Lecture Notes in Computer Science 10155

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

Gerhard P. Hancke
Konstantinos Markantonakis (Eds.)

Radio Frequency Identification and IoT Security

12th International Workshop, RFIDSec 2016
Hong Kong, China, November 30 – December 2, 2016
Revised Selected Papers

Springer

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

Konstantinos Markantonakis
University of London
Egham
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-62023-7 ISBN 978-3-319-62024-4 (eBook)
DOI 10.1007/978-3-319-62024-4

Library of Congress Control Number: 2017944356

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

Welcome to the proceedings of the 12th edition of RFIDSec. Since 2005, RFIDsec has become the premier venue devoted to security and privacy of radiofrequency identification (RFID). This year RFIDsec broadened its scope to security and privacy in all application areas related to any constrained devices, with the event being renamed the Workshop on RFID and IoT Security (previously Workshop on RFID Security and Privacy). This reflects the fact that the nature of radio-enabled item identification and automatic data capture has significantly changed over the years, driven by the interest in overarching applications such as the Internet of Things and cyber-physical systems. This year also marked the first occasion of RFIDSec being held outside of Europe and the USA. We were excited to host RFIDSec in Asia's World City.

RFIDsec 2016 assembled five technical sessions with exciting results in RFID and IoT security. Eleven regular papers and three short paper were selected after a rigorous review process of 30 submissions. The review procedure included a review phase, with each paper receiving at least three reviews, followed by discussion between the Program Committee members and the program chairs. The program also included three invited talks and one tutorial. In the first invited talk "Secure Proximity Verification and Localization: Challenges and Solutions." Aanjhan Ranganathan of ETH Zurich spoke about attacks on proximity and location systems, and presented some work on countermeasures for GPS spoofing attacks. In the second invited talk "IT+OT=IoT? On Security for Industrial Control Systems," Nils Tippenhauer of the Singapore University of Technology and Design talked about industrial IoT and presented practical examples of security issues within deployed industrial control systems. In the third talk, the audience were given a industry perspective on IoT security by Duncan Wong of the Hong Kong Applied Science and Technology Research Institute (ASTRI). Finally, David Cox of the University of Birmingham presented a tutorial on the Chameleon, an RFID emulater and reader platform developed by Kasper & Oswald GmbH.

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 did much organization behind the scenes. We greatly appreciate the input of the RFIDSec Steering Committee, whose help and advice was invaluable, and we would like to thank the Department of Computer Science at City University of Hong Kong for supporting for this event and providing assistance with general arrangements.

December 2016

Gerhard P. Hancke
Konstantinos Markantonakis

Organization

General Chair

Gerhard Hancke	City University of Hong Kong, Hong Kong, SAR China

Program Chairs

Gerhard Hancke	City University of Hong Kong, Hong Kong, SAR China
Konstantinos Markantonakis	Royal Holloway University of London, UK

Local Organizers

Yunhui Zhuang	City University of Hong Kong, Hong Kong, SAR China
Anjia Yang	Jinan University, PR China

Steering Committee

Lejla Batina	RU Nijmegen, The Netherlands
Srdjan Capkun	ETH Zurich, Switzerland
Yingjiu Li	Singapore Management University, Singapore
Andrew Martin	University of Oxford, UK
Ivan Martinovic	University of Oxford, UK
Christof Paar	Ruhr University Bochum, Germany
Bart Preneel	KU Leuven, Belgium
Ahmad-Reza Sadeghi	Technische Universität Darmstadt, Germany
Nitesh Saxena	University of Alabama at Birmingham, USA
Patrick Schaumont	Virginia Tech, USA

Program Committee

Raja Naeem Akram	Royal Holloway University of London,UK
Frederik Armknecht	Universität Mannheim, Germany
Gildas Avoine	INSA Rennes France and UCL, Belgium
Lejla Batina	Radboud University Nijmegen, The Netherlands
Mike Burmester	Florida State University, USA
Rajat Subhra Chakraborty	IIT Kharagpur, India
Sherman Chow	Chinese University of Hong Kong, Hong Kong, SAR China
Thomas Eisenbarth	WPI, Austria
Martin Feldhofer	NXP Semiconductors, Austria

Julio Hernandez-Castro	University of Kent, UK
Daniel Holcomb	UMass Amherst, USA
Qiao Hu	City University of Hong Kong, Hong Kong, SAR China
Xinyi Huang	Fujian Normal University, PR China
Michael Hutter	Cryptography Research, USA
Timo Kasper	Kasper & Oswald GmbH, Germany
Zhe Liu	Nanjing University of Aeronautics and Astronautics, PR China
Joseph Liu	Monash University, Australia
N.W. Lo	National Taiwan University of Science and Technology, Taiwan
Stefan Mangard	TU Graz, Austria
Ivan Martinovic	University of Oxford, UK
Aikaterini Mitrokotsa	Chalmers University of Technology, Sweden
David Oswald	University of Birmingham, UK
Bart Preneel	KU Leuven COSIC and iMinds, Belgium
Daniel Ramotsoela	University of Pretoria, South Africa
Aanjhan Ranganathan	ETH Zurich, Switzerland
Matt Robshaw	Impinj, USA
Kazuo Sakiyama	University of Electro-Communications, Japan
Damien Sauveron	XLIM (UMR University of Limoges/CNRS 7252), France
Nitesh Saxena	University of Alabama at Birmingham, USA
Patrick Schaumont	Virginia Tech, USA
Willy Susilo	University of Wollongong, Australia
Nils Ole Tippenhauer	Singapore University of Technology and Design, Singapore
Avishai Wool	Tel Aviv University, Israel
Bin Xiao	Hong Kong Polytechnic University, Hong Kong, SAR China
Anjia Yang	Jinan University, PR China
Chan Yeob Yuen	Khalifa University, UAE
Yunhui Zhuang	City University of Hong Kong, Hong Kong, SAR China
Lavinia Dinca	City University of Hong Kong, Hong Kong, SAR China

Additional Reviewers

Zheng Gong
Lin Hou
Jia-Nan Liu
Pedro Maat Massolino
Veelasha Moonsamy
Ajaya Neupane
Peter Pessl
Maliheh Shirvanian
Prakash Shrestha
Bo Sun
Thomas Unterluggauer
Xu Yang
Yuexin Zhang
Chuan Zhao

Sponsoring Institutions

City University of Hong Kong, Hong Kong, SAR China

Contents

Protocols

Side Channel and Hardware

Cards and Tokens

Proximity

Communication