Lecture Notes in Computer Science 11689

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

Nuttapong Attrapadung ·
Takeshi Yagi (Eds.)

Advances in Information and Computer Security

14th International Workshop on Security, IWSEC 2019
Tokyo, Japan, August 28–30, 2019
Proceedings

Springer

Editors
Nuttapong Attrapadung
National Institute of Advanced Industrial Science and Technology
Tokyo, Japan

Takeshi Yagi
NTT Security (Japan) KK
Tokyo, Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-26833-6 ISBN 978-3-030-26834-3 (eBook)
https://doi.org/10.1007/978-3-030-26834-3

LNCS Sublibrary: SL4 – Security and Cryptology

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

Preface

The 14th International Workshop on Security, IWSEC 2019, was held at the Multi-Purpose Digital Hall, Ookayama Campus, Tokyo Institute of Technology, Tokyo, Japan, during August 28–30, 2019. The workshop was co-organized by ISEC (the Technical Committee on Information Security in Engineering Sciences Society of IEICE) and CSEC (the Special Interest Group on Computer Security of IPSJ).

This year, we categorized topics of interests into two tracks, namely, Cryptography Track (Track A) and Cybersecurity and Privacy Track (Track B); each track is formed by separate Program Committee members. We received 63 submissions, 42 in Track A and 21 in Track B, out of which two papers were withdrawn before the review process. After extensive reviews and shepherding, we accepted 18 regular papers (12 from Track A and six from Track B) and five short papers (three from Track A and two from Track B). Each submission was anonymously reviewed by four reviewers. These proceedings contain revised versions of the accepted papers. Track A consists of the sessions on public-key primitives, symmetric-key primitives, cryptanalysis, and cryptographic protocols. Track B consists of the sessions on malware detection and classification, intrusion detection and prevention, Web and usable security, and forensics.

The Best Paper Awards were given to "An Efficient F4-style Based Algorithm to Solve MQ Problems" by Takuma Ito, Naoyuki Shinohara, and Shigenori Uchiyama, and to "Towards Efficient Detection of Malicious VBA Macros with LSI" by Mamoru Mimura and Taro Ohminami. The Best Student Paper Award was given to "CCA-Secure Leakage-Resilient Identity-Based Key-Encapsulation from Simple (not q-type) Assumptions" by Toi Tomita, Wakaha Ogata, and Kaoru Kurosawa. In addition to the presentations of the accepted papers, the workshop also featured two keynote talks, a poster session, and invited talk sessions from domestic symposiums, namely, SCIS (Symposium on Cryptography and Information Security) and CSS (Computer Security Symposium). We also included a special session organized by AIMaP (Advanced Innovation powered by Mathematics Platform).

A number of people contributed to the success of IWSEC 2019. We would like to thank all authors for submitting their papers to the workshop, and also we are deeply grateful to the members of the Program Committee and to the external reviewers for their in-depth reviews and detailed discussions. We must mention that the selection of the papers was an extremely challenging task.

Last but not least, we would like to thank the General Co-Chairs, Toshihiro Yamauchi and Shiho Moriai, for leading the Organizing Committee, and we would also like to thank the members of the Organizing Committee for ensuring the smooth running of the workshop.

June 2019

Nuttapong Attrapadung
Takeshi Yagi

IWSEC 2019

14th International Workshop on Security
Organization

Tokyo, Japan, August 28–30, 2019

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

Shiho Moriai	National Institute of Information and Communications Technology, Japan
Toshihiro Yamauchi	Okayama University, Japan

Advisory Committee

Hideki Imai	University of Tokyo, Japan
Kwangjo Kim	Korea Advanced Institute of Science and Technology, the Republic of Korea
Christopher Kruegel	University of California, Santa Barbara, USA
Günter Müller	University of Freiburg, Germany
Yuko Murayama	Tsuda 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
Kai Rannenberg	Goethe University Frankfurt, Germany
Ryoichi Sasaki	Tokyo Denki University, Japan

Program Co-chairs

Nuttapong Attrapadung	AIST, Japan
Takeshi Yagi	NTT Security (Japan) KK, Japan

Local Organizing Committee

Kazumaro Aoki	Nippon Telegraph and Telephone Corporation, Japan
Keita Emura	National Institute of Information and Communications Technology, Japan
Shota Fujii	Hitachi, Ltd., Japan
Masahiro Fujita	Mitsubishi Electric Corporation, Japan
Yuichi Hayashi	Nara Institute of Science and Technology, Japan
Shoichi Hirose	The University of Fukui, Japan
Makoto Iguchi	Kii Corporation, Japan
Akira Kanaoka	Toho University, Japan
Ryo Kikuchi	Nippon Telegraph and Telephone Corporation, Japan
Yoshihiro Mizoguchi	Institute of Mathematics for Industry, Kyusyu University, Japan
Ken Naganuma	Hitachi, Ltd., Japan
Satsuya Ohata	AIST, Japan
Kazuma Ohara	NEC Corporation, Japan
Yuji Suga	Internet Initiative Japan Inc., Japan
Nobuyuki Sugio	NTT DOCOMO, Inc., Japan
Atsushi Takayasu	The University of Tokyo, Japan
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Yohei Watanabe	National Institute of Information and Communications Technology, Japan
Sven Wohlgemuth	Hitachi, Ltd., Japan
Dai Yamamoto	Fujitsu Limited, Japan
Masaya Yasuda	Institute of Mathematics for Industry, Kyusyu University, Japan

Program Committee

Track A: Cryptography Track

Kazumaro Aoki	NTT, Japan
Nuttapong Attrapadung	AIST, Japan
Olivier Blazy	University of Limoges, France
Bernardo David	Tokyo Institute of Technology, Japan
Itai Dinur	Ben-Gurion University, Israel
Antonio Faonio	IMDEA Software Institute, Spain
Takahiro Matsuda	AIST, Japan
Florian Mendel	Graz University of Technology, Austria
Kazuhiko Minematsu	NEC, Japan
Kirill Morozov	University of North Texas, USA
Fabrice Mouhartem	ENS Lyon, France and Microsoft Research, India
Thomas Peters	Université catholique de Louvain, Belgium
Yusuke Sakai	AIST, Japan
Jae Hong Seo	Hanyang University, Republic of Korea

Yannick Seurin	Agence Nationale de la Sécurité des Systemes d'Information, France
Willy Susilo	University of Wollongong, Australia
Katsuyuki Takashima	Mitsubishi Electric Corporation, Japan
Atsushi Takayasu	The University of Tokyo, Japan
Qiang Tang	New Jersey Institute of Technology, USA
Mehdi Tibouchi	NTT, Japan
Damien Vergnaud	Sorbonne Université, UPMC, CNRS, France
Yuyu Wang	Tokyo Institute of Technology, Japan
Yohei Watanabe	NICT, Japan
Rui Zhang	Chinese Academy of Sciences, China

Track B: Cybersecurity and Privacy Track

Mitsuaki Akiyama	Nippon Telegraph and Telephone Corporation, Japan
Josep Balasch	KU Leuven, Belgium
Gregory Blanc	Telecom SudParis, France
Yue Chen	Palo Alto Networks, USA
Daiki Chiba	Nippon Telegraph and Telephone Corporation, Japan
Herve Debar	Telecom SudParis, France
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalonia
Kimmo Halunen	VTT Technical Research Centre of Finland Ltd., Finland
Yuichi Hayashi	Nara Institute of Science and Technology, Japan
Akira Kanaoka	Toho University, Japan
Yuhei Kawakoya	Nippon Telegraph and Telephone Corporation, Japan
Frederic Majorczyk	DGA-MI/CentraleSupelec, France
Yoshihiro Oyama	University of Tsukuba, Japan
Hajime Shimada	Nagoya University, Japan
Junko Takahashi	Nippon Telegraph and Telephone Corporation, Japan
Yuta Takata	PwC Cyber Services LLC, Japan
Giorgos Vasiliadis	Qatar Computing Research Institute HBKU, Greece
Takeshi Yagi	NTT Security (Japan) KK, Japan
Takumi Yamamoto	Mitsubishi Electric Corporation, Japan

Additional Reviewers

Miguel Ambrona	Michalis Diamantaris	Koki Hamada
Carles Anglés-Tafalla	Maria Eichlseder	Keisuke Hara
Sarah Azouvi	Keita Emura	Junichirou Hayata
Michael Bamiloshin	Daniel Escudero	Ehsan Hesamifard
Pascal Bemmann	Scott Fluhrer	Takato Hirano
Alberto Blanco-Justicia	Daisuke Fujimoto	Atsunori Ichikawa
George Christou	Atsushi Fujioka	Akiko Inoue
Pratish Datta	Kaiwen Guo	Toshiyuki Isshiki

Mitsugu Iwamoto
Maxim Jourenko
Saqib A. Kakvi
Shuichi Katsumata
Craig Kenney
Suhri Kim
Michael Klooss
Takuma Koyama
Stefan Kölbl
Wen-Jie Lu
Sergio Martinez
Michael Meyer
Luca Nizzardo
Yasuyuki Nogami
Koji Nuida
Satsuya Ohata
Toshihiro Ohigashi
Javier Parra-Arnau
Arnab Roy
Jacob Schuldt
Vladimir Soukharev
Xiangyu Su
Koutarou Suzuki
Tadanori Teruya
Masayuki Tezuka
Guanyu Tian
Yacheng Wang
Erich Wenger
Friedrich Wiemer
Keita Xagawa
Takashi Yamakawa
Takanori Yasuda
Yusuke Yoshida
Masaya Yoshikawa

Contents

Malware Detection and Classification

Intrusion Detection and Prevention

Web and Usable Security

Public-Key Primitives 2

Cryptanalysis on Symmetric-Key Primitives

Cryptographic Protocols 2

Forensics