

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 Matthew Wright (Eds.)

Privacy Enhancing Technologies

12th International Symposium, PETS 2012
Vigo, Spain, July 11-13, 2012
Proceedings

Volume Editors

Simone Fischer-Hübner
Karlstad University
Department of Computer Science
Universitetsgatan 2, 65188, Karlstad, Sweden
E-mail: simone.fischer-huebner@kau.se

Matthew Wright
University of Texas at Arlington
Department of Computer Science and Engineering
500 UTA Blvd., Arlington, TX 76019, USA
E-mail: mwright@uta.edu

ISSN 0302-9743
ISBN 978-3-642-31679-1
DOI 10.1007/978-3-642-31680-7
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-31680-7

Library of Congress Control Number: 2012940986

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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)

Preface

Privacy and anonymity are increasingly important in the online world. Corporations, governments, and other organizations are realizing and exploiting their power to track users and their behavior. Approaches to protecting individuals, groups, but also companies and governments from profiling and censorship include decentralization, encryption, distributed trust, and automated policy disclosure.

The 2012 Privacy Enhancing Technologies Symposium (PETS 2012) addressed the design and realization of such privacy services for the Internet and other data systems and communication networks by bringing together privacy and anonymity experts from around the world to discuss recent advances and new perspectives.

PETS 2012 was held in Vigo, Spain, during July 11–13, 2012. It was the 12th in the series of events, and the fifth after the transition from workshop to symposium. The PETS symposium remains a premier scientific international event for publishing on both the theory and practice of privacy-enhancing technologies, and it has a broad scope that includes all facets of the field.

PETS 2012 received 72 submissions, which were all reviewed by at least three members of the international Program Committee (PC). Based on an intensive discussion among the reviewers and other PC members, 16 papers were finally accepted for presentation at the PETS symposium. Topics addressed by the accepted papers published in the proceedings include anonymization of statistics, content, and traffic, network traffic analysis, censorship-resistant systems, user profiling, training users in privacy risk management, and privacy for Internet and cloud-based services.

A further highlight of PETS 2012 was 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. HotPETs included an invited keynote talk by Moez Chakchouk, the head of the Tunisian Internet Agency. As with the previous four HotPETs in the past, there were no published proceedings for HotPETs. PETS also included a panel on “The impact of upcoming privacy legislation for PETs” organized and moderated by Marit Hansen and a rump session with brief presentations on a variety of topics. Additionally, a workshop on Provable Privacy was held in conjunction with PETS 2012.

We would like to thank all PETS and HotPETs authors, especially those who presented their work selected for the program, as well as all rump session presenters. Moreover, we are very grateful to all PC members and additional reviewers, who contributed with thorough reviews and actively participated in the PC discussions, ensuring a high quality of all accepted papers. We owe special thanks to the following PC members and reviewers, who volunteered to shepherd

some of the accepted papers: Emiliano De Cristofaro, Erman Ayday, Roger Dingledine, Thomas S. Benjamin, Nicholas Hopper, Aaron Johnson, Damon McCoy, and Arvind Narayanan.

We gratefully acknowledge the outstanding contributions of the PETS 2012 General Chair, Carmela Troncoso, the Local Arrangements Chair, Fernando Pérez-González, and of our webmaster since 2007, Jeremy Clark. Moreover, our gratitude goes to the HotPETs 2012 Chairs, Emiliano De Cristofaro and Julien Freudiger, who reviewed all HotPETs submissions and put together an excellent program. Last but not least, we would like to thank all sponsors of PETS 2012, including Ministerio de Economía y Cooperación (Spanish Ministry of Economy), Gradiant (Galician Research and Development Center in Advanced Telecommunications), and Ayuntamiento de Vigo (Vigo City Hall) for their generous support as well as Microsoft for its continued sponsorship.

May 2012

Simone Fischer-Hübner
Matthew Wright

Organization

Program Committee

Kevin Bauer	University of Waterloo, Canada
Thomas S. Benjamin	IBM Research Zurich, Switzerland
Jean Camp	Indiana University, USA
George Danezis	Microsoft Research, UK
Sabrina De Capitani Di Vimercati	DTI - Università degli Studi di Milano, Italy
Emiliano De Cristofaro	Palo Alto Research Center, USA
Roger Dingledine	The Tor Project, USA
Hannes Federrath	University of Hamburg, Germany
Julien Freudiger	EPFL, Switzerland
Simson Garfinkel	Naval Postgraduate School, USA
Rachel Greenstadt	Drexel University, USA
Nicholas Hopper	University of Minnesota, USA
Jean-Pierre Hubaux	EPFL, Switzerland
Renato Iannella	Semantic Identity, Australia
Aaron Johnson	Naval Research Laboratory, USA
Damon McCoy	George Mason University, USA
Alecia McDonald	Carnegie Mellon, USA
Steven Murdoch	University of Cambridge, UK
Shishir Nagaraja	University of Birmingham, UK
Arvind Narayanan	Stanford University, USA
Gregory Neven	IBM Research Zurich, Switzerland
Siani Pearson	HP Labs, UK
Kazuo Sako	NEC, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Michael Waidner	Fraunhofer SIT, Germany

Additional Reviewers

Acs, Gergely	Clauß, Sebastian	Herrmann, Dominik
Afroz, Sadia	Elahi, Tariq	Huguenin, Kevin
AlSabah, Mashael	Foresti, Sara	Humbert, Mathias
Anirban, Basu	Fuchs, Karl-Peter	Kadianakis, George
Appelbaum, Jacob	Furukawa, Jun	Kalabis, Lukas
Ayday, Erman	Garg, Vaibhav	Kohlweiss, Markulf
Basu, Anirban	Gerber, Christoph	Kreitz, Gunnar
Bilogrevic, Igor	Ghiglieri, Marco	Kuzu, Mehmet
Chothia, Tom	Henry, Ryan	Lindqvist, Janne

VIII Organization

Papanikolaou, Nick
Patil, Sameer
Pham, Vinh
Shokri, Reza
Simo, Hervais

Soriente, Claudio
Stopczynski, Martin
Tancock, David
Teranishi, Isamu
Uzun, Ersin

Wang, Qiyan
Zhang, Nan

Table of Contents

Session 1: User Profiling

Betrayed by Your Ads! Reconstructing User Profiles from Targeted Ads	1
<i>Claude Castelluccia, Mohamed-Ali Kaafar, and Minh-Dung Tran</i>	
Private Client-Side Profiling with Random Forests and Hidden Markov Models	18
<i>George Danezis, Markulf Kohlweiss, Benjamin Livshits, and Alfredo Rial</i>	

Session 2: Traffic Analysis

Understanding Statistical Disclosure: A Least Squares Approach	38
<i>Fernando Pérez-González and Carmela Troncoso</i>	
Website Detection Using Remote Traffic Analysis	58
<i>Xun Gong, Nikita Borisov, Negar Kiyavash, and Nabil Schear</i>	
k -Indistinguishable Traffic Padding in Web Applications	79
<i>Wen Ming Liu, Lingyu Wang, Kui Ren, Pengsu Cheng, and Mourad Debbabi</i>	
Spying in the Dark: TCP and Tor Traffic Analysis	100
<i>Yossi Gilad and Amir Herzberg</i>	

Session 3: Applied Differential Privacy

Secure Distributed Framework for Achieving ϵ -Differential Privacy	120
<i>Dima Alhadidi, Noman Mohammed, Benjamin C.M. Fung, and Mourad Debbabi</i>	
Differentially Private Continual Monitoring of Heavy Hitters from Distributed Streams	140
<i>T.-H. Hubert Chan, Mingfei Li, Elaine Shi, and Wenchang Xu</i>	
Adaptive Differentially Private Histogram of Low-Dimensional Data	160
<i>Chengfang Fang and Ee-Chien Chang</i>	

Session 4: PETs for Cloud Services and Smart Grids

PRISM – Privacy-Preserving Search in MapReduce	180
<i>Erik-Oliver Blass, Roberto Di Pietro, Refik Molva, and Melek Önen</i>	

Practical Privacy Preserving Cloud Resource-Payment for Constrained Clients	201
<i>Martin Pirker, Daniel Slamanig, and Johannes Winter</i>	

Fault-Tolerant Privacy-Preserving Statistics	221
<i>Marek Jawurek and Florian Kerschbaum</i>	

Session 5: Privacy Services

Evading Censorship with Browser-Based Proxies	239
<i>David Fifield, Nate Hardison, Jonathan Ellithorpe, Emily Stark, Dan Boneh, Roger Dingledine, and Phil Porras</i>	

Exploring the Ecosystem of Referrer-Anonymizing Services	259
<i>Nick Nikiforakis, Steven Van Acker, Frank Piessens, and Wouter Joosen</i>	

Session 6: User-Related Privacy Perspectives

Risk Communication Design: Video vs. Text	279
<i>Vaibhav Garg, L. Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber</i>	

Use Fewer Instances of the Letter “i”: Toward Writing Style Anonymization	299
<i>Andrew W.E. McDonald, Sadia Afroz, Aylin Caliskan, Ariel Stolerman, and Rachel Greenstadt</i>	

Author Index	319
---------------------------	-----