Security and Trust in Digital Rights Management: A Survey

Zhiyong Zhang[1,2], Qingqi Pei[1], Jianfeng Ma[1], and Lin Yang[3]
(Corresponding author: Zhiyong Zhang)

Ministry Of Education Key Laboratory of Computer Network and Information Security, Xidian University[1]
Taibai South Road No.2, Xi'an, Shannxi 710071, China (Email: xidianzzy@126.com)
Electronic Information Engineering College, Henan University of Science & Technology[2]
Xiyuan Road No.48, Luoyang, Henan 471003, China
The Research Institute, China Electronic Equipment & Systems Engineering Corporation[3]
Dacheng Road 13, Beijing 100141, China
(Received Aug. 22, 2008; revised and accepted Dec. 4, 2008 & Feb. 19, 2009)

Abstract

A successful transaction of digital contents is primarily dependent on security policies, trust relationships and benefit equilibriums among various participants in a DRM (Digital Rights Management)-enabling contents value chain ecosystem. We first analyzed basic value chain architectures in existence, together with some fundamental security and trust requirements. And then, a state-of-the-art anatomy of the security and trust related to DRM was presented from different stakeholder' perspectives. Next, some challenges for multi-party mutual trust, not just inclined to any of participants, were proposed based on the holistic consideration of the digital contents/rights protection and the benefits balance. Finally, a conclusion was drawn that the rights-benefits-centric DRM ecosystem and the resulting trust relationship are crucial for the survivability of the contents industry.

Keywords: Digital content industry, digital rights management, security, trust

1 Introduction

With the rapid developments of communication network technologies, the Next-Generation Internet, 3G and 4G wireless mobile network have been striding to a large-scale deployment and application. As a result, by using multiple network admission methods, users could access to digital resources and services in anytime, at anywhere, which is much easier than ever before. Under this circumstance, the copyright infringement, such as a free distribution, unauthorized usage, illicit sharing of copyrighted digital contents, will be a common phenomenon, as the contents like electric book, image, music, movie and application software are very easily duplicated without the deterioration in quality. Thus, the digital contents industry could be heavily damaged, and its value chain may also be interrupted. The issue of the copyrighted contents protection and legitimate usage is, therefore, crucial.

In order to solve the problem mentioned above, Digital Rights Management (abbr. DRM) has emerged at the beginning of the 1990s. DRM itself is an umbrella term involved both in the business realization of contents industry field and in the researches on multiple scientific disciplines, for instance, information technology, economics and law [62]. Besides, recently Mobile DRM 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 application. 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-protected digital products, which will interrupt the contents chain value. It is stated 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 flourish in [1]. 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 the establishment of the multi-

party trust relationship.

The main contributions of the paper are to give a systematic and state-of-the-art progress of DRM-related security policies, models, architectures and mechanisms respectively from main parties' points of view, and then to propose the advances and challenges for DRM trust issue. The remainder of this paper is organized as follows: Section 2 makes an analysis of several representative architectures of contents value chains and presents the particular relations among multi-party. The investigations of DRM security and trust lie mainly in the following two sections. Finally, some challenges for the trust issue and conclusive remarks are presented in Sections 5 and 6, respectively.

2 DRM Ecosystem and Contents Value Chain

2.1 Basic Architecture

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 the integrity validation of terminal devices.

In addition, some functional components/entities are also playing indispensable roles in DRM ecosystem. For example, Clearing House, which is responsible for the license processing, financial and event managements, together with DIMS (Distribution Information Management System) that supports a contract mechanism and maintains a program for interoperability, were both introduced in Lee's proposed distribution model [39]. As such components mentioned above are not the active participant participating in the revenues and profits allotment in the value chain, they are often seen as logic components or entities. A multi-party DRM ecosystem was presented for solving the interoperability obstacle for DRM wider acceptability and adoption [72]. The ecosystem refers merely to four entities: Creator, Distributor, User and Authority, which are the essential elements of a simple and practical business model of DRM value chain. The task of Distributor is to receive the contents that Creators produces, and then distribute them via appropriate channels such as Websites or physical media; Authority is responsible for issuing contents license based on usage rules provided by Creators, aiming at supervising the legitimate access to copyrighted contents.

In recent years, the need for the mobile industry to manage the usage of digital contents in a controlled manner has been dramatically growing, Mobile DRM being a consequence of that. As a leading industry forum and research organization, Open Mobile Alliance (abbr. OMA) has been concentrating on DRM-enabled mobile services, and presenting a series of DRM related specifications according to basic requirements of the market and consumers. Nowadays DRM Specs of Candidate Version 2.1 has already been published in Jul. 2007, which contains the openness, industry-wide interoperability and utility [48]. In the DRM Architecture Spec, it is stated that a large number of possible actors in a DRM ecosystem/value chain are in existence, such as content owners, developers and distributors, network service operators and manufacturers of terminal equipment, etc. However, as to the functional architecture, these participants are further simplified as a few logical functional entities like CI (Content Issuer), RI (Rights Issuer), and DRM Agent that is a key component located in the user terminal equipment and also called DRM Controller. From the perspective of the value chain, the OMA DRM should primarily consist of three major actors, which are the content provider, rights provider and user, respectively. It is conformable to the functionality of separate and non-synchronously delivery of contents and its corresponding usage license. Gallery [21] introduced three new entities - device manufacturer, DRM Agent installer and CMLA (Content Management Licensing Administrator) whose functionality is identical to CA's - on the basis of the OMA DRM architecture. However, these entities should not be considered as active parties because they do not have direct interest relations to other participants in the value chain. If mobile operators and telecom companies were taken into account, Mobile DRM value chain would be more complicated than the traditional contents supply chain [19]. Note that mobile operators could also play the same role as Rights Issuer in a practical business model.

Therefore, for the generic consideration simplicity, we focus mainly on four participants without losing generality, which have their own security policies and trust relationships. Here, Contents Provider (abbr. CP) that could include contents creators/owner, issuers and intermediary distributors that implement the functionality of OMA Contents Issuer; Rights Provider (abbr. RP) denotes a participant distributing digital rights and may be a copyrights owner, service provider or network operator of Mobile DRM; Device Provider (abbr. DP) provides digital device including consumer electronics for end users in DRM ecosystem; User obviously denotes a set of subscribers/consumers of digital contents, and purchased contents could be restrictedly shared among consumers through superdistribution mechanisms, as is shown in Figure 1.

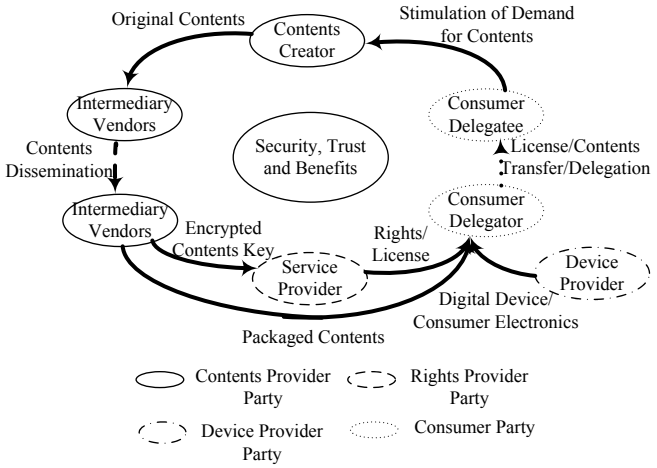

Figure 1: A general DRM value chain ecosystem

2.2 Fundamental Security and Trust Considerations

Nowadays the survivability of DRM value chain is chiefly dependent on security policies and trust mechanisms. The former is used to protect secure distribution of contents and its license, as well as the authorized usage and superdistribution, besides, the requirements of users' privacy protection and contents security are also met by security mechanisms; the latter is to provide a trust relation among the participants, ensuring that contents are used by a controlled manner in a trust terminal environment. Some basic security considerations and trust relationships are listed as follows:

2.2.1 Fundamental Security Requirements

Efforts have focused principally on contents/rights-centric security policies and enhanced mechanisms, since DRM technology has emerged. Recent attempts to improve users' privacy protection and contents security show that consumer-centered security considerations have been receiving more attentions. To sum up, a robust DRM system should meet the following security requirements:

1) Digital contents should be encrypted based on the cryptograph technology, and then consumers acquire encrypted contents by means of the Pull or Push mode. Note that the cipher key to encrypted contents and licenses are separately distributed by RP.

2) Much more DRM applications are requiring a fine-grained contents usage control and the rights definition, expression as well as interpretation. As a result, an interoperable, well-defined rights expression language is indispensable. By means of the language, the permission specified in contents usage license could be granularly defined in term of RP's security requirements, so that effectively restricts user's operations on purchased contents. Furthermore, the license could also be transferred in order to share a portion of contents/rights with other devices/users in an authorization domain, such as home network domain, and even a wider area.

3) The secure distribution, transmission and transfer of the contents and of their licenses are similar, and both are protected by means of such security mechanisms as cipher method. Besides, the execution of the license needs a close or trust environment, which includes trusted DRM Agent, trusted key storage, trusted I/O, and so forth.

4) Concerning a general DRM or Mobile DRM, CP and RP commonly provide digital contents and their usage licenses, respectively, but in some application scenarios or business models, there is an exception in which the functions of CP and SP are together accomplished by a unified participant. In consideration of the general value chain, a secure mechanism of the content cryptographic key transportation should be implemented between CP and RP.

5) For copyrights protection and pirate prosecution, CP generally needs to embed a section of imperceptible data into contents by using the watermarking technology, whereas the embed data is authenticated only by special equipments or approaches. Watermarking could have been adopted to authenticate information of the copyrights owners or original purchaser, further to prosecute malicious pirate behaviors, thus resolving the issue copyrights entanglement.

6) CP/RP-centric security policies to date focus on the secure dissemination, usage and monitoring of digital contents, so that users' information are to some extent being exposed to RP/CP. So users' privacy protection is a basic requirement from the viewpoint of user-centric security. Moreover, contents security also has a positive effect on dependability and survivability of the open devices environment. If the purchased contents contained a section of malicious codes, users' sensitive data and the terminal platform are much easier subject to attack and corrupt.

2.2.2 Essential Trust Relations

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 [13]. In DRM ecosystem, it is greatly difficult to distinguish the honest users with the dishonest users [40]. 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:

1) CP should trust the purchasers not to access any portion of the encrypted contents without acquiring the

decryption key in a certain license; the users also need to trust contents security and integrity.

2) 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.

3) 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.

Lacking of these above essential trusts, the contents value chain would not be survivable, meanwhile the DRM system would not be robust either. Furthermore, the multi-party trust relationships could not be achieved only by means of some enhanced security policies. On the contrary, both the gradual intensification of unilateral security and the neglect of user utility and acceptability would have a greatly negative effect on the value chain, consequently leading to an interruption or corruption of the value chain. The reason is that consumers do not accept DRM-protected contents with much higher costs and little usability than ever before, as is similar to the present status that DRM and anti-DRM fall into a drastic dispute. Bechtold [5] stated that, in the future, the explorations of value-centered technologies would become a focus.

3 Security Policies and Relevant Mechanisms

3.1 Contents Provider-Centric Security Policies and Mechanisms

In the DRM value chain, CP's goal is to protect digital contents security, so security policies available are commonly categorized into tow sorts: preventive and reactive one. The both differently denote the protection of contents in an entire life cycle by the encrypting and packaging beforehand [15, 77], as well as contents usage tracking and copyrights infringement authentication based on the watermark and biological features [35].

3.1.1 Cryptographic Techniques and Security Mechanisms

In decades, cipher techniques that include the cryptographic algorithm design and analysis, key management as well as the application of cipher-based secure protocols have increasingly developed on the basis of the classical Shamon Information Theory and Cryptographic Theory. In the process of the contents packaging and key dissemination, a choice of cipher algorithm would bring some impacts on overheads of the computing and storage, as well as on key security.

As digital contents are generally distributed through some public and mistrusted channels to receivers in such scenarios as DRM-enabling IPTV, Internet or mobile Audio/Video broadcast, recently DRM-related cipher researches have mainly been focusing on an improvement on performances of broadcast encryption schemas suitable for much wider applications. Broadcast encryption, which was introduced in 1993 by Fiat and Naor, is to protect digital contents from the illicit usage of non-authorized users including revoked purchasers, and to ensure that only the authorized consumer could access to encrypted contents in combination with the acquired contents key. Nam-Su Jho [32] proposed a Tree-based Circle broadcast encryption scheme, called TC scheme for short, which enjoys advantages of SD (Subset Difference) tree structure and PI (Punctured Interval) circular structure. Both SD and the improved LSD (Layered Subset Difference) have the small user-key size and little transmission overhead which is lower when the number r of revoked users changes very small; on the contrary, PI has better transmission overhead, when r is not too small. Compared with the other schemes mentioned above, the transmission overhead of TC is proportional to r like that of SD for small r, whereas it asymptotically becomes the same as that of the PI scheme when r grows.

The above schemes are all based on the symmetric-key broadcast encryption scheme, and there exist some disadvantages. Only a trusted designer of the system can broadcast contents to consumers, because encrypting contents requires the knowledge of sensitive information, whose disclosure would compromise the security of the entire scheme.

Nelly Fazio [17] systematically presented research on DRM-enabling cipher techniques for an improvement upon existing DRM cryptographic primitives, with a goal to widen their applicability in DRM scenario and to strengthen security guarantees, such as forward-security and chosen-ciphertext security. Based on the above analysis, an efficient forward-secure public-key broadcast encryption scheme for stateless receivers was represented. The approach enabled mutually mistrusting CPs to share a common broadcast channel in which contents were securely disseminated to their purchasers, in order to minimize the overhead associated with the maintenance of the broadcasting infrastructure. Meanwhile, each user only needs to store one piece of the secret information, so as to reduce the storage requirement of the end customers' devices.

Regarding contents superdistribution, which is an important mechanism used for legitimately sharing purchased digital products among devices/users. Oriented by the encrypted layered contents sharing, a JPEG2000 code streams superdistirbution system, which is based on the commutative Pohlig-Hellman exponentiation cipher, was presented in [8]. The proposed approach mainly included two sub-procedures, the first being the generation of secure package $M = \{L_0, L_1, \cdots, L_i\}$ at the CP back-end sever, where L_i denotes a quality layer that is enhanced in

the image quality when i grows. $M_i = \{L_0|L_1|L_2|\cdots|L_i\}$ denotes a new transcoded image, where "|" is a concatenation operator. It is obvious that the quality of M_i is higher with the increase of i. Then, if a consumer is intended to access M_i, he would execute a key acquisition protocol to acquire the corresponding key from a key server, which may belong to the RP side. The key acquisition protocol can ensure that the key server only have a knowledge that the consumer has requested a code stream of a certain particular quality, but does not know which concrete code stream the consumer has ever requested. In this way, the design objective to protect consumer's privacy is attained.

Presently, the sharing of digital contents is in general implemented among devices in an authorized domain, but most of the existing approaches are revealing the physical structure of the user domain, as directly resulting in an issue of a privacy disclosure [54]. For this, a home network oriented DRM system, which is by using the ID-based public key system and group signature protocol, was proposed to enable the access control of contents and the protection of the domain structure by the anonymity characteristic of the group signature. Thanks to the use of the ID-based public key, a number of public key certificate exchanges, public key directory storages and communications with the requirement of an online Trusted Third Party have been avoided.

3.1.2 Digital Watermarking and Copyright Infringement Tracing

Cryptograph-based copyrights protection is not consummate. Under certain circumstances, for example, an analogue environment, an attacker could record the signals of decrypted contents in the process of the contents rendering. Moreover, the emergence of more complicated attack approaches and tools also easily circumvents or disables cipher protections mechanisms sometimes [75]. To prosecute the illicit usage and copyrights infringement, digital watermarking is a reactive approach to authenticate the ownership of copyrighted contents and provide forensic proofs through the detection/decoding of the pre-embedded imperceptible watermark. A basic model for a general watermarking process is illustrated by Figure 2(a) in [73].

Generally, the following essential characteristics should be achieved for an effective and applicable watermarking scheme:

1) **Robustness** is a crucial feature. A useful digital watermark approach should be capable of resisting a wide scope of attack modes including signal processing attack and cryptographic attack, as well as of withstanding degradation of the host signal.

2) **Security** must rely only upon the secrecy of the watermark keys in term of the Kerkhoffs' principle of the cryptographic theory, whereas an attacker could know all the details of the embedding and detection algorithms.

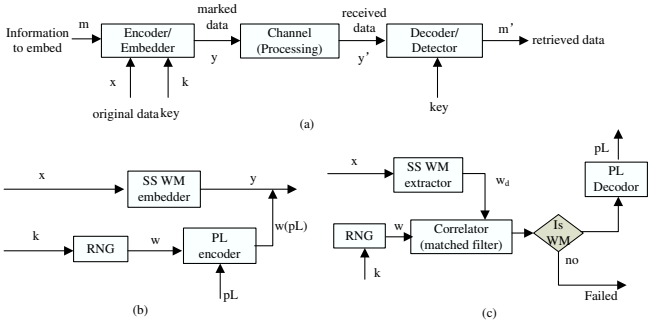

Figure 2: Generic watermarking model and spread spectrum watermarking embedder/detector

3) **Transparency** denotes that the embedded watermark does not influence the quality or the usability of the host signal, while the watermarked signal and original host signal are not distinguishable for any user including a hostile attacker.

4) **Capacity** is contrary to the robustness of watermarking. More robust approaches may lead to more overheads of the transmission channel capacity within the host signal, and vice versa. Thus, a tradeoff between the capacity and robustness should be considered according to an application scenario.

Recently, Steinebach [65] has proposed a novel requirement for DRM utility, which is a very fast embedding strategy, otherwise users would face unacceptable delays before they can download their marked contents. For this purpose, three effective strategies to support fast watermark embedding, such as container watermarking, client-server watermark and grid watermark, were analyzed and compared in detail.

Of various watermarking schemes in existence, Spread Spectrum (abbr. SS) is one of the most successful ones, and widely applied to DRM system. SS is a watermarking process that represents an embedded message by means of a set of pseudorandom codewords [12]. Michiel et al. [73] introduced the general principles of SS-based watermarking embedder and detector illustrated in Figure 2(b)-(c), and then, presented a pirate tracing application. As a category of Blind Embedding Watermark, Hafiz [41] proposed an approach to blind watermark detection/decoding for SS by using of Independent Component Analysis theory.

Note that much attempt to investigate on relevant techniques for the design of the watermarking embedding/detection has achieved the above basic features, which shows the potential utility of the watermark for DRM. However, the doubts about the applicability of the digital watermarking to the ownership problem have

also emerged along with the advances of fruitful researches. Sencar [64] specified several requirements for a watermarking-based ownership assertion system, which include the robustness, low false-positives, non-invertibility and involvement of a trusted party, as well as gave forth to a practical functional architecture reducing the false positive rate of the watermark detection scheme.

Similar to the digital watermarking in DRM, the cipher-based traitor tracking technology is applied to the DRM value chain in order to track the copyrights infringement and protect digital contents. Here traitor denotes a malicious attacker who is engaged in piracy, and he/she is detected by identifying several key segments of the contents and incorporating those in a number of different variations in contents [33]. For the sake of several key problems as the transmission rate and storage rates in traitor tracing, a public-key scheme with the optimal low transmission rate, that is to say asymptotically 1, which could implement efficient black-box traitor tracing and local public traceability, was also presented in [17]. In addition, some biometric-based techniques, such as human iris and fingerprint, have also been adopted to authenticate consumers' identities for the multimedia contents security [16].

3.2 Rights Provider-Centric Security Policies and Mechanisms

3.2.1 Digital Rights Expression and Persistent Usage Control

In DRM value chain, other than CP-centered preventive and reactive policies for the copyrights protection, there also exist RP-centric digital rights expressions and enforcements. 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 [4]. Existing representative RELs, for instance, XrML [14], ODRL [49] and MPEG-21 REL [29], have gradually progressed and been precisely specified in recent years. However, Jamkhedkar et al. [31] 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, a framework for extensible DRM services by means of a simplified core REL was proposed

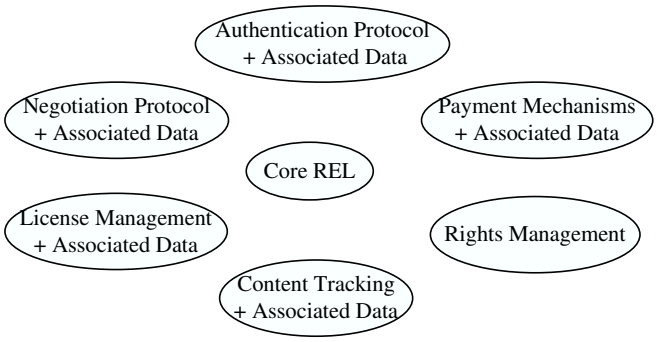

Figure 3: DRM extensible service architecture with an underlying simplified core REL

based on the hierarchy DRM architecture [30]. Figure 3 illustrates the separation mode of core REL and associated data with rights management, which is accomplished by the upper application-level transactional interaction.

The above architecture has two advantages, one being that it improved the capabilities of rights management by newly developed protocols without a modification of the core REL, the other being that it only needs to support a simplified core at a rendering device of consumers and lays complicated management functionalities, such as then authentication, payment and license management, at the back-end server side.

As is discussed above, the additional semantics of RELs have been introduced through increasing new XML tags, which constitute a primitive and underlying language that has such properties as flexibility, machine-understandability, human-readability, and expressivity. An unambiguous semantics is needed to ensure that REL-based rights specifications of copyrighted contents are non-conflicting. Thereby, some efforts are focusing on formal REL specifications. For instance, formal foundation for XrML and ODRL presented in [23, 24, 58], respectively; MPEG-21 REL ISO Standard with formal depictions was published in the realm of multimedia contents industry [29].

Also, Wang [74] made a comparison between RELs available and access control models, and proposed a series of fundamental design principles including the syntactic and semantic un-ambiguity, as well as the business models-supported expressiveness. In term of these rules, the formal method is helpful for an expression of digital rights.

As the logic is a simple and effective foundation on which far more expressive rights management can be built, the REL formalism and reasoning for digital rights have mainly been developed on the basis of logic approaches. A logic L^{lic}, is a precise and rigorous language proving properties of licenses and specifying consumers'

actions that are permitted or obligatory under some given conditions [59].

A set of *Acts*, similar to a set of permitted operations, was defined in L^{lic}, where each element denotes an action of an access to resource via terminal devices. Besides, there are a novel notion *run*, which is a function of temporal characteristic, and the associated time t with a three tuple *(names, l, act)*.

$$r : \aleph \mapsto \wp(Names \times Lic) \times Act(Names). \quad (1)$$

Where *Names* is a set of License names, *Lic* is a set of the license *l*, *Act (Names)* is a function from *Names* to *Act*, and $\aleph$ is a nonnegative integer denoting a discrete time value. Furthermore, a permission P is formally interpreted as Equation (2), that is to say, a permitted and executable action with respect to a named license at a given time.

$$P : \aleph \mapsto \wp(Act \times Names) \quad (2)$$

Further, several complicated temporal logic properties, such as the finite run and license, were formalized. Moreover, the satisfiability and verification of L^{lic} were presented to ensure the validity of the formula interpretation in the logic language. However, it did not cope with the administrative issue of digital rights. Owing to the simple and flexible foundation of the logic, the administrative rights would be easily built.

Chong et al. [7] represented some important disadvantages of XML-based RELs, such as the complicated and obscure syntax, the lack of formal semantics, and so on, and then made an analysis of key components and their relations in REL. A novel formal REL, called LicenseScript, was given based on Multiset Rewriting and Pure Prolog programming. LicenseScript is a license-centric logical expression, and able to capture the dynamic evolution, as well as the static terms and conditions of the license, consequently providing a concise and explicit formal semantics as follows.

A *license* is a term of the form $lic(content, \Delta, B)$, where *content* has an unique identifier representing the data the license refers to,Δ denotes a Prolog program and B is a set of bindings containing elements of the form $name \equiv value$, in which both *name* and *value* are ground terms.

According to the basic definition, provided that a consumer would be granted a permission of Play a until a given expiration date, this semantics could be formalized as the following simple license:

$$lic(a, \Delta, \{expires \equiv months/date/year\}), \quad (3)$$

where Δ consists of such a single clause as

$$Canplay(B, B) : -today(D), getvalue(B, \exp ires, Exp), Exp > D. \quad (4)$$

Also, both a rewrite rule and LicenseScript execution model were defined, and some aspects of technical, business and legal application were precisely formalized by the proposed logical language.

In addition, recent researches on digital rights expression and enforcement show that rights usage could be considered as a persistent access control, which is different from traditional access control policies and models, such as DAC, MAC and RABC. From this point of view, a formal REL presenting the persistent control without a boundary of control is required for DRM applications. Arnab et al. [3] proposed a LiREL (Liceseing REL), in which the contract and agreement between CP/RP and the purchaser was emphasized, mainly formalized the multi-party constraint, obligation and agreement in DRM value chain, and defined access control rules and related rights delegation policy.

A contract and DRM license of LiREL were formalized as Equations (5) and (6), respectively:

$$C = (a, b, \pi, \alpha) \quad (5)$$

$$L = (a, b, \pi, \gamma, \alpha, \kappa)||DSig_{\lambda}, \quad (6)$$

where C is a contract between a licensor a and licensee b; π, α, γ and κ respectively denotes a third party in a contents transaction, a contractual agreement, digital contents resource and constraints of contract C; $DSig_{\lambda}$ is a digital signature signed by a representative of a licensor λ.

Formally, the licensor, licensee and the third party were formally defined as the actors having a combination of constraint κ and obligation $\circ$ as Equations (7)-(12), and the agreement α represents a combination of a permission ρ, together with κ and $\circ$, as is shown in Equation (13):

$$a = \{\kappa_1 \circ_1, \kappa_2 \circ_2, ...\kappa_n \circ_n\}, a \neq \emptyset, n > 0 \quad (7)$$

$$k \in a \Rightarrow \exists l \in \gamma, k \in \text{authorised licensors of } (l) \quad (8)$$

$$\forall l \in \gamma, \exists k \in a, k \in \text{authorised licensors of } (l) \quad (9)$$

$$b = \{\kappa_1 \circ_1, \kappa_2 \circ_2, ...\kappa_n \circ_n\}, n \geq 0 \quad (10)$$

$$k \in b \Rightarrow \forall l \in \gamma, k \text{ get access to } l, \text{ under conditions } \alpha \quad (11)$$

$$\pi = \{\kappa_1 \circ_1, \kappa_2 \circ_2, ...\kappa_n \circ_n\}, n \geq 0 \quad (12)$$

$$\alpha = \{\rho_1 \kappa_1 \circ_1, \rho_2 \kappa_2 \circ_2, ...\rho_n \kappa_n \circ_n\}, n > 0 \quad (13)$$

$$\delta = (b', c, \pi', \gamma', \alpha', \kappa') \text{ where} \gamma' \subseteq \gamma, b' \subseteq b, c \not\subset b, c \not\subset a. \quad (14)$$

Delegation δ is a particular kind of ρ, and defined as a license L' between a delegator b' and delegatee c, as Equation (14), where π', α andκ' are different from π, α and κ of the license L between the delegator and original licensor, and do not need to be a subset of the corresponding set in L. However, the definition means that there may be non-monotone decreasing permissions and constraints, thus leading to the non-controllability of digital rights in a DRM system.

Last but not least, a Usage Control basic framework, which integrated Authorization-oBligation-Condition and was also called $UCON_{ABC}$, has already been proposed by Park and Sandhu at their earlier research on next-generation access control architecture [53]. The framework has an important characteristic of the persistent

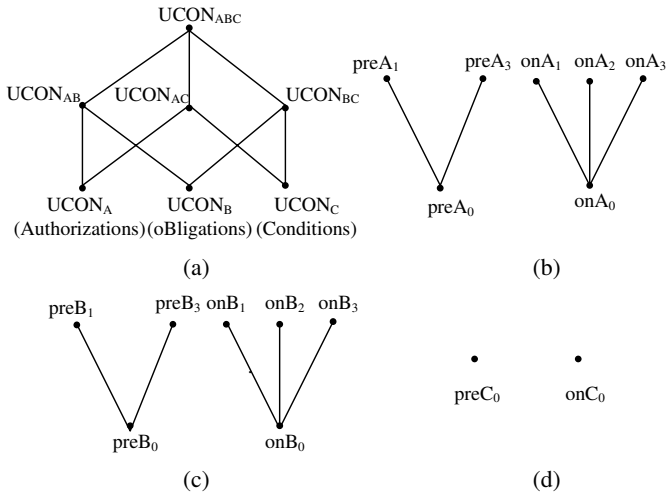

Figure 4: $UCON_{ABC}$ core models family

access control suitable for the DRM application, except a policy-neutral control with essential changeability and continuity, which also differs from conventional access controls. First, $UCON_{ABC}$'s changeability embodies the change of the usage contexts including entities' attributes, temporal and dimensional conditions. Second, these changes make it necessary for the usage decision and attributes update to occur at any time of the whole usage procedure, rather than only at the beginning of usage, as is an embodiment of the continuity. Figure 4(a) showed 4 combinations of $UCON_{ABC}$ models about the Auhthorization, oBligation and Condition, and Figure 4(b)-(d) illustrated 16 possible basic $UCON_{ABC}$ models, where a notation of '0' denotes the case that all attributes are immutable, and one of '1', '2', and '3' presented the updates of some mutable attributes may happen before (pre), during (ongoing), or after (post) the rights is exercised, respectively.

The Comparisons between common RELs and classical models in several aspects like the 'Not' permission property, constraint characteristic, copyrights implementation, formalization were shown in Table 1, where such symbols as " $\bigcirc$"" $\times$ " and " $-$ " depict the covering, lacking and not referring to corresponding characteristics or functionalities, respectively.

3.2.2 Rights Transfer and Contents Sharing

A legitimate share of digital rights relative to purchased contents is necessary for a complete DRM ecosystem and the extension of the value chain. To realize this, the first step is to present or extend a REL with rights transfer/delegation functionality. To date, OMA has not formalized syntaxes and semantics of rights transfer in REL Spec yet [50], which makes it impossible to implement the contents sharing, as well as to depict preconditions and constraints of the rights transfer in a DRM system adopting OMA DRM Specs. Though other RELs like ODRL and XrML, presented some transferable permissions of digital right, such as Sell, Lend, Give of ODRL [58], Delegation of XrML [24], these specifications are coarse-grained, consequently a fine-grained one is required in DRM business models. Due to the lack of the delegation characteristic in $UCON_{ABC}$, we [82] proposed a formal UCON model with the delegation capability, called $UCON_D$, which is an extension of UCON with two important intrinsic properties remaining. Considering the flexibility and precise syntax of BNF, and its being more applicable to a framework specification than the Set Theory and the First-Order Logic, the proposed complementary framework was formalized by means of the BNF Extension. The delegation framework could realize the rights transfer and contents sharing in a DRM system.

The second step is to consider realization mechanisms of rights transferring. RP generally distributes the usage license to purchaser by the binding of contents-permission-device (or user), thus it rigorously restricts the flexibility of the contents usage. Digital Video Broadcasting Project is an industry-led consortium, which was first to propose the concept "Authorized Domain" for sharing contents at different rendering devices [27]. Subsequently, OMA DRM Specs have adopted the concept, and realized the uniform domain management of RI, including the device's joining and leaving domain, registering and RO (Rights Object) acquisition from RI [48]. The approach could guarantee contents sharing within a domain that is composed of multiple devices, but RI becomes the bottleneck of the DRM system; and then, the shortcoming was improved through introducing a domain manager in the later version. Nowadays, contents sharing scenarios focus mainly on Home Network Domain [34] and Personal Entertainment Domain [36]. A secure domain architecture and secure protocols for DRM were proposed, which, however, did not supported the RO transferring and contents sharing [57]; Kim et al. [34] improved on this architecture for a home domain, and the Local Domain Manager he proposed substituted RI to accomplish the license distribution for domain membership devices, meanwhile the Delegated RO and Proxy Certificate have realized the function of rights delegation. This improved architecture is merely limited to the home domain, and it is worthwhile to consider how contents sharing by the rights transfer/delegation would be achieved in far wider domain. As far as a case that consumer could purchase contents from different providers and share them on different devices is concerned, the introduction to Domain Issuer in OMA DRM, instead of multiple Right Issuers, could better manage a sharing domain [37]. In combination with the remote attestation in the trusted computing, we implemented the trusted distributions and enforcement of a fine-grained digital rights transfer policy [80]. The new scheme is more advantageous than other relevant approaches in existence, as it did not restrict within the local domain environment, and accomplished the fine-grained rights transfer and contents sharing be-

Table 1: Comparisons of representative RELs and usage control model

Usage Control of Digital Rights	Specified REL				Formalized REL/Model		
	XrML	ODRL	OMA REL	MPEG-21 REL	LicenseScript	LiREL	$UCON_{ABC}$
'Not' Permission	−	◯	−	−	−	×	×
Constraint and obligation	◯	◯	×	×	◯	◯	◯
Copyright Implementation	×	×	×	−	◯	×	−
Rights Administration	×	×	×	×	◯	−	◯
Formalization	◯	◯	−	Set Notation	Multiset Rewriting + Prolog	Set Notation	Set Notation +Predicate
Transferability	◯	◯	×	◯	◯	◯	×

tween users without direct participation of Rights Issuer and Local Domain Manager.

3.2.3 Trusted Terminal Environment for DRM

Recent years have witnessed the application research on trusted computing technology in the realm of DRM, which refers to the trustworthily dissemination of the granted license presenting usage rules, the secure storage of contents and corresponding encryption keys, and the trusted execution of DRM Controller on the basis of several key techniques, such as the remote attestation, seal approach and integrated trusted platform. Being a basic software platform supporting the trusted execution of DRM Controller, the existing commodity OS could not effectively realize remote attestation and seal technique [60], and the mainstream OS of the open platform and their access control mechanisms could also not protect direct I/O of decrypted contents and the trusted enforcement of the license [38], so it is required to create a virtual technology-based isolation execution environment and to implement a trusted reference monitor with a MAC feature.

Cooper et al. [11] was the first to analyze taxonomy of trusted computing-enabling DRM solutions in existence, and they were primarily classified into four categories: the classic approach to protecting contents within a mainstream OS, the isolation approach to safeguarding data within a protected OS separated form the mainstream OS, the component-based approach to implementing a smaller security-sensitive component within the protected OS, and the MAC-enabling approach to realizing MAC policy between two kinds of OS. Then, a novel trusted computing-based DRM architecture was represented through introducing a security manager, which includes DRM services and the MAC service, and DRM-enabled virtual machine where the user applications run. The architecture enables users to select their own OS, without reducing security function.

Gallery [21] made a survey of the trusted computing 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. A TCG-based mobile platform architecture and required TPM instructions were pointed out in detail, and then from the perspectives of the terminal protection and the mobile code security, the remote-attestation-based mobile platform verification and the contents protection were discussed, respectively [20]. Besides, Zheng et al. have also provided a conceptual trusted mobile platform [83].

To accomplish the trusted measurement and the DRM application security, we [78] proposed a Xen-virtualization-based terminal platform architecture, as is shown in Figure 5,where several fundamental data streams among the key components were involved in that the access to platform hardware and system functions, integrity measurement and security evaluation, as well as trusted measurement merits storage, etc. The established virtualization environment based on the trusted kernel could implement the domain isolation execution and processes protections in a lesser trusted boundary, thus better satisfying the trustworthiness of AO (Attested Object), which is customarily a Guest OS kernel or host's upper applications, by the integrity measurement and report mechanisms provided by a series of TSS (Trusted Software Stack) function calls. The architecture integrated the bottom trusted hardware platform welded by a trusted chip, called TPM (Trusted Platform Module), with Xen-Hypervisor located in the upper layer. According to the Ring Architecture of X86, Hyperivsor runs in Ring 0, whereas Supervisor OS Kernel that provides functions of trusted OS kernel runs in Ring 1. Other upper Guest OS Kernels could access to virtual devices by means of the hardware devices virtualization that is provided by Hypervisor and Domain 0, where the Xen controller, named as Xend, is responsible for establishing, destroy-

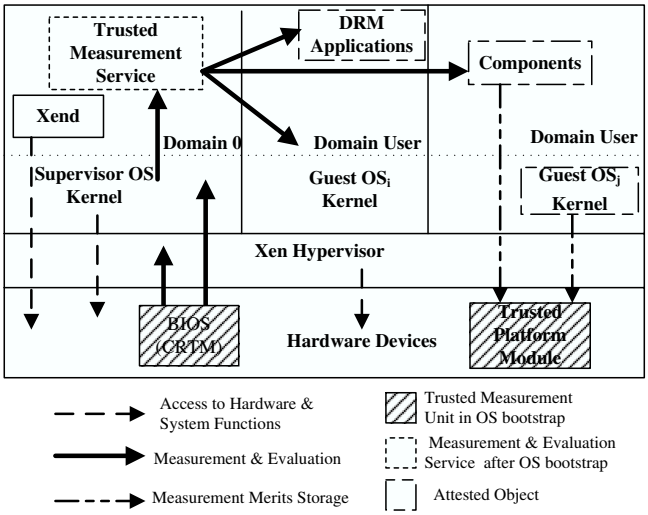

Figure 5: A Xen virtualization-based trusted platform architecture

ing and migrating a domain. Domain User where multiple applications run could implement the isolation execution of different components for security. TMS (Trusted Measurement Service) running in Domain 0 adopts the modified secure Linux kernel, and is in charge of measuring the AO's integrity after the platform bootstrap, whereas CRTM in BIOS is with responsibility for the integrity measurement from the startup of Hypervisor to the load of Supervisor OS Kernel and TMS. Note that,in this architecture, TMS and AO could be protected via the enhanced isolation approach. If AO was tampered, the integrity and trustworthiness of TMS would be still satisfied.

A trusted terminal platform provided by the device manufacturer is crucial for a general DRM system or Mobile DRM. Nowadays, in addition to trusted PC platform specified by TCG [66, 67], OpenTC in Europe and Chinese Trusted Computing Union, there exist a series of Specs about TMP (Trusted Mobile Platform). NTT DoCoMo, IBM and Intel were the first to publish TMP Specs that mainly depict the hardware, software and protocols, respectively [44, 45, 46]. TCG Mobile Phone Work Group (abbr. MPWG) [68] specified the instruction set and the data structure of the trusted module applicable to the mobile terminal in Mobile Trusted Module Spec [69] and Trusted Mobile Reference Architecture Spec [70]. Furthermore, a domain-isolation-based application engine was defined for the trusted mobile device, thus enhancing the security of the engine execution and access to data. The Open Mobile Terminal Platform (OMTP, for short) forum is also a famous organization dedicated to Mobile DRM and the application security framework. Some major requirements for OMA DRM V2.0-enabler terminal were proposed as a guide of the trusted mobile platform [51]. These industry specifications listed above are advantageous to realize the trusted environment of Mobile DRM, but TCG MPWG explicitly showed that they would not design DRM-related schemes [71].

3.2.4 Negotiation Mechanism between Contents Provider and Rights Provider

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. [84] 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 in [2]. 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 modelled 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.

3.3 Privacy and Security Considerations from Consumer's Perspective

3.3.1 Consumer Privacy Protection

With the deployment and application of DRM products, some user-centric issues, such as consumers privacy protection and private /fair usage rights, have become a focus from the technical and juristic viewpoints [76, 28, 42]. INDICARE (Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe), which is a Europe Union-funded project ended in Feb. 2006, was engaged in consumer issues related to DRM. Its objective is to raise consumer awareness and balance heterogeneous interests of multiple parties in the value chain. In this project,

Helberger et al. [25] made an investigation on consumers privacy protections and its effect on the DRM acceptability. Generally speaking, the privacy disclosure exists in two stages, one being the stage of the contents purchasing, in which consumer's unique identifier is submitted to CP for accomplishing the identity authentication, and the other being the usage procedure where user's detailed behaviors are tracked by the log approach. Note that both may lead to a potential control over consumer, and even yield a challenge for DRM acceptability.

A protection method of such the sensitive data and privacy as user identifier was represented based on a classical security principle called SOD (Separation-Of-Duty) [22]. In the scheme, SOD denotes the separation of purchased data from user names by means of a pseudonymous ID. CP could only know purchased contents without knowing the real identity of the consumer, whereas CA, an official entity independent from CP, understand user's name by the identity authentication, but no purchased data. A lightweight DRM system adopted this idea to implement the privacy protection in the process of the contents sharing.

In addition, in an authorized domain, the membership and structure information could be guaranteed from disclosing through the anonymous license transferring and the introduction of Domain Manager, and security is enhanced by using the identity-based cryptographic approach [10]. For a malicious consumer to illegally break the local software and transfer the decrypted key K_c to others, Chong et al. [8] explored a privacy-enhancing architecture based on the trusted hardware platform and TVMM (Trusted Virtual Machine Monitor). In the application layer, a contents rendering program was executed on top of a close-box virtual machine run above a protected-OS, and the platform remote attestation safeguarded K_c from the software tampering of pirates for the purpose of the illegal copy and free distribution to others. Also, an assessment report on familiar DRM products and services was presented in [18]. In the report, privacy assessments have been disclosed whether IT merchants/organizations are in compliance with Personal Information Protection and Electronic Documents Act that belongs to a part of the privacy legislation in Canada. As an essential principle of DRM acceptability for consumers, the privacy protection could be implemented by above listed schemes, but how to make a tradeoff between the privacy and necessary information used for authenticating purchasers' identities, tracking and controlling the piracy should acquire much more considerations, after all, the latter is original motivation of DRM techniques.

3.3.2 Mobile Application Security

Contents security is directly affecting the trustworthiness of DRM-protected digital products. As a category of digital contents, the application software, especially for the mobile application as a Java game, is faced with a mass of complicated and hostile attack. And, a mobile application embedded by malicious codes would tamper with the terminal security. For example, it may attempt to gain the privilege of the access to customers' personal data, harm users and even network operators, and so forth. A mobile application security framework for open OS platforms was proposed in [56], and the idea of the classified trust was employed to verify the trust level of a mobile application. Subsequently, in term of the result of the trust assessment, for example Untrusted level, Trusted one that is identified by the third party and Higher Trusted one that is identified by the operator, some access rights of the application could be permitted or prohibited, thus enabling the mobile terminal free from the malicious application. Santos [63] has proposed a generic and operator-oriented DRM framework supporting multiple approaches to implement the security of a J2ME application. The issues of the authorization and access control of Mobile codes, together with a robust OMA DRM for the mobile application were presented in [20].

Nowadays the content security mainly focuses on the Java application, and approaches available also are closely relative to the language-based security and the trusted Java Virtual Machine. There is a little of researches on the security and trust of other content types or formats, besides the quality evaluation of the digital contents or services. Much more efforts to cope with the issue should be required to improve DRM-enabling contents utility, and to stimulate end consumers' purchasing power.

4 Trust Model and Mechanisms for DRM

4.1 PKI-Based OMA DRM Trust Model

As a representative industry alliance engaging in DRM, OMA has ever proposed a trust model in DRM Architecture [48] and DRM Specification [52]. PKI being its basis, this model attempted to build a trust relationship between RI and DRM Agent run in the user device. If the Agent was verified to be a trusted component by using a non-revoked certificate that was issued by the TTP (Trusted Third Party) as CA, RI would trust the behaviors of the Agent. In other words, an Agent produced by a certain trusted manufacturer has the trustworthiness of the license enforcement. Similar to this case, DRM Agent could also trust a RI through the certificate-based authentication. Obviously, OMA DRM trust model mainly refers to trust relations between logical functional entities. However, this mutual trust is not sufficient for the general open terminal platforms and complicated network environment, because the certificate issued by CA could only ensure that the identity and origin of an entity is genuine without being able to guarantee the run-time behavioral trustworthiness, as it is a static trust.

Content Management License Administrator (abbr. CMLA), which is a Limited Liability Company sponsored by four distinguished IT companies, including In-

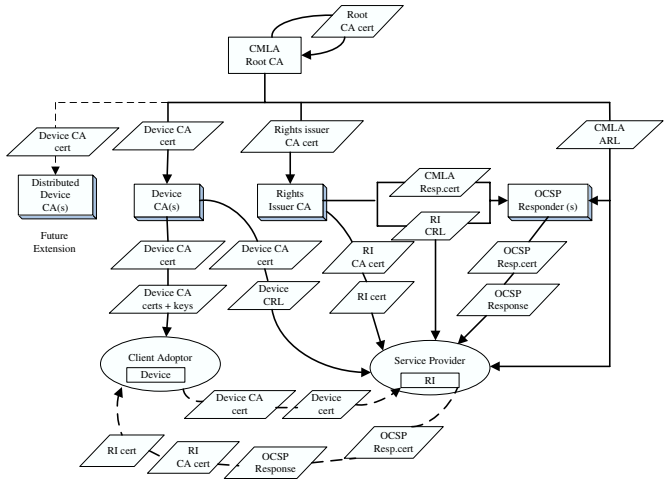

Figure 6: CMLA hierarchy PKI system

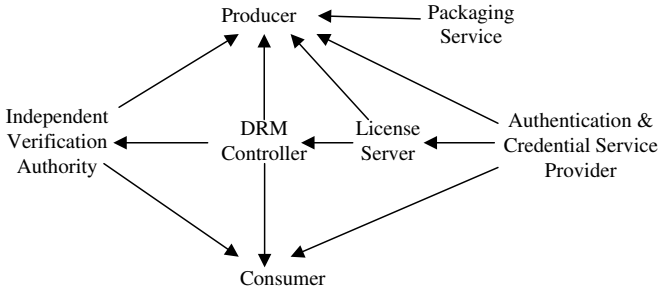

Figure 7: Web of trust among basic components and entities for DRM

tel, Nokia, MEI/Panasonic and Samsung, has made an active effort to realize the trust model for OMA DRM V2.0. As a holistic objective of CMLA is to enable a wide and trusted distribution of DRM contents in a large digital ecosystem, it plays a role of the PKI creator and administrator, and proposes a hierarchy PKI system in order to build the trust, as is illustrated in Figure 6 [9]. The proposed PKI system is composed of some basic entities, such as Root CA, Device CA(s), RI CA and OCSP (Online Certificate Status Protocol) Responder, which is a key entity to provide the verification of the certificate validity in Internet X.509 PKI, as well as a series of certificate objects issued by various CAs. Meanwhile, CMLA represented some fundamental requirements of a robust DRM realization, and Certifications Principles for Service Provider and Client Adopter (device). These principles are used to justify whether consumers' devices including DRM Agent, applications and services, are well implemented or not, that is to say meeting CMLA Compliance and Robustness Rules. Note that CMLA does not replace or modify OMA DRM Specs, nor is it a prerequisite or requirement for the OMA DRM architecture. So there may be other trust models except CMLA in the DRM ecosystem. Though no doubt that CMLA supported and extended the trust model of OMA, both have the same disadvantages that the run-time trustworthiness of entities could not be guaranteed, and that they do not provide verification mechanisms and realization approaches to improving multi-party trust in the DRM ecosystem. Moreover, the overhead of establishing PKI also must be taken into account.

4.2 Web of Trust in DRM Ecosystem

Arnab [2] presented a standpoint that the trust in a DRM system is determined by how much confidence the Producer and Consumer have in the implementations of DRM components and services. However, the trust relationship would be easy to break along with an increase of entities that need to be trusted, and the traditional trust chain is linear and not completely suitable for depicting the trust relations among DRM components. For this, a conceptual web architecture of the trust for DRM was proposed, as is shown in Figure 7, where an arrow from entity A to B means that A is trusted by B. Also, a key distribution scheme, including the contents decryption key and the license key, was designed based on the trust web.

The entities were categorized into three sorts in the trust web. The first sort is a set of several active entities such as Contents Producer and Consumer in the DRM value chain; the second one is a set of basic components/services indispensable to a DRM system, such as DRM Controller, License Server and Packaging Service; the last one includes Independent Verification Authority that is trusted by Producer and Consumer to verify the trustworthiness of DRM Controller, and Authentication and Credentials Service Producer which mainly implement access control functions and authentication mechanisms. And, both could be recognized as an active entity or a service affiliated to any active party like CMLA. In the web of trust, RP was not explicitly shown, but License Server should belong to an implicit RP similar to RI. Besides, there is only the conceptual multi-party trust architecture, and its trust was established on the basis of the secure key dissemination and storage, lacking a more practical trust mechanism other than the OMA trust model.

4.3 Trusted-Computing-Based Trust Mechanisms

As previously discussed in Sub-Section 3.2.3, a trusted computing environment is an important feature of the user device rendering digital contents. Furthermore, a DRM Controller verified by TTP in such a trusted platform strengthens trust relationship between CP/RP and Consumer. Ntzel et al. [43, 47] stated that OMA DRM V2.0 was the first step to increase the trustworthiness of DRM, but existing PC platforms lack the essential secu-

rity, and consequently such key as the device private key that is the security anchor of a DRM system will not be secure to be installed and stored. An obfuscation technique-based software approach to protecting the device private key was proposed in combination with Trusted Computing. The approach could be used on the untrustworthy platform like Windows, and the trusted computing provides a trust root for DRM to improve the security and trust of the usage license enforcement. Last but not least, the mutual trust between DRM Provider and Consumer was also discussed. On the one hand, Provider should trust user not to misuse contents and ensure license/RO to be trustworthily executed by DRM Controller. On the other hand, users need to trust Provider to legally handle their confidential data or privacy.

As an interesting topic, how to manage and protect the event notification in a trusted system was discussed in [61], with a goal to enable the contents/rights providers and distributor to know the usage status of multimedia contents through establishing the trusted event reporting mechanisms for DRM. These approaches have already introduced into MPEG-21 Specification.

5 Challenges for Multi-Party Trust in DRM

A successful digital transaction generally depends on three key factors: security, trust and benefit [55]. 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. A DRM trust infrastructure is involved with the techniques and managerial processes that enable the system components trustworthy [1]. Also, with regard to a DRM ecosystem, the trust relationship further embodies various participants' mutual trust. As an open issue in DRM, and even digital world, the trust is facing with challenges as follows:

1) In a DRM ecosystem, a multi-party mutual trust is necessary for the survivability of the entire value chain, which at least should includes CP, RP, DP and Consumer. How the involved trust relations are identified to create a contractual agreement or technical for contents business model.

2) Trust for DRM should be comprehensive, which means it should be not only static trust implemented by certification and authentication to key components and entities, but also dynamic trust for components' behaviors and services' security.

3) From different participants' perspectives, existing security policies have been gradually improved and enhanced, strengthening multi-party trust. However, the value chain is broken due to strict usage control and security policies. It should be noted that an underlying trust for DRM value chain should be a balance of multi-party benefit. When the balance is achieved, trust relations among participants would be steady and persistent. Therefore, there is also a challenge for multi-party trust based on security policies and balanced benefit, which means that the trust is benefit balance oriented with legitimate and controlled usage of contents as the basis.

Recently, several attempts to explore benefit balance of DRM have emerged. Heileman et al. [26] made a game-based analysis how to adopt DRM protection technologies or not have effect on benefits for contents vendor and purchaser. A game-theoretic approach to explore digital rights ownership was proposed for optimally balancing benefits between contents industry and individual consumer, not just benefiting the either of both [6]. The Chang's main attempts, from economics and law standpoints, to solve the debate over the DRM ecosystem show that sharing access rights between both parties would be the best outcome for the whole society, and not lean to any of both.

In order to achieve a benefit equilibrium among the participants of contents value chain, we proposed a benefits-centric Multi-Participant Trust Architecture (abbr. MPTA), which is based on game-theoretic rational adoptions of security policies for the parties, and formalized the definitions of the security component and service, the security policy and its utility, as well as the Nash Equilibriums of the multi-participant game under pure and mixed security policy profile [79]. Due to the introduction to Game theory, MPTA enables participants to acquire optimal benefits balance when fundamental security requirements are met, and Nash Equilibrium of the game is the chosen security policies combinations from the participants' perspectives. To our best knowledge, it is the first framework integrating the game theory to discuss the trust issue in DRM ecosystem. Besides, a cooperative game among digital Contents Provider, Rights/Service Provider and digital Devices Provider, as well as a non-cooperative game between Providers and Consumers were analyzed in [81]. In combination with the analyses, a stable core allocation of benefits and Nash Equilibriums were found out, respectively. So, it is clearly concluded that the cooperative game has important super-addivitity and convexity, thus simultaneous adoptions of security policies with external relativity being helpful to achieve Pareto Optimality by using a pre-established cooperative relation; and that Pareto Optimality also exists between Providers and Consumer with the increase of users' purchase transactions when both have a repeated game.

6 Conclusive Remarks and Future Work

DRM is a multi-disciplinary and complicated research topic, and the DRM-enabling contents industry is also a complex value chain involved with various stakehold-

ers and corresponding interests. From the perspective of technology, existing approaches focus on contents protection, secure dissemination and controlled usage, and these mechanisms are indispensable to the DRM ecosystem, but not sufficient. Mutual trust relations among participants would be a crucial and essential factor of ensuring the survivability of DRM-protected contents industry. Moreover, from a novel standpoint of benefits balance, trust relationship is more stable and effective than only adoption of security policy. The paper makes a detailed survey of research progresses of security policy and trust mechanisms on DRM, and proposes several challenges for multi-party trust in DRM value chain ecosystem. In our opinions, trust establishment should be rights-and-benefits-centric and based on optimal usage of security policies.

Our future works aim at establishing an effective multi-party trust relationship based on the game-theoretic analyses and simulations of the adoptions and deployments of typical security policies, such as trusted computing-enabling contents and licenses security. For this purpose, we primarily explore the cost-effective security issues for two scenarios as digital contents acquisition and sharing, looking for corresponding Nash Equilibriums of a holistic payoffs of participants. The original motivations of these researches are to establish benefit-centered trust relationship based on a rational adoption of security policies, and to ensure maximum benefit and minimum cost when necessary and fundamental security policies are adopted.

Acknowledgments

We are very grateful to Professor Yinghua Min, who is a IEEE Fellow from Institute of Computing Technology, Chinese Academy of Sciences, for his valuable suggestions. Also, we would like to show gratitude to anonymous reviewers for their helpful comments and suggestions. The work was supported in part by the General Program of National Natural Science Foundation of China under Grant No. 60803150, the Key Program of National Natural Science Foundation of China under Grant No. 60633020, and China National 111 Program of Introducing Talents of Discipline to Universities Grant No.B08038.

References

[1] H. Abie, "Frontiers of DRM knowledge and technology," *International Journal of Computer Science and Network Security*, vol. 7, no. 1, pp. 216-231, 2007.

[2] A. Arnab, *Towards a General Framework for Digital Rights Management*, University of CAPE TOWN, June 2007.

[3] A. Arnab and A. Hutchison, "Persistent access control: a formal model for DRM," *Proceedings of 2007 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 41-53, Oct. 2007.

[4] C. Barlas, *Digital Rights Expression Languages*, JISC Technology and Standards Watch, July 2006.

[5] S. Bechtold, "The present and future of digital rights management," *Proceedings of the Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution*, pp. 6-7, Dec. 2006

[6] Y. Chang, "Who should own access rights? A game-theoretical approach to striking the optimal balance in the debate over digital rights management," *Artificial Intelligence and Law*, no. 15, pp. 323-356, 2007.

[7] C. Chong, *Experiments in Rights Control Expression and Enforcement*, University of Twente, Enschede, The Netherlands, 2005.

[8] D. Chong and R. Deng, "Privacy-enhanced superdistribution of layered content with trusted access control," *Proceedings of 2006 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 37-43, Oct. 2006.

[9] *Content Management License Administrator Technical Report Revision Ver. 1.2-070326*, CMLA: Client Adopter Agreement, Mar. 2007.

[10] C. Conrado, M. Petkovic, and W. Jonker, "Privacy-preserving digital rights management," *Proceedings of 2004 SIAM International Conference on Data Mining*, LNCS 3178, pp. 83-99, 2004.

[11] A. Cooper and A. Martin, "Towards an open, trusted digital rights management platform," *Proceedings of 2006 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 79-87, Oct. 2006.

[12] L. Coria, P. Nasiopoulos, and R. Ward, "A robust content-dependent algorithm for video watermarking," *Proceedings of 2006 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 97-101, Oct. 2006.

[13] *Digital Trust, vol. 3 - Intellectual Property Protection*, 2007. (http://www.csc.com/aboutus/leadingedge-forum/knowledgelibrary/uploads/LEF_2007Digital-TrustVol3.pdf)

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

[15] K. Fan, W. Mo, S. Cao, X. Zhao, and Q, Pei, "Advances in digital rights management technology and application," *ACTA Electronica Sinica*, vol. 35, no. 6, pp. 1139-1147, 2007.

[16] K. Fan, M. Wang, W. Mo, Z. Wang, Q. Pei, and J. Shen, "An iris biometric-based digital multimedia content protection scheme," *ACTA Electronic Sinica*, vol. 16, no. 2, pp. 271-275, 2007.

[17] N. Fazio, *On Cryptographic Techniques for Digital Rights Management*, New York University, Sep. 2006.

[18] D. Fewer, P. Gauvin, and A. Cameron, *Digital Rights Management Technologies and Consumer Privacy*, Canada Internet Policy and Public Interest Clinic, 2007. (http://www. Cippic.com/drm)

[19] E. Furregoni, A. Rangone, F. Renga, and M. Valsecchi, "The mobile digital contents distribution scenario," *Proceedings of Sixth International Conference on the Management of Mobile Business*, Toronto, Ontario, Canada, pp. 32-40, July 2007.

[20] E. Gallery, *Authorisation Issues for Mobile Code in Mobile Systems*, Royal Holloway, University of London, 2007.

[21] E. Gallery and C. J. Mitchell, "Trusted mobile platforms," *Proceedings of Foundations of Security Analysis and Design*, LNCS 4677, pp. 282-323, 2007.

[22] R. Grimm and P. Aichroth, "Privacy protection for signed media files: A separation-of-duty approach to the lightweight DRM (LWDRM) system," *Proceedings of 2004 Workshop on Multimedia and Security*, Magdeburg, Germany, pp. 93-99, Sep. 2004.

[23] J. Halpern and V. Weissman, "A formal foundation for XrML," *Proceedings of 17th IEEE Workshop on Computer Security Foundations*, pp. 251-263, June 2004.

[24] J. Halpern and V. Weissman, "A formal foundation for XrML," *Journal of the ACM*, vol. 55, no. 1, pp. 4-45, 2008.

[25] N. Helberger, N. Dufft, S. Gompel, K. Kerenyi, B. Krings, and R. Lambers, *Digital Rights Management and Consumer Acceptability*, Dec. 2004. (http://www.indicare.org)

[26] G. Heileman, P. Jamkhedkar, J. Khoury, and C. Hrncir, "The DRM game," *Proceedings of 2007 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 54-62, Oct. 2007.

[27] C. Hibbert, *A Copy Protection and Content Management System from The DVB*, The DVB Consortium, 2008. (http://www.dvb.org/ documents/ newsletters/ DVB-SCENE-05-Copy Protection Article. pdf)

[28] E. Hinkes, "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.

[29] ISO/IEC 21000-5, *Information Technology-Multi Media Framework Part 5: Rights Expression Language*, 2004.

[30] P. Jamkhedkar and G. Heileman, "DRM as a layered system," *Proceedings of 2004 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 11-21, Oct. 2004.

[31] P. Jamkhedkar, G. Heileman, and I. Ortiz, "The problem with rights expression languages," *Proceedings of 2006 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 59-67, Oct. 2006.

[32] N. Jho, E. Yoo, J. Cheon, and M. Kim, "New broadcast encryption scheme using tree-based circle," *Proceedings of 2005 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 37-44, Nov. 2005.

[33] H. Jin, J. Lotspiech, and S. Nusser, "Traitor tracing for prerecorded and recordable media," *Proceedings of 2004 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 83-90, Oct. 2004.

[34] H. KIM, Y. Lee, B. Chung, H. Yoon, J. Lee, and K. Jung, "Digital rights management with right delegation for home networks," *Proceedings of 9th International Conference on Information Security and Cryptology*, LNCS 4296, pp. 233-245, 2004.

[35] P. Koster and W. Jonker, *Digital Rights Management*, 2008. (http://www.springerlink.com/ index/v317858416435v64.pdf)

[36] P. Koster, F. Kamperman, P. Lenoir, and K. Vrielink, "Identity-based DRM: Personal entertainment domain," *Proceeding of Transactions on Data Hiding and Multimedia Security*, LNCS 4300, pp. 104-122, 2006.

[37] P. Koster, J. Montaner, N. Koraichi, and S. Iacob, "Introduction of the domain issuer in OMA DRM," *Proceedings of 2007 4th Annual IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, United States, pp. 940-944, Jan. 2007.

[38] U. Kuhn, K. Kursawe, and S. Lucks, "Secure data management in trusted computing," *Proceedings of 7th International Workshop on Cryptographic Hardware and Embedded Systems*, LNCS 3659, pp. 324-338, 2005.

[39] J. Lee, S. Hwang, S. Jeong, K. Yoon, C. Park and J. Ryou, "A DRM framework for distributing digital contents through the Internet," *ETRI Journal*, vol. 25, no. 6, pp. 423-436, Dec. 2003.

[40] Q. Liu, R. Naini, and N. Sheppard, "Digital rights management for content distribution," *Proceedings of the 2003 Australasian Information Security Workshop*, Adelaide, Australia, pp. 49-58, 2003.

[41] H. Malik, A. Khokhar, and R. Ansari, "Improved watermark detection for spread-spectrum based watermarking using independent component analysis," *Proceedings of 2005 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 102-111, Nov. 2005.

[42] S. Nair, B. Popescu, C. Gamage, B. Crispo, and A. Tanenbaum, "Enabling DRM-preserving digital content redistribution," *Proceedings of the Seventh IEEE International Conference on E-Commerce Technology*, pp. 151-158, July 2005.

[43] J. Ntzel and A. Beyer, "Towards trust in digital rights management systems," *Proceedings of Third International Conference on Trust and Privacy in Digital Business*, LNCS 4083, pp. 162-171, 2006.

[44] NTT DoCoMo, IBM, Intel Corporation, *Trusted Mobile Platform-Hardware Architecture Description*, Oct. 2004.

[45] NTT DoCoMo, IBM, Intel Corporation, *Trusted Mobile Platform-Software Architecture Description*, Oct. 2004.

[46] NTT DoCoMo, IBM, Intel Corporation, *Trusted Mobile Platform-Protocol Specification Document*, Oct. 2004.

[47] J. Ntzel and A. Beyer, "How to increase the security of Digital Rights Management systems without

affecting consumer's security," *Proceedings of International Conf. on Emerging Trends in Information and Communication Security*, LNCS 3995, pp. 368-380, 2006.

[48] Open Mobile Alliance Specification, *DRM Architecture Candidate Ver. 2.1*, July 2007.

[49] *Open Digital Rights Language (ODRL) version 1.1*, 2002. (http://www.w3.org/TR/odrl)

[50] Open Mobile Alliance Specification, *DRM Rights Expression Language Candidate Ver. 2.1*, July 2007.

[51] Open Mobile Terminal Platform Forum Report, *Application Security Framework, Open Mobile Terminal Platform*, Sep. 2007. (http://www.omtp.org/pdf/archived_papers/OMTP_Application_Security_Framework_v2_0.pdf)

[52] Open Mobile Alliance Specification, *DRM Specification Candidate Ver. 2.1*, July 2006.

[53] J. Park and R. Sandhu, "The $UCON_{ABC}$ usage control model," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 128-174, 2004.

[54] Q. Pei, J, Ma and J. Dai, "Digital rights management for home networks using ID-based public key system and group signature," *Chinese Journal of Electronics*, vol. 16, no. 4, pp. 653-669, Oct. 2007.

[55] O. Petrovic, M. Fallenbock, C. Kittl, and T. Wolkinger, "Vertrauen in digitale transaktionen, " *Wirtschafts Informatik*, vol. 45, no. 1, pp. 53-66, 2003.

[56] E. Pisko, K. Rannenberg, and H. Heiko Robnagel, "Trusted computing in mobile platforms," *Datenschutz und Datensicherheit*, vol. 29, no. 9, pp. 526-530, 2005.

[57] B. Popescu, B. Crisop, A. Tanenbaum, and F. Kamperman, "A DRM security architecture for home networks," *Proceedings of 4th ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 1-10, Oct. 2004.

[58] R. Pucella and V. Weissman., "A formal foundation for ODRL," *Workshop on Issues in the Theory of Security*, Barcelona, Spain, Apr. 2004.

[59] R. Pucella and V. Weissman, "A logic for reasoning about digital rights," *Proceedings of 2002 15th IEEE Workshop on Computer Security Foundations*, pp. 282-294, Dec. 2002.

[60] J. Reid and W. Caelli, "DRM, trusted computing and operating system architecture," *Proceedings of 2005 the Australasian Information Security Workshop*, Newcastle, Australia, pp.127-136, 2005.

[61] E. Rodrguez and J. Delgado, "Trust in event reporting mechanisms for DRM," *Proceedings of 2007 4th Annual IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, United States, pp. 1058-1062, Jan. 2007.

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

[63] N. Santos, P. Pereira, and L. Silva, "A generic DRM framework for J2ME applications," *Proceedings of First International Mobile IPR Workshop: Rights Management of Information Products on the Mobile Internet*, Helsinki, Finland, pp. 53-66, Aug. 2003.

[64] H. Sencar and N. Memon, "Watermarking and ownership problem: A revisit," *Proceedings of 2005 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 93-101, Nov. 2005.

[65] M. Steinebach, E. Hauer, and P. Wolf, "Efficient watermarking strategies," *Proceedings of Third International Conference on Automated Production of Cross Media Content for Multi-channel Distribution*, pp. 65-71, Nov. 2007.

[66] Trusted Computing Group Specification, *TCG Specification Architecture Overview Revision 1.3*, Mar. 2007. (https://www.trustedcomputinggroup.org/)

[67] Trusted Computing Group Specification, *TCG PC Specific Implementation Specification*, Aug. 2003. (https://www.trustedcomputinggroup.org/specs/PCClient)

[68] Trusted Computing Group Report, *Mobile Phone Working Group Use Case Scenarios ver. 2.7*, 2005. (https://www.trustedcomputinggroup.org/groups/mobile)

[69] Trusted Computing Group Specification, *TCG Mobile Trusted Module Specification Ver. 1.0*, June 2007. (https://www.trustedcomputinggroup.org/groups/mobile)

[70] Trusted Computing Group Specification, *TCG Mobile Reference Architecture Ver. 1.0*, June 2007. (https://www.trustedcomputinggroup.org/groups/mobile)

[71] Trusted Computing Group Report, *Mobile Trusted Module Specification FAQ*, June 2007. (https://www.trustedcomputinggroup.org/groups/mobile)

[72] B. Vassiliadis, V. Fotopoulos, A. N. Skodras, "Decentralising the digital rights management value chain by means of distributed license catalogues," *Proceeding of 2006 IFIP Artificial Intelligence Applications and Innovations*, vol. 204, pp. 689-696, 2006.

[73] M. Veen, A. Lemma, M. Celik, and S. Katzenbeisser, *Forensic Watermarking in Digital Rights Management*, 2008. (http://www.springerlink.com/index/x587u1278360x52n.pdf)

[74] X. Wang, *Design Principles and Issues of Rights Expression Languages for Digital Rights Management*, 2008. (http://www.contentguard.com/drmwhitepapers/Design_principles_and_issues_of_REL_for_DRM.pdf)

[75] P. Wolf, M. Steinebach, and K. Diener, "Complementing DRM with digital watermarking: Mark, search, retrieve," *Online Information Review*, vol. 31, no. 1 pp. 10-21, 2007.

[76] H. Xie, "Protecting fair use from digital rights management in China," *Proceedings of 2007 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 33-38, Oct. 2007.

[77] Y. Yu and Z. Tang, "A survey of the research on digital rights management," *Chinese Journal of Computers*, vol. 28, no. 12, pp. 1957-1968, 2005.

[78] Z. Zhang, Q. Pei, J. Ma, and L. Yang, "Implementing trustworthy dissemination of digital contents by using a third party attestation proxy-enabling remote attestation model," *Proceedings of 2008 Inter-*

national Conference of Multimedia and Information Technology, Three Gorge, China, Dec. 2008.

[79] Z. Zhang, Q. Pei, J. Ma, and L. Yang, "A benefits-centric multi-participant trust architecture for DRM-enabling digital contents value chain ecosystem," *Proceedings of International Seminar of Business and Information Management*, Wuhan, China, Dec. 2008.

[80] Z. Zhang, Q. Pei, J. Ma, L.Yang, and K. Fan, "A fine-grained digital rights transfer policy and trusted distribution and enforcement," *Proceedings of International Conference of Computational Intelligence and Security*, pp. 457-462, Dec. 2008.

[81] Z. Zhang, Q. Pei, J. Ma, L. Yang, and K. Fan, "Cooperative and non-cooperative game-theoretic analyses of adoptions of security policies for DRM," *Proceedings of 5th IEEE International Workshop on Digital Rights Management Impact on Consumer Communications, Satellite Workshop of 6th IEEE Consumer Communications & Networking Conference*, Las Vegas, Nevada, USA, Jan. 2009.

[82] Z. Zhang, L. Yang, Q. Pei, and J. Ma,"Research on usage control model with delegation characteristics based on OM-AM methodology," *Proceeding s of IFIP International Conference on Network and Parallel Computing & Workshop on Networks System Security*, Dalian, China, pp. 238-243, Sep. 2007.

[83] Y. Zheng, "A conceptual architecture of a trusted mobile environment," *Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, Lyon, France, pp. 75-81, June 2006.

[84] Y. Zheng, D. He, H. Wang, and X. Tang., "Secure DRM scheme for future mobile networks based on trusted mobile platform," *Proceedings of 2005 International Conference on Wireless Communications, Networking and Mobile Computing*, Wuhan, China, pp. 1164-1167, 2005.

Zhiyong Zhang received his BSc, MEng degree in Computer Science from Henan Normal University and Dalian University of Technology, China, in 1998, 2003, respectively. He is now a Ph.D. Candidate in Key Laboratory of Computer Network & Information Security (Chinese Ministry of Education), at Xidian University. He is also an associate professor at Henan University of Science & Technology, Technical Specialist of Digital Rights Management Workshop Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee, Member of IEEE (2006), ACM (2008) and Japan IEICE (2008), and also Senior Member of China Computer Federation (M'04, S'08). His research interests include Digital Rights Management and contents protection, trusted computing and access control. He has published over 25 scientific papers on the above research fields.

Qingqi Pei received his BEng, MEng and Ph.D. degrees in Computer Science and Cryptography from Xidian University, in 1998, 2005 and 2008, respectively. He is now an associate professor and a vice-director of CNIS Laboratory, also a member of ACM and Japan IEICE, and Senior Member of Chinese Institute of Electronics. His research interests focus on digital contents protection and trusted computing.

Jianfeng Ma received his BSc degree in Mathematics from Shannxi Normal Univ. in 1985, and acquired his MEng, PhD degrees in Computer Science and Cryptography from Xidian Univ., in 1988 and 1995, respectively. He was a visiting researcher at Nanyang Technological Univ., Singapore, from 1999 to 2001, and now is a doctorial supervisor at Xidian Univ. and director of CNIS. He is also a member of IEEE, and Senior Member of Chinese Institute of Electronics. His research interests include wireless network security and cryptography.

Lin Yang received the BEng, MEng and PhD degrees from National Univ. of Defense Technology of China in 1993, 1996 and 1998, respectively. He is a researcher in The Research Institute, China Electronic Equipment & Systems Engineering Corporation and doctorial supervisor of Xidian Univ. Currently his research interests include system security and network security.