

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

Satoshi Obana · Koji Chida (Eds.)

Advances in Information and Computer Security

12th International Workshop on Security, IWSEC 2017
Hiroshima, Japan, August 30 – September 1, 2017
Proceedings

Editors
Satoshi Obana 
Hosei University
Tokyo
Japan

Koji Chida
NTT Corporation
Tokyo
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-64199-7 ISBN 978-3-319-64200-0 (eBook)
DOI 10.1007/978-3-319-64200-0

Library of Congress Control Number: 2017947500

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

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.

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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 12th International Workshop on Security (IWSEC 2017) was held at the International Conference Center Hiroshima, in Hiroshima, Japan, during August 30 – September 1, 2017. The workshop was co-organized by the Technical Committee on Information Security in Engineering Sciences Society of the Institute of Electronics, Information and Communication Engineers and the Special Interest Group on Computer Security of Information Processing Society of Japan.

This year, the workshop received 37 submissions. Finally, 11 papers were accepted as regular papers, and three papers were accepted as short papers. Each submission was anonymously reviewed by at least three reviewers, and these proceedings contain the revised versions of the accepted papers. In addition to the presentations of the papers, the workshop also featured a poster session. The keynote speeches were given by Khaled El Emam and by Kazue Sako.

The best paper award was given to “On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers” by Akinori Hosoyamada and Kazumaro Aoki, and the best student paper award was given to “Not All Browsers Are Created Equal: Comparing Web Browser Fingerprintability” by Nasser Mohammed Al-Fannah and Wanpeng Li.

A number of people contributed to the success of IWSEC 2017. We would like to thank the authors for submitting their papers to the workshop. The selection of the papers was a challenging and dedicated 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.

Last but not least, we would like to thank the general co-chairs, Kazuto Ogawa and Masayuki Terada, for leading the local Organizing Committee, and we would also like to thank the members of the local Organizing Committee for their efforts to ensure the smooth running of the workshop.

May 2017

Satoshi Obana
Koji Chida

IWSEC 2017

12th International Workshop on Security Organization

Hiroshima, Japan, August 30 – September 1, 2017

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 Information Processing Society of Japan)

General Co-chairs

Kazuto Ogawa
Masayuki Terada

Japan Broadcasting Corporation, Japan
NTT DOCOMO, Japan

Advisory Committee

Hideki Imai
Kwangjo Kim

The University of Tokyo, Japan
Korea Advanced Institute of Science and Technology,
Korea

Christopher Kruegel
Günter Müller
Yuko Murayama
Koji Nakao

University of California, Santa Barbara, USA
University of Freiburg, Germany
Tsuda College, Japan
National Institute of Information and Communications
Technology, Japan

Eiji Okamoto
C. Pandu Rangan
Kai Rannenber
Ryoichi Sasaki

University of Tsukuba, Japan
Indian National Academy of Engineering, India
Goethe University Frankfurt, Germany
Tokyo Denki University, Japan

Program Co-chairs

Satoshi Obana
Koji Chida

HOSEI University, Japan
NTT, Japan

Local Organizing Committee

Hiroaki Anada	University of Nagasaki, Japan
Atsushi Fujioka	Kanagawa University, Japan
Takuya Hayashi	Kobe University, Japan
Takato Hirano	Mitsubishi Electric Corporation, Japan
Hiroyuki Inoue	Hiroshima City University, Japan
Akira Kanaoka	Toho University, Japan
Yutaka Kawai	Mitsubishi Electric Corporation, Japan
Takaaki Mizuki	Tohoku University, Japan
Ken Naganuma	Hitachi, Ltd., Japan
Yoshitaka Nakamura	Future University Hakodate, Japan
Tetsushi Ohki	Shizuoka University, Japan
Go Ohtake	Japan Broadcasting Corporation, Japan
Masakazu Soshi	Hiroshima City University, Japan
Yuji Suga	Internet Initiative Japan Inc., Japan
Yu Tsuda	National Institute of Information and Communications Technology, Japan
Sven Wohlgemuth	Hitachi, Ltd., Japan
Takumi Yamamoto	Mitsubishi Electric Corporation, Japan
Kan Yasuda	NTT, Japan

Program Committee

Mohamed Abid	University of Gabes, Tunisia
Mitsuaki Akiyama	NTT, Japan
Elena Andreeva	KU Leuven, Belgium
Reza Azarderakhsh	Florida Atlantic University, USA
Josep Balasch	KU Leuven, Belgium
Gregory Blanc	Télécom SudParis, France
Olivier Blazy	Université de Limoges, France
Aymen Boudguiga	Institute for Technological Research SystemX, France
Kai-Chi Chang	National Center for Cyber Security Technology, Taiwan
Yue Chen	Florida State University, USA
Céline Chevalier	Université Panthéon-Assas, France
Sabrina De Capitani di Vimercati	DI - Università degli Studi di Milano, Italy
Herve Debar	Télécom SudParis, France
Itai Dinur	Ben-Gurion University, Israel
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalonia
Oriol Farràs	Universitat Rovira i Virgili, Spain
Atsushi Fujioka	Kanagawa University, Japan
Dawu Gu	Shanghai Jiao Tong University, China
Roberto Guanciale	KTH Royal Institute of Technology, Sweden
Florian Hahn	SAP, Germany
Atsuo Inomata	Tokyo Denki University, Japan

Akira Kanaoka	Toho University, Japan
Hiroaki Kikuchi	Meiji University, Japan
Hyung Chan Kim	The Affiliated Institute of ETRI, Korea
Yuichi Komano	Toshiba Corporation, Japan
Noboru Kunihiro	The University of Tokyo, Japan
Maryline Laurent	Télécom SudParis, France
Heejo Lee	Korea University, South Korea
Hyung Tae Lee	Nanyang Technological University, Singapore
Zhou Li	RSA Labs., USA
Frédéric Majorczyk	DGA-MI/CentraleSupélec, France
Florian Mendel	Graz University of Technology, Austria
Bart Mennink	Radboud University, The Netherlands
Kirill Morozov	Tokyo Institute of Technology, Japan
Koichi Mouri	Ritsumeikan University, Japan
Ivica Nikolić	Nanyang Technological University, Singapore
Ryo Nojima	National Institute of Information and Communications Technology, Japan
Alexis Olivereau	CEA LIST, France
Kaan Onarlioglu	Northeastern University, USA
Thomas Peyrin	Nanyang Technological University, Singapore
Yusuke Sakai	National Institute of Advanced Industrial Science and Technology, Japan
Yu Sasaki	NTT, Japan
Dominique Schröder	Friedrich-Alexander Universität Erlangen-Nürnberg, Germany
Yannick Seurin	Agence Nationale de la Sécurité des Systèmes d'Information, France
Yuji Suga	Internet Initiative Japan Inc., Japan
Willy Susilo	University of Wollongong, Australia
Mio Suzuki	National Institute of Information and Communications Technology, Japan
Katsuyuki Takashima	Mitsubishi Electric Corporation, Japan
Mehdi Tibouchi	NTT, Japan
Giorgos Vasiliadis	Qatar Computing Research Institute HBKU, Greece
Cong Wang	City University of Hong Kong, Hong Kong, SAR China
Sven Wohlgenuth	Hitachi, Ltd., Japan
Pa Pa Yin Minn	Yokohama National University, Japan
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Kan Yasuda	NTT, Japan
Maki Yoshida	National Institute of Information and Communications Technology, Japan
Rui Zhang	Chinese Academy of Sciences, China

Additional Reviewers

Arij Ben Amor
Avik Chakraborti
Christoph Egger
Lorenzo Grassi
Moeen Hasanalizadeh
Masahiro Ishii
Amandine Jambert
Sarrah Jebri
Jeong Jihoon
Saqib Kakvi

Marc Kaplan
Thijs Laarhoven
Jason Legrow
Gaëtan Leurent
Bernardo Magri
Giulio Malavolta
Michele Minelli
María Naya-Plasencia
Sk. Md. Mizanur Rahman
Alfredo Rial

Atsushi Takayasu
Yang Tao
Thomas Unterluggauer
Yuting Xiao
Zhengyu Yang
Takanori Yasuda
Youngho Yoo
Qian Zhang

Contents

Post-quantum Cryptography

- On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers 3
Akinori Hosoyamada and Kazumaro Aoki
- The Beauty and the Beasts—The Hard Cases in LLL Reduction 19
Saed Alsayigh, Jintai Ding, Tsuyoshi Takagi, and Yuntao Wang

System Security (1)

- Simple Infeasibility Certificates for Attack Trees 39
Ahto Buldas, Aleksandr Lenin, Jan Willemsen, and Anton Charnamord
- Enhanced TLS Handshake Authentication with Blockchain and Smart Contract (Short Paper) 56
Bingqing Xia, Dongyao Ji, and Gang Yao

Public Key Cryptosystems (1)

- Multipurpose Public-Key Encryption 69
Rui Zhang and Kai He
- Secure Certificateless Proxy Re-encryption Without Pairing 85
Veronika Kuchta, Gaurav Sharma, Rajeev Anand Sahu, Tarunpreet Bhatia, and Olivier Markowitch

System Security (2)

- Not All Browsers are Created Equal: Comparing Web Browser Fingerprintability 105
Nasser Mohammed Al-Fannah and Wanpeng Li
- Evasion Attacks Against Statistical Code Obfuscation Detectors 121
Jiawei Su, Danilo Vasconcellos Vargas, and Kouichi Sakurai

Cryptanalysis

- Analyzing Key Schedule of SIMON: Iterative Key Differences and Application to Related-Key Impossible Differentials 141
Kota Kondo, Yu Sasaki, Yosuke Todo, and Tetsu Iwata

Security Analysis of a Verifiable Server-Aided Approximate
Similarity Computation 159
*Rui Xu, Kirill Morozov, Anirban Basu, Mohammad Shahriar Rahman,
and Shinsaku Kiyomoto*

Cryptographic Protocols

Correction of a Secure Comparison Protocol for Encrypted Integers in IEEE
WIFS 2012 (Short Paper). 181
Baptiste Vinh Mau and Koji Nuida

Adaptive Security in Identity-Based Authenticated Key Agreement
with Multiple Private Key Generators 192
Atsushi Fujioka

Public Key Cryptosystems (2)

Deterministic Identity-Based Encryption from Lattices with More Compact
Public Parameters 215
Daode Zhang, Fuyang Fang, Bao Li, and Xin Wang

IND-PCA Secure KEM Is Enough for Password-Based Authenticated Key
Exchange (Short Paper) 231
Haiyang Xue, Bao Li, and Xianhui Lu

Author Index 243