

Securing Digital Video

Eric Diehl

Securing Digital Video

Techniques for DRM and Content Protection

Eric Diehl
Technicolor, Security & Content
Protection Labs
Ave. Belle Fontaine 1
Rennes 35576
France

ISBN 978-3-642-17344-8 ISBN 978-3-642-17345-5 (eBook)
DOI 10.1007/978-3-642-17345-5
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2012940230

ACM Computing Classification: E.3, H.5.1, K.6.5, K.4.4

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Acknowledgments

First of all, I would like to thank my wife for her constant support for this work and for her invaluable patience.

I would like to thank many colleagues and friends who carefully reviewed portions of the manuscript; their comments made this book more readable and attractive. First, my colleagues at Technicolor, including Michael Arnold, Jean-Marc Boucqueau, Gwenael Doerr, Alain Durand, Marc Eluard, Marc Joye, Andrew Hackett, Sylvain Lelievre, Mohamed Karroumi, Yves Maetz, Antoine Monsifrot, and Charles Salmon-Legagneur. Then my gratitude goes to friends, including Jukka Alve (SESKO), Olivier Bomsel (Ecole des Mines), Ton Kalker (DTS), Kevin Morgan (Arxan), Florian Pestoni (Adobe), Nicolas Prigent (Supelec), Arnaud Robert (Disney), Rei Safavi-Naini (University of Calgary), and Massimo Savazzi (Microsoft).

I would like to offer special thanks to Prof. Jean-Jacques Quisquater and Prof. Benoit Macq of the Université Catholique de Louvain. They made me believe that I could write such a book. Most probably, without them I would not have dared to begin this work.

Many thanks to Technicolor who allowed me to use illustrations from its bank of images.

I am grateful to Ronan Nugent and Springer, who showed keen interest in this book.

Eric Diehl

Contents

1	Introduction	1
2	Why Protect Video?	5
2.1	Introduction	5
2.2	Copyright Issues	6
2.3	Business Issues	10
2.4	A Brief Overview of Digital Piracy	14
3	A Tool Box	21
3.1	Different Needs, Different Tools	21
3.1.1	Controlling Access	21
3.1.2	Protecting the Asset	22
3.1.3	Forensic Marking	22
3.1.4	Thwarting Illegal Distribution	23
3.2	Cryptography	23
3.2.1	Introduction	23
3.2.2	Symmetric Cryptography	25
3.2.3	Asymmetric Cryptography	27
3.2.4	Hybrid Cryptosystems	29
3.3	Digital Watermarking	32
3.3.1	The Theory	32
3.3.2	Usage	35
3.3.3	Forensic Marking	36
3.3.4	Copy Control	40
3.3.5	Copyright Management	41
3.3.6	Monitoring, Monetization	43
3.4	Fingerprinting	44
3.5	Hardware Tamper-Resistance	45
3.5.1	Definition	45
3.5.2	Different Types of Components	46
3.5.3	Dedicated Countermeasures	50

- 3.6 Software Tamper-Resistance 53
 - 3.6.1 Introduction 53
 - 3.6.2 Prevent Analysis. 55
 - 3.6.3 Prevent Tampering 57
 - 3.6.4 Prevent Automation and Distribution 63
- 3.7 Rights Expression Language 64
- 3.8 Compliance and Robustness Rules 67

- 4 Modeling Content Protection 73**
 - 4.1 Introduction to Different Models 73
 - 4.2 Functional Model 73
 - 4.3 Transactional Model 76
 - 4.3.1 General Model 76
 - 4.3.2 Payment-Based Distribution 77
 - 4.3.3 Payment-Free Distribution 81
 - 4.4 Architectural Model 82
 - 4.5 The Four-Layer Model 83

- 5 The Current Video Ecosystem 89**

- 6 Protection in Broadcast 97**
 - 6.1 The Broadcast Flag 97
 - 6.2 Pay TV: The Ancestor 98
 - 6.3 How Pay TV Works 102
 - 6.4 DVB 108
 - 6.5 DVB-CI/CI+ 111
 - 6.6 OpenCable CableCARD 117

- 7 Protection in Unicast/Multicast 119**
 - 7.1 DRM 119
 - 7.2 Microsoft DRM 120
 - 7.2.1 Windows Media DRM 120
 - 7.2.2 PlayReady 126
 - 7.3 Apple Fairplay 127
 - 7.4 Adobe Flash Access 132
 - 7.5 Open Mobile Alliance 136
 - 7.6 Marlin 141
 - 7.7 Some Other Players 146

- 8 Protection of Pre-recorded/Recordable Medium 147**
 - 8.1 Anti-Ripping 147
 - 8.2 CSS: Content Scramble System 153
 - 8.3 MagicGate 157
 - 8.4 CPPM CPRM 159

- 8.5 Blu-Ray Discs 165
 - 8.5.1 AAC3 165
 - 8.5.2 Sequence Keys 167
 - 8.5.3 BD 168
 - 8.5.4 Watermarks 170

- 9 Protection Within the Home 173**
 - 9.1 The Home Network Problem 173
 - 9.2 Termination of DRM/CAS 174
 - 9.3 DTCP 177
 - 9.4 HDCP 179
 - 9.5 DVB-CPCM 181
 - 9.6 The Analog Hole 185

- 10 Digital Cinema 189**

- 11 The Next Frontier: Interoperability 193**
 - 11.1 Why Interoperability? 193
 - 11.2 Different Types of Interoperability 196
 - 11.2.1 The Vertical Approach 197
 - 11.2.2 The Horizontal Approach 198
 - 11.2.3 The Plug-In Approach 202
 - 11.2.4 The Translation Approach 205
 - 11.2.5 Interoperable Rights Locker 207
 - 11.3 Current Initiatives 211
 - 11.3.1 Coral 211
 - 11.3.2 Portable Interoperable File Format 213
 - 11.3.3 Digital Entertainment Content Ecosystem and UltraViolet 214
 - 11.3.4 KeyChest 217
 - 11.3.5 Digital Media Project 219
 - 11.4 Specific Problems 222
 - 11.4.1 Transcoding of Encryption 222
 - 11.4.2 Usage Rights Translation 223
 - 11.5 Drawbacks 227

- 12 Some Challenges/Goodies 229**
 - 12.1 Open-Source DRM 229
 - 12.2 Clear Content DRM 231
 - 12.3 DRM and Game Theory 235
 - 12.3.1 Introduction to Game Theory 235
 - 12.3.2 Current Research Topics 237

13 Conclusions	241
Appendix: Abbreviations—Acronyms.	243
References	249