Lecture Notes in Computer Science 7055

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Ari Juels Christof Paar (Eds.)

RFID
Security and Privacy

7th International Workshop, RFIDSec 2011
Amherst, MA, USA, June 26-28, 2011
Revised Selected Papers

Springer

Volume Editors

Ari Juels
RSA Laboratories/EMC
11 Cambridge Center
Cambridge, MA 02142, USA
E-mail: ajuels@rsa.com

Christof Paar
Ruhr University Bochum
Horst Görtz Institute for IT-Security
44780 Bochum, Germany
E-mail: christof.paar@rub.de

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-25285-3 e-ISBN 978-3-642-25286-0
DOI 10.1007/978-3-642-25286-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011944230

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

RFIDSec 2011, the 7th workshop on RFID Security and Privacy, was held in Amherst and Northampton, Massachusetts, USA, during June 26–28, 2011.

The workshop attracted 21 submissions, of which the Program Committee selected 12 for publication in the workshop proceedings. The accepted papers dealt with the topics of on-tag cryptography, attacks, security through physics, and protocol-level security. The Program Committee included 26 subject-matter experts from 14 countries, and represented academia, industry, and government.

An excellent array of invited talks complemented the paper sessions. Adi Shamir of the Weizmann Institute of Science (Israel) gave the RFIDSec 2011 keynote talk, "Minimalism in Cryptography," an overview of his recent results in the theory of cipher design. Srdjan Capkun highlighted the limitations of logical-layer privacy protections in his invited talk, "On Physical-Layer Identification of RFID Tags." At the workshop banquet, Collin Mulliner gave an update on NFC security ("Hacking Your NFC Phone and Service: The Good News and the Bad News"). Offering an industry perspective on the work of RFID (and other) standards bodies, Ravi Pappu informed and regaled workshop attendees with a talk entitled "The Making of Camels."

For the first time, RFIDSec offered tutorials in highly relevant areas. The four tutorials preceding the workshop were: Matt Reynolds and Ravi Pappu taught "The Physics of RFID," David Oswald and Timo Kasper, "Hands-on Side Channel Attacks Against Smart Cards and Other Tokens," Shane Clark, Ben Ransford, Mastooreh Salajegheh, and Hong Zhang, "Hands-on Programming of Batteryless, RFID-Scale Computers with Sensors," and Ari Juels, "Introduction to RFID Security and Privacy."

We wish to thank the generous sponsors of RFIDSec 2011: Microsoft Research, Mocana, Cryptography Research, the National Science Foundation, the Institute for Information Infrastructure Protection (I3P), the *RFID Journal*, DIFRwear, and UMass Amherst. Deep thanks are also due to Kevin Fu for his outstanding organizational efforts as General Chair, and to Wendy Cooper for her tireless support as Conference Coordinator.

August 2011

Ari Juels
Christof Paar

Organization

General Chair

Kevin Fu	UMass Amherst, USA

Program Chairs

Ari Juels	RSA Laboratories, USA
Christof Paar	Ruhr University Bochum, Germany

Program Committee

Gildas Avoine	UCL, Louvain-la-Neuve, Belgium
Lejla Batina	Radboud University Nijmegen, The Netherlands
Wayne Burleson	UMass Amherst, USA
Vanesa Daza	Universitat Pompeu Fabra, Spain
Josep Domingo-Ferrer	Univ.Rovira i Virgili, Spain
Henri Gilbert	France
Jorge Guajardo	Philips Research, The Netherlands
Julio César Hernández Castro	University of Portmouth, UK
Christian Damsgaard Jensen	DTU, Denmark
Süleyman Kardas	Tubitak Uekae, Turkey
Tom Karygiannis	NIST, USA
Farinaz Koushanfar	Rice University, USA
Kerstin Lemke-Rust	Universität Bonn-Rhein-Sieg, Germany
Antoni Martinez-Balleste	Rovira i Virgili University, Spain
Florian Michahelles	ETHZ, Switzerland
David Molnar	Microsoft Research Redmond, USA
Karsten Nohl	Security Research Labs, Germany
Berna Ors	Istanbul Technical University, Turkey
Axel Poschmann	Nanyang Technical University, Singapore
Kazuo Sakiyama	Univ.of Electro Communic., Japan
Nitesh Saxena	NYU-Poly, USA
Joshua Smith	University of Washington, USA
Agusti Solanas	Rovira i Virgili University, Spain
Juan E. Tapiador	University of York, UK
Ingrid Verbauwhede	KU Leuven, Belgium
Avishai Wool	Tel Aviv University, Israel

External Reviewers

T. Akishita
M.A. Bingol
X. Carpent
T. Halevi
Y. Hanatani
C.H. Kim
P. Peris-Lopez
B. Martin
A. Mirhoseini
J.M. Seguí
J. Takahashi
R. Trujillo-Rasúa
M. Valis
M.G. Vasco
J. Voris
A. Vosoughi
Y. Oren

RFIDSec 2011 Sponsors

Cryptography Research
DIFRwear
I3P
Microsoft Research
Mocana
National Science Foundation
RFID Journal
UMass Amherst

RFIDSec Steering Committee

Manfred Aigner	TU Graz, Austria
Gildas Avoine (Chair)	UCL, Louvain-la-Neuve, Belgium
Kevin Fu	UMass Amherst, USA
Yingjiu Li	Singapore Management University, Singapore
Christof Paar	Ruhr University Bochum, Germany
Bart Preneel	KU Leuven, Belgium
Vincent Rijmen	TU Graz, Austria; KU Leuven, Belgium

Table of Contents