Mobile Digital Rights Management

Zheng Yan
Nokia Research Center
zheng.z.yan@nokia.com

Abstract

This paper presents a technical overview of current state in Mobile Digital Rights Management (MDRM). Main aspects, such as a DRM system's requirements and architectures are studied. MDRM technologies, such as rights definition languages, cryptography and digital watermarking are discussed. The paper also analyzes the limitations and extra requirements for developing Mobile DRM systems, classifies MDRM based on content types, and proposes MDRM use case models and a MDRM terminal structure. Further more, important issues are discussed regarding the success of MDRM challenge.

1 Introduction

With the rapid growth of the Internet communications, the Internet has become one of the most efficient distribution channels of digital contents for commerce. At present this channel is being extended to mobile area. Certainly, It is ideal to distribute all divers of digital information via networks to consumers' desk-top devices or portable devices. But digital contents, if not protected and managed, can be easily copied, altered, defaced, and distributed to a large number of recipients. Digital Rights Management (DRM), which permits the smooth, secure, trusted movement of digital works from creators and publishers to sellers and consumers, as well as among consumers, is needed for addressing this problem.

In the future, encrypted credit cards, micro-payments, and digital cash will be established in mobile devices. Commerce with digital contents will become a suitable area for both electronic and mobile domains. Mobile DRM (MDRM), the base-bone of future mobile media commerce is the first issue should be addressed. The Mobile DRM is a set of actions, procedures, policies, product properties, and tools that an entity uses to manage its rights in digital contents according to requirements over mobile networks. This paper aims to give an overview of the current state of the MDRM, to analyzes requirements and to discusses technologies, use case models and challenges for developing the MDRM.

2 State of the art

2.1 Basic requirements

The Digital Rights Management concerns techniques, processes, procedures and algorithms related to establishing a trusted computing environment, and trusted infrastructure for the secure preparation, transmission, and prevention of misuse and/or consumption of protected digital contents.

General requirements are proposed in an IETF draft on a Digital Rights Trading System [1]. In this draft, a digital-right is defined as "a digital representation of the right to claim the services or goods". This definition limits digital-rights for claiming services or goods, does not contain usage rights for controlling content's consuming. Therefore, this proposal cannot be applied to a DRM system that ensures content integrity, secures copyright, controls content usage and manages rights acquisition, specification, as well as granting. But it is a good reference for proposing basic requirements of a DRM system.

1. From scalability point of view, "it MUST handle diverse types of rights issued by different issuers".
2. From system security point of view, "it MUST prevent illegal acts" on both rights and contents. For the rights, it MUST prevent them from alternation, forgery, duplicate-redemption, reproduction, and repudiation, and SHOULD ensure privacy. For the contents, it MUST protect their integrity, prevent illegal copy, and make sure the contents are used correctly according to the consumer's rights, as well as provide trust manageability. Because different customer has different preference, privacy may not be a mandatory requirement.
3. From business point of view, "it MUST be practical in terms of scalability, simplicity, implementation / operation cost and efficiency".

2.2 System architecture

Fig. 1 illustrates a lifecycle of digital rights. Typically, there are four stages:

1. Package stage: The operators of this stage are authors or content providers who conduct the following
   - Create rights protection requirements
   - Specify digital rights management policies
   - Specify conditions fee, time, access
   - Specify tracking requirements
2. Sell/protect stage: The handlers of this stage are service providers who do the following works
   - Define pricing

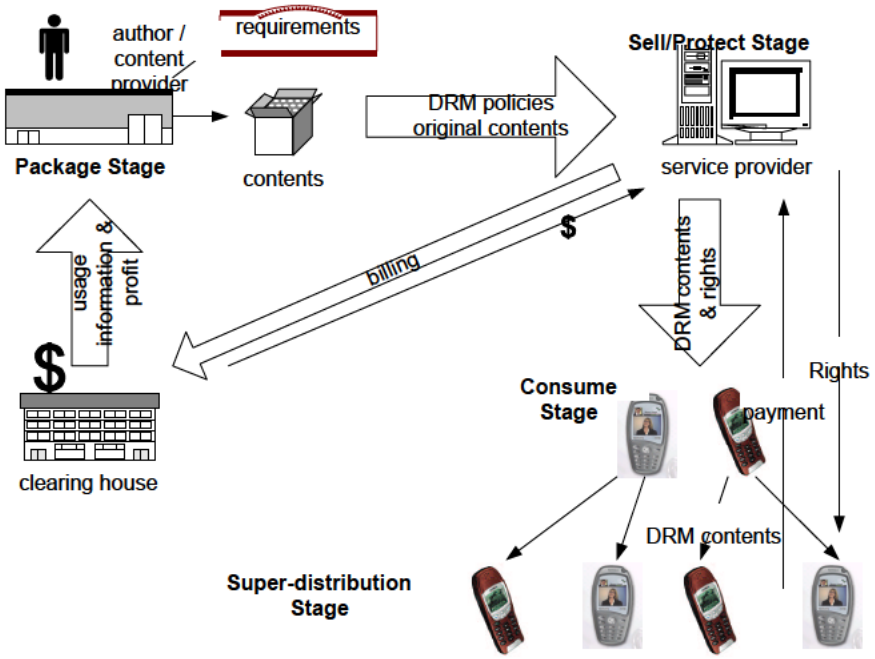

Figure 1: A lifecycle of digital rights

- Define business model
- Specify watermarks
- Package contents with DRM protection
- Distribute contents
- Communicate financial clearinghouse for billing
- Track the usage of contents

3. Consume stage: In this stage, the contents are consumed by a user who determines allowed rights to be purchased. Besides,
   - Contents are customized for that particular user
   - DRM client (e.g. a MDRM device) verifies purchased rights and contents, controls content consuming, rejects illegal activities, and tracks content usage
4. Super-distribution stage: The user can also super-distribute DRM controlled contents to another user who gets additional digital rights from the service provider for consuming protected contents. This activity may continue many times. But no matter how content is distributed, it should be DRM protected.

There are three kinds of system architecture to realize digital rights management: centralized rights management, distributed rights management and semi-distributed rights management.

Centralized rights management:

The rights are managed by a trusted party (a secure server) based on accounts. Any processing of the rights is handled by sending a request to an account manager through a network. Generally, on-line verification is needed in order to prevent duplicated rights redemption. However, this type of system is expensive because accounts have to be maintained for each service provider and for each user. Therefore, it is hard to support system scalability. Additionally, account-based systems have been designed to protect accounts from malicious users but provide less protection from malicious managers. Therefore, the trust policy of these systems is imbalanced. Some Internet coupon systems, such as CoolSavings and ClipACoupon, use this architecture. And this technology is generally used for developing server-based mobile advertisement systems.

Distributed rights management:

There are two approaches to realize it. One is using a tamper-resistant device, like a smart card or a Personal Trusted Device (PTD). In the tamper-resistant device based system, digital rights are stored in a trusted device and circulated among devices. The tamper-resistant device can protect digital-right from both malicious users and malicious service providers. Thus, this kind of system seems to have a bright future especially in the application area of tickets and coupons since one smart card or PTD can store and manage diverse tickets without the cost of maintaining rights centrally. However, these systems create several issues that are hard to overcome, i.e. who should be responsible for issuing a smart card or a PTD if it is shared by multiple applications, how to achieve high performance given the memory and CPU constraints of the small devices. Moreover, the business issue with smart cards or PTDs is that the devices for smart card or PTD verification are not very common especially as user terminals such as PC.

In general, PTD-based solution is suitable for such applications as eTicket, eCoupon, eLicense, etc.

The other approach is using a self-protecting container, which is the key element in InterTrust's commerce platform [11]. The secured container DigiBox enables the association of rules and controls via cryptographic means with information content, to specify the types of content usage permitted and the consequences of usage. Containers are manipulated by using a trusted rights protection application in order to make the protected content available according to its associated access control rules. Payment is generally conducted when a consumer wants to open the container (pay when use, or download first pay later). Similar functionality is provided by IBM's "cryptolope" container [12, 14]. The secure container allows rights management components to be integrated with content in highly flexible and configurable control structures. This approach enables true super-distribution and can support virtually any network topology and any number of participants, including distributors, re-distributors, information retailers, corporate content users, and consumers. But it requires pervasive deployment of tamper-resistant hardware devices to perform secure processing of protected contents. Container technology is playing an increasingly important role as a building block for sophisticated digital rights management system.

Container-based architecture is achieving leadership in the digital content distribution, e.g., eBook, eMusic, eImage, and software, etc.

Semi-distributed rights management:

This architecture tries to combine the advantages of the above two ways and overcome their disadvantages. In [13], a proposed scheme uses a ticket-account server to manage user's rights. The personal rights are not managed by the service provider, but the user himself or someone delegated to manage the account. A smart card is used only for authentication. This approach aims to reduce the account management cost and avoid bottlenecks caused by smart cards. Payment consideration during the rights circulation is ignored in this scheme. Therefore, it is difficult to practice payment for rights transference between users if using this scheme.

3 Technologies

This part introduces technologies for achieving mobile digital rights management.

3.1 DRM languages

A good digital-right representation is necessary in the MDRM system. The representations could be different. There are several candidates available, which are from different sources.

Digital rights expressed by relational database [2]

Jams Barker and his colleagues at Case Wstern Reserve University (CWRU) worked out a database representation, defined as a set of relational database tables and their interpretation. More than 10 basic tables are used to describe the right-properties, together with a large number of administrative, logging and support tables. The advantage of this method is the values in columns of the tables are not restricted by software, but rather by administrators' entries in the support tables. This permits tailoring to any installation's needs together with validity checking of permission table entries. It is convenient to achieve semantics, syntax and security requirements by making use of database technologies. But it is inefficient if table relationships become complicated. And it is only suitable for centralized rights management architecture. Some digital libraries support this digital rights expression.

Xerox's DPRL (Digital Property Rights Language) [3]

Xerox's DPRL (Digital Property Rights Language) is a language that can be used to specify rights for digital contents. It provides a mechanism in which different terms and conditions related to access, fee and time can be specified and enforced for the different operations on digital documents, such as view, print, and copy. Rights specifications are represented as statements in DPRL. Different rights can be specified for different parts of a digital work using a work specification. Within a work specification, different sets of rights applicable to this work are specified. Rights can be grouped into named-groups called "rights groups". Each right within a rights group is associated with a set of conditions. Conditions can be of different types: fee to be paid, time to use, type of access, type of watermark, type of device on which the operation can be performed, and so on. It also allows different categories of rights, such as transfer rights, render rights, derivative-work rights, file-management rights and configuration rights.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.