Lecture Notes in Computer Science 8651

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, Zürich, 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, Saarbruecken, Germany

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

Nitesh Saxena · Ahmad-Reza Sadeghi (Eds.)

Radio Frequency Identification

Security and Privacy Issues

10th International Workshop, RFIDSec 2014
Oxford, UK, July 21–23, 2014
Revised Selected Papers

Springer

Editors

Nitesh Saxena
Computer and Information Science
University of Alabama at Birmingham
Birmingham, AL
USA

Ahmad-Reza Sadeghi
Technische Universität Darmstadt
Darmstadt
Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-13065-1 ISBN 978-3-319-13066-8 (eBook)
DOI 10.1007/978-3-319-13066-8

Library of Congress Control Number: 2014955536

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

© Springer International Publishing Switzerland 2014
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

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Preface

This volume contains the proceedings of the 10th International Workshop on RFID Security (RFIDSec), held at St. Anne's College, Oxford, UK, from July 21 to 23, 2014. For a decade, RFIDSec has been the primary forum where international experts from academia, industry, and government present, debate, discuss, and advance the security and privacy aspects of RFID. First time in the history of RFIDSec, the workshop was colocated with the WiSec conference, an established venue centred on wireless security. This conglomeration of the two communities led to a synergistic development and discussion of new cross-disciplinary ideas.

This year, we assembled a diverse program of nine regular papers and four short papers selected by the Program Committee. All submissions received three reviews from the 23 members of the Program Committee chosen by the Program Co-chairs, assisted by the 13 external reviewers. The conference opened up with an invited talk "Clustering Distance Bounding Protocols" by Prof. Gildas Avoine, INSA Rennes, a known expert in RFID Security and Privacy. The talk focused on distance bounding protocols, a widely studied topic within the RFIDSec community. The second talk was a keynote speech given by John O'Donnell, Cisco Systems's Internet of Everything (IoE) Pre Sales Consultants Manager. His talk "IoT – Connecting the Unconnected Securely" examined real-world security problems within the IoT field. The highlights of this year's technical program were timely and fundamental topics such as RFID power-efficiency, privacy, authentication and side channels, and key exchange.

We thank the General Chairs, Andrew Martin and Ivan Martinovic, both from the University of Oxford, UK, for their dedicated work and the excellent local organization of the workshop, the RFIDSec Steering Committee members for their guidance and support, all the authors for the high-quality submissions, and all the Program Committee members and the external reviewers for contributing their expertise to the selection of the papers for the program. Without their service and contribution, setting up such a conference would have been impossible.

July 2014

Ahmad-Reza Sadeghi
Nitesh Saxena

Organization

Program Committee

Gildas Avoine	Université catholique de Louvain, Belgium
Lejla Batina	Radboud University Nijmegen, The Netherlands
Mihai Bucicoiu	University Politehnica of Bucharest, Romania
Srdjan Capkun	ETH Zürich, Switzerland
Mauro Conti	University of Padua, Italy
Bruno Crispo	University of Trento, Italy
Roberto Di Pietro	Roma Tre University, Italy
Thomas Eisenbarth	Worcester Polytechnic Institute, USA
Aurélien Francillon	Institut Eurécom, France
Tzipora Halevi	Polytechnic Institute of New York University, USA
Gerhard Hancke	City University of Hong Kong, Hong Kong
Jaap-Henk Hoepman	Radboud University Nijmegen, The Netherlands
Mehran Kermani	Rochester Institute of Technology, USA
Karl Koscher	University of Washington, USA
Kari Kostiainen	ETH Zürich, Switzerland
Farinaz Koushanfar	Rice University, USA
Yingjiu Li	Singapore Management University, Singapore
Mark Manulis	University of Surrey, UK
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Pankaj Rohatgi	Cryptography Research Inc., USA
Ahmad-Reza Sadeghi	Technische Universität Darmstadt, Germany
Nitesh Saxena	University of Alabama at Birmingham, USA
Babins Shrestha	University of Alabama at Birmingham, USA
Joshua Smith	University of Washington, USA
Ersin Uzun	PARC, USA
Jonathan Voris	Columbia University, USA
Avishai Wool	Tel Aviv University, Israel

Contents