Digital Rights Management Ecosystem and its Usage Controls: A Survey

Zhiyong Zhang


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]
Digital Rights Management Ecosystem and its Usage Controls: A Survey
Zhiyong Zhang

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](image)

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]](image)

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, UCONABC, 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, UCONABC 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 UCONABC models on Authorization, Obligation, and Condition, and Figure 5(b)–(d) illustrates 16 possible basic UCONABC 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.

![UCONABC core model family](image)

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 $\bigcirc$, $\times$, and - represent the covering, lacking of, and not referring to corresponding characteristics or functionalities.

<table>
<thead>
<tr>
<th>Usage Control of Digital Rights</th>
<th>Representative Specified RELs</th>
<th>Formalized RELs/Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XrML</td>
<td>ODRL</td>
</tr>
<tr>
<td>‘Not’ Permission</td>
<td>-</td>
<td>$\bigcirc$</td>
</tr>
<tr>
<td>Constraint and obligation</td>
<td>$\bigcirc$</td>
<td>$\bigcirc$</td>
</tr>
<tr>
<td>Copyrights</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>Implementation Rights Administration</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>Formalization</td>
<td>$\bigcirc$</td>
<td>$\bigcirc$</td>
</tr>
<tr>
<td>Transferability</td>
<td>$\bigcirc$</td>
<td>$\bigcirc$</td>
</tr>
</tbody>
</table>
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 UCONABC, we [85] proposed a formal usage control model with delegation capability, called UCOND (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. UCOND framework with delegation functionality](image-url)
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.

![Digital Rights Specification](image1.png)

![Transferable Digital Rights Specification](image2.png)

**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 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

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

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.
Digital Rights Management Ecosystem and its Usage Controls: A Survey

Zhiyong Zhang


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 AP²RA (Attestation Proxy Party RA) [113], as shown in Table 3.
<table>
<thead>
<tr>
<th>Key Mechanisms/Performances</th>
<th>TCG-RA [100]</th>
<th>PBRA [110, 111]</th>
<th>SBRA [112]</th>
<th>AP²RA [113]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Measurement Mechanism</td>
<td>integrity of binary codes</td>
<td>security properties of platform</td>
<td>semantic of upper software</td>
<td>integrity of binary codes and security properties</td>
</tr>
<tr>
<td>Trusted Report Mechanism</td>
<td>basic configurations of platform</td>
<td>security properties</td>
<td>checking semantics of SW</td>
<td>capabilities of platform</td>
</tr>
<tr>
<td>Trusted Third Party-Supported Message Confidentiality</td>
<td>×</td>
<td>O</td>
<td>×</td>
<td>O</td>
</tr>
<tr>
<td>Message Integrity</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Message Anti-Deny</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Anti-Attack on APP</td>
<td>-</td>
<td>O</td>
<td>-</td>
<td>O</td>
</tr>
<tr>
<td>Anti-Collusion Attack</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>O</td>
</tr>
<tr>
<td>Anti-Replay Attack</td>
<td>O</td>
<td>O</td>
<td>-</td>
<td>O</td>
</tr>
<tr>
<td>Privacy Protection Overhead</td>
<td>Lower</td>
<td>Medium</td>
<td>-</td>
<td>Higher</td>
</tr>
<tr>
<td>Overhead</td>
<td>Lower</td>
<td>Higher</td>
<td>Medium</td>
<td>Higher</td>
</tr>
</tbody>
</table>

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 AP²RA 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](image-url)
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 AP²RA 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.

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.2011HASTIT035), 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


Digital Rights Management Ecosystem and its Usage Controls: A Survey
Zhiyong Zhang


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, Cybernetics 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.