Lecture Notes in Computer Science 10418

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

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

Springer

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

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	Japan Broadcasting Corporation, Japan
Masayuki Terada	NTT DOCOMO, Japan

Advisory Committee

Hideki Imai	The University of Tokyo, Japan
Kwangjo Kim	Korea Advanced Institute of Science and Technology, Korea
Christopher Kruegel	University of California, Santa Barbara, USA
Günter Müeller	University of Freiburg, Germany
Yuko Murayama	Tsuda College, Japan
Koji Nakao	National Institute of Information and Communications Technology, Japan
Eiji Okamoto	University of Tsukuba, Japan
C. Pandu Rangan	Indian National Academy of Engineering, India
Kai Rannenberg	Goethe University Frankfurt, Germany
Ryoichi Sasaki	Tokyo Denki University, Japan

Program Co-chairs

Satoshi Obana	HOSEI University, Japan
Koji Chida	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/CentraleSupelec, 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 Wohlgemuth	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
Sarra 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