

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

Kazuo Sakiyama Masayuki Terada (Eds.)

Advances in Information and Computer Security

8th International Workshop on Security, IWSEC 2013
Okinawa, Japan, November 18-20, 2013
Proceedings



Springer

Volume Editors

Kazuo Sakiyama
The University of Electro-Communications
Department of Informatics
1-5-1 Chofugaoka, Chofu
Tokyo 182-8585, Japan
E-mail: sakiyama@uec.ac.jp

Masayuki Terada
NTT DOCOMO, Inc.
Research Laboratories
3-6 Hikari-no-oka, Yokosuka
Kanagawa 239-8536, Japan
E-mail: teradam@nttdocomo.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-41382-7 e-ISBN 978-3-642-41383-4
DOI 10.1007/978-3-642-41383-4
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013949481

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, 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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

IWSEC 2013, the 8th International Workshop on Security, was held at Okinawaken Shichouson Jichikaikan in Okinawa, Japan, during November 18–20, 2013. The workshop was co-organized by ISEC in ESS of IEICE (Technical Committee on Information Security in Engineering Sciences Society of the Institute of Electronics, Information and Communication Engineers) and CSEC of IPSJ (Special interest group on Computer Security of the Information Processing Society of Japan).

We received 63 submissions, of which 20 were accepted for publication. Each submission was anonymously reviewed by at least three reviewers, and these proceedings contain the revised versions of the accepted papers. There were also two keynote talks that were selected at the discretion of the general co-chairs and program co-chairs. The talks were given by Sebastian Faust and Nobuaki Hoshino. In addition to the presentations of the papers and the keynote talks, the workshop also featured a poster session.

The Best Paper Award was given to “Solving Google’s Continuous Audio CAPTCHA with HMM-Based Automatic Speech Recognition,” by Shotaro Sano, Takuma Otsuka, and Hiroshi G. Okuno, and the Best Student Paper Award was given to “Improvement of Faugère *et al.*’s Method to Solve ECDLP,” by Huang Yun-Ju, Christophe Petit, Naoyuki Shinohara, and Tsuyoshi Takagi.

Our deepest appreciation goes to the Program Committee. The selection of the papers was a challenging and delicate task, and we are deeply grateful to the members of the Program Committee and the external reviewers for their in-depth reviews and detailed discussions.

A number of people contributed to the success of IWSEC 2013. We would like to thank all of the authors of submissions. Their great work made IWSEC 2013 a worthwhile conference. We are also grateful to Andrei Voronkov for developing EasyChair, which was used for the paper submission, reviews, discussions, and preparation of these proceedings.

Last but not least, we would like to thank the general co-chairs, Toshiaki Tanaka and Masakatsu Nishigaki, for leading the local Organizing Committee, and we also would like to thank the members of the local Organizing Committee for their dedicated efforts to ensure the smooth running of the workshop.

August 2013

Kazuo Sakiyama
Masayuki Terada

IWSEC 2013

8th International Workshop on Security

Okinawa, Japan, November 18–20, 2013

Co-organized by

ISEC in ESS of IEICE

(Technical Committee on Information Security in Engineering Sciences Society
of the Institute of Electronics, Information and Communication Engineers)

and

CSEC of IPSJ

(Special interest group on Computer Security of the Information Processing
Society of Japan)

General Co-chairs

Toshiaki Tanaka

Masakatsu Nishigaki

KDDI R&D Laboratories Inc., Japan

Shizuoka University, Japan

Advisory Committee

Hideki Imai

Kwangjo Kim

Chuo University, Japan

Korea Advanced Institute of Science and
Technology, Korea

Günter Müller

Yuko Murayama

Koji Nakao

University of Freiburg, Germany

Iwate Prefectural University, Japan

National Institute of Information and
Communications Technology, Japan

Eiji Okamoto

C. Pandu Rangan

Ryoichi Sasaki

University of Tsukuba, Japan

Indian Institute of Technology, Madras, India

Tokyo Denki University, Japan

Program Co-chairs

Kazuo Sakiyama

Masayuki Terada

University of Electro-Communications, Japan

NTT DOCOMO, Inc., Japan

Local Organizing Committee

Yuki Ashino	NEC, Japan
Takuro Hosoi	The University of Tokyo, Japan
Takehisa Kato	IPA, Japan
Akinori Kawachi	Tokyo Institute of Technology, Japan
Yuichi Komano	Toshiba, Japan
Koji Nuida	AIST, Japan
Anand Prasad	NEC, Japan
Kouichi Sakurai	Kyushu University, Japan
Yuji Suga	Internet Initiative Japan Inc., Japan
Mio Suzuki	National Institute of Information and Communications Technology, Japan
Alf Zugenmaier	Munich Universities of Applied Sciences, Germany

Program Committee

Rafael Accorsi	University of Freiburg, Germany
Toru Akishita	The University of Tokyo, Japan
Claudio Ardagna	Università degli Studi di Milano, Italy
Nuttapong Attrapadung	AIST, Japan
Andrey Bogdanov	Technical University of Denmark, Denmark
Sanjit Chatterjee	Indian Institute of Science, India
Koji Chida	NTT, Japan
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Bart De Decker	Katholieke Universiteit Leuven, Belgium
Isao Echizen	National Institute of Informatics, Japan
Sebastian Faust	EPFL, Switzerland
Dario Fiore	Max Planck Institute for Software Systems, Germany
Eiichiro Fujisaki	NTT, Japan
David Galindo	CNRS/LORIA, France
Dieter Gollmann	Hamburg University of Technology, Germany
Goichiro Hanaoka	AIST, Japan
Swee-Huay Heng	Multimedia University, Malaysia
Naofumi Homma	Tohoku University, Japan
Mitsugu Iwamoto	University of Electro-Communications, Japan
Tetsu Iwata	Nagoya University, Japan
Angelos Keromytis	Columbia University, USA
Hiroaki Kikuchi	Meiji University, Japan
Hyung Chan Kim	ETRI, Korea
Takeshi Koshihira	Saitama University, Japan
Noboru Kunihira	The University of Tokyo, Japan
Kwok-Yan Lam	National University of Singapore, Singapore

Kanta Matsuura	The University of Tokyo, Japan
Koichi Mouri	Ritsumeikan University, Japan
Takashi Nishide	University of Tsukuba, Japan
Wakaha Ogata	Tokyo Institute of Technology, Japan
Takeshi Okamoto	Tsukuba University of Technology, Japan
Thomas Peyrin	Nanyang Technological University, Singapore
Raphael Phan	Multimedia University, Malaysia
Axel Poschmann	Nanyang Technological University, Singapore
Anand Prasad	NEC, Japan
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Kai Rannenber	Goethe University Frankfurt, Germany
Yu Sasaki	NTT, Japan
Patrick Schaumont	Virginia Tech., USA
Joshua Schiffman	AMD, USA
Jae Hong Seo	Myongji University, Korea
Francesco Sica	Nazarbayev University, Kazakhstan
Yuji Suga	Internet Initiative Japan Inc., Japan
Takeshi Sugawara	Mitsubishi Electric Corporation, Japan
Tsuyoshi Takagi	Kyushu University, Japan
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Satoru Tezuka	Tokyo University of Technology, Japan
Ryuya Uda	Tokyo University of Technology, Japan
Damien Vergnaud	ENS, France
Guilin Wang	University of Wollongong, Australia
Jian Weng	Jinan University, China
Sven Wohlgemuth	Technische Universität Darmstadt, Germany
Keita Xagawa	NTT, Japan
Dai Yamamoto	Fujitsu Laboratories, Japan
Toshihiro Yamauchi	Okayama University, Japan
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Kazuki Yoneyama	NTT, Japan
Maki Yoshida	Osaka University, Japan
Katsunari Yoshioka	Yokohama National University, Japan
Hiroshi Yoshiura	University of Electro-Communications, Japan
Rui Zhang	CAS, China
Yunlei Zhao	Fudan University, China
Alf Zugenmaier	Munich Universities of Applied Sciences, Germany

External Reviewers

Elias Athanasopoulos	Olivier Blazy	Ji-Jian Chin
Aydin Aysu	Christina Boura	Keita Emura
Rouzbeh Behnia	Chien-Ning Chen	Sho Endo
Begül Bilgin	Shan Chen	Aurore Guillevic

Jian Guo	Sascha Koschinat	Kyoji Shibutani
Koki Hamada	Sebastian Kutzner	Koichi Shimizu
Yoshikazu Hanatani	Martin M. Lauridsen	Seonghan Shin
Ryotaro Hayashi	Hyung Tae Lee	Koutarou Suzuki
Matthias Hiller	Zhenhua Liu	Mostafa Taha
Takato Hirano	Atul Luykx	Syh-Yuan Tan
Masatsugu Ichino	Changshe Ma	Mehdi Tibouchi
Dai Ikarashi	Takahiro Matsuda	Markus Tschersich
Motohiko Isaka	Shin'ichiro Matsuo	Shigenori Uchiyama
Kenta Ishii	Qixiang Mei	Berkant Ustaoglu
Takanori Isobe	Kunihiko Miyazaki	Daniele Venturi
Tadahiko Ito	Kirill Morozov	Srinivas Vivek
Kangkook Jee	Pratyay Mukherjee	Dai Watanabe
Mahavir Jhanwar	Sayantan Mukherjee	Lars Wolos
Christian Kahl	Debdeep Mukhopadhyay	Jing Xu
Satoshi Kai	Ivica Nikolic	Jun Yajima
Akira Kanaoka	Ryo Nishimaki	Shota Yamada
Akinori Kawachi	Ryo Nojima	Takashi Yamakawa
Yutaka Kawai	Toshihiro Ohigashi	Naoto Yanai
Vasileios P. Kemerlis	Akira Otsuka	Masaya Yasuda
Ryo Kikuchi	Nguyen Phuong Ha	Kenji Yasunaga
Minkyu Kim	Michalis Polychronakis	Wei-Chuen Yau
Naoto Kiribuchi	Ahmad Sabouri	Shun'ichi Yokoyama
Nobuaki Kitajima	Minoru Saeki	Hui Zhang
Hiroki Koga	Yusuke Sakai	Zongyang Zhang
Masanobu Koike	Koichi Sakumoto	
Georgios Kontaxis	Masahito Shiba	

Table of Contents

Software and System Security

Secure Log Transfer by Replacing a Library in a Virtual Machine	1
<i>Masaya Sato and Toshihiro Yamauchi</i>	
Static Integer Overflow Vulnerability Detection in Windows Binary	19
<i>Yi Deng, Yang Zhang, Liang Cheng, and Xiaoshan Sun</i>	
Solving Google’s Continuous Audio CAPTCHA with HMM-Based Automatic Speech Recognition	36
<i>Shotaro Sano, Takuma Otsuka, and Hiroshi G. Okuno</i>	
Constructions of Almost Secure Frameproof Codes Based on Small-Bias Probability Spaces	53
<i>José Moreira, Marcel Fernández, and Grigory Kabatiansky</i>	

Cryptanalysis

Differential Power Analysis of MAC-Keccak at Any Key-Length	68
<i>Mostafa Taha and Patrick Schaumont</i>	
Generic State-Recovery and Forgery Attacks on ChopMD-MAC and on NMAC/HMAC	83
<i>Yusuke Naito, Yu Sasaki, Lei Wang, and Kan Yasuda</i>	
New Property of Diffusion Switching Mechanism on CLEFIA and Its Application to DFA	99
<i>Yosuke Todo and Yu Sasaki</i>	
Improvement of Faugère <i>et al.</i> ’s Method to Solve ECDLP	115
<i>Yun-Ju Huang, Christophe Petit, Naoyuki Shinohara, and Tsuyoshi Takagi</i>	

Privacy and Cloud Computing

Statistics on Encrypted Cloud Data	133
<i>Fu-Kuo Tseng, Yung-Hsiang Liu, Rong-Jaye Chen, and Bao-Shuh Paul Lin</i>	
Toward Practical Searchable Symmetric Encryption	151
<i>Wakaha Ogata, Keita Koikiwa, Akira Kanaoka, and Shin’ichiro Matsuo</i>	

Unconditionally Secure Oblivious Transfer from Real Network Behavior 168
Paolo Palmieri and Olivier Pereira

Cryptographically-Secure and Efficient Remote Cancelable Biometrics Based on Public-Key Homomorphic Encryption 183
Takato Hirano, Mitsuhiro Hattori, Takashi Ito, and Nori Matsuda

Public Key Cryptosystems

Efficient Algorithm for Tate Pairing of Composite Order 201
Yutaro Kiyomura and Tsuyoshi Takagi

How to Factor N_1 and N_2 When $p_1 = p_2 \bmod 2^t$ 217
Kaoru Kurosawa and Takuma Ueda

Achieving Chosen Ciphertext Security from Detectable Public Key Encryption Efficiently via Hybrid Encryption 226
Takahiro Matsuda and Goichiro Hanaoka

Cryptanalysis of the Quaternion Rainbow 244
Yasufumi Hashimoto

Security Protocols

On Cheater Identifiable Secret Sharing Schemes Secure against Rushing Adversary 258
Rui Xu, Kirill Morozov, and Tsuyoshi Takagi

One-Round Authenticated Key Exchange without Implementation Trick 272
Kazuki Yoneyama

Attacks to the Proxy Re-Encryption Schemes from IWSEC2011 290
Toshiyuki Isshiki, Manh Ha Nguyen, and Keisuke Tanaka

Game-Theoretic Security for Bit Commitment 303
Haruna Higo, Keisuke Tanaka, and Kenji Yasunaga

Author Index 319