Lecture Notes in Computer Science 2009
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Hannes Federrath (Ed.)

Designing Privacy Enhancing Technologies

International Workshop on Design Issues
in Anonymity and Unobservability
Berkeley, CA, USA, July 25-26, 2000
Proceedings

Springer

Series Editors

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

Volume Editor

Hannes Federrath
FU Berlin, Institut Informatik
Takustr. 9, 14195 Berlin, Germany
E-mail: federrath@inf.tu-dresden.de

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Designing privacy enhancing technologies : proceedings / International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, USA, July 25 - 26, 2000. Hannes Federrath (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2009)
ISBN 3-540-41724-9

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

ISSN 0302-9743
ISBN 3-540-41724-9 Springer-Verlag Berlin Heidelberg New York

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

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by PTP Berlin, Stefan Sossna
Printed on acid-free paper SPIN 10782052 06/3142 5 4 3 2 1 0

Preface

This workshop addresses the design and realization of anonymity services for the Internet and other communication networks. The main topics of the workshop are

- Attacks on Systems,
- Anonymous Publishing,
- Mix Systems,
- Identity Management, and
- Pseudonyms and Remailers.

Anonymity and unobservability have become "hot topics" on the Internet. Services that provide anonymous and unobservable access to the Internet are useful for electronic commerce applications (obviously with the need for strong authenticity and integrity of data) as well as for services where the user wants to remain anonymous (e.g. web-based advisory services or consultancy).

I would like to thank the other members of the program committee John Borking, Marit Köhntopp, Andreas Pfitzmann, Avi Rubin, Adam Shostack, Michael Waidner, and Sonja Zwissler for their helpful hints, for doing the reviews, and for their patience. A special thanks is dedicated to Lila Finhill of ICSI for her help in all administrative and financial concerns, and Christian Schindelhauer for his support on LaTeX.

July 2000 Hannes Federrath

Organization

This workshop was held at the International Computer Science Institute (ICSI), Berkeley, California, July 25-26, 2000.

Program Committee

John Borking	Registratiekamer Netherlands
Hannes Federrath	ICSI, Berkeley
Marit Köhntopp	Privacy Commissioner Schleswig-Holstein, Germany
Andreas Pfitzmann	Dresden University of Technology, Germany
Avi Rubin	AT&T Research
Adam Shostack	Zero-Knowledge Systems, Montreal, Canada
Michael Waidner	IBM Zurich Research Lab
Sonja Zwissler	ICSI, Berkeley

Sponsoring Institutions

International Computer Science Institute, Berkeley, USA
Zero-Knowledge Systems, Montreal, Canada

Table of Contents