Digital Rights Management Ecosystem and its Usage Controls: A Survey

[1,2] Zhiyong Zhang
[1]*Electronics Information Engineering College, Henan University of Science and Technology, Luoyang 471003, P. R. of China*
[2] *School of Management, Xi'an Jiaotong University, Xi' an 710049, P. R. of China*
E-mail: z.zhang@ieee.org
doi:10.4156/jdcta.vol5. issue3.26

Abstract

Progressive and dynamic developments in the digital content industry are significantly dependent on copyright protection. Effective usage control technologies can guarantee that end consumers are able to legally access, transfer, and share copyrighted contents and corresponding digital rights. From the technical and managerial perspectives, we give a wide survey on state-of-the-art of Digital Rights Management (DRM) systems. This paper starts with a generic DRM ecosystem that effectively supports two typical application scenarios, and the ecosystem builds multi-stakeholder trust and maximizes risk management opportunities. And also, a holistic and comprehensive investigation of usage control models, policies, and mechanism were made in detail. These include, but are not limited to, multiple comparisons of rights expression languages, security models, authorization management, rights transfer, and trustworthy utilization of secure end-user digital devices or consumer electronics. Finally, a range of open issues and challenges for DRM ecosystems are highlighted. A variety of controllable and traceable rights sharing among e-users, in combination with security risk management, will be the key for emerging social network services.

Keywords*: Digital Rights Management, Security, Usage Control, Social Network Services*

1. Introduction

Recent years have seen rapid developments in information and communication technology and the next-generation Internet. 3G/4G wireless mobile networks have also undergone large-scale deployment and application. Flexible and versatile network admission modes enable convenient connections to existing and future digital resources "for anyone, anytime, anywhere, on any device." Along with rapid developments, however, copyright infringement has also become prevalent, with issues such as free distribution, unauthorized use, and illicit sharing of copyrighted digital content. The most sought-after proprietary content includes electronic books, images, music, movies, and application software mainly due to the ease with which these products can be duplicated while retaining the high quality of the reproduction. These illegal practices have a negative effect on content protection and legal usage, making potential risks to the digital content industry. Thus, appropriate solutions for content protection and legal usage are urgently needed, especially for attractive triple play services in China.

Digital Rights Management (DRM) emerged in the early 1990s as a realistic response to the aforementioned threats. It was regarded as a tangible way to safeguard the rights and benefits of multimedia content owners, copyright holders, digital service providers, and even consumers in content value chains. DRM is an umbrella term for research or multiple scientific disciplines, such as information security, copyright law, and technical realizations [1-4], as well as business realizations of the digital content industry, including DRM economics [5], business modes [6], and DRM price policies [7, 8].

Throughout the past decades, the emphasis on a DRM technical and managerial perspective has primarily been dealt with from a preventive approach to content protection. The major focus has been on cryptographic security and usage controls on digital content/rights, as well as on the reactive mechanisms of digital watermarking used for combating piracy. Typically, there are mobile DRM applications that have the capacity to effectively implement digital copyright management for mobile e-commerce and e-content transactions, such as Mobile Internet Protocol Television (IPTV) DRM [9] and personal digital content/rights transfer [10]. DRM-protected mobile content service is listed among the four kinds of DRM killer applications in North America and the European Union.

This study undertakes a holistic and comprehensive survey of DRM ecosystems and their usage controls, including related rights expression languages (REL), models, architectures, and mechanisms. We also highlight a range of open issues and challenges that industry professionals currently face. The remainder of this paper is organized as follows. In Section 2, a background on DRM ecosystems and their essence is presented. In the succeeding section, we investigate usage control approaches in relation to piracy and security risk mitigation for digital content (assets). Finally, some open issues are discussed in Section 4.

2. DRM Ecosystem Background

DRM is a digital content value chain, also called DRM ecosystem, and it 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.

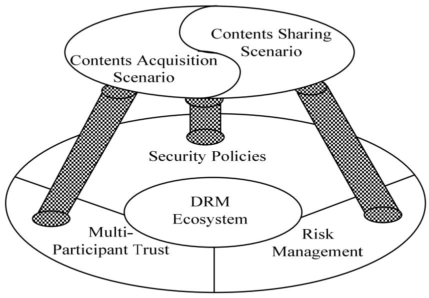

Figure 1. Three essential factors and two typical application scenarios in DRM ecosystem

DRM security policies are primarily intended for implementing content protection, usage control, and copyright infringement tracking in versatile networks for content acquisition scenarios [11, 12]. Of these policies, preventive measures are oriented by secure content distribution, trustworthy storage, authorized usage, and intellectual property protection [13]. Content security schemes refer to broadcast cryptography [14-16], and cipher-key management and secret sharing [17]. Usage control covers formalized rights expression and application [18], DRM rights control models [19], secure terminal environments for end-users [20, 21], and other guidelines through which authorized usage permissions are reliably executed [22]. In addition, reactive countermeasures for combating piracy include digital watermarking techniques, which have been proved highly effective in continuously tracking and authenticating legal copyrights on pirated digital assets [23]. Recent research has focused on improving digital watermarking authentication schemes for robustness, [24, 25], and on some novel watermarking mechanisms, such as Exchangeable Image File meta-data formatted-based digital image watermarking [26], hardware-aided multimedia watermarking [27], and a novel algorithm suitable for a multi-user multi-permission environment [28]. Bio-based fingerprint detection for copyright infringement authentication [29], and Traitor Tracing technologies [30, 31] have been used for DRM to strengthen digital media protection.

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 [32] and End-to-End DRM security architecture [33]. Recent studies on E-Commerce consumer security and management will be helpful for copyright owners to rationally adopt and deploy necessary security policies to control risks that are based on a cost-benefit tradeoff; examples of these risks include consumer security perception [34, 35] and protection behaviors [36], online user behavior modes [37], trust and privacy concern over online purchasing [38], and E-Commerce security architecture application [39]. In addition, with the rapid development of open-resource systems for enterprise, Software as a Service (SaaS) initiatives enable consumers to acquire and use typical application software [40]. At the same time, security is of primary importance, and Enterprise-DRM (also called Enterprise Rights Management, or ERM) for enterprise data security applications has recently emerged [41]. The key challenge for ERM is achieving highly configurable options for workflow, information flow, and security, especially with regard to usage control for confidential or sensitive data [42].

For multi-party trust in a DRM ecosystem, a basic trust infrastructure, in a narrow sense, is involved in the techniques and managerial processes that will allow system logic entities or physical components to function effectively. Broadly speaking, a mutual multi-participant trust relationship between all the stakeholders in a DRM ecosystem should exist. As an open issue in DRM and the digital world, the examination of multi-party trust between stakeholders should includes 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. Use case depicting the content sharing scenario is shown in Figure 2. 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 challenges, and are dedicating themselves to exploring effective countermeasures and solutions.

DRM usage control, combined with security risk management, has been emphasized on preventive security policies. Figure 2 depicts the security risk in a general Sharers' social network; content sharing increases the risks to copyrighted digital assets. These risks can be controlled by the security policies from Providers, i.e., the Content Provider, Right Provider, and Device Provider. The ultimate objective of risk management by Providers is to control the security risk involved in performing related usage control functions and mechanisms to an acceptable level, while safeguarding the rights and benefits of stakeholders who hold valuable assets. Providers also address ubiquitous security vulnerabilities and hostile attacks. However, successfully assessing the risks to copyrighted contents remains an unresolved issue in DRM. Recently, we proposed a DRM security-utility analytic approach for the adoption of security policies [43, 44], and fuzzy security risk management in a content/rights sharing scenario using soft computing [45]. We effectively identified, assessed, and controlled risks in the copyrighted content value chain.

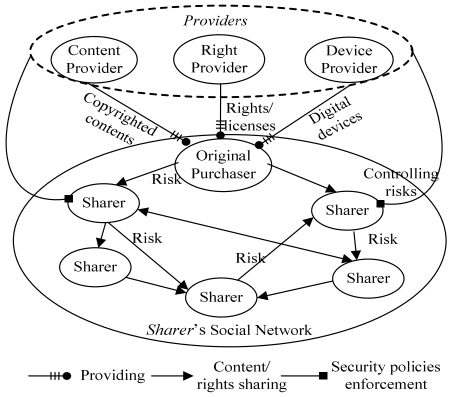

Figure 2. Security risks of e-content/rights sharing in a generic consumer social network

In the past two years, we have proposed a DRM security-utility analytic approach to the adoption of cost-effective security policies based on cooperative and non-cooperative game theory [43, 44]. We also explored the fuzzy security risk management in a user-tree-centric content/rights sharing scenario using soft computing [45]. Our goal was to effectively identify, assess, and control risks in the copyrighted content value chain, and develop a successful model that would achieve multi-stakeholder trust and optimal balance for DRM ecosystems. In addition, we presented a business model establishment and risk controlling process for DRM, as illustrated by Figure 3.

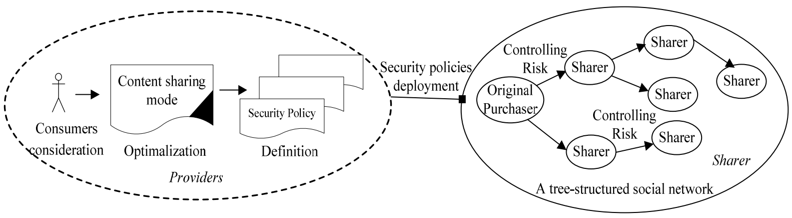

Figure 3. Business model establishment and risk control process

The process primarily includes a range of user considerations, optimal adoption of content sharing modes, and security policy specifications and deployments, which are represented in detail as follows:

- A digital content/service vendor should consider the number of sharers adopting the generic security devices. They should also take into account a number of other factors. For example, the considerable investment on, and deployment of enhanced security policies on every sharer is not cost-effective and optimal, as a certain quantity of sharers can access shared content in generic devices or open terminal platforms because of limited sharable digital rights and high costs of enhanced security devices.
- Based on the dynamic security policy, content providers may adopt a modest sharing style as a common model for proprietary content sharing between consumers, who constitute a type of social network. Users can share purchased content/licenses with their relatives, friends, or colleagues.
- Content/service providers can allow intended sharers to choose enhanced security devices by effectively restricting the number of shareable digital rights when consumers use a general device. Thus, device vendors can increase their benefits by selling enhanced-security devices.

In combination with the establishment of a business model, content/service providers implement and deploy security policies in a manner that protects the digital content/assets against illegal copying, abuse, and dissemination in the entire life cycle of content transaction, as well as usage and sharing, while acquiring considerable benefits.

3. DRM-Enabling Usage Controls

3.1. Digital Rights Expression Languages

3.1.1. Representative RELs

Generally, an REL is employed by content/right providers to specify content usage policies, which are controlled by a number of combined grant rules that allow for concrete rights/permissions under specified conditions and constraints [46, 47]. Some representative RELs are available and these include extensible rights Markup Language (XrML) [48], Open Digital Rights Language (ODRL) [49], and MPEG-21 [50], which have gradually progressed and have been precisely described in recent years. As previously stated, the additional semantics of RELs have been introduced by increasing new XML tags. These constitute a primitive and underlying language that is flexible, machine-understandable, human-readable, and expressive. An unambiguous semantics is required to ensure that REL-based rights specifications of copyrighted content are non-conflicting.

Therefore, some studies have been focusing on formal REL specifications. For example, the formal foundation for XrML and ODRL are presented in [51, 52], respectively. In addition, the MPEG-21 REL ISO Standard with formal depictions was introduced in the multimedia content industry [50]. Jamkhedkar et al proposed a formalized core model of digital rights as a basis for generic RELs, and clearly presented the map relations between the novel model and the abovementioned XrML, ODRL, and Creative Commons License [53]. Given the lack of formalized semantics of OMA REL, Reference [54] employed an executable algebra language, called CafeOBJ, to resolve the problem and realize the automatic tools for checking the behaviors of license sets. Sheppard discussed the issue of the translation between XML-REL and virtual machine programs, and proposed a novel concept, Rights Expression Compiler, which is used for the formalized definitions and precise translations of RELs [55]. For the validation of digital rights, Sachana implemented an effective method for checking rights consistency [56, 57].

3.1.2. Logic-Based Rights Formalism

As logic is a generic and effective foundation on which far more expressive and complete functionalities of rights management can be built, REL formalism and reasoning for digital rights have been developed primarily on the basis of logical approaches. A logic-based REL, called L^{lic}, is a precise and rigorous language, proving properties of licenses and specifying consumer actions that are permitted or obligatory under given conditions [58]. In L^{lic}, for example, the properties of contracts and agreements between content/right providers and consumers are emphasized, and formalized constraints, obligations, and agreements (which are predefined by DRM ecosystem participants) are produced in detail. Meanwhile, usage control rules and policies with rights deletion characteristics are included in the logic-based REL. The major contributions made by Pucella et al. are several complicated temporal logic properties, such as the finite run and license. Moreover, the satisfiability and verification of L^{lic} were presented to ensure the validity of formula interpretation in the logic language. However, this method failed to cope with the administrative issue of digital rights. Given the simple and flexible foundation of the logic, administrative rights would be easily built.

Lithium, which is a formalism language for presenting usage control policies, has considerably more expressive grammar and clearer semantics based on one-order logic. Halpern defined its map translation with XrML and ODRL [59].

Chong et al. [60] revealed some important disadvantages of the XML-based RELs in existence. These include complicated and obscure syntax, lack of formal semantics, and so on. They wanted to analyze the key components of these XMLs and their relationship with RELs. They developed a novel formal REL, called *LicenseScript*, based on Multi-set Rewriting and Pure Prolog programming. *LicenseScript* is a license-centric logical expression. It has the ability to capture the dynamic evolution, as well as the static terms and conditions of the license, and consequently provide a concise and explicit formal semantics.

3.1.3. REL Design and Applications

As a general guidance on REL design, Jamkhedkar et al. proposed some issues on REL availability and open hierarchy architecture, and proposed a design principle for multi-layer inter-operability and a prototype in line with the principles [61]. Wang [62] compared available RELs and access control models. He also proposed a series of fundamental design principles, including syntactic and semantic un-ambiguity, as well as business model-supported expressiveness. In terms of these rules, the formal method is crucial to expressing digital rights.

Recently, in considering copyright control rules of the entire life cycle in a DRM ecosystem, García has proposed an ontology- and rule-based approach to dynamic modeling, which includes Ontology X-based Creation Model and Rights Model. He has also offered guidance for the development and deployment of copyright protection systems [63, 64].

In DRM applications, Rafi introduced a role concept to MPEG-21 REL, improving the expressivity of the original language [65]. In addition, Reference [66] designed a Role-Based Access Control

(RBAC)-based online audio and video DRM system. Mandatory Access Control (MAC) policies have also emerged in DRM applications [67].

3.2. Usage Control Architectures, Managements, and Models

3.2.1. Extensive Framework and Security Management

With extensive business models and increasing digital rights, the expressive functionalities and semantics of available RELs have gradually improved. Jamkhedkar et al. [68] addressed the significant issue of "language bloat." Some new DRM-related business models tend to be continuously introduced to DRM ecosystems, but the current RELs may be incapable of specifying material rights and their management in any particular scenario. As a consequence, a certain REL would be extended on the basis of the original REL so that it can support multiple business models. The reason this issue emerges is largely due to the lack of a separation of rights expression and rights management, which in turn results in REL becoming more complicated and difficult to operate. Therefore, a framework for extensible DRM services through a simplified core REL was proposed based on the hierarchy DRM architecture [69]. Figure 4 illustrates the separation mode of core REL and associated data with rights management, which is accomplished by the upper application-level transactional interaction.

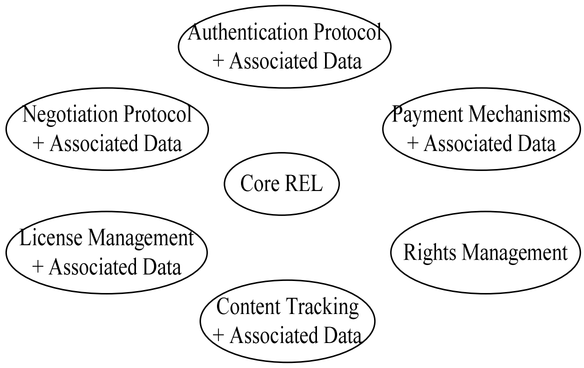

Figure 4. Security service framework with a simplified core REL [69]

The above-mentioned architecture has two advantages. First, it improves the capabilities of rights management through newly developed protocols without a modification of the core REL. Second, it needs to support only a simplified core at a rendering device of consumers and lays complicated management functionalities, such as authentication, payment, and license management at the back-end server side.

Conversely, some disadvantages of a generic conceptual model still exist. Without trusted authorizations and usage controls, more effort is required on some security mechanisms and secure protocols related to rights management, license sharing, and user authentication.

Recent studies on rights enforcement and management have clearly showed that rights management is a vulnerability of DRM ecosystems [70]. As a result, a four-layer security framework was introduced. This framework is based on bottom-to-top content protection, rights enforcement, rights management, and trust management. Aside from this, rights usage can be considered a persistent access control, which is different from traditional access control policies and models, such as DAC, MAC and RABC, together with their model extensions [71], authorization management [72] and command implementation [73]. From this point of view, a formal REL representing persistent control without a control boundary is required for DRM applications [74].

3.2.2. Usage Control Models and Applications

A basic usage control framework, $UCON_{ABC}$, which integrates Authorization-Obligation-Condition, has been proposed by Park and Sandhu in their earlier research on next-generation access control architecture [75]. The framework has persistent access control suitable for DRM applications, except that it is a policy-neutral control with essential changeability and continuity, which also differs from conventional access controls. First, $UCON_{ABC}$ changeability embodies the change in usage contexts, including the attributes, and temporal and dimensional conditions of entities. Second, these changes give rise to the necessity for usage decision and attribute update to occur at any time during the entire usage procedure, rather than only at the beginning of usage. This is an embodiment of continuity. Figure 5(a) shows four combinations of $UCON_{ABC}$ models on Authorization, Obligation, and Condition, and Figure 5(b)–(d) illustrates 16 possible basic $UCON_{ABC}$ models, where 0 means that all attributes are immutable, and 1, 2, and 3 represent the updates of some mutable attributes that may arise before (pre), during (ongoing), or after (post) the rights are exercised.

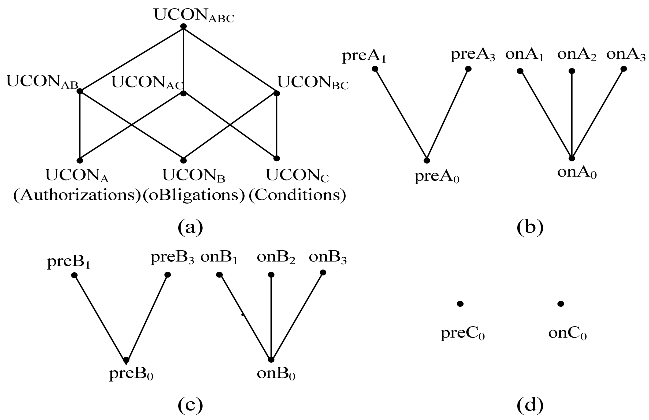

Figure 5. $UCON_{ABC}$ core model family [75]

UCON is a policy-neutral basic architecture that completely implements DAC, MAC, and RBAC security policies, which has already been proved. Pretschner presented a systematic classification based on usage control availability, implementation, and non-functionality [19]. Nair and Tanenbaum developed a DRM-enabling Trishul-UCON framework, and implemented a cross-application DRM policy based on Java Virtual Machine middleware [76].

The comparison between common RELs and classical models in several aspects, such as the "*Not*" permission property, constraint characteristics, and copyrights implementation and formalization are listed in Table 1. Symbols such as ○, ×, and - represent the *covering*, *lacking of*, and *not referring* to corresponding characteristics or functionalities.

Table 1. Comparison of representative RELs and usage control model

Usage Control of Digital Rights	Representative Specified RELs				Formalized RELs/Model		
	XrML	ODRL	OMA REL	MPEG-21 REL	License Script	LiREL	$UCON_{ABC}$
'Not' Permission	-	○	-	-	-	×	×
Constraint and obligation	○	○	×	×	○	○	○
Copyrights Implementation	×	×	×	-	○	×	-
Rights Administration	×	×	×	×	○	-	○
Formalization	○	○	-	Set Notation	Multi-set Rewriting + Prolog	Set Notation	Set Notation +Predicate
Transferability	○	○	×	○	○	○	×

When typical DRM applications emerged, some temporal-spatial extensions for usage control models were developed. Muhlbauer [77] improved traditional rights controls based on proposed location constraints, by which consumers can access sensitive data resources with a spatial change in mobile terminals. In the scheme, a non-instantaneous display usage control is realized based on MPEG-21 REL and Intellectual Property Management and Protection components, in combination with HTTP-HELD protocol-supported trusted location services. In addition, providing a complicated technical category of non-instantaneous access control makes his scheme more effective. Interestingly, the issues on the reply attacks of rights objects, including dynamic rights such as play period, print count, and expire time, were addressed in [78]. A novel mechanism for controlling and managing usage on consumable rights exists—a vital motivator to prevent malicious users from re-using an expired “old license” through backup, especially among domain devices.

Regarding usage interoperability and management in DRM, Jamkhedkar et al proposed a formal model including semantics for interoperability, with a result of finding a tradeoff between flexibility and usability [79]. In addition, there recently exist a context and role-based access control model for digital content [80], threshold based group-oriented nominative proxy signature scheme (TB-GO-NPSS) for delegating signing ability [81], as well as a typical DRM application of personal privacy protections in social networks [82] and dynamic coalition of data service providers [83].

3.3. Secure Transferring and Legitimate Sharing of Digital Rights

3.3.1. Rights Transfer-Supported RELs and Depictions

Legal sharing of digital rights, relative to purchased content, is necessary for a complete DRM ecosystem and the extension of the value chain. Above all, it presenting or extending an REL with rights transfer/delegation functionality is essential. To date, the Open Mobile Alliance (OMA) has not formalized the syntaxes and semantics of rights transfer in REL Spec, making implementing content sharing or depicting preconditions and constraints of rights transfer in a DRM system (which adopts OMA DRM specifications) impossible [84]. Although other RELs including ODRL and XrML can present transferable permission of digital rights, such as Sell, Lend, Give of Open Digital Rights Language (ODRL) [52] and Delegation of XrML [51], these specifications are coarse grained. Consequently, a fine-grained specification is required in DRM business models. Because of the lack of delegation in $UCON_{ABC}$, we [85] proposed a formal usage control model with delegation capability, called $UCON_D$ (Fig. 6), which is an extension of UCON with two important intrinsic properties. Considering the flexibility and precise syntax of Backus-Naur Form (BNF), and its wider applicability to a framework specification compared with Set Theory and First-Order Logic, the proposed complementary framework was formalized by BNF Extension. Thus, the delegation framework can realize the rights transfer and content sharing in a DRM system.

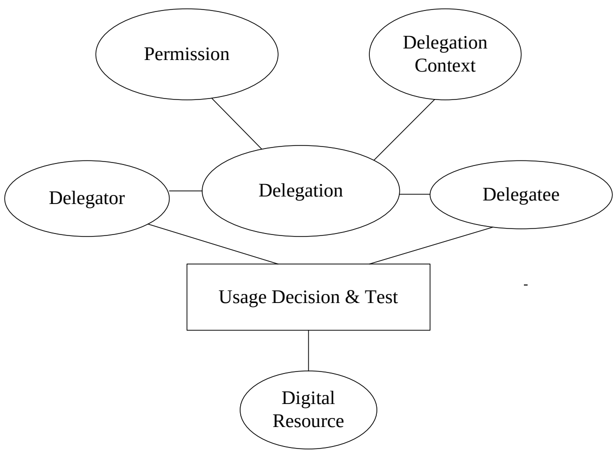

Figure 6. $UCON_D$ framework with delegation functionality

Based on the framework above, we proposed a fine-grained security policy for rights transfer in a generic DRM application [86]. Moreover, using the extensible ODRL, we specified two kinds of digital rights objects, illustrated in Figure 7(a) and (b), respectively.

```
<o-ex:rights
  xmlns:delegate=”http:/www.mispb.com/rbac/transfer-
dd”>
  <o-ex:context>
     <o-dd:uid>RightsObjectID</o-dd:uid>
  </o-ex:context>
  <o-ex:agreement>
   <o-ex:asset>
    <o-ex:context>
       <o-dd:uid>ContentID</o-dd:uid>
    </o-ex:context>
   </o-ex:asset>
  <o-ex:permission>
   <o-dd:basicPermission>
     <o-ex:constraint>
        count_constraint OR datatime_constraint  OR...
    </o-ex:constraint>
   </o-dd:basicPermission>
   <transfer:transferPermission>
     <o-dd:basicPermission>
        <o-ex:permissionConstraint>
         count_constraint OR datatime_constraint  OR...
       </o-ex:permissionConstraint>
       <o-ex:transferConstraint>
         transferDepth OR transferCardinality OR
         transferTimelimit
       </o-ex:transferConstraint>
     </o-dd:basicPermission/>
   </transfer:transferPermission>
 </o-ex:permission>
</o-ex:agreement>
</o-ex:rights>
```

(a) Digital Rights Specification

```
<o-ex:rights
    xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
    xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
    xmlns:delegate=”http:/www.mispb.com/rbac/transfer-dd”>
<o-ex:context>
    <o-dd:uid>TranferableRightsObjectID</o-dd:uid>
</o-ex:context>
<o-ex:agreement>
   <o-ex:asset>
    <o-ex:context>
       <o-dd:uid>ContentID</o-dd:uid>
    </o-ex:context>
  </o-ex:asset>
<o-ex:permission>
  <o-dd:basicPermission_1>
     <o-ex:constraint>
       <o-dd:count>count_constraint_1</o-dd:count>
       <o-dd:datetime>datatime_constraint _1</o-dd:datetime>
         …
     </o-ex:constraint>
  </o-dd:basicPermission_1>
  <o-dd:basicPermission_2>
       basicPermisson_2 constraint
  </o-dd:basicPermission_2>
  <transfer:transferPermission>
       transferPermisson_1
  </transfer:transferPermission>
 </o-ex:permission>
</o-ex:agreement>
</o-ex:rights>
```

(b) Transferable Digital Rights Specification

Figure 7. Extensible ODRL-based rights specification

3.3.2. Rights Sharing Mechanisms and Implementation

In general, content providers distribute usage licenses to purchasers by binding the contents-permission-device (or user). Therefore, the flexibility of content usage is rigorously restricted. The Digital Video Broadcasting Project is an industry-led consortium, which was the first to propose the concept of “Authorized Domain” for sharing content in different rendering devices [87]. Subsequently, OMA DRM specifications have adopted the concept and realized the uniform domain management of Rights Issuer (RI), including the device’s joining and leaving the domain, and registering and RO (Rights Object) acquisition from RI [88]. This approach can guarantee content sharing within a domain that is composed of multiple devices; however, RI becomes the bottleneck of the DRM system. This shortcoming was addressed with the introduction of a domain manager in a later version.

Content sharing scenarios currently focus on Digital Home Domain [89, 90] and Personal Entertainment Domain [91]. Reference [92] proposed domain security architectures and corresponding protocols for DRM, but they did not support RO transfer and content sharing. Consequently, Kim et al. [89] improved the above-mentioned architecture for a home domain, and the newly proposed Local Domain Manager (LDM) substituted for RI to accomplish the license distribution for domain membership devices. Meanwhile, Delegated RO and Proxy Certificate have also realized rights delegation. The scheme introduces a potential attack object, that is to say LDM, and increases overhead. As far as consumer purchase from different providers and sharing on different devices are concerned, the introduction of Domain Issuer (DI) to OMA DRM, instead of multiple RIs, enables better management of a sharing domain [93]. A detailed comparison of our scheme [86] with those of others is listed in Table 2.

Table 2. Comparison and analysis of rights sharing schemes

Key Functions/ Performances	OMA [84]	Popescu's [92]	Kim's [89]	Koster's [93]	Ours [86]
Contents Sharing	○	○	○	○	○
Local Domain	○	○	Limit	Limit	-
License Enforcement	×	×	LDM	DI	No need for LDM
RO & TRO Distribution	Domain-based RO	×	Proxy Certificate-DRO	Domain-based RO	Extensible ODRL-TRO
Transfer Granularity	Coarse-grained	-	Fine-grained	-	Fine-grained
Sharing Constraints	×	×	○	×	○
Time Limitation	○	×	○	×	○
DRM Controller Trust	×	×	×	×	○
Rights Revocation	RI Control	LRL & GDRL	PC & PCRL	DI Control	TRO RL
Cipher	PKI	Symmetry	PKI	PKI	PKI
Overhead	Medium	Small	Large	Large	Large

Barhoush et al. presented 11 security requirements of digital content multicast, and comprehensively analyzed available DRM commodity applications [94]. Some disadvantages were identified and improvements were applied based on the proposed security standards. In rights super-distribution and sharing mechanisms, addressing the challenge of limited license configurations in rights dissemination, Reference [95] developed an Onion Policy Administration-based DRM model, by which both content creators and distributors can configure license with traceability, resulting in the enhanced efficiency and security of rights sharing. Bhatt et al. developed a Personal DRM prototype of the Motorola E680i smart mobile phone [9]. Using the novel terminal, end consumers themselves can program digital license and transfer them among devices, enabling personal content sharing. With regard to temporal rights sharing, Lee investigated a re-distribution approach and secure protocol among front-end user devices—an important study in extensions of digital rights sharing [96]. Feng and Tang adopted Ergodic Encryption and machine authentication to share purchased license, significantly reducing the overhead caused by dependence on the authorized domain [97]. These schemes are only suitable for a limited domain environment, such as Digital Home Network. Extending them to a wider area remains an issue for further research.

3.4. Enhanced Security of Digital Devices and Trusted Rights Execution

3.4.1. Trusted Computing and Its Specifications from the IT Industry

Consumer trustworthiness and secure terminal environments are essential factors for safeguarding rights executions and in protecting content providers or copyright owners against malicious tampering. Furthermore, these factors have a direct effect on multi-party trust in a DRM ecosystem. Fortunately, the advancements and applications of trusted computing in DRM systems are helpful in establishing trust. These applications refer to the responsible dissemination of granted licenses, secure storage of digital contents and their corresponding encryption keys, and the trustworthy behaviors of the DRM Controller. Moreover, there are several dominant DRM-enabling trusted computing techniques, such as remote attestation, seal approach, and integrated trusted platform.

Gallery [98] surveyed a trusted computing group and its basic properties, and proposed a robust realization of a trusted Mobile DRM, including the secure storage of the device key and the secure distribution of sealed contents. The Trusted Computing Group (TCG)-based mobile platform architecture and required Trusted Mobile Platform (TMP) instructions were described in detail. For terminal protection and mobile code security, remote attestation-based mobile platform verification and content protection were discussed [99].

In the trusted computing industry, a trusted PC platform specified by TCG [100, 101], OpenTC in Europe, and Chinese Trusted Computing Union already exists, along with a series of specifications for TMP. NTT DoCoMo, IBM, and Intel were the first to publish TMP specifications that describe hardware, software, and protocols [102]. TCG Mobile Phone Work Group (MPWG) depicted the instruction set and the data structure of trusted modules applicable to mobile terminals in Mobile Trusted Module Specification [103] and Trusted Mobile Reference Architecture Specification [104]. Furthermore, a domain isolation-based application engine was defined for the trusted mobile device, which has enhanced the security of engine execution and access to data. The Open Mobile Terminal Platform forum (jointly sponsored by AT&T, Hutchison 3G, and T-Mobile) is a famous organization dedicated to Mobile DRM and the application of security frameworks. Some major requirements for OMA DRM V2.0-enabler terminal were proposed as a guide for trusted mobile platforms [105]. These industry specifications are advantageous to realizing the trusted environment of Mobile DRM. TCG MPWG has explicitly supported the implementation of DRM robustness in use cases [106].

3.4.2. Trusted Computing Techniques and DRM Applications

Being a basic software platform supporting the trusted execution of DRM Controllers, the existing commodity operating system (OS) cannot effectively realize remote attestation and seal technique [107], and the mainstream OS of open platforms and their access control mechanisms cannot protect the direct I/O of decrypted content and the trusted enforcement of the license [108]. Consequently, creating a virtual technology-based isolation execution environment is necessary for the implementation of a trusted reference monitor with a MAC feature. Feng et al. proposed the TPM-based DRM architecture, TBDRM, to ensure the fundamental security and freshness of digital license in its life cycle [109]. As a contentious topic, Reference [20] addressed an approach to privacy protection based on TPM and trusted computing techniques.

Of all concepts and mechanisms related to Trusted Computing, Remote Attestation (RA) is important because it aims for remote platform attestation in networked device environments; these include digital content server and user clients in DRM. Four common measurement modes and corresponding attestation mechanisms are currently in use: TCG-RA [100, 101], Property-Based RA (PBRA)[110, 111], Semantic-Based RA (SBRA)[112], and AP^2RA (Attestation Proxy Party RA) [113], as shown in Table 3.

Table 3. Comparison of Key Mechanisms among RA Schemes

Key Mechanisms/ Performances	**TCG-RA [100]**	**PBRA [110, 111]**	**SBRA [112]**	**AP^{2}RA [113]**
Trusted Measurement Mechanism	integrity of binary codes	security properties of platform	semantic of upper software	integrity of binary codes and security properties
Trusted Report Mechanism	basic configurations of platform	security properties	checking semantics of SW	capabilities of platform
Trusted Third Party-Supported	×	○	×	○
Message Confidentiality	○	○	○	○
Message Integrity	○	○	○	○
Message Anti-Deny	○	○	○	○
Anti-Attack on APP	-	○	-	○
Anti-Collusion Attack	×	×	×	○
Anti-Replay Attack	○	○	-	○
Privacy Protection	Lower	Medium	-	Higher
Overhead	Lower	Higher	Medium	Higher

To accomplish trusted measurement and DRM application security, we proposed a conceptual Xen virtualization-based terminal platform architecture that can be adopted to implement remote attestation on DRM controllers and applications, in combination with a trusted and secure Linux-class–based Supervisor OS and AP^{2}RA mode in Figure 8. The established virtualization environment based on the trusted kernel can implement domain isolation execution and process protection in a less trusted boundary. Thus, it satisfies the trustworthiness of Attested Object (which is customarily a Guest OS kernel-like Windows or upper applications through integrity measurements and report mechanisms provided by a series of Trusted Software Stack function calls. The architecture integrated the bottom trusted hardware platform welded by a trusted chip, called Trusted Platform Module (TPM), with the trusted Supervisor OS separated from Xen-Hypervisor (located at the upper layer of the device hardware).

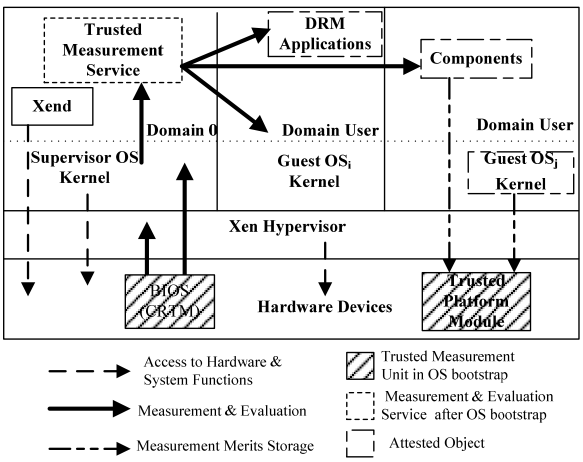

Figure 8. Xen Virtualization-based end consumer terminal platform for DRM applications

An applied framework suitable for DRM-enabling content distribution is illustrated in Figure 9. The architecture consists of a front-end XPA-enabling terminal platform, back-end digital streaming media content server, Attestation Proxy Server, and Integrity Reference and Security Policies Database conformable to the TCG-IMM model. The frame emphasizes both the static integrity of the end-user platform in the entire system bootstrap procedure, and the dynamic integrity of DRM applications using AP^{2}RA and run-time shot snaps. The authentication of user identity is also a primary functional step that ensures the legitimacy of the user requesting access to media content prior to content distribution.

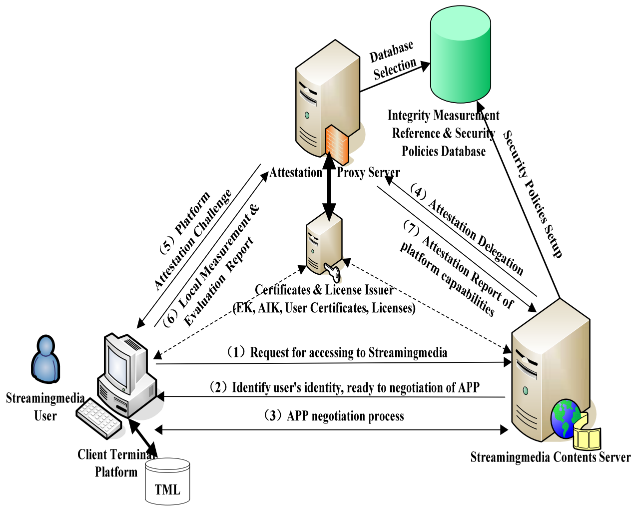

Figure 9. Trusted computing-based secure distributions of copyrighted streaming media content

4. Conclusions

During the past decades, researchers, digital content industry engineers, and administrators have relied on state-of-the-art DRM technologies and initiatives to protect valuable multimedia content and service assets against serious copyrights infringement [114]. With the rapid developments in and increased sophistication of the digital content industry, there is an ongoing consumer requirement for digital content/rights sharing. To achieve secure and trustworthy redistributions, some open issues and challenges confront the DRM industry. These usage controls are highlighted below.

- Content providers/copyright owners face security risks because of the uncontrollability and abuses that result from sharing, transferring, and spreading digital content when they are extended from a local authorization domain. An example is the distribution of content from a home network or personal entertainment domain to a wider-area social network. Therefore, identifying, assessing, and controlling these risks is an open issue, and an in-depth investigation on the theoretical model and related mechanisms of rights dissemination has become a critical problem and application research frontier.
- Emerging trusted computing devices and applications, combined with trusted computing specifications from the IT industry, are the enabler of DRM systems and their usage controls. With enhanced security platform, whether for general-purpose digital devices or special-purpose consumer electronics, greater efforts on the implementation of inter-operable and trusted rights transfer, as well as the assurance of interconnected applications at versatile terminals and all types of networks, are necessary for an effective DRM ecosystem.
- An integrated and cross-domain platform or infrastructure for triple play, which provides content providers with secure web services for general user authentication and managements, can safeguard against unauthorized, uncontrollable, and insecure usage and sharing of digital rights. Its establishment is an important challenge, and can drive the creation of a progressive and healthy content industry.

5. Acknowledgments

We would like to express our gratitude to the anonymous reviewers of this paper for their helpful comments and suggestions. The work was sponsored by the National Natural Science Foundation of China (Grant No.61003234, No.60803150), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No.2011HASTIT015), China Postdoctoral Science Foundation (Grant No.20100471611), Henan Province Key Technologies R & D Program (Grant No.092102210295), and Henan University of Science & Technology Doctors Research Fund (Grant No.09001470).

6. References

[1] Hinkes EM, "Access Controls in the Digital Era and the Fair Use/First Sale Doctrines", Santa Clara Computer and High-Technology Law Journal, vol. 23, no.4, pp.685-726, 2007.
[2] Rosenblatt B, "DRM, Law and Technology: an American Perspective", Online Information Review, vol. 31, no.1, pp.73-84, 2007.
[3] Lian SG, Multimedia Content Encryption: Techniques and Applications, Auerbach Publication, Taylor & Francis Group, UK, 2008.
[4] Lian SG. Multimedia Communication Security: Recent Advances, Nova Publishers, USA, 2009.
[5] Kiema I, "Commercial Piracy and Intellectual Property Policy", Journal of Economic Behavior & Organization, vol. 68, no.1, pp.304-318, 2008.
[6] Regner T, Barria JA, Pitt JV, et al, "An Artist Life Cycle Model for Digital Media Content: Strategies for the Light Web and the Dark Web", Electronic Commerce Research and Applications, vol. 8, no. 6, pp.334-342, 2009.
[7] Lesk M, Stytz MR, Trope RL, "Digital Rights Management and Individualized Pricing", IEEE Security & Privacy, vol. 6, no.3, pp.76-79, 2008.
[8] Li YM, Lin CH, "Pricing schemes for digital content with DRM mechanisms", Decision Support Systems, vol.47, no.4, pp.528-539, 2009.
[9] Nishimoto Y, Imaizumi H, Mita N, "Integrated Digital Rights Management for Mobile IPTV Using Broadcasting and Communications", IEEE Transactions on Broadcasting, vol. 55, no. 2, pp.419-424, 2009.
[10] Bhatt S, Sion R, Carbunar B, "A Personal Mobile DRM Manager for Smartphones", Computers & Security, vol. 28, no. 6, pp.327-340, 2009.
[11] Kim Y, Howard J, Ravindranath S, et al, "Problem Analyses and Recommendations in DRM Security Policies", In Proceedings of the First European Conference on Intelligence and Security, pp.165-178, 2008.
[12] Wu CC, Lin CC, Chang CC, "Digital rights management for multimedia content over 3G mobile networks", Expert Systems with Applications, vol. 37, no. 10, pp.6787-6797, 2010.
[13] Fan YC, Shen JH, "DFT-Based SoC/VLSI IP Protection and Digital Rights Management Platform", IEEE Transactions on Instrumentation and Measurement, vol. 58, no. 6, pp.2026-2033, 2009.
[14] Ak M, Kaya K, Selcuk AA, "Optimal Subset-Difference Broadcast Encryption with Free Riders", Information Sciences, vol. 179, no. 20, pp.3673-3684, 2009.
[15] Hou SH, Uehara T, Satoh T, et al, "Integrating Fingerprint with Cryptosystem for Internet-based Live Pay-TV System", Security and Communication Networks, vol. 1, no. 6, pp.461-472, 2008.
[16] Lian S, "Secure Video Distribution Scheme Based on Partial Encryption", International Journal of Imaging Systems and Technology, vol. 19, no. 3, pp.227-235, 2009.
[17] Fazio N, On Cryptographic Techniques for Digital Rights Management, New York University, 2006.
[18] Liu Eliot ZH, Fung Richard YK, Chung David WK, "Chinese MPEG-21 rights expression language: Enhancing digital rights management adoption to digital libraries in Hong Kong", In Proceedings of the Fifth International Workshop on Digital Rights Management Impact on Consumer Communications, pp.11-15, 2009.
[19] Pretschner A, Hilty M, Schütz F, et al, "Usage Control Enforcement: Present and Future", IEEE Security & Privacy, vol. 6, no. 4, pp.44-53, 2008.
[20] Stamm S, Sheppard NP, Reihaneh SN, "Implementing Trusted Terminals with a TPM and SITDRM", Electronic Notes in Theoretical Computer Science, vol. 197, no. 1, pp.73-85, 2008.
[21] Frattolillo F, Landolfi F, Marulli F, "A novel approach to DRM systems", In Proceedings of 12th IEEE International Conference on Computational Science and Engineering, pp.492-497, 2009.
[22] Gasmi Y, Sadeghi AR, Stewin P, et al, "Flexible and Secure Enterprise Rights Management based on Trusted Virtual Domains", In Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing, pp.71-80, 2008.

[23] Thomas T, Emmanuel S, Subramanyam AV, 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.
[24] Singhal N, Lee YY, Kim CS, et al, “Robust image watermarking using local Zernike moments”, Journal of Visual Communication and Image Representation, vol. 20, no. 6, pp.408-419, 2009.
[25] Phan RC, “Tampering with a Watermarking-based Image Authentication Scheme”, Pattern Recognition, vol. 41, no. 11, pp.3493-3496, 2008.
[26] Huang HC, Fang WC, “Metadata-based Image Watermarking for Copyright Protection”, Simulation Modelling Practice and Theory, vol. 18, no. 4, pp.436-445, 2010.
[27] Kougianos E, Mohanty SP, Mahapatra RN, “Hardware assisted watermarking for multimedia”, Computers and Electrical Engineering, vol. 35, no. 2, pp.339-358, 2009.
[28] Poon HT, Miriand A, Zhao JY, “An Improved Watermarking Technique for Multi-user, Multi-right Environments”, Multimedia Tools and Applications, vol. 42, no. 2, pp.161-181, 2009.
[29] Lian SG, Chen X, “Secure and traceable multimedia distribution for convergent Mobile TV services”, Computer Communications, vol. 33, no. 14, pp.1664-1673, 2010.
[30] Nakayama H, Jamalipour A, Kato N, “Network-Based Traitor-Tracing Technique Using Traffic Pattern”, IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp.300-313, 2010.
[31] Jin HX, Lotspiech J, Nelson M, et al, “Adaptive Traitor Tracing for Large Anonymous Attack”, In Proceedings of the 8th ACM Workshop on Digital Rights Management, pp 29-38, 2008.
[32] Banerjee S, Karforma S, “A Prototype Design for DRM based Credit Card Transaction in E-Commerce”, ACM Ubiquity, vol. 9, no. 18, pp.1-9, 2008.
[33] Hidalgo A, Albors J, Lopez V, “Design and Development Challenges for an E2E DRM Content Business Integration Platform”, International Journal of Information Management, vol. 29, no. 5, pp.389-396, 2009.
[34] Kim C, Tao W, Shin N, et al, “An empirical study of customers’ perceptions of security and trust in e-payment systems”, Electronic Commerce Research and Applications, no. 9, pp.84-95, 2010.
[35] Chang HH, Chen SW, “Consumer perception of interface quality, security, and loyalty in electronic commerce”, Information & Management, no. 46, pp.411-417, 2009.
[36] Svantesson D, Clarke R, “A best practice model for e-consumer protection”, Computer Law & Security Review, vol. 2, no. 6, pp.31-37, 2010.
[37] Lin WB, Wang MK, Hwang KP, “The combined model of influencing on-line consumer behavior”, Expert Systems with Applications, no. 37, pp.3236-3247, 2010.
[38] McCole P, Ramsey E, Williams J (2010) Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. Journal of Business Research 63(9): 1018–1024
[39] Padmavathi G, Annadurai S, “A security framework for Content-Based Publish–Subscribe system”, Electronic Commerce Research and Applications, no. 5, pp.78-90, 2006.
[40] Leea SM, Olsona DL, Leea SH, “Open process and open-source enterprise systems”, Enterprise Information Systems, vol. 3, no. 2, pp.201-209, 2010.
[41] Chen CL, “A Secure and Traceable E-DRM System based on Mobile Device”, Expert Systems with Applications, vol. 35, no. 3, pp.878-886, 2008.
[42] Everett C, “Is DRM fit for purpose?”, Computer Fraud & Security, no. 4, pp.5-7, 2010.
[43] Zhang ZY, Pei QQ, Ma JF, et al, “Cooperative and Non-Cooperative Game-Theoretic Analyses of Adoptions of Security Policies for DRM”, In Proceedings of the Fifth International Workshop on Digital Rights Management Impact on Consumer Communications, pp.6-10, 2009.
[44] Zhang ZY, Pei QQ, Yang L, et al, “Establishing multi-party trust architecture for DRM by using game-theoretic analysis of security policies”, Chinese Journal of Electronics, vol. 18, no. 3, pp.519-524, 2009.
[45] Zhang ZY, Lian SG, Pei QQ, “Fuzzy Risk Assessments on Security Policies for Digital Rights Management”, Neural Network World, vol. 20, no. 3, pp.265-284, 2010.
[46] Zhang ZY, Pei QQ, Yang L, et al, “Security and Trust of Digital Rights Management: A Survey”, International Journal of Network Security, vol. 9, no. 3, pp.247-263, 2009.
[47] Barlas C, Digital Rights Expression Languages (DRELs). JISC Technology and Standards Watch, vol.6, no.3, pp.1-42, 2006.
[48] eXtensible rights Markup Language (XrML) 2.0 Specification, ContentGuard Inc, 2001. (available at http://www.xrml.org/)
[49] Open Digital Rights Language (ODRL) Version 2.0 Draft, ODRL Initiative, 2010. (available at http://odrl.net/2.0/WD-ODRL-Vocab-20100527.html)
[50] Information Technology-Multimedia Framework Part 5: Rights Expression Language, ISO/IEC 21000-5, 2004. (available at http://www.iso.org/)
[51] Halpern J, Weissman V, “A formal foundation for XrML”, Journal of the ACM, vol. 55, no. 1, pp.4-45, 2004.
[52] Pucella R, Weissman V, “A Formal Foundation for ODRL”, In Proceedings of 2004 IEEE Workshop on Issues in the Theory of Security, 2004.

[53] Jamkhedkar P, Heileman G, “A Formal Conceptual Model for Rights”, In Proceedings of the 8th ACM Workshop on Digital Rights Management, pp.29-38, 2008.
[54] Triantafyllou N, Ouranos I, Stefaneas P, “Algebraic Specification for OMA REL licenses”, In Proceedings of 2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp.376-381, 2009.
[55] Sheppard NP, Reihaneh SN, “On the Operational Semantics of Rights Expression Languages”, In Proceedings of the 9th ACM Workshop on Digital Rights Management, pp.17-27, 2009.
[56] Sachana A, Emmanuela S, Dasa A, et al, “Privacy Preserving Multiparty Multilevel DRM Architecture”, In Proceedings of the Fifth International Workshop on Digital Rights Management Impact on Consumer Communications, pp.1-5, 2009.
[57] Sachana A, Emmanuela S, Kankanhalli MS, “Efficient License Validation in MPML DRM Architecture”, In Proceedings of the 9th ACM Workshop on Digital Rights Management, pp 73-82, 2009.
[58] Pucella R, Weissman V, “A Logic for Reasoning about Digital Rights”, In Proceedings of 2002 IEEE Workshop on Computer Security Foundations, pp.282-294, 2002.
[59] Halpern JY, Welssman V, “Using First-Order Logic to Reason about Policies”, ACM Transactions on Information and Systems Security, vol. 11, no. 4, pp.1-41, 2008.
[60] Chong CN, Experiments in rights control expression and enforcement. University of Twente, The Netherlands, 2005.
[61] Jamkhedkar P, Heileman G, “Digital Rights Management Architectures”, Computers and Electrical Engineering, vol. 35, no. 2, pp.376-394, 2009.
[62] Wang X, Design Principles and Issues of Rights Expression Languages for Digital Rights Management, 2005. (available at www.contentguard.com/drmwhitepapers/Design_principles_and_issues_of_REL_for_DRM.pdf)
[63] García R, Gil R, “Content Value Chains Modeling using a Copyright Ontology”, Information Systems, vol. 35, no. 4, pp.483-495, 2010.
[64] García R, Gil R, “Copyright Licenses Reasoning an OWL-DL Ontology”, Law, Ontologies and the Semantic Web, no. 188, pp.145-162, 2009.
[65] Rafi M, Eleuldj M, Guennoun Z, “Improvement of MPEG-21 Right Expression Language”, In Proceedings of 2009 IEEE/ACS International Conference on Computer Systems and Applications, pp.997-1004, 2009.
[66] Tsai DR, Chen WY, Liang CH, et al, “Role-Based Access Control of Digital Right Management” In Proceedings of 2009 Fifth International Joint Conference on INC, IMS and IDC, pp.1131-1134, 2009.
[67] Caelli WJ, “Modernising MAC: New Forms for Mandatory Access Control in an Era of DRM”, In Proceedings of 2007 IFIP International Federation for Information Processing, pp.433-442, 2007.
[68] Jamkhedkar P, Heileman G, Ortiz I, “The Problem with Rights Expression Languages”, In Proceedings of 2006 6th ACM Workshop on Digital Rights Management, pp.59-67, 2006.
[69] Jamkhedkar P, Heileman G, “DRM as a Layered System”, In Proceedings of 2004 4th ACM Workshop on Digital Rights Management, pp.11-21, 2004.
[70] Diehl E, “A Four-Layer Model for Security of Digital Rights Management”, In Proceedings of 2004 4th ACM Workshop on Digital Rights Management, pp.19-27, 2008.
[71] Zhang ZK, Geng YP, Xiao JG, et al, "Cardinality Constraint Access Control Model and Implementation", Advances in Information Sciences and Service Sciences, vol. 3, no. 1, pp.10-18, 2011.
[72] Cai Z, Liu MF, Guo XG, et al, "An Improved IBE Authorization Protocol on Grid Computing System", International Journal of Advancements in Computing Technology, vol. 3, no. 1, pp. 53-57, 2011.
[73] Lee TY, Lee HM, Chen WY, Chen HS, "Processing Logical Access Control Command in Computer System", International Journal of Digital Content Technology and its Applications, vol. 2, no. 2, pp.11-15, 2008.
[74] Arnab A, Hutchison A, “Persistent Access Control: A Formal Model for DRM”, In Proceedings of 7th ACM Workshop on Digital Rights Management, pp.41-53, 2007.
[75] Park J, Sandhu R, “The $UCON_{ABC}$ Usage Control Model”, ACM Transactions on Information and System Security, no. 1, pp.128-174, 2004.
[76] Nair SK, Tanenbaum AS, Gheorghe G, et al, “Enforcing DRM Policies Across Applications”, In Proceedings of 2006 6th ACM Workshop on Digital Rights Management, pp.87-94, 2008.
[77] Muhlbauer A, Reihaneh SN, Salim F, et al, “Location constraints in digital rights management”, Computer Communications, vol. 31, no. 6, pp.1173-1180, 2008.
[78] Abbadi IM, Alawneh M, “Replay Attack of Dynamic Rights within an Authorised Domain”, In Proceedings of 3rd International Conference on Emerging Security Information, Systems and Technologies, pp.148-154, 2009.
[79] Jamkhedkar PA, Heileman GL, Lamb CC, “An interoperable usage management framework”, In Proceedings of the 10th Annual ACM Workshop on Digital Rights Management, pp.73-87, 2010.
[80] Wu MY, Chen YW, Ke CK, “Design and implementation of a context and role-based access control model for digital content”, In Proceedings of IET International Conference on Frontier Computing - Theory, Technologies and Applications, pp.253-257, 2010.

[81] Huang CC, Lo CC, "Threshold based group-oriented nominative proxy signature scheme for digital rights management", In Proceedings of the Sixth International Workshop on Digital Rights Management Impact on Consumer Communications, pp.1-5, 2010.
[82] Morin, Jean-Henry, Towards socially-responsible management of personal information in social networks,Lecture Notes in Computer Science, vol.6045, pp.108-115, 2010.
[83] Salim F, Sheppard NP, Reihaneh SN, "A rights management approach to securing data distribution in coalitions", In Proceedings of 4th International Conference on Network and System Security, pp.560-567, 2010.
[84] DRM Rights Expression Language Candidate Version 2.1, Open Mobile Alliance, 2007. (available at http://www.openmobilealliance.org/)
[85] Zhang ZY, Yang L, Pei QQ, et al, "Research on Usage Control Model with Delegation Characteristics Based on OM-AM Methodology", In Proceedings of IFIP International Conference on Network and Parallel Computing, pp.238-243, 2007.
[86] Zhang ZY, Pei QQ, Ma JF, et al, "A Fine-grained Digital Rights Transfer Policy and Trusted Distribution and Enforcement", In Proceedings of International Conference on Computational Intelligence and Security, pp. 457-462, 2008.
[87] Hibbert C, A copy protection and content management system from The DVB, The DVB Consortium, 2005. (available at http://www.dvb.org/documents/newsletters/DVB SCENE-05-Copy ProtectionArticle.pdf)
[88] DRM Architecture Candidate Version 2.1, Open Mobile Alliance, 2007. (available at http://www.openmobilealliance.org/)
[89] Kim H, Lee Y, Chung B, et al, "Digital Rights Management with Right Delegation for Home Networks", In Proceedings of the 9th International Conference on Information Security and Cryptology, pp.233-245, 2006.
[90] Lee J, Jeong Y, Yoon K, et al, "DRM Applied Contents Share in Digital Home", In Proceedings of 13th IEEE International Symposium on Consumer Electronics, pp.64-66, 2009.
[91] Koster P, Kamperman F, Lenoir P, et al, "Identity-Based DRM: Personal Entertainment Domain", In Proceedings of 9th IFIP International Conference on Communications and Multimedia Security, pp.42-54, 2005.
[92] Popescu BC, Crispo B, Kampermanf F, et al, "A DRM Security Architecture for Home Networks", In Proceedings of 4th ACM Workshop on Digital Rights Management, pp.1-10, 2004.
[93] Koster P, Montaner J, Koraichi N, et al, "Introduction of the domain issuer in OMA DRM", In Proceedings of 4th Annual IEEE Consumer Communications and Networking Conference, pp.940-944, 2007.
[94] Barhoush M, Atwood JW, "Requirements for enforcing digital rights management in multicast content distribution", Telecommunication Systems, no. 45, pp.3-20, 2010.
[95] Sans T, Cuppens F, Nora CB, "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.
[96] Lee S, Kim J, Hong SJ, "Redistributing Time-based Rights between Consumer Devices for Content Sharing in DRM System", International Journal of Information Security, vol. 8, no. 4, pp.263-273, 2009.
[97] Feng X, Tang Z, Yu YY, "An Efficient Contents Sharing Method for DRM", In Proceedings of 2009 Consumer Communications and Networking Conference, pp.1-5, 2009.
[98] Gallery E, Mitchell CJ, "Trusted Mobile Platforms", In Proceedings of 2007 International Conference on Foundations of Security Analysis and Design, pp.282-323, 2007.
[99] Gallery E, Authorisation Issues for Mobile Code in Mobile Systems. Royal Holloway, University of London, United Kingdom, 2007.
[100] TCG Specification Architecture Overview Revision 1.4, Trusted Computing Group, 2007. (available at https://www.trustedcomputinggroup.org)
[101] TCG Design, Implementation, and Usage Principles, Trusted Computing Group, 2009. (available at https://www.trustedcomputinggroup.org)
[102] Trusted Mobile Platform-Hardware Architecture Description, Software Architecture Description, Protocol Specification Document, NTT DoCoMo, IBM, Intel Corporation, 2007. (available at http://xml.coverpages.org/)
[103] TCG MPWG Mobile Trusted Module Specification V1.0, Trusted Computing Group, 2008. (available at https://www.trustedcomputinggroup.org)
[104] TCG MPWG Mobile Reference Architecture, Trusted Computing Group, 2008. (available at https://www.trustedcomputinggroup.org)
[105] Application Security Framework, Open Mobile Terminal Platform, 2007. (available at http://www.omtp.org/pdf/archived_papers/OMTP_Application_Security_Framework v2.0.pdf)
[106] Mobile Phone Work Group Selected Use Case Analysis Specification Version 1.0, Trusted Computing Group, 2009. (available at https://www.trustedcomputinggroup.org)

[107] Reid JF, Caelli WJ, "DRM, Trusted Computing and Operating System Architecture", In Proceedings of 2005 Australasian Information Security Workshop, pp.127-136, 2005.
[108] Kuhn U, Kursawe K, Lucks S, "Secure Data Management in Trusted Computing", In Proceedings of the 7th International Workshop on Cryptographic Hardware and Embedded Systems, pp. 324-338, 2005.
[109] Yu AM, Feng DG, Liu R, "TBDRM: A TPM-Based Secure DRM Architecture", In Proceedings of 2009 International Conference on Computational Science and Engineering, pp.671-677, 2009.
[110] Sadeghi A, Stuble C, "Property-based Attestation for Computing Platforms: Caring about properties, not mechanisms", In Proceedings of the 2004 New Security Paradigms Workshop, pp.67-77, 2004.
[111] Chen L, Landfermann R, Lohr H, "A Protocol for Property-Based Attestation", In Proceedings of the First ACM Workshop on Scalable Trusted Computing, pp.7-16, 2006.
[112] Haldar V, Semantic Remote Attestation, University of California, USA, 2006.
[113] Zhang ZY, Pei QQ, Ma JF, et al, "Implementing Trustworthy Dissemination of Digital Contents by Using a Third Party Attestation Proxy-Enabling Remote Attestation Model", In Proceedings of 2008 International Conference on MultiMedia and Information Technology, pp.322-325, 2008.
[114] Lian SG, Zhang Y, Handbook of research on secure multimedia distribution, IGI Global, USA, 2009.

Biography

Zhiyong Zhang, earned his Master, PhD. degrees in computer science from Dalian University of Technology and Xidian University, China, respectively. He is currently an associate professor at Henan University of Science & Technology, China, and a post-doctoral fellow of Xi'an Jiaotong University, China. His research interests include Digital Rights Management and soft computing for security, trusted computing and access control. Recent years, he has published over 40 scientific papers in the above mentioned fields.

Dr. Zhang is Technical Committee Member for IEEE Systems, Man, Cybermetics Society TC on Soft Computing, Technical Committee Member for Chinese Association for Artificial Intelligence TC on Intelligent Digital Contents Security, Member of Digital Rights Management Specialists Work Group Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee, IEEE Member (2006) and ACM Professional (2008). Besides, he is an Guest Editor of International Journal of Digital Content Technology and Its Applications, Chair/Co-Chair for IAS 2009 Invited Session on Digital Rights Management, CIS 2009 Workshop on Digital Rights Management & Contents Protection, HPCS 2010 Special Session on Trusted Ubiquitous Networks & Multimedia Contents Protection, ICGEC 2010 Invited Session on Security and Trust in Ubiquitous Networks, MINES 2010 Special Session on Security, Privacy and Copyright in Multimedia Social Network, HPCS 2011 Special Session on Digital Home Networks & Multimedia Contents Protection, ICGEC 2011 Invited Session on Digital Rights Management, as well as TPC Member for numerous international conferences.