Digital Rights Management Ecosystem: Open Issues and Challenges

Zhiyong Zhang
Electronics Information Engineering College, Henan University of Science and Technology, Luoyang 471003, P. R. of China
E-mail: z.zhang@ieee.org

Abstract

Digital rights management ecosystem is a comprehensive copyrighted contents value chain and its measures to counteract copyright infringements, and nowadays there is primarily involved with security-centric policies and mechanisms. Regarding the ecosystem enabling contents acquisition and share scenarios, we highlighted a range of open issues and frontier challenges on hard security and soft computing in the ecosystem, such as the usage control in digital home networks, multi-stakeholder trust and assessment in multimedia social networks, as well as security risk management for digital contents and rights redistribution led by the limited security and uncertain trust, in order to establish a prosperous and healthy digital contents industry.

Keywords*: Digital Rights Management ecosystem, Security, Soft computing, Multimedia Social Network, Risk management*

1. Introduction

Digital Rights Management (DRM) emerged in the early 1990s as a realistic response to the copyrights infringement threats. It was regarded as a tangible way to safeguard the legal rights and benefits of multimedia content owners, copyright holders, digital service providers, and even consumers at end of the content value chain. DRM is an umbrella term for multiple scientific disciplines research, including information security technology [1, 2], copyrights law, business modes, and DRM economics. Throughout the past decades, the emphasis on DRM technology has primarily been laid on preventive and reactive approaches to the copyrighted content protection and combating piracy, for instance, preventive cryptographic security and usage controls on digital contents/rights, as well as on the reactive forensics adopting digital watermarking techniques.

2. DRM Ecosystem

DRM ecosystem denotes the digital content value chain and its effective measures to copyrights protection as a whole, referring to the entire life cycle of digital content from creation and packaging to dissemination for usage and sharing. From a novel technical-managerial perspective, we presented a general DRM ecosystem comprehensively involved with security policies, multi-participant trust, and risk management, which would support two representative application scenarios: contents acquisition and contents sharing, as shown by Figure 1.

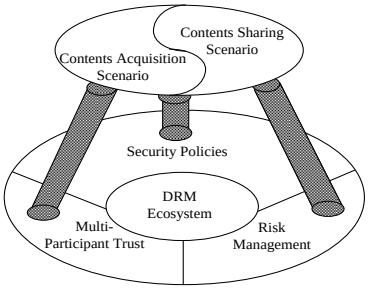

Figure 1. Three essential factors and two typical application scenarios in DRM ecosystem

First, DRM security policies and mechanisms have ever been focus on implementing the copyrighted contents protection and copyright infringement tracking in versatile internet applications for content acquisition scenarios. Of these policies, the preventive include secure content distribution, cipher-key management, authorized usage control and privacy protection, and secure terminal environments for end-users. And, the reactive measure to combat piracy is involved with digital watermarking techniques, which have been proved highly effective in continuously tracking and authenticating legal copyrights on pirated digital assets. In addition, adaptive patchwork algorithms for audio watermarking and traitor tracing technology have also been used for DRM to strengthen digital media protections.

With in-depth studies on security techniques and wide establishment of industrial specifications, DRM has already been adopted in numerous information management systems and applications, such as E-Commerce–oriented DRM systems and End-to-End DRM security architecture. And also, Enterprise-DRM (also called Enterprise Rights Management or ERM) for enterprise data security applications has recently emerged. Its objective is to achieve highly configurable options for workflow, information flow, and security, especially with regard to usage control for confidential or sensitive data.

Second, a successful digital transaction generally depends on three key factors: security, trust and benefit. The former two factors are aiming to guarantee a secure and persistent process concerning contents business, and the last factor is an essential requirement for the DRM value chain ecosystem. In a narrow sense, a basic trust infrastructure for DRM is involved with the techniques and managerial processes that enable the system logic entities or physical components trustworthy. In addition, broadly speaking, there needs to be a mutual multi-participant trust relationship among various stakeholders in a DRM ecosystem.

In DRM ecosystem, the examination of multi-party trust between stakeholders should include the following aspects: (a) In a DRM ecosystem, multi-party mutual trust is necessary for the survival of the entire value chain. This must include content providers, services/rights purveyors, device vendors, and end consumers. Trust relationships involved should be identified to create a feasible business model for content transactions from a technical or managerial perspective. (b) Trust in DRM should be comprehensive, which means that it should be not only static—implemented by certification and authentication to key components and entities—but also dynamic—trust in the behaviors of essential components and the security of digital services. In multi-party trust establishment and strengthening, usage control and other security mechanisms also play an important role.

Finally, the emerging trend of legal and flexible sharing of purchased contents is essential to extend the content value chain and improve user digital experience. However, because of the inherent vulnerability of general-purpose devices, copyrighted digital content or assets are subject to complicated and severe risks of piracy and abuse in content usage and sharing scenarios. Digital content/service providers have been facing these security risk management challenges, and are dedicating themselves to exploring effective countermeasures and solutions.

3. Open Issues and Challenging Applications

3.1. Usage Control in Digital Home Networks

With the rapid development of 3G/4G, there are emerging mobile DRM applications capable for effectively implementing digital copyright management for mobile e-commerce and e-content transactions, such as Mobile Internet Protocol Television (IPTV) DRM [3] and personal digital content/rights transfer [4]. DRM-protected mobile content service is listed among the four kinds of DRM killer applications in North America and the European Union.

Typically, in a generic digital home network (DHN), there are numerous and versatile digital devices nowadays such as PCs, IPTVs, smart phones, PDAs, and MP3/MP4 players. General users are eager to play DRM content freely and legally on their own devices in digital home network domains [5-7]. For this, cryptography and usage control play an important role in DHN. A DRM system for the home network, which is based on the ID-based public key system and group signature protocol, was presented to enable access control of contents and protection of domain privacy by the anonymity characteristic of group signature [8]. Reference [9] introduced an Onion Policy Administration (OPA)-based DRM model by which both content creators and distributors can configure license with traceability; this leads to greater efficiency and security of rights sharing. Bhatt et al. developed a

Personal DRM prototype of the Motorola E680i smart mobile phone [4]. Using the novel terminal, end consumers can set the digital license and flexibly transfer this among devices, resulting in personal content sharing. On temporal rights sharing, Lee made an interesting investigation on a redistribution approach and secured protocol among front-end user devices. The effort is of significance in the extension of digital rights sharing [10]. Feng and Tang adopted Ergodic Encryption and machine authentication to share purchased license, significantly reducing the overhead due to dependence on the authorized domain [11].

Generally speaking, we have a clear research motivation on DRM-enabling digital home networks. There remains, however, a lack of formalized fine-grained usage control model and necessary security analyses on cross-domain security management, usage constraint rules, and rights transferring. With the guidance of the formalized security model, flexible DRM applications would be easily implemented in DHN. Therefore, this is a burning open issue and facing challenge for us.

3.2. Trust Assessment in Multimedia Social Networks

Recent years have witnessed the emergence of Multimedia Social Network (MSN), which is a typical Internet application platform based on Small World Network (SWN) theory and social relations among people in digital community and society, even digital world as a whole [12]. Users of MSN can feasibly exchange, share and interoperate multimedia data, and further boost interactions with a series of well-defined functions. For this, there exists the essential trust issue to be solved.

The growth and the small world nature of web-based social networks offer great potential for the application of intelligent e-community, which combines social networks and personal preferences. How can trust information be explored in web-based social networks and how can such information be integrated into the trust assessment of social networks? These are the main issues addressed in social network applications. To find solutions, many researchers have conducted extensive research on trust relationship description and trust transfer, and attempted to apply trust mechanisms in social networks by researching on trust assessment and small world nature.

Golbeck et al. [13] described the trust relationship as follows: trust is a kind of belief and a kind of guarantee, and the entity's behavior in the future can elicit results as good as expected. They used {0, 1} to represent trust relationship, in which 0 stands for distrust and 1 stands for trust. Trust is indicated to have transferability, asymmetry and subjectivity, and the influences these attributes have over information inference are discussed.

Yuan et al [14, 15] revealed that the trust network is formed based on the inter-node trust relationship and is generally regarded as a small world network. Few researchers have examined the assumption that the trust network is a small world network due to the dynamism of the trust network. Reference [14] presented the traditional way of examining the small world feature. Here, if a trust network has a relatively large concentration coefficient and a shorter path length, it is indicated to be a small world network. Further, Yuan et al [15] concluded that considering the dynamic changes in the trust network, and the fact that the proposed method only adopts static data at a particular time point, it can only offer limited proof that the trust network has the small world feature at that particular time point. Moreover, this is insufficient in proving that the dynamic trust network is a small world network. Hence, they presented a new examination method to prove that the scale-free network is a kind of small world network.

Figure 2 depicts a social network and its user trust relations denoted by an arrow, and social relationship by using a real line. Obviously, there is a direct trust between User A and User B in the same SWN, and a cross-SWN indirect trust between User A and User C through User B. The key challenge is to find out both effective algorithms for trust assessments and feasible experimental methods for soft computing assessment verifications.

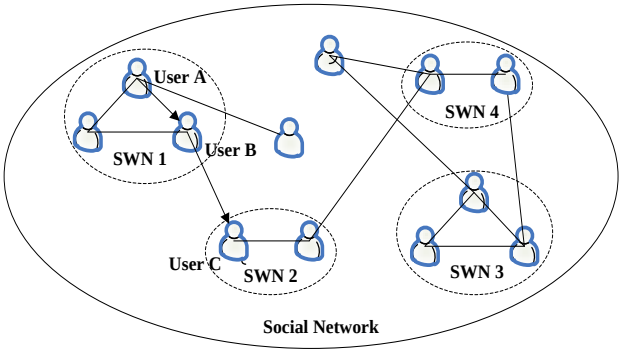

Figure 2. A social network and its user trust relations

3.3. Security Risk Management for Digital Contents and Rights Redistribution

Risk management is an important 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 [16]. There 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 [17].

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 [18]. In general, the decision of which to use should depend on what you are attempting to achieve. 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 computing technology [19].

The potential security risk in a general sharer social network is illustrated by Figure 3, in which the contents/rights sharing and limited security gives birth to the potential risks to copyrighted digital assets. And, these risks could be controlled by the enhanced security policies from Providers, which is composed of Content Provider (CP), Right Provider (RP) and Device Provider (DP). However, how to successfully assess these risks to copyrighted contents is still an unsolved issue and challenge for DRM ecosystem nowadays.

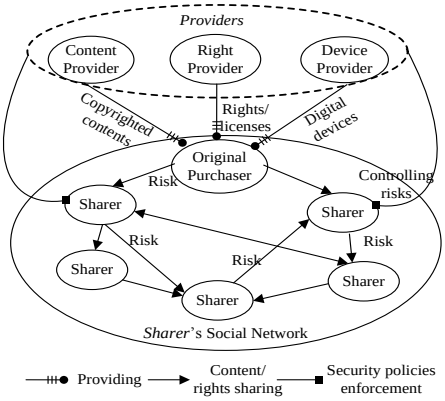

Figure 3. Security risks of e-content/rights sharing in a generic consumer social network

Considering the rational decision-making on the adoptions of security policies for DRM, an ultimate goal is merely to prioritize these policies. Therefore, there needs an 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.

Summarily speaking, these above mentioned aspects are integrated into a business model establishment and risk controlling, as shown by Figure 4, in order to enable the IPR (Intellectual Property Rights)-enabling contents industry to flourish. Thus, the phenomenon that digital users reject DRM technologies and DRM-enabled digital products, even interrupt the contents chain value, will be changed in combination with balancing the rights and interests of the various stakeholders in DRM ecosystem.

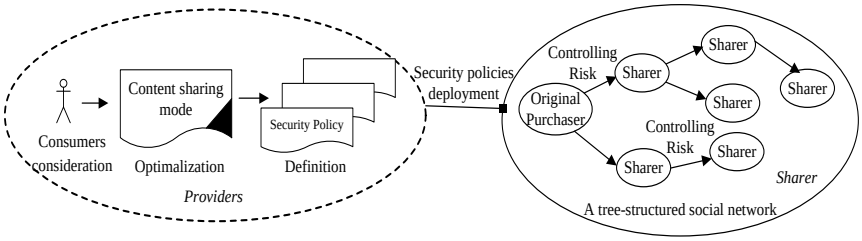

Figure 4. Business model establishment and risk controlling

4. Conclusions

During the past decades, digital content industry researchers, engineers, policies-maker and administrators have employed state-of-the-art DRM technologies and initiatives to protect valuable multimedia content and service assets against serious copyrights infringement. With the rapid developments of versatile Internet applications and increased sophistication of DRM ecosystem, we addressed some open issues and challenges from a novel perspective on DRM security technology and soft computing, as a help for explorers to seek the countermeasures to piracy.

5. Acknowledgments

The work was sponsored by the National Natural Science Foundation of China (Grant No.61003234), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No.2011HASTIT015), China Postdoctoral Science Foundation (Grant No.20100471611), and Henan University of Science & Technology Doctors Research Fund (Grant No.09001470).

6. References

[1] Alexander Pretschner, Manuel Hilty, Florian Schütz, Christian Schaefer, Thomas Walter, "Usage Control Enforcement: Present and Future", IEEE Security & Privacy, Institute of Electrical and Electronics Engineers Inc., vol. 6, no. 4, pp.44-53, 2008.
[2] Yajun Jiang, Bo Yang, "A Privacy-preserving Digital Rights Management Protocol based on Oblivious Transfer Scheme", International Journal of Digital Content Technology and its Applications, Advanced Institute of Convergence Information Technology, vol. 5, no. 5, pp. 337-341, 2011.
[3] Y. Nishimoto, N. Mita, H. Imaizumi, "Integrated Digital Rights Management for Mobile IPTV Using Broadcasting and Communications", IEEE Transactions on Broadcasting, IEEE Broadcast Technology Society, vol. 55, no. 2, pp.419-424, 2009.
[4] Siddharth Bhatt, Radu Sion, Bogdan Carbunar, "A Personal Mobile DRM Manager for Smartphones", Computers & Security, Elsevier Ltd, vol. 28, no. 6, pp.327-340, 2009.
[5] Chi-Man Pun, Jing-Jing Jiang, "Adaptive Patchwork Method for Audio Watermarking Based on Neural Network", International Journal of Digital Content Technology and its Applications, Advanced Institute of Convergence Information Technology, vol. 5, no. 5, pp. 84-94, 2011.
[6] JungSoo Lee, Yeonjeong Jeong, Kisong Yoon, Jihyun Park, "DRM applied contents share in digital home", In: Proceedings of the 13th IEEE International Symposium on Consumer Electronics, pp.64-66, 2009.
[7] Heeyoul Kim, Younho Lee, Yongsu Park, "A robust and flexible digital rights management system for home networks", Journal of Systems and Software, Elsevier Inc., vol.83, no.12, pp.2431-2440, 2010.
[8] Qingqi Pei, Jianfeng Ma, Jinxiu Dai, Kefeng Fan, "Digital rights management for home networks using ID-based public key system and group signature", China Journal of Electronics, Chinese Institute of Electronics, vol. 16, no.4, pp.653-669, 2007.
[9] Thierry Sans, Frédéric Cuppens, Cuppens-Boulahia Nora, "OPA: onion policy administration model-another approach to manage rights in DRM", In: Proceedings of 2007 IFIP International Federation for Information Processing, pp.349-360, 2007.
[10] Sangho Lee, Jong Kim, Sung Je Hong, "Redistributing Time-based Rights between Consumer Devices for Content Sharing in DRM System", International Journal of Information Security, Springer Verlag, vol.8, no.4, pp.263-273, 2009.
[11] Xue Feng, Zhi Tang, Yinyan Yu, "An efficient contents sharing method for DRM", In: Proceedings of 2009 Consumer Communications and Networking Conference, pp.1-5, 2009.
[12] L. Srensen, "User managed trust in Social Networking-comparing Facebook, MySpace and Linkedin", In Proceedings of the 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, pp.427-486, 2009.
[13] Jennifer Golbeck, James Hendler, "Inferring Binary Trust Relationships in Web-Based Social Networks", ACM Transactions on Internet Technology, Association for Computing Machinery, vol.6, no.4, pp. 497-529, 2006.
[14] Weiwei Yuan, Donghai Guan, Young-Koo Lee, Sungyoung Lee, Sung Jin Hur, "Improved trust-aware recommender system using small-worldness of trust networks", Knowledge-Based Systems, Elsevier, vol.23, no.3, pp.232-238, 2010.
[15] Weiwei Yuan, Donghai Guan, Young-Koo Lee, Sungyoung Lee, "The small-world trust network", Applied Intelligence, Springer Netherlands, vol.32, no.2, pp.1-12, 2010.
[16] Donald L. Buckshaw, Gregory S. Parnell, Willard L. Unkenholz, Donald L. Parks, James M. Wallner, O.Sami Saydjari, "Mission Oriented Risk and Design Analysis of Critical Information Systems", Military Operations Research, Military Operations Research Society, vol.10, no.2, pp.19-38, 2005.
[17] Shelby Evans, James Wallner, "Risk-based Security Engineering through the Eyes of the Adversary", In: Proceedings of the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop, pp.158-165, 2005.
[18] Thomas R. Peltier, Information Security Risk Analysis 2nd edition, Auerbach Publications, New York, USA, 2005.
[19] Andy Jones, Debi Ashenden, Risk Management for Computer Security, Elsevier Inc Press, Burlington, USA, 2005.

Biography

Zhang Zhiyong received his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, China, in 2003 and 2009, respectively, and post-doctoral fellowship at Xi'an Jiaotong University, China.
He is currently associate professor with College of Electronics Information Engineering, Henan University of Science & Technology, and research interests include digital rights management and soft computing, trusted computing and access

control, as well as security risk management. Recent years, he has published over 40 scientific papers on the above research fields, and held 3 authorized patents.

Dr. Zhang is IEEE Senior Member, IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing, Membership for Digital Rights Management Technical Specialist Workgroup Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee, Topic Editor-in-Chief of International Journal of Digital Content Technology and Its Applications. Besides, he is Chair/Co-Chair and TPC Member for numerous international workshops/sessions on Digital Rights Management and contents security.