Nyberg</i>	
Recovering RC4 Permutation from 2048 Keystream Bytes if j Is Stuck.....	306
<i>Subhamoy Maitra and Goutam Paul</i>	
Related-Key Chosen IV Attacks on Grain-v1 and Grain-128	321
<i>Yuseop Lee, Kitae Jeong, Jaechul Sung, and Seokhie Hong</i>	
Signature Generation and Detection of Malware Families	336
<i>V. Sai Sathyanarayan, Pankaj Kohli, and Bezawada Bruhadeshwar</i>	
Reducing Payload Scans for Attack Signature Matching Using Rule Classification	350
<i>Sunghyun Kim and Heejo Lee</i>	
Implicit Detection of Hidden Processes with a Feather-Weight Hardware-Assisted Virtual Machine Monitor	361
<i>Yan Wen, Jinjing Zhao, Huaimin Wang, and Jiannong Cao</i>	

FormatShield: A Binary Rewriting Defense against Format String Attacks	376
<i>Pankaj Kohli and Bezawada Bruhadeshwar</i>	
Advanced Permission-Role Relationship in Role-Based Access Control	391
<i>Min Li, Hua Wang, Ashley Plank, and Jianming Yong</i>	
Enhancing Micro-Aggregation Technique by Utilizing Dependence-Based Information in Secure Statistical Databases	404
<i>B. John Oommen and Ebaa Fayyouri</i>	
Montgomery Residue Representation Fault-Tolerant Computation in $GF(2^k)$	419
<i>Silvana Medoš and Serdar Boztas</i>	
A Tree-Based Approach for Computing Double-Base Chains	433
<i>Christophe Doche and Laurent Habsieger</i>	
Extractors for Jacobians of Binary Genus-2 Hyperelliptic Curves	447
<i>Reza Rezaeian Farashahi</i>	
Efficient Modular Arithmetic in Adapted Modular Number System Using Lagrange Representation	463
<i>Christophe Negre and Thomas Plantard</i>	
Author Index	479