Lecture Notes in Computer Science 8231

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

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

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	KDDI R&D Laboratories Inc., Japan
Masakatsu Nishigaki	Shizuoka University, Japan

Advisory Committee

Hideki Imai	Chuo University, Japan
Kwangjo Kim	Korea Advanced Institute of Science and Technology, Korea
Günter Müller	University of Freiburg, Germany
Yuko Murayama	Iwate Prefectural University, Japan
Koji Nakao	National Institute of Information and Communications Technology, Japan
Eiji Okamoto	University of Tsukuba, Japan
C. Pandu Rangan	Indian Institute of Technology, Madras, India
Ryoichi Sasaki	Tokyo Denki University, Japan

Program Co-chairs

Kazuo Sakiyama	University of Electro-Communications, Japan
Masayuki Terada	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 Koshiba	Saitama University, Japan
Noboru Kunihiro	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 Rannenberg	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
Begul Bilgin	Shan Chen	Aurore Guillevic

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

Table of Contents

Software and System Security

Cryptanalysis

Privacy and Cloud Computing

Public Key Cryptosystems

Security Protocols