

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

University of Dortmund, 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 of Computer Science, Saarbruecken, Germany

Ian Goldberg Mikhail J. Atallah (Eds.)

Privacy Enhancing Technologies

9th International Symposium, PETS 2009
Seattle, WA, USA, August 5-7, 2009
Proceedings



Springer

Volume Editors

Ian Goldberg

University of Waterloo, David R. Cheriton School of Computer Science

200 University Avenue West, Waterloo, ON, N2L 3G1, Canada

E-mail: iang@cs.uwaterloo.ca

Mikhail J. Atallah

Purdue University, Department of Computer Science

305 North University Street, West Lafayette, IN 47907-2107, USA

E-mail: mja@cs.purdue.edu

Library of Congress Control Number: 2009930653

CR Subject Classification (1998): H.5, H.4, H.3, I.2, I.3, I.7, J.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-642-03167-6 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-03167-0 Springer Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg holds the exclusive right of distribution and reproduction of this work, for a period of three years starting from the date of publication.

springer.com

Printed in Germany

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

Printed on acid-free paper SPIN: 12719389 06/3180 5 4 3 2 1 0

Message from the Program Chairs

The 2009 Privacy Enhancing Technologies Symposium was held at the University of Washington in Seattle during August 5–7, 2009. This was the ninth in this series of meetings, and the second 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 14 peer-reviewed papers, selected from 44 submissions. Each submission was reviewed by at least four members of the Program Committee. This was the second 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. HotPETs this year included a program of 14 presentations of 10–20 minutes each; as was the case last year, there were no published proceedings for HotPETs. PETS also included the traditional “rump session,” with brief presentations on a variety of topics.

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: Alastair Beresford, Lorrie Cranor, Claudia Diaz, Steven Murdoch, and Carmela Troncoso. It is also a pleasure to acknowledge the contribution of our General Chair, Adam Shostack, who worked tirelessly on the local arrangements and logistical aspects of the symposium. The University of Washington helped to host the symposium, and our webmaster since 2007, Jeremy Clark, did his usual outstanding job at evolving and maintaining the symposium’s website. Our gratitude also goes to the HotPETs Chairs, Andrei Serjantov and Thomas Heydt-Benjamin, who put together an outstanding HotPETs program, as well as to Vitaly Shmatikov, who chaired the PET Award Selection Committee, and Roger Dingledine, for handling the stipends. Finally, in these tight economic times, we are particularly grateful to Microsoft for its sponsorship and support; it played a central role in helping attendees—especially students—meet registration and travel costs.

May 2009

Ian Goldberg
Mikhail Atallah

Organization

Organizers

General Chair
Program Chairs

PET Award Chair
Stipends Chair
HotPETs Chairs

Adam Shostack (Microsoft, USA)
Ian Goldberg (University of Waterloo, Canada)
Mikhail Atallah (Purdue University, USA)
Vitaly Shmatikov (University of Texas, USA)
Roger Dingleline (The Tor Project, USA)
Thomas Heydt-Benjamin (IBM Research
Zurich, Switzerland)
Andrei Serjantov (The Free Haven Project,
UK)

Program Committee

Alessandro Acquisti
Michael Backes

Mira Belenkiy
Alastair Beresford
Nikita Borisov

Lorrie Cranor
George Danezis
Sabrina De Capitani di

Vimercati
Claudia Diaz
Roger Dingleline
Alexandre Evfimievski
Philippe Golle
Rachel Greenstadt
Thomas Heydt-Benjamin
Apu Kapadia
Bradley Malin
Tal Malkin
Nick Mathewson
David Molnar
Steven Murdoch
Andreas Pfitzmann
Len Sassaman
Andrei Serjantov
Paul Syverson

Carnegie Mellon University, USA
Saarland University and Max Planck Institute
for Software Systems, Germany

Microsoft, USA
University of Cambridge, UK
University of Illinois at Urbana-Champaign,
USA

Carnegie Mellon University, USA
Microsoft Research Cambridge, UK

Università degli Studi di Milano, Italy
K.U. Leuven, Belgium

The Tor Project, USA
IBM Almaden Research Center, USA
Palo Alto Research Center, USA
Drexel University, USA

IBM Research Zurich, Switzerland
MIT Lincoln Laboratory, USA
Vanderbilt University, USA
Columbia University, USA
The Tor Project, USA

University of California, Berkeley, USA
University of Cambridge, UK
Dresden University of Technology, Germany
K.U. Leuven, Belgium
The Free Haven Project, UK
Naval Research Laboratory, USA

Marianne Winslett

University of Illinois at Urbana-Champaign,
USA

Matthew Wright

University of Texas at Arlington, USA

Ting Yu

North Carolina State University, USA

External Reviewers

Titus Abraham

Sadia Afroz

Elli Androulaki

Claudio Agostino Ardagna

Sruthi Bandhakavi

Stefan Berthold

John Bethencourt

Rainer Boehme

Katrin Borcea-Pfitzmann

Seung Geol Choi

Sebastian Clauß

Ariel Elbaz

David Evans

Michael Gagnon

Aris Gkoulalas-Divanis

Ragib Hasan

Keith Irwin

Peter Johnson

Zach Jorgensen

Hahna Kane

Benjamin Kellermann

Matthias Kirchner

Kush Kothari

Robert Lass

Grigorios Loukides

Homin Lee

Karsten Loesing

Grigorios Loukides

Nayantara Mallesh

Aaron Massey

Kazuhiro Minami

Esfandiar Mohammadi

Meredith L. Patterson

John Paulett

Stefanie Poetzsch

Sören Preibusch

Mariana Raykova

Sasha Romanosky

Aakash Shah

Entong Shen

Alex Simma

Robin Snader

Sandra Steinbrecher

Evan Sultanik

Evimaria Terzi

Carmela Troncoso

Patrick Tsang

Binh Vo

Wei Wei

Jan Werner

Charles Wright

Seung Yi

Charles Zhang

Table of Contents

Ninth Privacy Enhancing Technologies Symposium

Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden?	1
<i>Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M. Sadeh</i>	
Regulating Privacy in Wireless Advertising Messaging: FIPP Compliance by Policy vs. by Design	19
<i>Heng Xu, John W. Bagby, and Terence Ryan Melonas</i>	
A Comparative Study of Online Privacy Policies and Formats	37
<i>Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor</i>	
Vida: How to Use Bayesian Inference to De-anonymize Persistent Communications	56
<i>George Danezis and Carmela Troncoso</i>	
Scalable Link-Based Relay Selection for Anonymous Routing	73
<i>Micah Sherr, Matt Blaze, and Boon Thau Loo</i>	
Using Linkability Information to Attack Mix-Based Anonymity Services	94
<i>Stefan Schiffner and Sebastian Clauß</i>	
Physical Layer Attacks on Unlinkability in Wireless LANs	108
<i>Kevin Bauer, Damon McCoy, Ben Greenstein, Dirk Grunwald, and Douglas Sicker</i>	
RequestPolicy: Increasing Web Browsing Privacy through Control of Cross-Site Requests	128
<i>Justin Samuel and Beichuan Zhang</i>	
Enlisting ISPs to Improve Online Privacy: IP Address Mixing by Default	143
<i>Barath Raghavan, Tadayoshi Kohno, Alex C. Snoeren, and David Wetherall</i>	
Privacy-Preserving Policy-Based Information Transfer	164
<i>Emiliano De Cristofaro, Stanislaw Jarecki, Jihye Kim, and Gene Tsudik</i>	

Privacy-Preserving Computation and Verification of Aggregate Queries on Outsourced Databases	185
<i>Brian Thompson, Stuart Haber, William G. Horne, Tomas Sander, and Danfeng Yao</i>	
APOD: Anonymous Physical Object Delivery	202
<i>Elli Androulaki and Steven Bellovin</i>	
On the Optimal Placement of Mix Zones	216
<i>Julien Freudiger, Reza Shokri, and Jean-Pierre Hubaux</i>	
Privacy-Preserving Face Recognition	235
<i>Zekeriya Erkin, Martin Franz, Jorge Guajardo, Stefan Katzenbeisser, Inald Lagendijk, and Tomas Toft</i>	
Author Index	255