Lecture Notes in Computer Science 9866

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

Matt Bishop · Anderson C.A. Nascimento (Eds.)

Information Security

19th International Conference, ISC 2016
Honolulu, HI, USA, September 3–6, 2016
Proceedings

Springer

Editors
Matt Bishop
University of California
Davies, CA
USA

Anderson C.A. Nascimento
University of Washington
Tacoma, WA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-45870-0 ISBN 978-3-319-45871-7 (eBook)
DOI 10.1007/978-3-319-45871-7

Library of Congress Control Number: 2016949632

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing Switzerland 2016
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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

This volume contains the papers presented at the 19th Annual International Conference on Information Security (ISC 2016) held on September 3–6, 2016, in Honolulu, Hawaii, USA.

Held annually, the Information Security Conference is an international conference covering research in the theory and applications of information security. It started as a workshop in 1997 and became a conference in 2001. It has been held on five different continents.

Rui Zhang from the University of Hawaii, USA and Masahiro Mambo, from Kanazawa University, Japan organized ISC 2016, in cooperation with the International Association for Cryptologic Research.

Submissions to ISC 2016 were required to be anonymous. The 76 submitted papers were reviewed using a double-blind process. Selecting the final accepted papers was a difficult task that demanded many rounds of interaction. As a result, the Program Committee accepted 19 full papers (resulting in an acceptance rate of 25 %) and 7 short papers. We would like to thank the Program Committee for their valuable work.

We also thank Rui Zhang and Masahiro Mambo for the superb work they did organizing the conference. We are grateful to the ISC Steering Committee for their support, to Depeng Li for handling the local arrangements, and the creators and maintainers of Easychair, the superb platform we used to manage the review process.

Finally, we would like to thank all the authors who submitted papers to ISC 2016. They are the main reason for the success of this conference.

September 2016

Matt Bishop
Anderson C.A. Nascimento

Organization

Information Security Conference 2016, Honolulu, Hawaii, USA, September 7–9, 2016

General Chairs

Masahiro Mambo	Kanazawa University, Japan
Rui Zhang	University of Hawaii, USA

Program Chairs

Matt Bishop	University of California, Davis, USA
Anderson C.A. Nascimento	University of Washington, Tacoma, USA

Local Arrangements

Depeng Li	University of Hawaii, USA

Steering Committee

Colin Boyd	Norwegian University of Science and Technology, Norway
Ed Dawson	Queensland University of Technology, Australia
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	Kanazawa University, Japan
Eiji Okamoto	University of Tsukuba, Japan
Susanne Wetzel	Stevens Institute of Technology, USA
Rui Zhang	University of Hawaii, USA
Yuliang Zheng	University of Alabama at Birmingham, USA

Program Committee

Gail-Joon Ahn	Arizona State University, USA
Luis Antunes	University of Porto, Portugal
Diego Aranha	State University of Campinas, Brazil
Claudio Ardagna	Università degli Studi di Milano, Italy
Elias Athanasopoulos	Vrije Universiteit Amsterdam, The Netherlands
Nuttapong Attrapadung	AIST, Japan
Tuomas Aura	Aalto University, Finland
Elisa Bertino	Purdue University, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Matt Bishop	UC Davis, USA
Liqun Chen	Hewlett Packard Labs, USA
Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong, China

Bruno Crispo	University of Trento, Italy
Paolo D'Arco	University of Salerno, Italy
Naccache David	Ecole Normale Supérieure, France
Yvo Desmedt	The University of Texas at Dallas, USA
Roberto Di Pietro	Bell Labs, USA
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Christian Gehrmann	Swedish Institute of Computer Science, Sweden
Dieter Gollmann	Hamburg University of Technology, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Jong Guo	Shandong University, China
Xinyi Huang	Fujian Normal University, China
Kangkook Jee	Columbia University, USA
Sokratis Katsikas	Center for Cyber and Information Security, NTNU, Norway
Stefan Katzenbeisser	TU Darmstadt, Germany
Vasileios Kermelis	Brown University, USA
Helger Lipmaa	University of Tartu, Estonia
Yao Liu	University of South Florida, USA
Patrick Longa	Microsoft Research, USA
Di Ma	University of Michigan-Dearborn, USA
Masahiro Mambo	Kanazawa University, Japan
Mark Manulis	University of Surrey, UK
Fabio Martinelli	IIT-CNR, Italy
Catherine Meadows	NRL, USA
Jean-Francois Misarsky	Orange Labs, France
Refik Molva	EURECOM, France
Yi Mu	University of Wollongong, Australia
Anderson Nascimento	University of Washington, USA
Miyako Ohkubo	NICT, Japan
Eiji Okamoto	University of Tsukuba, Japan
Charalampos Papamanthou	University of Maryland, College Park, USA
Josef Pieprzyk	Queensland University of Technology, Australia
Michael Polychronakis	Stony Brook University, USA
Joachim Posegga	University of Passau, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Indrajit Ray	Colorado State University, USA
Kui Ren	State University of New York at Buffalo, USA
Rei Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Miguel Soriano	Universitat Politècnica de Catalunya, Spain
Claudio Soriente	Telefonica Research and Development, Spain
Martijn Stam	University of Bristol, UK
Vijay Varadharajan	Macquarie University, Australia
Guilin Wang	Huawei International Pte Ltd, Singapore
Susanne Wetzel	Stevens Institute of Technology, USA
Stephen Wolthusen	Royal Holloway, University of London, UK

Junjie Zhang	Wright State University, USA
Rui Zhang	University of Hawaii, USA
Ziming Zhao	Arizona State University, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

Contents

Cryptanalysis

Truncated and Multiple Differential Cryptanalysis of Reduced Round Midori128 3
Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef

Improved Linear Cryptanalysis of Round-Reduced ARIA. 18
Ahmed Abdelkhalek, Mohamed Tolba, and Amr M. Youssef

Partial Key Exposure Attacks on CRT-RSA: General Improvement for the Exposed Least Significant Bits 35
Atsushi Takayasu and Noboru Kunihiro

Cryptanalysis and Improved Construction of a Group Key Agreement for Secure Group Communication 48
Jun Xu, Lei Hu, Xiaona Zhang, Liqiang Peng, and Zhangjie Huang

Enhanced Correlation Power Analysis by Biasing Power Traces 59
Changhai Ou, Zhu Wang, Degang Sun, Xinping Zhou, Juan Ai, and Na Pang

Damaging, Simplifying, and Salvaging p-OMD 73
Tomer Ashur and Bart Mennink

Cryptographic Protocols

Blind Password Registration for Two-Server Password Authenticated Key Exchange and Secret Sharing Protocols. 95
Franziskus Kiefer and Mark Manulis

Chip Authentication for E-Passports: PACE with Chip Authentication Mapping v2 115
Lucjan Hanzlik and Mirosław Kutyłowski

AEP-M: Practical Anonymous E-Payment for Mobile Devices Using ARM TrustZone and Divisible E-Cash 130
Bo Yang, Kang Yang, Zhenfeng Zhang, Yu Qin, and Dengguo Feng

Universally Composable Two-Server PAKE. 147
Franziskus Kiefer and Mark Manulis

Yet Another Note on Block Withholding Attack on Bitcoin Mining Pools . . . 167
Samiran Bag and Kouichi Sakurai

Network and Systems Security and Access Control

Cyber Security Risk Assessment of a DDoS Attack. 183
Gaute Wangen, Andrii Shalaginov, and Christoffer Hallstensen

Moving Target Defense Against Network Reconnaissance with Software Defined Networking 203
Li Wang and Dinghao Wu

Uni-ARBAC: A Unified Administrative Model for Role-Based Access Control 218
Prosunjit Biswas, Ravi Sandhu, and Ram Krishnan

SKALD: A Scalable Architecture for Feature Extraction, Multi-user Analysis, and Real-Time Information Sharing. 231
George D. Webster, Zachary D. Hanif, Andre L.P. Ludwig, Tamas K. Lengyel, Apostolis Zarras, and Claudia Eckert

Privacy and Watermarking

Leveraging Internet Services to Evade Censorship. 253
Apostolis Zarras

Analyzing Randomized Response Mechanisms Under Differential Privacy . . . 271
Atsushi Waseda and Ryo Nojima

Models and Algorithms for Graph Watermarking 283
David Eppstein, Michael T. Goodrich, Jenny Lam, Nil Mamano, Michael Mitzenmacher, and Manuel Torres

Software Security

Policy-Based Implicit Attestation for Microkernel-Based Virtualized Systems. 305
Steffen Wagner and Claudia Eckert

Generalized Dynamic Opaque Predicates: A New Control Flow Obfuscation Method 323
Dongpeng Xu, Jiang Ming, and Dinghao Wu

A Bayesian Cogntive Approach to Quantifying Software Exploitability Based on Reachability Testing 343
Guanhua Yan, Yunus Kucuk, Max Slocum, and David C. Last

Control Flow Integrity Enforcement with Dynamic Code Optimization 366
Yan Lin, Xiaoxiao Tang, Debin Gao, and Jianming Fu

Encryption, Signatures and Fundamentals

Impossibility on the Provable Security of the Fiat-Shamir-Type Signatures in the Non-programmable Random Oracle Model 389
Masayuki Fukumitsu and Shingo Hasegawa

Efficient Functional Encryption for Inner-Product Values with Full-Hiding Security 408
Junichi Tomida, Masayuki Abe, and Tatsuaki Okamoto

MQSAS - A Multivariate Sequential Aggregate Signature Scheme 426
Rachid El Bansarkhani, Mohamed Saied Emam Mohamed, and Albrecht Petzoldt

Cryptanalysis of Multi-Prime Φ-Hiding Assumption 440
Jun Xu, Lei Hu, Santanu Sarkar, Xiaona Zhang, Zhangjie Huang, and Liqiang Peng

Author Index 455