Lecture Notes in Computer Science 2320

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

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

Tomas Sander (Ed.)

Security and Privacy in Digital Rights Management

ACM CCS-8 Workshop DRM 2001
Philadelphia, PA, USA, November 5, 2001
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

Tomas Sander
InterTrust STAR Lab. - New Jersey
821 Alexander Rd., Princeton, NJ 08540-6303, USA
E-mail: sander@intertrust.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Security and privacy in digital rights management : revised papers / ACM CCS-8 Workshop DRM 2001, Philadelphia, PA, USA, November 5, 2001. Thomas Sander (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2320)
ISBN 3-540-43677-4

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, K.4.4, K.5

ISSN 0302-9743
ISBN 3-540-43677-4 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 DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN 10846660 06/3142 5 4 3 2 1 0

Preface

The ACM Workshop on Security and Privacy in Digital Rights Management is the first scientific workshop with refereed proceedings devoted solely to this topic. The workshop was held in conjunction with the Eighth ACM Conference on Computer and Communications Security (CCS-8) in Philadelphia, USA on November 5, 2001.

Digital Rights Management technology is meant to provide end-to-end solutions for the digital distribution of electronic goods. Sound security and privacy features are among the key requirements for such systems.

Fifty papers were submitted to the workshop, quite a success for a first-time workshop. From these 50 submissions, the program committee selected 15 papers for presentation at the workshop. They cover a broad area of relevant techniques, including cryptography, system architecture, and cryptanalysis of existing DRM systems. Three accepted papers are about software tamper resistance, an area about which few scientific articles have been published before. Another paper addresses renewability of security measures. Renewability is another important security technique for DRM systems, and I hope we will see more publications about this in the future. I am particularly glad that three papers cover economic and legal aspects of digital distribution of electronic goods. Technical security measures do not exist in a vacuum and their effectiveness interacts in a number of ways with the environment for legal enforcement. Deploying security and anti-piracy measures adequately requires furthermore a good understanding of the business models that they are designed to support.

We felt there was a need for a workshop devoted to DRM in order to create an interdisciplinary forum for the exchange of ideas from a number of relevant areas. The lively discussions at the workshop suggest that we were not mistaken.

During the conference pre-proceedings were made available. Final versions were prepared by the authors shortly after the workshop and have been included in this volume without further review.

It is a great pleasure for me to thank everyone whose help and contribution made the workshop a success. The 17 program committee members did a great job in reviewing and selecting the papers within a tight schedule. Mike Reiter was the General Chair of our host conference CCS-8 and took very good care of all the organizational aspects of the workshop. I would like to thank Microsoft Research for access to their committee software for the review process. Mike Freedman helped with running the committee software. I would further like to thank the ACM CCS-8 conference organizers and our sponsoring organization, the ACM, for being such great hosts. Special thanks go to Stuart Haber, who gave an invited talk introducing and surveying modern DRM technology.

As this goes to press the jury is still out about the practical effectiveness of security measures in DRM systems. Much more real-world data and experience

are needed. Fortunately we will see the first mass deployments in 2002, and thus we may reasonably hope to gain some insights from these deployments for future workshops focusing on DRM.

February 2001 Tomas Sander

Conference Organizers

Program Chair

Tomas Sander, InterTrust STAR Lab

Program Committee

Eberhard Becker, University of Dortmund
Dan Boneh, Stanford University
Karlheinz Brandenburg, Fraunhofer Institute for Integrated Circuits IIS-A
Leonardo Chiariglione, CSELT
Drew Dean, SRI International
Joan Feigenbaum, Yale University
Edward Felten, Princeton University
Yair Frankel, eCash Technologies
Markus Jakobsson, RSA Laboratories
Paul Kocher, Cryptography Research
John Manferdelli, Microsoft Research
Kevin McCurley, IBM Research
Moni Naor, Weizmann Institute
Fabien Petitcolas, Microsoft Research
Pamela Samuelson, University of California, Berkeley
Hal Varian, University of California, Berkeley
Moti Yung, CertCo

General Chair, ACM CCS-8

Michael K. Reiter, CMU

Table of Contents

Cryptanalysis

Economics, Legal Aspects