

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

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

Siddika Berna Ors Yalcin (Ed.)

Radio Frequency Identification: Security and Privacy Issues

6th International Workshop, RFIDSec 2010
Istanbul, Turkey, June 8-9, 2010
Revised Selected Papers



Springer

Volume Editor

Siddika Berna Ors Yalcin
Istanbul Technical University
Faculty of Electrical and Electronics Engineering
Department of Electronics and Communication Engineering
34469 Maslak, Istanbul, Turkey
E-mail: siddika.ors@itu.edu.tr

Library of Congress Control Number: 2010937761

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, H.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-16821-3 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-16821-5 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

RFIDSec 2010, the 6th workshop on RFID Security, was held in İstanbul, Turkey, June 8–9, 2010. The workshop was sponsored by the FP7 Project ICE (Grant Agreement No: 206546) of The Scientific and Technological Research Council of Turkey—National Research Institute of Electronics and Cryptology (TÜBİTAK-UEKAE).

The workshop attracted a record number of 47 submissions from 23 countries, of which the Program Committee selected 17 for publication in the workshop proceedings, resulting in an acceptance rate of 40%. The review process followed strict standards: each paper received at least three reviews. The Program Committee included 31 members representing 13 countries and 5 continents. These members were carefully selected to represent academia, industry, and government, as well as to include world-class experts in various research fields of interest to RFIDSec. The Program Committee was supported by 38 external reviewers.

Additionally, the workshop included three excellent invited talks. Ari Juels from RSA Laboratories discussed his vision of RFID security, in a talk entitled “The Physical Basis of RFID Security.” Pim Tuyls from Intrinsic-ID described his experiences in a talk entitled “Hardware Intrinsic Security.” Serge Vaudenay from EPFL discussed his vision of privacy in RFID systems in a talk entitled “Privacy Models for RFID Schemes.”

I deeply thank A. Murat Apohan and Serhat Sağdıçoğlu, the General Chair and Co-chair of RFIDSec 2010, for their excellent and always timely work on managing the local organization and orchestrating conference logistics. I would like to deeply thank the Steering Committee of RFIDSec for their trust, constant support, guidance, and kind advice on many occasions. Special thanks go to Vincent Rijmen, Manfred Aigner, and Gildas Avoine, who were always first to respond to my questions and concerns, and often volunteered the advice and support needed to resolve a wide array of challenging issues associated with the fair, firm, and transparent management of the evaluation process.

Finally, I would like to profoundly thank and salute all the authors from all over the world who submitted their papers to this workshop, and entrusted us with a fair and objective evaluation of their work. I appreciate your creativity, hard work, and commitment to push forward the frontiers of science.

June 2010

Berna Örs

Organization

RFIDSec 2010 was organized by The Scientific and Technological Research Council of Turkey—National Research Institute of Electronics and Cryptology (TÜBİTAK-UEKAE).

Executive Committee

Conference Chair	A. Murat Apohan <i>TÜBİTAK-UEKAE, Turkey</i>
Conference Co-chair	Serhat Sağdıçoğlu <i>TÜBİTAK-UEKAE, Turkey</i>
Program Chair	Berna Örs <i>İstanbul Technical University, Turkey</i>
Local Organizations	Müzeyyen Gökçen Arslan <i>TÜBİTAK-UEKAE, Turkey</i> Hüseyin Demirci <i>TÜBİTAK-UEKAE, Turkey</i>

Program Committee

Manfred Aigner	TU Graz, Austria
Özgür B. Akan	Middle East Technical University, Turkey
Mete Akgün	TÜBİTAK-UEKAE, Turkey
Gildas Avoine	UCL, Louvain-la-Neuve, Belgium
Lejla Batina	Radboud University Nijmegen, The Netherlands and Katholieke Universiteit Leuven, Belgium
Mike Burmester	Florida State University, USA
Ufuk Çağlayan	Boğaziçi University, Turkey
Vanessa Daza	Universitat Pompeu Fabra, Catalonia, Spain
Stephan Engberg	Priway ApS, Denmark
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalonia, Spain
Julio Cesar Hernandez-Castro	University of Portsmouth, UK
Talha Işık	Middle East Technical University, Turkey
Christian Damsgaard Jensen	Technical University of Denmark, Denmark
Yongki Lee	University of California, Los Angeles, USA
Kerstin Lemke-Rust	Ruhr Universität Bochum, Germany
Antoni Martinez-Balleste	Universitat Rovira i Virgili, Catalonia, Spain
Florian Michahelles	ETHZ, Switzerland
David Molnar	Microsoft Research Redmond, USA

VIII Organization

Axel Poschmann	Nanyang Technological University, Singapore
Damith Ranasinghe	University of Adelaide, Australia
Ahmad-Reza Sadeghi	Ruhr Universitat Bochum, Germany
Kazuo Sakiyama	The University of Electro Communications, Japan
Bernd Sieker	Universitat Bielefeld, Germany
Agusti Solanas	Rovira i Virgili University, Catalonia, Spain
Andrea Soppera	British Telecom, UK
François-Xavier Standaert	UC Louvain-la-Neuve, Belgium
Paul Syverson	Naval Research Laboratory, USA
Juan E. Tapiador	University of York, UK
Alp Üstündağ	İstanbul Technical University, Turkey
Avishai Wool	Tel Aviv University, Israel

Referees

Atakan Arslan	Selçuk Kavut	Pedro Peris-Lopez
Santoso Bagus	Yutaka Kawai	Thomas Plos
Selçuk Baktır	Chong-Hee Kim	Gökay Saldamlı
Muhammed Ali Bingöl	Mehmet Sabır Kiraz	Erkay Savaş
Sandra Dominikus	Miroslav Knezevic	Jorn Marc Schmidt
Özgür Ergül	Heiko Knospe	Ali Aydın Selçuk
Albert Fernández-Mir	Benjamin Martin	Stefaan Seys
Flavio Garcia	Tania Martin	Dave Singelee
Yoshikazu Hanatani	Charlotte Miolane	Rolando Trujillo Rasua
Michael Hutter	Miyako Ohkubo	Pim Vullers
Orhun Kara	Yaman Özelçi	Christian Wachsmann
Süleyman Kardaş	Thomas Brochmann	Lei Wang
Timo Kasper	Pedersen	Erich Wenger

Sponsoring Institutions

The Scientific and Technological Research Council of Turkey—National Research Institute of Electronics and Cryptology (TÜBİTAK-UEKAE)
FP7 project ICE (Grant Agreement No: 206546)

Table of Contents

Invited Talk 1

The Physical Basis of RFID Security	1
<i>Ari Juels</i>	

Session 1

Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model	2
<i>Nitesh Saxena and Jonathan Voris</i>	
Cryptanalysis of the David-Prasad RFID Ultralightweight Authentication Protocol	22
<i>Julio Cesar Hernandez-Castro, Pedro Peris-Lopez, Raphael C.-W. Phan, and Juan M.E. Tapiador</i>	
Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones	35
<i>Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis</i>	
Strong Authentication and Strong Integrity (SASI) Is Not That Strong	50
<i>Gildas Avoine, Xavier Carpent, and Benjamin Martin</i>	

Invited Talk 2

Privacy Models for RFID Schemes	65
<i>Serge Vaudenay</i>	

Session 2

On the Claimed Privacy of EC-RAC III.	66
<i>Junfeng Fan, Jens Hermans, and Frederik Vercauteren</i>	
EC-RAC: Enriching a Capacious RFID Attack Collection	75
<i>Ton van Deursen and Saša Radomirović</i>	
Anonymous RFID Authentication Using Trusted Computing Technologies	91
<i>Kurt Dietrich</i>	

Tree-Based RFID Authentication Protocols Are Definitively Not Privacy-Friendly	103
<i>Gildas Avoine, Benjamin Martin, and Tania Martin</i>	

Invited Talk 3

Hardware Intrinsic Security	123
<i>Pim Tuyls</i>	

Session 3

Privacy-Preserving Pattern Matching for Anomaly Detection in RFID Anti-Counterfeiting	124
<i>Florian Kerschbaum and Nina Oertel</i>	
Time Measurement Threatens Privacy-Friendly RFID Authentication Protocols	138
<i>Gildas Avoine, Iwen Coisel, and Tania Martin</i>	
Anonymous Authentication for RFID Systems	158
<i>Frederik Armknecht, Liqun Chen, Ahmad-Reza Sadeghi, and Christian Wachsmann</i>	
Leakage-Resilient RFID Authentication with Forward-Privacy	176
<i>Shin'ichiro Matsuo, Le Trieu Phong, Miyako Ohkubo, and Moti Yung</i>	

Session 4

An ECDSA Processor for RFID Authentication	189
<i>Michael Hutter, Martin Feldhofer, and Thomas Plos</i>	
Towards a Practical Solution to the RFID Desynchronization Problem	203
<i>Gerhard de Koning Gans and Flavio D. Garcia</i>	

Session 5

Optimal Security Limits of RFID Distance Bounding Protocols	220
<i>Orhun Kara, Süleyman Kardaş, Muhammed Ali Bingöl, and Gildas Avoine</i>	
The Poulidor Distance-Bounding Protocol	239
<i>Rolando Trujillo-Rasua, Benjamin Martin, and Gildas Avoine</i>	
A Lightweight Implementation of Keccak Hash Function for Radio-Frequency Identification Applications	258
<i>Elif Bilge Kavun and Tolga Yalcin</i>	

Author Index	271
--------------------	-----