Security, Trust and Risk in Digital Rights Management Ecosystem

Zhiyong Zhang
Cultural Property Preservation & Digitization Research Center
Henan University of Science and Technology
Luoyang, P. R. of China
zhangzy@mail.haust.edu.cn

ABSTRACT

In the last decades, Digital Rights Management (DRM) technology has been laid emphasis on digital contents protection and related security policies, mechanisms and implementation. In order to effectively protect digital assets with copyrights against piracy and misuse, it is necessary for the contents value chain as a whole to investigate on some open issues and advances. The paper proposed three fundamental aspects regarding security, trust and risk, as underlies DRM Ecosystem. And then, digital rights negotiation and multi-level contents verification, multi-participant trust framework, as well as the risk management, were addressed so as to uphold two generic DRM application scenarios, with an ultimate goal to meet key requirements of security, interoperability and usability.

KEYWORDS: Digital Rights Management, Security Policies, Trust, Risk Management, Interoperability

1. INTRODUCTION

In order to positively protect Intellectual Property and to realize the legitimate and controlled usage on digital contents (assets), DRM has become a focus for the society as a whole, where the contents industry, academic realms, governments and even some civil liberty are involved in. 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 law [1]. Besides, recently Mobile DRM technology, which is oriented by a mobile network application scenario, has been paying more attention to the effective protection of digital contents in the whole life cycle for the mobile network environment. In North America and European Union, DRM-protected mobile contents service is listed among the four kinds of DRM killer applications.

It should be noted that, in the last decades, regardless of general DRM or Mobile DRM, the emphasis has been primarily laid on the research on the contents protection, which is based mainly on cryptographic security and the contents usage permission that is accomplished by Rights Expression Language and Usage Control, as well as on the digital watermark technology used for prosecuting pirate. Apparently the above two roadmaps are both at the standpoints of the digital contents provider or digital rights provider, and the main countermeasure of copyrights infringement is to look for positive security policies, even further enhanced policies. Consequently, digital users may reject DRM technologies and DRM-enabled digital products, which will interrupt the contents chain value. It should be indicated that DRM should balance the interests of the various stakeholders in the value chain, and enable the IPR (Intellectual Property Rights)-enabling contents industry to have a prosperous future. Therefore, from the perspective of DRM value chain's survivability, DRM should embody not merely security policies but the interest balance of involved parties, especially for an establishment of the multi-party trust relationship and effective risk management.

With respect to a holistic and comprehensive contents value chain forming a generic DRM Ecosystem, Figure 1 indicates three underling aspects on security policies, multi-participant trust and risk management. They together uphold two typical DRM application scenarios, which are digital content acquisition and digital contents sharing, respectively. So, DRM has an ultimate goal to realize security, interoperability and usability in these above mentioned scenarios, by using security policies and mechanisms, as well as the trust establishment and risk management.

978-1-4244-6829-4/10/$26.00 ©2010 IEEE

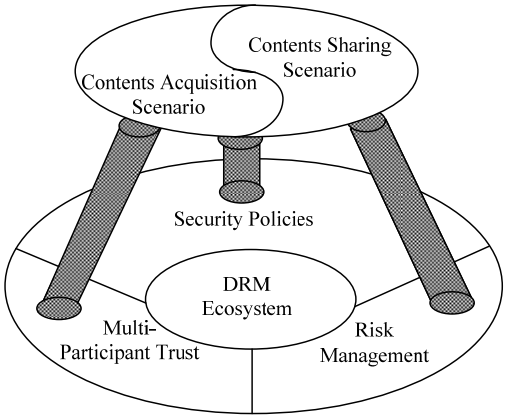

Figure 1. Security Policies, Multi-Participant Trust and Risk Management in DRM Ecosystem

2. DRM SECURITY

In the DRM value chain, Contents Provider (CP)'s goal is to protect digital contents security, so security policies available are commonly categorized into two sorts: preventive and reactive one. The both differently denote the protection of contents in an entire life cycle by the cryptographic techniques beforehand [2, 3], as well as contents usage tracking and copyrights infringement authentication based on the watermark and biological features [4, 5].

In addition, In DRM value chain, other than CP-centered preventive and reactive policies for the copyrights protection, there also exist Rights Provider (RP)-centric digital rights expressions and usage control [6]. The former is involved in REL (Rights Expression Language), and the latter mainly implement the controlled usage of digital rights predefined by RP by using a certain REL. In a generally way, REL is employed to specify the contents usage policies, which are composed of a group of grant rules depicting some concrete rights/permissions under the given conditions and constraints. Existing representative RELs, for instance, XrML [7], ODRL [8] and MPEG-21 REL [9], have gradually progressed and been precisely specified in recent years. However, Jamkhedkar et.al. [10] addressed a significant issue of "language bloat". Some new DRM-related business models tend to be continuously introduced to DRM ecosystem, but the current RELs may be incapable of specifying material rights and their managements in any particular scenario, as a consequence, a certain REL would been extended on the basis of the original REL so that it could support multiple business models. The reason why the issue emerges is due largely to the lack of a separation of rights expression and rights management, directly resulting in REL being more complicated and even difficult to operate. Therefore, we still need much attempt to solve the issue.

The above mentioned approaches to the copyrights protection primarily focus on digital contents/services side. It should be noted that the following two issues need to pay much more attentions from DRM Ecosystem's perspective, especially in combination with some needful user-side considerations as follows.

2.1. Contents Verification and Trusted Execution

Recent years have witnessed the rapid development and ubiquitous applications of communication networks, and meanwhile these networks make it convenient to intentionally or unconsciously spread various types of malicious codes, such as viruses, worm, and so on. There, information systems and digital assets have been subject to drastic attacks and severe risks. As a special style of digital contents, taking Java-class application as an example, we examine at the emerging issue of contents security from user's perspective, and safeguard user devices against Java-class application embedded or infected by malicious codes by using the contents verification and trusted execution.

The subsection firstly presents a multi-level security policy for the Java application verification based on the certificate mechanism, as is shown by Figure 2. In the security policy, the verification is implemented at CP side, digital services provider side, and user end, respectively. For CP, Java applications should be submitted to the third party as Java Verification Serves in order to assure the application security, prior to distributing them to consumers directly or indirectly. Subsequently, the verification service would provide CP with a corresponding signed certification, in which an integrity measurement metric generated by a generic hash function. Considering some business models and application scenarios, these applications could be indirectly distributed via an integrated digital services purveyor, for instance Services Provider in MDRM. Under this circumstance, Services Provider needs to further verification the contents certificates and integrity measurement metrics, and then is responsible for pushing the valuable contents to target consumers, or publishing a contents warehouse pulling an intended purchasers. Note that Services Provider may also give an attached signed certificate used for certified Java applications, such as Java game, electronic book reader, etc. At end user side, the related certifications and integrity metrics of these acquired applications are verified by a security component employed for restricting the executions of uncertificated application.

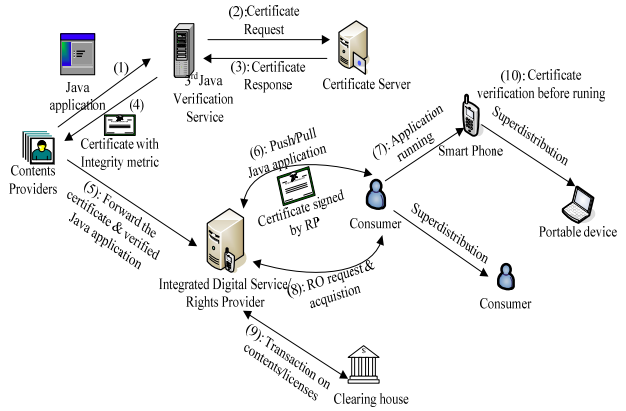

Figure 2. Multi-Level Contents Verification

With regard to the trusted execution of versatile Java applications, the thesis proposes two kinds of methods for protecting user devices and data by resisting the malicious codes /applications. One is to only adopt the above mentioned certification and integrity checkout mechanisms, and the other is based on the running integrity as an enhanced security. The former is a common scheme that is successfully implemented by using an added security component, as is a cost-effective security policy but the existence of the security vulnerabilities, and the latter needs to the trusted computing-enabling devices and related Snapshot mechanism to accomplish the integrity checkout. No doubt that the adoption of the trusted computing-enabling techniques gives birth to higher costs, especially for consumers, so the certificate-based contents verification and trusted execution would be one of typical security policies.

2.2. Transaction-Based Digital Rights Negotiation

In a generic DRM value chain, CP and RP are not only responsible for the dissemination of digital contents and rights (or licenses) respectively, but also are integrated into a practical party. Here, the former scenario is merely discussed. Usually CP needs to transfer a contents encrypted key to RP, and then RP further encapsulates the key in a contents usage license to an end purchaser. Due to the collaboration and interest relationship between the two self-governed parties, a sort of negotiation mechanism is necessary to be established in the preliminary stage of the DRM ecosystem. In a mobile DRM system, CP and RP may also be two isolated business entities affiliated to one or more mobile network operators, and Zheng et. al. [11] presented a RO negotiation that specified permissions and constraints granted to consumers based on a marriage of TMP and OMA DRM functional architecture. The proposed negotiation mechanism is only limited to digital rights in the every transactional session of the contents pull (or downloading), thus enhancing the trust relationship between both, but a pre-established business negotiation is also indispensable when a trust-efficiency tradeoff is taken into consideration.

Several electronic negotiation mechanisms, such as an auction, bidding and bargaining, were analyzed with an emphasis on the latter two approaches and proposed relative protocols for the DRM value chain [12]. In contrast with the RO negotiation mentioned above, the approaches to the license negotiation were mainly involved with such two parties as RP and Consumer, but it is also suitable for a creation of business cooperation between CP and RP in the DRM ecosystem. What is more, Arnab modeled the proposed protocols by using Colored Petri-Net, and further verified the reachability, liveness, boundedness and safety. Of the two mechanisms, the bargaining is more interactive than the bidding in the negotiation processing, and fitter to establish trust relationship based on business benefits.

In some DRM systems, CP is responsible for the production, formatting and packaging of digital contents and related metadata, and then provide them and corresponding usage licenses for consumers them by a secure channel and protect these copyrighted digital assets against tampering, circumventing and disseminating without the consents of copyrights owners. Moreover, in a more common situation, CP merely needs to be as a contents purveyor, and the provision of rights objects and the functionality of clearing house are in the charge of digital service/rights providers as RP. Thus, when consumers have a request of digital rights for authorized usages of purchased contents, there exists a negotiation whether or not the requested permissions are employed without the rights collisions, between RP and CP who is generally an owner of digital rights. If the negotiation is successful, the negotiated usage rights would be included in a RO by using a specific REL.

The rights negotiation mechanisms are categorized into the application-based negotiation and transaction-based negotiation. The former denotes that the negotiation process occurs at the preliminary phase of a DRM application system, so that a trust relationship is established at the same time. The negotiation mechanism is suitable for relatively stable rights requirements for a sort of consumers, and its managerial countermeasure can adopt the role-based or group-based approaches, with a disadvantage that rights assignment is not flexible for any consumer. The pro of the latter is secure and non-collision rights assignment in a session of contents transactions, but its con is of increase the session-level overheads owing to large numbers of negotiation

processes. As one of typical security policies discussed in the following chapter, the negotiation process is shown by Figure 3.

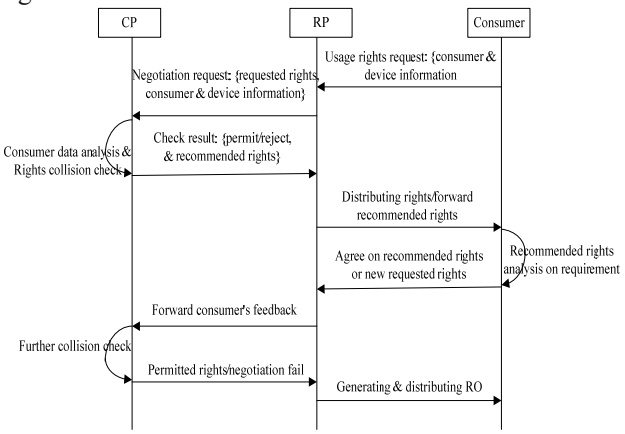

Figure 3. Transaction-Based Right Negotiation Process

In the negotiation process, only one time negotiation is permitted in order to simplify negotiation steps and reduce procedural overheads.

3. DRM TRUST AND RISK

3.1. Multi-Participant Trust in DRM 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 digital contents value chain, also called DRM value chain, 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 is also looked upon as a participant focusing on some special functions, such as key management, certificate issue, identities authentication and integrity validations of terminal devices.

Trust in DRM value chain, which belongs to an aspect of trust relations in the digital world, is a crucial and complicated challenge for realizing copyrights protection. In DRM ecosystem, it is greatly difficult to distinguish the honest users with the dishonest users. Generally speaking, contents consumers are treated as potential attackers or illegal users, and therefore CP/RP adopts some enhanced security policies mentioned above to establish a kind of trust relationship with them. Basic trusts are listed as follows in a roust DRM system:

- CP should trust the purchasers not to access any portion of the encrypted contents without acquiring the decryption key in a certain license. Users also need to trust contents security and integrity.
- RP needs to ensure that the usage license is trustworthily executed on the front-end user device, which is to say, the user should have a close or trusted environment.
- As CP and RP are collaboratively providing contents and the corresponding licenses referred to digital rights in a DRM business model, there needs an effective negotiation-based trust relationship between them.

Based on the above mentioned a general value chain and anatomy of fundamental trust relationships, a Multi-Party Trust Architecture (MPTA) for DRM was proposed, as is shown in Figure 4 [13]. It is a multi-layer framework, and also embodies a methodology of hierarchical analysis. In MPTA, the above two layers consist of DRM value chain and fundamental requirements of security for participants. According to these requirements, there are a group of security components and services that are categorized into basic and optional security component/service denoted by BSC/BSS, OSC/OSS respectively. They can be adopted by participants to implement various practical security policies. So, the forth layer presents a set of security policies for every party. Further, the party in value chain is considered as a Rational Agent (RA) that can reasonably choose and use a certain security policy, and the consideration is from the assumption of rational agents in Game Theory.

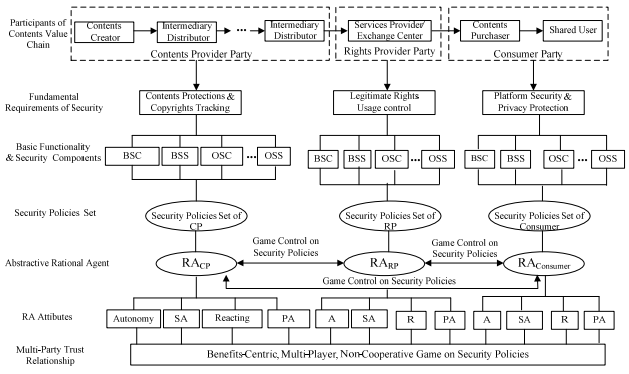

Figure 4. Multi-Participant Trust Architecture for DRM Ecosystem

From the viewpoint of DRM value chain, the rationality of adopting security policies is based on Rational Agents' game, in which security policies as strategies (or actions) would be rationally chosen, as a result the benefits

balance would be achieved. Note that Rational Agent should have four basic attributes:

- Autonomy denotes an ability of Rational Agent to independently make decision on use of strategy.
- Social Ability (abbr. SA) depicts a capability of considering practical effects of other Rational Agents' actions on self.
- Reacting on adoption of strategy in term of the opposite Rational Agents' choices.
- Pro-Activeness (abbr. PA) embodies a goal-driven action on rationally acquiring maximum benefits.
-

3.2. Security Risk Management and Utility Category

The emerging trend for the legitimate and flexible sharing of purchased contents is helpful to extend the content value chain and improving user experiences. However, owing to the inherent vulnerability of general-purpose devices, copyrighted digital contents or assets are subject to complicated and severe risks of piracy and abuse in content sharing scenario, and digital content/services providers faced with these challenges have been dedicating themselves to exploring on countermeasures in recent years.

Risk management is an essential concept in the realm of finance and business, and allows business managers to balance operational and economic costs of protective measures and achieve benefits through protecting business processes that support business and enterprise objectives, even military missions [14]. Risk management is an integrated process used to identify, control, and minimize the impact of uncertain risky events, and is mainly made up of four distinct steps: risk analysis, risk assessment, risk mitigation, and risk control. The ultimate objective of the risk management program is to reduce the risk of performing some activities or functions to an acceptable level. In addition, recent attentions to information security breaches have led to an increased awareness of information security issues, and related security risk management is an effective approach to achieve the information assurance and to control risks to valuable assets and information systems in the case of the ubiquitous security vulnerabilities and hostile attacks [15]. Figure 5 depicts the security risk in a general Sharers' social network, in which the content sharing gives birth to the risks to copyrighted digital assets. And, these risks could be controlled by the security policies from *Providers*, which is composed of CP, RP and Device Provider (DP). However, how to successfully assess these risks to copyrighted contents is still an unsolved issue for DRM nowadays.

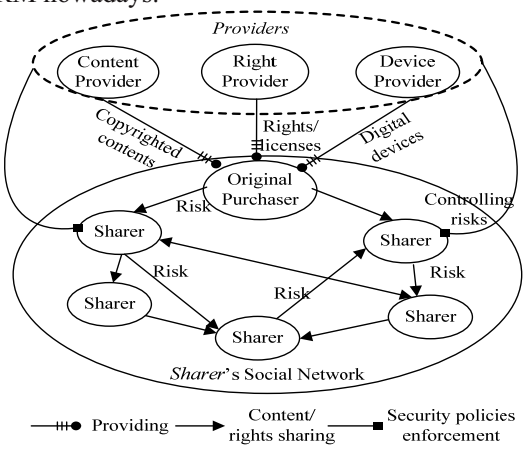

Figure 5. Security Risks in a Generic User Social Network for Contents/Rights Sharing

In conducting the risk assessment, most of the considerations are should be given to the pros and cons of quantitative and qualitative assessments. The main advantage of the qualitative style of risk assessment is that it can prioritize different risks and resort to corresponding security actions. However, this kind of approach makes a cost--benefit analysis of risk controls more difficult. Differently, the quantitative risk assessment provides a measurement of the impacts' magnitude, as is suitable for the cost—benefit analysis. Since it depends on the numerical ranges used to express the measurement, the meaning of the quantitative risk assessment may be unclear, requiring the results to be interpreted in a qualitative manner [16].

Through adopting proactive security policies, we would gain the positive utilities and considerable benefits. The positive utility of security policies is categorized into two aspects: one is general utility, and the other is Risk-Controlled Utility (RCU) [17]. The former is the return of security investment, for instance, Providers acquires much more benefits owing to the increase of purchasing contents when providing consumers with enhanced security policies/mechanism, such as Java applications security and multi-factor user authentication in the contents transactions. And the latter denotes the expectancy utility resulted in the adoptions of security policies controlling risks, and the expected risk utility is a potential benefit from Providers' perspective. In other words, if the occurrence rate of a security risk is little, or the severity factor of the risk is negligible, the risk utility is inconsiderable and the adoptions of corresponding security policies controlling the risk would be not cost-effective. So, RCU analysis is of significance for rational adoptions of security policies.

Nowadays, of the existing analytic styles, the qualitative data analysis enable us to keep the picture of risk as rich as possible for as long as possible. Therefore, risk assessment now tends to be moving toward the soft end of technology [18]. Considering the rational decision-making on the adoptions of security policies for DRM in the thesis, our ultimate goal is merely to prioritize these policies based on the RCU analysis. Therefore, the thesis integrated qualitative approach with quantitative one to estimate the security risks to valuable digital contents owing to copyrights infringements and abuse, further acquiring the corresponding risk utility owing to the adoption of enhanced security polices in the scenario.

4. CONCLUSION

The paper proposed some open issues and challenges in DRM Ecosystem, from a holistic perspective of the contents value chain. Thereinto, security, trust and risk would become three essential aspects, and as a whole support such general applications as digital contents acquisition and digital contents sharing. These attempts to realize DRM security, interoperability and usability need to pay much more attentions in the near future.

ACKNOWLEDGEMENTS

The work was sponsored by National Natural Science Foundation of China Grant No.60803150, Henan Province Key Technologies R & D Program Grant No.092102210295, and Henan University of Science & Technology Young Scholar Fund Grant No.2008QN010.

REFERENCES

[1] B. Rosenblatt, "DRM, law and technology: an American perspective," *Online Information Review*, Vol.31, No.1, pp.73-84, 2007.

[2] M.Ak, K.Kaya and A. A. Selcuk, "Optimal Subset-Difference Broadcast Encryption with Free Riders," *Information Sciences*, Vol.179, No.20, pp.3673-3684, 2009.

[3] S. Lian, "Secure Video Distribution Scheme Based on Partial Encryption," *International Journal of Imaging Systems and Technology*, Vol.19, No.3, pp.227-235, 2009.

[4] T. Thomas, S. Emmanuel and A. V. Subramanyam, et al, "Joint Watermarking Scheme for Multiparty Multilevel DRM Architecture," *IEEE Transactions on Information Forensics and Security*, Vol.4, No.4, pp.758-767, 2009.

[5] H. T. Poon, A. Miriand and J. Y. Zhao, "An Improved Watermarking Technique for Multi-user, Multi-right Environments," *Multimedia Tools and Applications*, Vol.42, No.2, pp.161-181, 2009.

[6] A. Pretschner, M. Hilty and F. Schütz, et al, "Usage Control Enforcement: Present and Future," *IEEE Security & Privacy*, Vol.6, No.4, pp.44-53, 2008.

[7] *eXtensible rights Markup Language (XrML) 2.0 Specification*, ContentGuard Incorporation, Nov, 2001.

[8] *Open Digital Rights Language (ODRL) version 1.1*, Available: http://www.w3.org/TR/odrl.

[9] *Information technology---Multimedia framework Part 5: Rights Expression Language*, ISO/IEC 21000-5, 2004.

[10] P. Jamkhedkar, G. Heileman and I. Ortiz, "The problem with Rights Expression Languages," 2006 ACM Workshop on Digital Rights Management, Alexandria, Virginia, USA, Oct, 2006.

[11] Y. Zheng, D. He and H. Wang, et al, "Secure DRM scheme for future mobile networks based on Trusted Mobile Platform," 2005 International Conference on Wireless Communications, Networking and Mobile Computing, pp.1164-1167, 2005.

[12] A. Arnab, "Towards a general framework for Digital Rights Management," Ph.D. Dissertation, University of CAPE TOWN, Jun, 2007.

[13] Z. Zhang, Q. Pei and J. Ma, et al, "A Benefits-Centric Multi-Participant Trust Architecture for DRM-Enabling Digital Contents Value Chain Ecosystem," 2008 International Seminar on Business and Information Management, Wuhan, China, Dec, 2008.

[14] D. Buckshaw, G. Pamell and W. Unkenholz, "Mission Oriented Risk and Design Analysis of Critical Information Systems," *Military Operations Research*, Vol.10, No.2, pp.19-38, 2005.

[15] S. Evans and J. Wallner, "Risk-based Security Engineering through the Eyes of the Adversary," 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, pp.158-165, 2005.

[16] T. Peltier, Information Security Risk Analysis 2nd Edition, Auerbach Publications, New York, 2005.

[17] Z. Y. Zhang, S. G. Lian and Q. Q. Pei, "Fuzzy Risk Assessments on Security Policies for Digital Rights Management," *Neural Network World*, Vol. 20, No.3, pp.1-19, 2010.

[18] A. Jones A and D. Ashenden, Risk Management for Computer Security, Elsevier Inc Press, 2005.