

Lecture Notes in Computer Science

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

2696

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Joan Feigenbaum (Ed.)

Digital Rights Management

ACM CCS-9 Workshop, DRM 2002
Washington, DC, USA, November 18, 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 Editor

Joan Feigenbaum
Yale University
Department of Computer Science
P.O. Box 208285, New Haven, CT 06520-8285, USA
E-mail: joan.feigenbaum@yale.edu

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.2.0, D.4.6, K.6.5, F.3.2, H.5, J.1, K.4.1

ISSN 0302-9743

ISBN 3-540-40410-4 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: 10927984 06/3142 5 4 3 2 1 0

Preface

Increasingly, the Internet is used for the distribution of digital goods, including digital versions of books, articles, music, and images. This new distribution channel is a potential boon to both producers and consumers of digital goods, because vast amounts of material can be made available conveniently and inexpensively. However, the ease with which digital goods can be copied and redistributed makes the Internet well suited for unauthorized copying, modification, and redistribution. Adoption of new technologies such as high-bandwidth connections and peer-to-peer networks is currently accelerating both authorized and unauthorized distribution of digital works.

In 2001, the ACM initiated an annual series of workshops to address technical, legal, and economic problems posed by the digital distribution of creative works. The 2002 ACM Workshop on Digital Rights Management (DRM 2002), held in Washington, DC on November 18, 2002, was the second in this annual series. This volume contains the papers presented at that very well attended and stimulating workshop.

The success of DRM 2002 was the result of excellent work by many people, to whom I am extremely grateful. They include Sushil Jajodia, Charles Youman, and Mary Jo Olsavsky at George Mason University, the members of the Program Committee, my assistant, Judi Paige, and my student Vijay Ramachandran.

April 2003
New Haven, CT, USA

Joan Feigenbaum
Program Chair, DRM 2002

Program Committee

Yochai Benkler (New York University, Law School)
Dan Boneh (Stanford University, Computer Science Dept.)
Willms Buhse (Bertelsmann Digital World Services)
Joan Feigenbaum (Yale University, Computer Science Dept.)
Neil Gandal (Tel Aviv University, Public Policy Dept.)
John Manferdelli (Microsoft, Windows Trusted-Platform Technologies)
Moni Naor (Weizmann Institute, Computer Science and Applied Math Dept.)
Florian Pestoni (IBM, Almaden Research Center)
Tomas Sander (Hewlett-Packard Labs)
Michael Waidner (IBM, Zurich Research Center)
Moti Yung (Columbia University, Computer Science Dept.)

Organization

DRM 2002 was held in conjunction with the 9th ACM Conference on Computer and Communication Security (CCS-9) and was sponsored by ACM/SIGSAC.

Table of Contents

ACM DRM 2002

A White-Box DES Implementation for DRM Applications	1
<i>Stanley Chow, Phil Eisen, Harold Johnson (Cloakware Corporation), and Paul C. van Oorschot (Carleton University)</i>	
Attacking an Obfuscated Cipher by Injecting Faults	16
<i>Matthias Jacob (Princeton University), Dan Boneh (Stanford University), and Edward Felten (Princeton University)</i>	
Breaking and Repairing Asymmetric Public-Key Traitor Tracing	32
<i>Aggelos Kiayias (University of Connecticut) and Moti Yung (Columbia University)</i>	
Key Challenges in DRM: An Industry Perspective	51
<i>Brian A. LaMacchia (Microsoft Corporation)</i>	
Public Key Broadcast Encryption for Stateless Receivers	61
<i>Yevgeniy Dodis and Nelly Fazio (New York University)</i>	
Traitor Tracing for Shortened and Corrupted Fingerprints	81
<i>Reihaneh Safavi-Naini and Yejing Wang (University of Wollongong)</i>	
Evaluating New Copy-Prevention Techniques for Audio CDs	101
<i>John A. Halderman (Princeton University)</i>	
Towards Meeting the Privacy Challenge: Adapting DRM	118
<i>Larry Korba (National Research Council of Canada) and Steve Kenny (Independent Consultant)</i>	
Implementing Copyright Limitations in Rights Expression Languages	137
<i>Deirdre Mulligan and Aaron Burstein (University of California)</i>	
The Darknet and the Future of Content Protection	155
<i>Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman (Microsoft Corporation)</i>	
Replacement Attack on Arbitrary Watermarking Systems	177
<i>Darko Kirovski and Fabien A.P. Petitcolas (Microsoft Research)</i>	
FAIR: Fair Audience InfeRence	190
<i>Rob Johnson (University of California) and Jessica Staddon (Palo Alto Research Center)</i>	

Theft-Protected Proprietary Certificates 208
 Alexandra Boldyreva (University of California)
 and Markus Jakobsson (RSA Laboratories)

Author Index 221