

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2482

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Roger Dingledine
Paul Syverson (Eds.)

Privacy Enhancing Technologies

Second International Workshop, PET 2002
San Francisco, CA, USA, April 14-15, 2002
Revised Papers



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Roger Dingledine
The Free Haven Project
144 Lake St., Arlington, MA 02474, USA
E-mail: arma@freehaven.net

Paul Syverson
Naval Research Laboratory
Washington DC 20375, USA

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): E.3, C.2, D.4.6, K.6.5, K.4, H.3, H.4, I.7

ISSN 0302-9743

ISBN 3-540-00565-X Springer-Verlag Berlin Heidelberg New York

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10870570 06/3142 5 4 3 2 1 0

Preface

The second Privacy Enhancing Technologies workshop (PET 2002), held April 14–15, 2002 in San Francisco, California, continued the enthusiasm and quality of the first workshop in July 2000 (then called “Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability,” LNCS 2009).

The workshop focused on the design and realization of anonymity and anti-censorship services for the Internet and other communication networks. For convenience it was held at the Cathedral Hill Hotel just prior to the Twelfth Conference on Computers, Freedom, and Privacy (CFP 2002), but it was not formally affiliated with that conference.

There were 48 submissions of which we accepted 17. The program committee listed on the next page made the difficult decisions on which papers to accept, with additional reviewing help from Oliver Berthold, Sebastian Clauß, Lorrie Cranor, Stefan Köpsell, Heinrich Langos, Nick Mathewson, and Sandra Steinbrecher. Thanks to all who helped and apologies to anyone we have overlooked. Thanks also to everyone who contributed a submission.

Besides the contributed papers we were honored to have an invited talk by someone who as much as anyone could be said to have started the entire technology field of anonymity and privacy: David Chaum. The talk covered his recently developed voting technology based on visual secret sharing, and as if that weren’t enough, also described new primitives for electronic cash. There was also a lively rump session, covering a variety of new and upcoming technologies.

Adam Shostack served as general chair. The workshop ran remarkably smoothly – and in fact ran at all – thanks to Adam, who also personally took on the financial risk that we would break even. Thank you Adam.

June 2002

Roger Dingledine and Paul Syverson

Privacy Enhancing Technologies 2002
San Francisco
April 14–15, 2002

Program Committee

John Borking, Dutch Data Protection Authority
Lance Cottrell, Anonymizer.com
Roger Dingledine, The Free Haven Project (Co-chair)
Hannes Federrath, Freie Universitaet Berlin
Markus Jakobsson, RSA Laboratories
Marit Köhntopp, Independent Centre for Privacy Protection
Andreas Pfitzmann, Dresden University of Technology
Avi Rubin, AT&T Labs – Research
Paul Syverson, Naval Research Lab (Co-chair)
Michael Waidner, IBM Zurich Research Lab

General Chair

Adam Shostack, Zero-Knowledge Systems

Table of Contents

Privacy-Enhancing Technologies for the Internet, II: Five Years Later	1
<i>Ian Goldberg</i>	
Detecting Web Bugs with Bugnosis: Privacy Advocacy through Education	13
<i>Adil Alsaïd and David Martin</i>	
Private Authentication	27
<i>Martín Abadi</i>	
Towards an Information Theoretic Metric for Anonymity	41
<i>Andrei Serjantov and George Danezis</i>	
Towards Measuring Anonymity	54
<i>Claudia Díaz, Stefaan Seys, Joris Claessens, and Bart Preneel</i>	
Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data	69
<i>Günter Karjoth, Matthias Schunter, and Michael Waidner</i>	
Privacy Enhancing Profile Disclosure	85
<i>Péter Dornbach and Zoltán Németh</i>	
Privacy Enhancing Service Architectures	99
<i>Tero Alamäki, Margareta Björkstén, Péter Dornbach, Casper Gripenberg, Norbert Györbíró, Gábor Márton, Zoltán Németh, Timo Skyttä, and Mikko Tarkiainen</i>	
Dummy Traffic against Long Term Intersection Attacks	110
<i>Oliver Berthold and Heinrich Langos</i>	
Protecting Privacy during On-Line Trust Negotiation	129
<i>Kent E. Seamons, Marianne Winslett, Ting Yu, Lina Yu, and Ryan Jarvis</i>	
Prototyping an Armored Data Vault	144
<i>Alex Iliev and Sean Smith</i>	
Preventing Interval-Based Inference by Random Data Perturbation	160
<i>Yingjiu Li, Lingyu Wang, and Sushil Jajodia</i>	
Fingerprinting Websites Using Traffic Analysis	171
<i>Andrew Hintz</i>	

VIII Table of Contents

A Passive Attack on the Privacy of Web Users
Using Standard Log Information 179
Thomas Demuth

Covert Messaging through TCP Timestamps 194
John Giffin, Rachel Greenstadt, Peter Litwack, and Richard Tibbetts

Almost Optimal Private Information Retrieval 209
Dmitri Asonov and Johann-Christoph Freytag

Unobservable Surfing on the World Wide Web: Is Private Information
Retrieval an Alternative to the MIX Based Approach? 224
Dogan Kesdogan, Mark Borning, and Michael Schmeink

Author Index 239