Lecture Notes in Computer Science 7344

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

Stefan Katzenbeisser Edgar Weippl
L. Jean Camp Melanie Volkamer
Mike Reiter Xinwen Zhang (Eds.)

Trust and Trustworthy Computing

5th International Conference, TRUST 2012
Vienna, Austria, June 13-15, 2012
Proceedings

Springer

Volume Editors

Stefan Katzenbeisser
Melanie Volkamer
Technical University Darmstadt, Germany
E-mail: katzenbeisser@seceng.informatik.tu-darmstadt.de
and melanie.volkamer@cased.de

Edgar Weippl
Vienna University of Technology and SBA Research, Austria
E-mail: edgar.weippl@tuwien.ac.at

L. Jean Camp
Indiana University, Bloomington, IN, USA
E-mail: ljcamp@indiana.edu

Mike Reiter
University of North Carolina at Chapel Hill, USA
E-mail: reiter@cs.unc.edu

Xinwen Zhang
Huawei America R&D, Santa Clara, CA, USA
E-mail: xinwen.zhang@huawei.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-30920-5 e-ISBN 978-3-642-30921-2
DOI 10.1007/978-3-642-30921-2
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012938995

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

LNCS Sublibrary: SL 4 – Security and Cryptology

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

This volume contains the proceedings of the 5th International Conference on Trust and Trustworthy Computing (TRUST) held in Vienna, Austria, during June 13–15, 2012. Continuing the tradition of the previous conferences, which were held in Villach (2008), Oxford (2009), Berlin (2010) and Pittsburgh (2011), TRUST 2012 featured both a technical and a socio-economic track. TRUST thus continues to provide a unique interdisciplinary forum for researchers, practitioners and decision makers to explore new ideas in designing, building and using trustworthy computing systems. This year's technical track provided a good mix of topics ranging from trusted computing and mobile devices to applied cryptography and physically unclonable functions, while the socio-economic track focused on the emerging field of usable security.

Out of 36 submissions to the technical track and 12 submissions to the socio-economic track, we assembled a program consisting of 20 papers. In addition, TRUST 2012 featured a poster session for rapid dissemination of the latest research results, invited talks, as well as a panel discussion on future challenges of trust in mobile and embedded devices.

We would like to thank everyone for their efforts in making TRUST 2012 a success: the members of the Organizing Committee, in particular Yvonne Poul, for their tremendous help with all aspects of the organization; the members of the Program Committees of both tracks for their efforts in selecting high-quality research papers to be presented at the conference; all external reviewers who helped to maintain the quality of theconference; the keynote speakers and panel members; and most importantly all authors who submitted their work to TRUST 2012. Finally, we express our gratitude to our sponsors Intel and Hewlett-Packard, whose support was crucial for the success of TRUST 2012.

April 2012

L. Jean Camp
Stefan Katzenbeisser
Mike Reiter
Melanie Volkamer
Edgar Weippl
Xinwen Zhang

Organization

Steering Committee

Alessandro Acquisti	Carnegie Mellon University, USA
Boris Balacheff	Hewlett Packard, UK
Paul England	Microsoft, USA
Andrew Martin	University of Oxford, UK
Chris Mitchell	Royal Holloway, University of London, UK
Sean Smith	Dartmouth College, USA
Ahmad-Reza Sadeghi	TU Darmstadt / Fraunhofer SIT, Germany
Claire Vishik	Intel, UK

General Chairs

Edgar Weippl	Vienna University of Technology and SBA Research, Austria
Stefan Katzenbeisser	TU Darmstadt, Germany

Program Chairs (Technical Strand)

Mike Reiter	University of North Carolina at Chapel Hill, USA
Xinwen Zhang	Huawei, USA

Program Committee (Technical Strand)

Srdjan Capkun	ETHZ Zurich, Switzerland
Haibo Chen	Fudan University, China
Xuhua Ding	Singapore Management University, Singapore
Jan-Erik Ekberg	Nokia Research Center
Cedric Fournet	Microsoft Research, UK
Michael Franz	UC Irvine, USA
Tal Garfinkel	VMWare
Trent Jaeger	Penn State University, USA
Xuxian Jiang	NCSU, USA
Apu Kapadia	Indiana University, USA
Jiangtao Li	Intel Labs
Peter Loscocco	NSA, USA
Heiko Mantel	TU Darmstadt, Germany
Jonathan McCune	Carnegie Mellon University, USA

Bryan Parno	Microsoft Research, UK
Reiner Sailer	IBM Research, USA
Matthias Schunter	IBM Zurich, Switzerland
Jean-Pierre Seifert	DT-Lab, Germany
Elaine Shi	PARC, USA
Sean Smith	Dartmouth College, USA
Christian Stueble	Sirrix AG, Germany
Edward Suh	Cornell University, USA
Neeraj Suri	TU Darmstadt, Germany
Jesse Walker	Intel Labs
Andrew Warfield	University of British Columbia, Canada

Program Chairs (Socio-economic Strand)

L. Jean Camp	Indiana University, USA
Melanie Volkamer	TU Darmstadt and CASED, Germany

Program Committee (Socio-economic Strand)

Alexander De Luca	University of Munich, Germany
Angela Sasse	University College London, UK
Artemios G. Voyiatzis	Industrial Systems Institute/ATHENA R.C, Greece
Eleni Kosta	Katholieke Universiteit Leuven, Belgium
Gabriele Lenzini	University of Luxembourg, Luxembourg
Guenther Pernul	Regensburg University, Germany
Heather Lipford	University of North Caronlina at Charlotte, USA
Ian Brown	University of Oxford, UK
Jeff Yan	Newcastle University, UK
Kristiina Karvonen	Helsinki Institute for Information Technology, Finland
Mario Cagalj	University of Split, Croatia
Mikko Siponen	Universtiyof Oulu, Finland
Pam Briggs	Northumbria University, UK
Peter Buxmann	TU Darmstadt, Germany
Peter Y A Ryan	University of Luxembourg, Luxembourg
Randi Markussen	University of Copenhagen, Denmark
Simone Fischer-Huebner	Karlstad University, Sweden

Sonia Chiasson	Carleton University, Canada
Stefano Zanero	Politecnico di Milano, Italy
Sven Dietrich	Stevens Institute of Technology, USA
Tara Whalen	Carleton University, Canada
Yolanta Beres	HP Labs, USA
Yang Wang	Carnegie Mellon University, USA
Debin Liu	PayPal

Publicity Chair

Marcel Winandy	Ruhr University Bochum, Germany

Table of Contents

Technical Strand

Authenticated Encryption Primitives for Size-Constrained Trusted Computing 1
Jan-Erik Ekberg, Alexandra Afanasyeva, and N. Asokan

Auditable Envelopes: Tracking Anonymity Revocation Using Trusted Computing 19
Matt Smart and Eike Ritter

Lockdown: Towards a Safe and Practical Architecture for Security Applications on Commodity Platforms 34
Amit Vasudevan, Bryan Parno, Ning Qu, Virgil D. Gligor, and Adrian Perrig

Experimenting with Fast Private Set Intersection 55
Emiliano De Cristofaro and Gene Tsudik

Reliable Device Sharing Mechanisms for Dual-OS Embedded Trusted Computing 74
Daniel Sangorrín, Shinya Honda, and Hiroaki Takada

Modelling User-Centered-Trust (UCT) in Software Systems: Interplay of Trust, Affect and Acceptance Model 92
Zahid Hasan, Alina Krischkowsky, and Manfred Tscheligi

Clockless Physical Unclonable Functions 110
Julian Murphy

Lightweight Distributed Heterogeneous Attested Android Clouds 122
Martin Pirker, Johannes Winter, and Ronald Toegl

Converse PUF-Based Authentication 142
Ünal Kocabaş, Andreas Peter, Stefan Katzenbeisser, and Ahmad-Reza Sadeghi

Trustworthy Execution on Mobile Devices: What Security Properties Can My Mobile Platform Give *Me*? 159
Amit Vasudevan, Emmanuel Owusu, Zongwei Zhou, James Newsome, and Jonathan M. McCune

Verifying System Integrity by Proxy 179
Joshua Schiffman, Hayawardh Vijayakumar, and Trent Jaeger

Virtualization Based Password Protection against Malware in Untrusted Operating Systems 201
Yueqiang Cheng and Xuhua Ding

SmartTokens: Delegable Access Control with NFC-Enabled Smartphones 219
Alexandra Dmitrienko, Ahmad-Reza Sadeghi, Sandeep Tamrakar, and Christian Wachsmann

A Belief Logic for Analyzing Security of Web Protocols 239
Apurva Kumar

Provenance-Based Model for Verifying Trust-Properties 255
Cornelius Namiluko and Andrew Martin

Socio-economic Strand

On the Practicality of Motion Based Keystroke Inference Attack 273
Liang Cai and Hao Chen

AndroidLeaks: Automatically Detecting Potential Privacy Leaks in Android Applications on a Large Scale 291
Clint Gibler, Jonathan Crussell, Jeremy Erickson, and Hao Chen

Why Trust Seals Don't Work: A Study of User Perceptions and Behavior 308
Iacovos Kirlappos, M. Angela Sasse, and Nigel Harvey

Launching the New Profile on Facebook: Understanding the Triggers and Outcomes of Users' Privacy Concerns 325
Saijing Zheng, Pan Shi, Heng Xu, and Cheng Zhang

Author Index 341