Lecture Notes in Computer Science

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, Chennai, 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

Information Security Theory and Practice

11th IFIP WG 11.2 International Conference, WISTP 2017 Heraklion, Crete, Greece, September 28–29, 2017 Proceedings



Editors Gerhard P. Hancke City University of Hong Kong Hong Kong China

Ernesto Damiani University of Milan Milan Italy

 ISSN 0302-9743
 ISSN 1611-3349
 (electronic)

 Lecture Notes in Computer Science
 ISBN 978-3-319-93523-2
 ISBN 978-3-319-93524-9
 (eBook)

 https://doi.org/10.1007/978-3-319-93524-9

Library of Congress Control Number: 2018947334

LNCS Sublibrary: SL4 - Security and Cryptology

© IFIP International Federation for Information Processing 2018

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 the registered company Springer International Publishing AG part of Springer Nature

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 11th WISTP International Conference on Information Security Theory and Practice attracted research contributions covering theoretical and practical aspects of security and privacy, especially for future ICT technologies. Technical concepts such as ambient intelligence, cyber-physical systems, and Internet of Things provide a vision of an information society in which: (a) people and physical systems are surrounded with intelligent interactive interfaces and objects, and (b) environments are capable of recognizing and reacting to the presence of different individuals or events in a seamless, unobtrusive, and invisible manner. The success of future ICT technologies will depend on how secure these systems are and to what extent they protect the privacy of individuals and individuals trust them.

In response to the call for papers, 35 papers were submitted to the conference from 20 different countries. Each paper was reviewed by at least three members of the Program Committee, and evaluated on the basis of its significance, novelty, and technical quality. The reviewing was double-blind, with the identities of the authors not revealed to the reviewers of the papers and the identities of the reviewers not revealed to the authors. The Program Committee's work was carried out electronically; each paper received at least three reviews followed by a Program Committee discussion to finalize decisions. Of the submitted papers, the Program Committee accepted eight full papers and four short papers. The technical contributions were presented in five technical sessions, and the program also included three invited talks by Prof. George Spanoudakis (City University London, UK), Prof. Fabio Martinelli (National Research Council of Italy, Italy), and Dr. Louis Marinos (ENISA, Greece).

We thank all authors and participants who contributed to make this event a great success, the Technical Program Committee members and additional reviewers who worked on the program, and the volunteers who handled aspects of the organization behind the scenes. We greatly appreciate the input from members of the WISTP Steering Committee, whose help and advice was invaluable, and the support of IFIP WG 11.2: Pervasive Systems Security. We would also like to thank the general chair, Ioannis Askoxylakis, and the other local organizers at FORTH-ICS for supporting for this event and providing assistance with general arrangements.

September 2017

Gerhard P. Hancke Ernesto Damiani

Organization

General Chair

FORTH-ICS, Greece
Università degli Studi di Milano, Italy City University of Hong Kong, Hong Kong, SAR China

Local Organizers

Nikolaos Petroulakis	FORTH-ICS, Greece
Andreas Miaoudakis	FORTH-ICS, Greece
Panos Chatziadam	FORTH-ICS, Greece

Steering Committee

Angelos Bilas	FORTH-ICS and University of Crete, Greece
Sara Foresti	Università degli Studi di Milano, Italy
Javier Lopez	University of Malaga, Spain
Konstantinos	ISG-SCC, Royal Holloway University of London, UK
Markantonakis	
Joachim Posegga	Institute of IT-Security and Security Law at the University of Passau, Germany
Jean-Jacques Quisquater	ICTEAM, Catholic University of Louvain, Belgium
Damien Sauveron	XLIM, University of Limoges, France
Program Committee	

Mohamed Ahmed Abdelraheem	SICS, Swedish ICT, Sweden
Raja Naeem Akram	Royal Holloway, University of London, UK
Fahad Alharby	Naif Arab University for Security Sciences, Saudi Arabia
Claudio A. Ardagna	Università degli Studi di Milano, Italy
Ioannis Askoxylakis	FORTH-ICS, Greece
Hervé Chabanne	Morpho, France
Serge Chaumette	LaBRI, University of Bordeaux, France

Mauro Conti José María De Fuentes Kurt Dietrich Ruggero Donida Labati Sara Foresti Flavio Garcia Yong Guan Julio Hernandez-Castro Michael Hutter Sushil Jajodia Süleyman Kardas Mehmet Sabir Kiraz Andrea Lanzi Maryline Laurent Albert Levi Tieyan Li Javier Lopez Vashek Matyas Sjouke Mauw Nele Mentens Alessio Merlo David Naccache Vladimir A. Oleshchuk Joachim Posegga Kai Rannenberg Kouichi Sakurai Pierangela Samarati Siraj Ahmed Shaikh Nils Tippenhauer

Denis Trcek Michael Tunstall Umut Uludag Anjia Yang Stefano Zanero Vincent Zhuang

University of Padua, Italy Universidad Carlos III de Madrid, Spain NXP Semiconductors. Netherlands Università degli Studi di Milano, Italy Università degli Studi di Milano, Italy University of Birmingham, UK Iowa State University, USA University of Kent, UK Cryptography Research, USA George Mason University, USA Batman University, Turkey TUBITAK Bilgem, Turkey Università degli studi di Milano, Italy Institut Mines-Telecom, France Sabanci University, Italy Huawei, Singapore University of Malaga, Spain Masaryk University, Czech Republic University of Luxembourg, Luxembourg KU Leuven, Belgium University of Genoa, Italy Ecole Normale Suprieure, France University of Agder, Norway University of Passau, Germany Goethe University Frankfurt, Germany Kyushu University, Japan Università degli Studi di Milano, Italy Coventry University, UK Singapore University of Technology and Design, Singapore University of Ljubljana, Slovenia Cryptography Research, USA TUBITAK Bilgem, Turkey Jinan University, China Politecnico di Milano, Italy City University of Hong Kong, SAR China

Additional Reviewers

Duygu Karaoglan Altop Martin Gunnarsson Chhagan Lal Jiasi Weng Christophe Petit Davide Quarta Madeline Cheah Warren Connell Yuto Nakano Ming Li Yasir Khan Yanjiang Yang Wenjie Yang Partha Sarathi Roy Sridhar Venkatesan Giuseppe Cascavilla Chunhua Su Andreea-Ina Radu Fei Xie

Sponsoring Institutions

CyberSure Project (http://www.cybersure.eu/)

Contents

Security in Emerging Systems

A Secure and Trusted Channel Protocol for UAVs Fleets Raja Naeem Akram, Konstantinos Markantonakis, Keith Mayes, Pierre-François Bonnefoi, Amina Cherif, Damien Sauveron, and Serge Chaumette	3
Philanthropy on the Blockchain Danushka Jayasinghe, Sheila Cobourne, Konstantinos Markantonakis, Raja Naeem Akram, and Keith Mayes	25
Security of Data	
Long White Cloud (LWC): A Practical and Privacy-Preserving Outsourced Database Shujie Cui, Ming Zhang, Muhammad Rizwan Asghar, and Giovanni Russello	41
JACPoL: A Simple but Expressive JSON-Based Access Control Policy Language	56
Trusted Execution	
EmLog: Tamper-Resistant System Logging for Constrained Devices with TEEs <i>Carlton Shepherd, Raja Naeem Akram,</i> <i>and Konstantinos Markantonakis</i>	75
How TrustZone Could Be Bypassed: Side-Channel Attacks on a Modern System-on-Chip	93
Defences and Evaluation	

Formalising Systematic Security Evaluations Using Attack Trees	
for Automotive Applications.	113
Madeline Cheah, Hoang Nga Nguyen, Jeremy Bryans,	
and Siraj A. Shaikh	

Examination of a New Defense Mechanism: Honeywords Ziya Alper Genç, Süleyman Kardaş, and Mehmet Sabir Kiraz	130
AndroNeo: Hardening Android Malware Sandboxes by Predicting Evasion Heuristics	140
Protocols and Algorithms	
A More Efficient 1–Checkable Secure Outsourcing Algorithm for Bilinear Maps Öznur Kalkar, Mehmet Sabir Kiraz, İsa Sertkaya, and Osmanbey Uzunkol	155
A Selective Privacy-Preserving Identity Attributes Protocol for Electronic Coupons Pau Conejero-Alberola, M. Francisca Hinarejos, and Josep-Lluís Ferrer-Gomila	165
Revisiting Two-Hop Distance-Bounding Protocols: Are You Really Close Enough?	177
Author Index	189