

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

Simone Fischer-Hübner Nicholas Hopper (Eds.)

Privacy Enhancing Technologies

11th International Symposium, PETS 2011
Waterloo, ON, Canada, July 27-29, 2011
Proceedings

Volume Editors

Simone Fischer-Hübner

Karlstad University, Department of Computer Science

Universitetsgatan 1, 65188 Karlstad, Sweden

E-mail: simone.fischer-huebner@kau.se

Nicholas Hopper

University of Minnesota, Department of Computer Science and Engineering

200 Union Street SE, Minneapolis, MN 55455, USA

E-mail: hopper@cs.umn.edu

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-22262-7

e-ISBN 978-3-642-22263-4

DOI 10.1007/978-3-642-22263-4

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011930843

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© by Authors 2011

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.

The use of general descriptive names, registered names, trademarks, 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.

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)

Message from the Program Chairs

The 2011 Privacy-Enhancing Technologies Symposium was held at the University of Waterloo in Waterloo, Canada, during July 27-29, 2011. It was the 11th in this series of meetings, and the fourth after the transition from workshop to symposium. PETS remains a premier forum for publishing research on both the theory and the practice of privacy-enhancing technologies, and has a broad scope that includes all facets of the field.

The PETS program this year included a diverse set of 15 peer-reviewed papers, selected from 61 submissions. Each submission was reviewed by at least three members of the Program Committee. This was the fourth year of the popular HotPETs session, designed as a venue to present exciting but still preliminary and evolving ideas, rather than formal and rigorous completed research results. As in past years, there were no published proceedings for HotPETs. PETS also included the traditional “rump session,” with brief presentations on a variety of topics, and a panel entitled “On the Ethics of Research on Tor Users.”

In addition to the peer-reviewed sessions, PETS 2011 included an invited panel dedicated to the memory of Andreas Pfitzmann, who passed away in September 2010. Andreas was a pioneer in privacy research, and one of the founders of this symposium. As a computer scientist with the rare ability to clearly explain important positions to both scientists and policy makers, he was influential in shaping both German and European technology policy. His absence is a great loss to our community and we dedicated this meeting to his memory.

We are grateful to all of the authors who submitted, to the PETS and HotPETs speakers who presented their work selected for the program, and to the rump session participants. We are also grateful to the Program Committee members, and to the external reviewers who assisted them, for their thorough reviews and participation in discussions – they were central to the resulting high-quality program. The following subset of these reviewers gracefully volunteered to continue their work as shepherds helping the authors improve their papers and address the reviewer comments and suggestions: Simson Garfinkel, Gregory Neven, Matthew Wright, Tom Benjamin, and Roger Dingledine. It is also a pleasure to acknowledge the contribution of our General Chairs, Katrina Hanna and Ian Goldberg, and our webmaster since 2007, Jeremy Clark, who did his usual outstanding job at evolving and maintaining the symposium’s website. Our gratitude also goes to the HotPETs Chairs, Carmela Troncoso and Julien Freudiger, who put together an outstanding HotPETs program. Finally, we are particularly grateful to Microsoft for its continued sponsorship and support.

May 2011

Simone Fischer-Hübner
Nicholas Hopper

Organization

General Chairs	Ian Goldberg (University of Waterloo, Canada)
	Katrina Hanna (Research in Motion, Canada)
Program Chairs	Simone Fischer-Hübner (Karlstad University, Sweden)
	Nicholas Hopper (University of Minnesota, USA)
PET Award Chair	Claudia Diaz (K.U. Leuven, Belgium)
Stipends Chair	Roger Dingledine (The Tor Project, USA)
HotPETS Chairs	Julien Freudiger (EPFL, Switzerland)
	Carmela Troncoso (K.U. Leuven, Belgium)

Program Committee

Kevin Bauer	University of Waterloo, Canada
Jean Camp	Indiana University, USA
George Danezis	Microsoft Research, UK
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Claudia Diaz	K.U. Leuven, Belgium
Roger Dingledine	The Tor Project, USA
Hannes Federrath	University of Regensburg, Germany
Julien Freudiger	EPFL, Switzerland
Simson Garfinkel	Naval Postgraduate School, USA
Rachel Greenstadt	Drexel University, USA
Thomas S. Benjamin	Cryptocracy LLC, USA
Jean-Pierre Hubaux	EPFL, Switzerland
Aaron Johnson	University of Texas at Austin, USA
Bradley Malin	Vanderbilt University, USA
Damon McCoy	University of California San Diego, USA
Aleecia McDonald	Carnegie Mellon University, USA
David Molnar	Microsoft Research, USA
Steven Murdoch	University of Cambridge, UK
Shishir Nagaraja	IIT Delhi, India
Arvind Narayanan	Stanford University, USA
Gregory Neven	IBM Research - Zurich, Switzerland
Pierangela Samarati	University of Milan, Italy
Adam Smith	Pennsylvania State University, USA
Carmela Troncoso	K.U. Leuven, Belgium
Matthew Wright	University of Texas at Arlington, USA

External Reviewers

Ero Balsa	Grigorios Loukides
Aaron Beach	Nick Mathewson
Igor Bilogrevic	Stephen McLaughlin
Michael Brennan	Prateek Mittal
Maria Dubovitskaya	Thomas Ristenpart
Elizabeth Durham	Len Sassaman
Sara Foresti	Stefan Schiffner
Daniel Halperin	Andrei Serjantov
Urs Hengartner	Micah Sherr
Ryan Henry	Reza Shokri
Victor Heorhiadi	Paul Syverson
Mathias Humbert	Acar Tamersoy
Murtuza Jadliwala	Eugene Vasserman
Ravi Jhawar	Nevena Vratonjic
Zi Lin	Nan Zhang
Giovanni Livraga	

Table of Contents

How Unique and Traceable are Usernames?	1
<i>Daniele Perito, Claude Castelluccia, Mohamed Ali Kaafar, and Pere Manils</i>	
Text Classification for Data Loss Prevention	18
<i>Michael Hart, Pratyusa Manadhata, and Rob Johnson</i>	
P3CA: Private Anomaly Detection Across ISP Networks	38
<i>Shishir Nagaraja, Virajith Jalaparti, Matthew Caesar, and Nikita Borisov</i>	
Quantifying Location Privacy: The Case of Sporadic Location Exposure	57
<i>Reza Shokri, George Theodorakopoulos, George Danezis, Jean-Pierre Hubaux, and Jean-Yves Le Boudec</i>	
Privacy in Mobile Computing for Location-Sharing-Based Services	77
<i>Igor Bilogrevic, Murtuza Jadliwala, Kübra Kalkan, Jean-Pierre Hubaux, and Imad Aad</i>	
On the Practicality of UHF RFID Fingerprinting: How Real is the RFID Tracking Problem?	97
<i>Davide Zanetti, Pascal Sachs, and Srdjan Capkun</i>	
An Accurate System-Wide Anonymity Metric for Probabilistic Attacks	117
<i>Rajiv Bagai, Huabo Lu, Rong Li, and Bin Tang</i>	
DefenestraTor: Throwing Out Windows in Tor	134
<i>Mashael AlSabah, Kevin Bauer, Ian Goldberg, Dirk Grunwald, Damon McCoy, Stefan Savage, and Geoffrey M. Voelker</i>	
Privacy-Implications of Performance-Based Peer Selection by Onion-Routers: A Real-World Case Study Using I2P	155
<i>Michael Herrmann and Christian Grothoff</i>	
Privacy-Friendly Aggregation for the Smart-Grid	175
<i>Klaus Kursawe, George Danezis, and Markulf Kohlweiss</i>	
Plug-In Privacy for Smart Metering Billing	192
<i>Marek Jawurek, Martin Johns, and Florian Kerschbaum</i>	

Scramble! Your Social Network Data	211
<i>Filipe Beato, Markulf Kohlweiss, and Karel Wouters</i>	
A Constraint Satisfaction Cryptanalysis of Bloom Filters in Private Record Linkage	226
<i>Mehmet Kuzu, Murat Kantarcioglu, Elizabeth Durham, and Bradley Malin</i>	
Efficient Proofs of Attributes in Pairing-Based Anonymous Credential System	246
<i>Amang Sudarsono, Toru Nakanishi, and Nobuo Funabiki</i>	
Broker-Based Private Matching	264
<i>Abdullatif Shikfa, Melek Önen, and Refik Molva</i>	
Author Index	285