Security, Trust and Risk in Digital Rights Management Ecosystem

Zhang Zhiyong

Science Press
Beijing

Security, Trust and Risk in

Digital Rights Management Ecosystem

Zhang Zhiyong

Science Press
Beijing

Responsible Editors: Lin Jian Liu Chao

Brief Introduction

The monograph has an objective to make an interesting insight on security, trust and risk in DRM ecosystem from interdisciplinary perspective. The state-of-the-art of DRM technologies is firstly presented, and then the book proposed a tradeoff between DRM security and utility by cost-effectively adopting and deploying of security policies and mechanisms, in order to implement an optimal security-utility equilibrium and establish the multi-stakeholder trust in DRM ecosystem. And also, the book has an in-depth investigation on security risk management in the copyrighted contents value chain. Finally, a comprehensive multimedia DRM application case for digital home networks was highlighted.

This monograph is intended for research scientists, engineers, developers and high-level administrators of digital rights management ecosystems and applications, and also for advanced-level students in computer science, information technology and management science.

Published by Science Press
16 Donghuangchenggen North Street
Beijing 100717, P. R. China

Printed in Beijing

ISBN 978-7-03-034335-2

Preface

Up to now, Digital Rights Management (DRM) has been still a burning and challenging research topic since 1990s. In digital world and the DRM-enabling digital contents value chain, various stakeholders don't fully trust one another due to their own rights and benefits, thus leading to a fact that the security techniques become the basis of multi-participant trust. Existing security technology-related works primarily focus on contents protections and secure disseminations by using cryptographic algorithms and secure protocols, trusted and controlled usages of copyrighted digital assets at the general-purpose or special-purpose user terminal devices, together with watermarking-based copyrights infringements tracking and prosecutions. No doubt that these typical security policies and usage restrictions are indispensable to DRM ecosystem, but the other cover of a coin, they give birth to several unexpected issues, such as the weaker system interoperability and usability, as well as higher security overheads. The simple adoptions of those general or increasingly enhanced security policies for DRM ecosystem would have negative influences on the utilities of participants without the consideration of the rational decision-making. Therefore, the adoptions of DRM security policies, the establishment of multi-stakeholder trust and security risk management become three essential aspects.

The monograph has an objective to make an interesting insight on security, trust and risk in DRM ecosystem from interdisciplinary perspective. There are involved with a tradeoff between DRM security and utility, in order to implement an optimal security-utility equilibrium and establish a multi-participant trust for various participants in the contents value chain, by cost-effectively adopting and deploying of security policies and mechanisms. And also, inspired by risk management, we made in-depth investigation on security risk management in contents value chain. Finally, we gave a DRM application case for Digital Home Network and a prototype on copyrighted multimedia contents. The main research contributions of the monograph are listed as follows:

1) In combination with recently emerging trusted computing-enabling

enhanced security technologies,some novel security schemes and applications for DRM were addressed. The monograph proposes an Attestation Proxy Party-supported Remote Attestation (AP^2RA) model and its secure protocol,which have an essential characteristic of the privacy protection of terminal devices held by end users. Besides,the monograph implements the rights delegation/transfer policy,thus meeting the consumers' requirement for sharing purchased digital contents in their social networks.

2) A systematic and comprehensive formalized analytic framework is proposed,and it is used for presenting the utility of DRM security components/services and composite policies, and further accomplishing the rational decision-making on adoptions of various security policies. The novel framework is involved in the cooperative and non-cooperative game-theoretic analysis,the weights assessments of utility-influencing factors based on Fuzzy Analytic Hierarchy Process.

3) Aiming at the typical security policies available,the monograph lays an emphasis on addressing a non-cooperative game model among contents providers, rights/services purveyors and end users in a scenario of digital contents acquisitions. It is found that there exists Nash Equilibrium and its precondition,which is security policies profile(s) with the optimal benefits for participants. The Swarm-based simulation experiments verified our analytic results and clearly presently various participants' tendency to adopt a certain optimal policies with the increase of contents transactions and the reduction of managerial and session-level costs and overheads resulted from the higher security. In addition,considering the introduction of devices vendors in contents value chain,a cooperative game was represented among various purveyors as digital contents, rights and devices, and the refined analysis shows that providers together adopt and deploy enhanced security policies would give birth to maximum utilities for participants, and the corresponding Nash Equilibrium is Pareto Optimality.

4) For a more complicated DRM application scenario, where digital contents sharing commonly exist,the monograph attempts to an exploration on a Dynamic and Mixed Game (DMG) between *Providers* and *Sharer*,and have a goal to investigate into several concrete preconditions under which two participants could adopt the enhanced security policies of the remote

attestation, so that the optimal security utility would be achieved. For this, a simplified contents sharing tree structure, which is belongs to a specific style of the Social Network, is proposed, and *Providers*' optimal strategies and their preconditions are finally gained by using the game-theoretic analysis, DMG algorithm designing and Swarm simulation experiments on the game in term of *Sharer's* three kinds of sharing modes.

5) In addition, inspired by security risk management, the monograph proposes a novel concept of Risk-Controlled Utility as a quantitative and qualitative assessment method for enhanced security policies, and further makes an analysis the influences of different contents sharing modes on total benefits of *Providers* in the case of digital contents copyrights infringements. As a result, the effective sharing mode and business model suitable for the contents sharing scenario were highlighted in the monograph.

The monograph is organized as follows:

In Chapter 1, the state-of-the-art of DRM technologies was primarily investigated, including security policies, models, architectures and mechanisms. Importantly, a generic contents value chain ecosystem was presented in detail. In the end of this chapter, we clearly addressed the research motivation and scope, when facing the challenges of severe piracy in DRM ecosystem.

In Chapter 2, based on a survey on the emerging trusted computing technology, we focus on DRM applications-supporting enhanced security policies and mechanisms, with an objective to effectively improve security and trustworthiness of DRM ecosystem. Subsequently, in the same chapter, two existing security policies are refined to be used for the protections of end user devices and for the rights negotiation between contents providers and service purveyors.

In Chapter 3, we mainly propose a novel and systematic approach to rational decision-making and cost-effective adoptions of DRM security policies for participants in contents value chain, thus enabling stakeholders to acquire their own optimal benefits.

In Chapter 4, there is a comprehensive analysis of the utility of proposed security policies and attempt to the game-theoretic adoption of optimal security policies combination(s) under various circumstances.

In Chapter 5, in a contents sharing scenario, a much more complicated dynamic and mixed game is represented, and its corresponding Swarm-based simulation experiments are made to observe the optimal strategy (move) for participants.

In Chapter 6, the risk utility of utility-influencing factors are proposed and calculated in combination with the qualitative and quantitative security risk assessments. And also the risk utility of security policies is refined, consequently giving birth to a rational and cost-effective business model.

In Chapter 7, an application case in DRM-enabling digital home network is represented at length. It firstly proposes a usage control model and a novel approach to digital contents sharing for Digital Home Network respectively, which satisfies the requirements for family users. Besides, a PIK-based DRM system scheme is designed, so that achieve effective user authentication, secure distribution of digital content and usage control of rights.

In Chapter 8, we highlight future works and digital rights management in Multimedia Social Network as an open issue.

This monograph is intended for research scientists, engineers, developers and high-level administrators of digital rights management ecosystems and applications, and also for advanced-level students in computer science, information technology and management.

Zhang Zhiyong
March, 2012

Contents

Preface
Chapter 1 Introduction ········· 1
1. 1 DRM Backgrounds ········· 2
1. 1. 1 DRM Definitions ········· 2
1. 1. 2 A Generic Contents Value Chain Ecosystem ········· 4
1. 1. 3 Three Aspects of DRM Ecosystem ········· 6
1. 2 State-of-The-Art DRM ········· 9
1. 2. 1 Cryptographic Security & Digital Watermarking ········· 10
1. 2. 2 Digital Rights Expression and Usage Control ········· 15
1. 2. 3 User Privacy Protection and Contents Security ········· 21
1. 2. 4 DRM Trust Models ········· 23
1. 3 Research Motivation and Scope ········· 25
1. 4 Monograph Outline ········· 27
1. 5 Conclusion ········· 29
References ········· 29
Chapter 2 Enhanced Security Policies for DRM ········· 36
2. 1 Fundamental Security Requirements in DRM ········· 38
2. 2 Trusted Computing and Remote Attestation ········· 40
2. 2. 1 Trusted Computing Background ········· 40
2. 2. 2 Trusted Computing and Its Features ········· 41
2. 2. 3 Remote Attestation ········· 46
2. 3 AP^{2}RA Model and Secure Protocol ········· 50
2. 3. 1 Privacy Protection and AP^{2}RA Model ········· 50
2. 3. 2 Security Protocol ········· 56
2. 3. 3 Analysis and Comparisons ········· 59
2. 4 Trusted Computing-enabled Digital Rights Sharing ········· 62
2. 4. 1 Usage Control with Delegation Characteristics ········· 62
2. 4. 2 Fine-Grained Digital Rights Transfer Policy ········· 69
2. 4. 3 AP^{2}RA-Based Contents Dissemination System ········· 70
2. 4. 4 Trusted Distribution on Transferable Rights ········· 73

2.5 Digital Rights Negotiation and Contents Security ······ 79
2.5.1 Transaction-Based Digital Rights Negotiation ······ 79
2.5.2 Contents Verification and Trusted Execution ······ 81
2.6 Conclusion ······ 83
References ······ 83
Chapter 3 Formalized DRM Security-Utility and Game-Theoretical Analysis ··· 88
3.1 Requirements for Trust in DRM ······ 89
3.1.1 Essential Trust Relations ······ 89
3.1.2 Conceptual Multi-Participant Trust Architecture ······ 90
3.2 Formalized Game-Theoretical Adoptions of Security Policies ······ 92
3.2.1 DRM Security Policies and Properties ······ 92
3.2.2 Non-Cooperative Game on Security Polices ······ 94
3.2.3 Cooperative Game on Security Polices ······ 96
3.3 Fuzzy Analytic Hierarchy Process on Utility-Factor Weights ······ 96
3.3.1 Analytic Hierarchy Process and Fuzzy Assessment ······ 96
3.3.2 Hierarchy Process Structure and Consistency Matrix ······ 97
3.3.3 FAHP-Based Weights Assessment ······ 98
3.4 Conclusion ······ 98
References ······ 98
Chapter 4 Basic Security-Utility and Game Analysis in Contents Acquisition Scenario ······ 100
4.1 DRM Typical Security Policies ······ 102
4.1.1 Typical Security Policy Set ······ 102
4.1.2 Security Policies Relativity ······ 104
4.2 Security Utility Analysis ······ 104
4.2.1 Payoff Functions of Security Policies Combinations ······ 104
4.2.2 Utility-Factors Weights Assessment and Calculation ······ 107
4.3 Non-Cooperative Game on Typical Policies Set ······ 110
4.3.1 A Non-Cooperative Game Model ······ 110
4.3.2 Nash Equilibriums and Conditions ······ 113
4.3.3 Swarm Simulations and Discussions ······ 114
4.4 Cooperative Game for Typical Policies ······ 118
4.4.1 Security Benefits Super-Additiontivity and Convexity ······ 118
4.4.2 Establishment of Multi-Participant Cooperation ······ 120

4. 5 Conclusion ········ 120
References ········ 121
Chapter 5 Dynamic Mixed Game Analysis of Security Policies in Contents Sharing Scenario ········ 122
5. 1 Rights Delegation and Transfer for Contents Sharing ········ 123
5. 2 Dynamic and Mixed Game for Contents Sharing ········ 125
5. 2. 1 Rights Sharing Tree and DMG ········ 125
5. 2. 2 An Algorithm for DMG ········ 129
5. 3 Swarm-Based Simulation Experiments ········ 130
5. 3. 1 Basic Simulation Environment and Procedure ········ 131
5. 3. 2 Simulations Experiments on Different Sharing Modes ········ 131
5. 4 Conclusion ········ 137
References ········ 138
Chapter 6 DRM Risk Management ········ 140
6. 1 Risk Utility of Security Policy ········ 141
6. 1. 1 Security Risk Management and Utility Category ········ 141
6. 1. 2 Pros and Cons of Qualitative and Quantitative Assessments ······ 143
6. 1. 3 An Analytic Approach to Risk-Controlled Utility ········ 144
6. 2 Risk-Controlled Utility Analysis and Business Model ········ 147
6. 2. 1 Risk Utility of TC-Enabling Security Policy ········ 147
6. 2. 2 Sharing Modes and Maximum Benefits of Contents Purveyor ··· 149
6. 2. 3 Simulation Experiments ········ 151
6. 2. 4 Related Discussions and Business Model ········ 153
6. 3 Conclusion ········ 156
References ········ 156
Chapter 7 DRM Application Case for Digital Home Network ········ 158
7. 1 A DRM Usage Control Model for Digital Home Network ········ 160
7. 1. 1 Formalized Role-based, Cross-Domain Usage Control Model for DHN ········ 160
7. 1. 2 Visual Modeling of the RCDUCM for DHN ········ 163
7. 1. 3 An Application Case of the RCDUCM for DHN ········ 167
7. 2 A Novel Approach to Digital Contents Sharing for Digital Home Network ········ 169
7. 2. 1 Background and Motivation ········ 170

7.2.2 Classification of Roles and Distribution of Permissions for DHN ······ 172
7.2.3 A Novel Approach to Digital Contents Sharing for DHN ······ 175
7.2.4 Analysis of Performance and Security ······ 180
7.3 A Novel DRM Security Scheme and Its Prototype System Implementation ······ 182
7.3.1 DRM System Architecture ······ 183
7.3.2 DRM System Security Mechanism ······ 185
7.3.3 Playback Control Based on Cryptography and License ······ 187
7.3.4 Implementation of DRM Prototype System ······ 189
7.4 Conclusion ······ 191
References ······ 192
Chapter 8 Further Works and Open Issue ······ 195
8.1 Further Works ······ 196
8.2 Trust Evaluation in Multimedia Social Network ······ 198
8.2.1 Introduction ······ 198
8.2.2 Advance on Trust Evaluation in Social Networks ······ 199
8.3 Open Issue and Topics ······ 209
8.4 Conclusion ······ 209
References ······ 210
Appendix A ······ 212
Appendix B ······ 216
Acknowledgments ······ 219

Chapter 1

Introduction

With the rapid development of communication network technologies, the next-generation Internet, 3G and 4G wireless mobile networks have been striding to the large-scale deployments and applications. As a result, by using multiple network admission methods, users could access to digital resources and services in anytime, at anywhere, which is much easier than ever before. Under this circumstance, the copyright infringement behaviors, such as the illicit copy, malicious distribution, unauthorized usage, free sharing of copyrights-protected digital contents, have already become a common phenomena, as the contents like electric book, image, music, movie and application software are very easily duplicated without the deterioration in quality. Thus, the digital contents industry could be heavily damaged, and its value chain may also be interrupted. So, the copyrighted contents protection and legitimate usages are, therefore, crucial.

The chapter is organized as follows: firstly, the chapter in detail presents DRM backgrounds, including some classical definitions, the concept of DRM ecosystem and its essential aspects in Section 1. 1, and then gives an insight into the state-of-the-art DRM, referring to cryptographic security, usage controls and trust models in the contents value chain. Based on the investigations, our research motivation and discussed scope was represented from a novel perspective in the following section. The organization of the monograph is listed at the end of the chapter.

1. 1 DRM Backgrounds

1. 1. 1 DRM Definitions

To efficiently upload the digital contents industry and solve the drastic piracy issue in colorful digital age and digital world, DRM technologies have emerged at the beginning of 1990s, and have a variety of applications from the end of 1990s (Becker et al. ,2003). Recent years have witnessed the significant progress on DRM-enabling techniques, and we are faced with new challenges and opportunities to cope with the piracy much more effectively.

Nowadays, there are several representative DRM definitions listed as follows:

1) Digital rights management (DRM) is a systematic approach to copyright protection for digital media. The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content

they've purchased. DRM products were developed in response to the rapid increase in online piracy of commercially marketed material, which proliferated through the widespread use of peer-to-peer file exchange programs. Typically DRM is implemented by embedding code that prevents copying, specifies a time period in which the content can be accessed or limits the number of devices the media can be installed on[1].

2) The first-generation of DRM focused on security and encryption as a means of solving the issue of unauthorized copying, which is, locks the content and limits its distribution to only those who pay (Ianella, 2001). The second-generation of DRM covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders' relationships.

3) The early DRM focused on the persistent protection of digital content against unauthorized access as well as on the effective enforcement of assigned usage rights (ContentGuard, 2005). Besides, a newer DRM is the persistent management of a digital object under a set of terms and conditions throughout its life cycle.

4) Digital rights management (DRM) is a term for access control technologies that are used by hardware manufacturers, publishers, copyright holders and individuals to limit the use of digital content and devices[2].

The term is used to describe any technology that inhibits uses of digital content that is not desired or intended by the content provider. The term does not generally refer to other forms of copy protection, which can be circumvented without modifying the file or device, such as serial numbers or key-files. It can also refer to restrictions associated with specific instances of digital works or devices.

5) Open Mobile Alliance (OMA) DRM makes a logical separation of DRM Content from Rights Objects(OMA DRM, 2007a). DRM Content and Rights Objects may be requested separately or together, and they may be delivered separately or at the same time. For example, a user can select a piece of content, pay for it, and receive DRM Content and a Rights Object in the same transaction. Later, if the Rights Object expires, the user can go back and acquire a new Rights Object, without having to download the DRM Content again.

Interoperable DRM solutions alleviate such problems and thereby increase consumer satisfaction. But interoperability has even more advantages:

[1] http://searchcio.techtarget.com/definition/digital-rights-management

[2] From Wikipedia, the free encyclopedia

①It facilitates the delivery of digital assets in complex supply chains involving many different parties. It enables a persistent and consistent management of rights even in multi-tier supply chains.

②It decreases barriers for the creation of a single European or even worldwide market for digital assets. By standardizing, it decreases the cost of setting up and running DRM systems and their complexity,making DRM cheaper and more reliable.

③It makes digital assets more valuable,as they can be used in more situations. Resulting demand increases can benefit producers with higher profits and consumers with lower costs.

④It enables new businèss models. If more types of usage behavior and user peculiarities are covered by DRM,business can create special offers taking into account individual tastes.

6)The legal context for DRM is copyright law(Rosenblatt,2007). Some relevant aspects of USA copyright law have similarities with those of European Union (EU) countries by virtue of their common derivation from the WIPO Copyright Treaty of 1996 (WCT) (WIPO,1996).

Most EU countries have private copying provisions in their copyright laws,which allow consumers to create copies of legitimately obtained content for their own use or that of family members. But,the USA has no private copying concept in its copyright law (with a narrow exception for audio works). Instead,it has two relevant concepts: Fair Use (17 USC § 107) and First Sale (17 USC § 109) .

Fair Use is similar to Fair Dealing in UK copyright law. It is a set of principles that guide courts when deciding whether uses of copyrighted works are defensible against infringement charges. The principles include such considerations as the purpose and character of the use,including whether the use is of commercial nature,and the effect of the use on the market for the work.

Generally,DRM is an umbrella term involved both in business realizations of the contents industry and in valuable explorations on multiple scientific disciplines,for instance,information technology,economics and copyrights law.

1.1.2 A Generic Contents Value Chain Ecosystem

In despite of different definitions or depictions in existence,DRM system has such essential functions:digital contents coding and identification,package and distribution, digital rights assertion and usage, copyrights infringement tracking and monitoring, which are enabled in the entire life cycle of digital contents from the creation, distribution and consumption to monitoring. The copyrighted digital contents value chain, also called DRM ecosystem, is composed of various participants implementing the above functionalities. Apparently, with regard to a general DRM system, the entire value chain principally includes the contents creator, intermediary distributor, rights holder/issuer and end purchaser. Under some circumstances, certification authority (CA) is also looked upon as a participant focusing on some special functions, such as key management, certificate issue, identities authentication and the integrity validation of terminal devices.

In addition, some functional components/entities are also playing indispensable roles in DRM ecosystem. For example, Clearing House, which is responsible for the license processing, financial and event managements, together with distribution information management system (DIMS) that supports a contract mechanism and maintains a program for interoperability, were both introduced in Lee's proposed distribution model (Lee et al., 2003). As such components mentioned above are not the active participant participating in the benefits and profits allotment in the value chain; they are often seen as logic components or entities.

A multi-party DRM ecosystem was presented for solving the interoperability obstacle for DRM wider acceptability and adoption (Vassiliadis et al., 2006). The ecosystem refers merely to four entities: creator, distributor, user and authority, which are the essential elements of a simple and practical business model of DRM value chain. The task of distributor is to receive the contents that creators produces, and then distribute them via appropriate channels such as websites or physical media. Authority is responsible for issuing contents license based on usage rules provided by creators, aiming at supervising the legitimate access to copyrighted contents.

In recent years, the need for the mobile industry to manage the usage of digital contents in a controlled manner has been dramatically growing, mobile DRM being a consequence of that. As a leading industry forum and research organization, OMA has been concentrating on DRM-enabled mobile services, and presenting a series of DRM related specifications according to basic requirements of the market and consumers. Nowadays *DRM Architecture Specification of Candidate Version 2.1* has already been published in Jul. 2007, which contains the openness, industry-wide interoperability and utility (OMA DRM, 2007a). In the *DRM Architecture Spec.*, it is stated that a large number of possible actors in a DRM ecosystem/value chain are in existence, such as content owners, developers and distributors, network service operators and manufacturers of terminal equipment, etc. However, as to the functional architecture, these participants are further simplified as a few logical functional entities like CI (content issuer), RI (rights issuer), and DRM agent that is a key component located in the user terminal equipment and also called DRM controller. From the perspective of the value chain, the OMA DRM should primarily consist of three major actors, which are the content provider, rights provider and user, respectively. It is conformable to the functionality of separate and non synchronously delivery of contents and its corresponding usage license.

Gallery and Mitchell (2007) introduced three new entities—device manufacturer, DRM agent installer and content management licensing administrator (CMLA) whose functionality is identical to CA's—on the basis of the OMA DRM architecture. However, these entities should not be considered as active parties because they do not have direct interest relations to other participants in the value chain. If mobile operators and telecom companies were taken into account, mobile DRM value chain would be more complicated than the traditional contents supply chain (Furregoni et al., 2007). Note that mobile operators could also play the same role as RI in a practical business model.

Therefore, for the generic consideration simplicity, we focus mainly on four participants without losing generality, which have their own security policies and trust relationships. Here, contents provider (CP) that could include contents creators/owner, issuers and intermediary distributors that implement the functionality of OMA CI. Rights provider (RP) denotes a participant distributing digital rights and may be a copyrights owner, service provider or network operator of Mobile DRM. Device provider (DP) provides digital device including consumer electronics for end users in DRM ecosystem. User obviously denotes a set of subscribers/consumers of digital contents, and purchased contents could be restrictedly shared among consumers through super distribution mechanisms, as is shown in Figure 1.1.

1.1.3 Three Aspects of DRM Ecosystem

DRM ecosystem refers to the entire life cycle of digital content from creation and packaging to dissemination for usage and sharing. Therefore, security policies, multi-participant trust, and risk management are involved in the generic DRM ecosystem that supports two representative applications: content acquisition/transaction scenarios and content sharing, as shown by Figure 1.2.