Present State and Piracy Control Using Interoperable Digital rights Management

Priyanka Gupta

ABSTRACT
This paper focuses on technological solutions, such as Digital rights Management System(DRMS) which enable on one hand rights protection of intellectual property digital content, and on the other hand it should increase security and privacy of Confidential and personal information exchange over semi-open or open networks such as the Internet. The objective of this Digital Rights Management architecture is to provide an efficient means for translation of media across different DRM formats in use. Our aim is to hide DRM's presence and the process of its conversion from the format supported by one device to a format supported by another, thus making DRM interoperable while complying with content fair usage policies.

DEFINITION OF DIGITAL RIGHTS MANAGEMENT
'Digital Rights Management' is not a new concept and has had many names over the past several years. For example, a few large companies and public entities began research into "Electronic Copyright Management" in the early 1990s (Pitk.nen & V.lim.ki2000) such as CITED funded by the European Community. This was leading to "first generation DRMS". The last few years, people first started to use the term "Electronic Rights Management" and later "Digital Rights Management"(DRM).

INTRODUCTION
The evolution of the internet as a content provider can be seen both as an opportunity and a threat for those who create or publish their work. This growth has allowed publishers to monetize their creative work, and target the audiences in new markets that did not exist in the past. However, technologies have also been used against the interest of owners of intellectual property who would like fair use of their content and protection against its piracy.
The first widespread use of Digital Rights Management tools in 2002, was for the prevention of illegal replication of copyrighted audio from compact discs manufactured by BMG, Arista and RCA. DRM has slowly advanced and is now used in combination with many more forms of digital content including software, enterprise networks, television broadcasting, copyrighted video and e-books.
As DRM has grown, its proponents have created different DRM formats resulting in the fragmentation of the technology. This has also caused each format to have limited device playback support. Increasing support for different DRM formats is expensive for device manufacturers to implement. Content distributors choose to support DRM systems supported by popular devices, limiting their ability to address a broader set of devices being used by consumers. Content providers are in turn forced to address a much smaller market because of this DRM format fragmentation.
Using the Domain Interoperability Manager, consumers are unaware about the difference in format compatibility between different devices, and stores used to acquire digital content. Users associate their devices with the DIM so that it may acquire the license certificates, encryption and re-signature algorithms for all devices used in the local network. The focus of is on minimizing the change required by providing a framework for interconversion between DRM systems used in existing devices while preserving the features(quality, security, etc) of the source content.

DESCRIPTION
There are currently many DRM formats in use to prevent digital media and content from being reproduced in ways that violate copyright law. Each device manufacturer supports different DRM formats and embeds an associated decryption module in the devices it manufactures. This over time has resulted in the encapsulation of content in a variety of different formats, each having different proponents in the industry. As each format has a few proponents and no standard DRM format exists, the formats have forced their consumers to choose one manufacturer over another because of the lack of a method that allows purchased content to be played back on all devices. It is thus very tedious for consumers to use purchased media on devices that don't support the DRM scheme used by the store used to acquire the content.
This paper focuses on the creation of a DRM architecture that will help broaden content cross-compatibility to make it available on a large set of devices complying with the architecture. This architecture makes use of a Domain Interoperability Manager(DIM) module that is responsible for interconversion of different DRM formats.

DRM systems are essentially made up of the following subsystems:
Content Service provides the data to be used by the content providers to pull data and content creators to push data(music, movies, e-books, etc.).
Access Services allows the content to be accessed by a specific device whenever required.
License Service issues a certificate to the content in DIM module.
Tracking Service helps the DIM in the identification of circumvented devices.
Payment Service is used for transactions to be performed during the purchase of content.

ISSN: 2278 – 1323

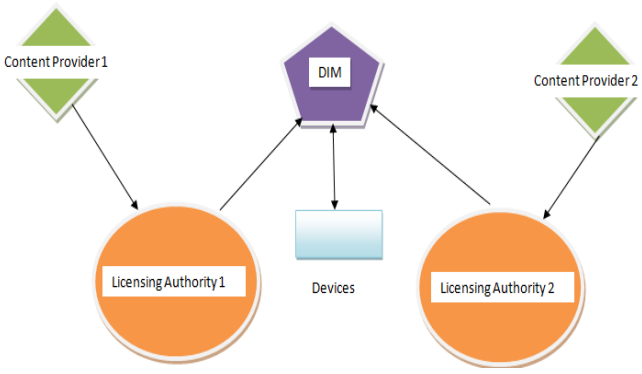
Import Service requests for the conversion of data from source format to required import format following which it transfers the content to the destination.
Identification Service authenticates clients and devices before transferring the purchased media.

The DRM Architecture defines sets of entities in the system that take part in the construction of a DIM structure.

Content Provider - The source of any digital content distributed or made available for sale on the internet. The source may be any organization, company or instituition.
Devices -Any electronic equipment used to access the different media or content purchased or downloaded.
License Authority -An organization that defines the end user license agreement which contains the contract between the licensor and purchaser. The contract establishes the rights and warranties that the buyer must accept to protect digital content. All devices using license-bound content must be compliant with the associated DRM system.
DIM -The Device Interoperable Manager transfers the content of the purchaser in formats understood by compliant devices. For performing interoperability, its the duty of the DIM to guarantee that the content which is transferred is compatible with compliant devices without losing the embedded rights defined by the licensing authority.

WORKING OF THE DOMAIN INTEROPERABILITY MANAGER

The DIM keeps the track of the devices and the content providers. If content is provided in DRM Format A through Provider P_A, the work of the DIM is to transcode and transfer content in a compatible form to all devices it keeps record of. If the device to be transferred to does not support the original DRM format, the DIM is required to convert it to the format supported by the device. The DIM also stores the certificates provided by the licensing organizations to prevent certified devices from breaching the contract.

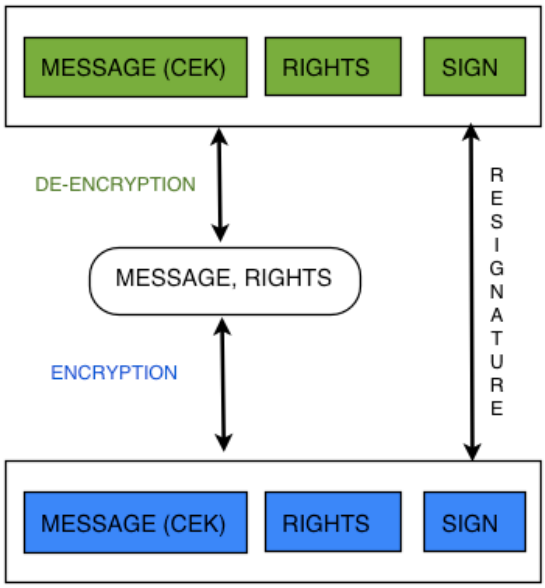


Device D_A using DRM format A will have a certificate stored from the licensing authority which allows the transfer of content of Provider A to it. This process is accomplished after authentication and verification of the compliant device. After this the content is easily transferred through the DIM to device D_A using secure and encrypted channels. At the end of the transaction the device D_A contains the content (MESSAGE) with content encryption key(CEK), license which includes the usage rights, the public key (PKD_A) and the signature of the device(SIGN).
If the same content in DRM format A has to be transferred to a Device D_B, the DIM is responsible for transcoding its message and rights and resigning its signature from format A to B so that it may be played back on Device D_B.
When transfer of content purchased in one format to a device supporting another format, then a secure environment should be established and there should be no change in the message or the rights defined when the change from one DRM format to another DRM format occurs.

ARCHITECTURE PROTOCOL DETAILS

Protocol 1 DIM supporting similar importing and exporting formats

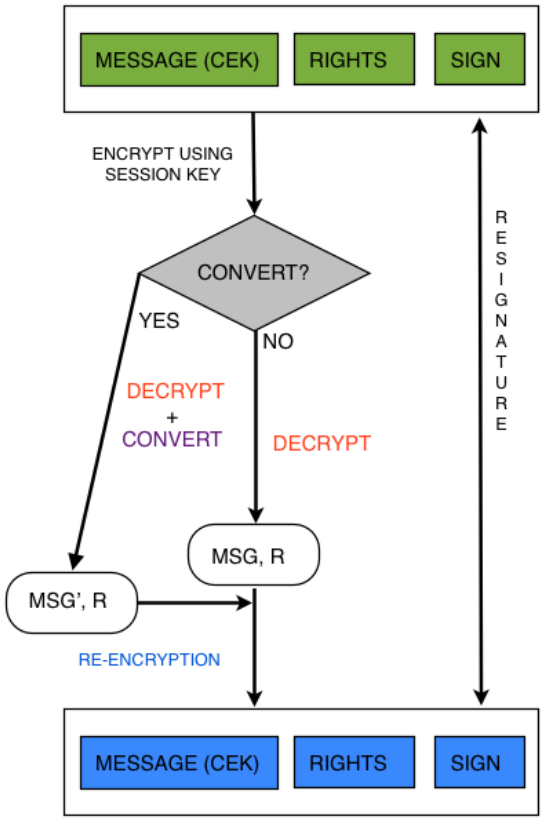
The first protocol proposes a DIM which is not allowed to access unprotected content. This protocol assumes that both the importing and exporting DRM systems contain similar encryption and signature procedure and homogeneous licensing and content formats. The transfer of content is possible only when the DIM translates the license in such a manner that it is encrypted and signed using the public key of the exporting system.
In the figure below, the boxes in green color signify the components of DRM A. The message is encoded with its content encryption key, its rights are defined and the signature of provider A is stored. The work of the DIM is to convert the message given by provider A in a format which could be understood by provider B. This process is made possible by the Re-encryption function. This function first de-encrypts the content using CEK of provider A along with its rights. In the next stage the content and rights are re-encrypted with CEK of provider B.
Similarly, the signature of provider A can be resigned to obtain an appropriate signature of provider B using the proxy re-signature function stored on the DIM. The DIM is allowed to translate signatures from one form to another without knowing its pattern or structure.



Security is maintained through this protocol because re-signature and re-encryption functions do not obtain any private or unprotected information. Thus by encryption

privacy is maintained and integrity of the content and the license is achieved through the signature key.
The re-encryption key has a unique value for each device as it uses a combination of the public key of the DRM format along with the private key of the device being transferred to. This unique key further increases the security of the content being transferred. Thus compromising the DIM alone will not result in a successful attack on the system.
This method is useful as devices used to import content will not require any change in the way it usually handles the DRM specified. However the participating devices will be required to render content in similar formats as this protocol relies on a re-encryption and re-signature process where the DIM is unaware about how to interpret unprotected content.

Protocol 2 DIM supporting different importing and exporting formats



Protocol 2 provides flexibility in the DRM formats being used. The device being exported to might use a content format that may be a lot different from the format used by the content provider used to import the content from. In this case, the DIM also does the job of converting the encrypted message (if required), so that it be exported correctly to the device it is being transferred to. The device transfer takes place without revealing the private keys of either device in the two-way synchronization. As a connection with the DIM on the network is established a session key is generated and used to encrypt messages being transferred to and from any two devices instead of revealing each device's private key. This way the DIM can convert the message and rights without compromising the security of the devices.

In figure 4, the message in DRM format A (in green) is encrypted using the session key and sent across the network to the DIM. The DIM decides whether the message M requires a conversion of the rights expression language and message content into another formats in case the importing device uses a different format. If so, it decrypts the message, converts it to message M' and passes it through the re-encryption function of the target device. If the message doesn't require conversion, the DIM simply passes it unchanged to the re-encryption function which generates a message that can be understood at the destination.
Since the signature binds the content to its rights, we use a similar signature, as shown in protocol 1, to prevent a splicing attack. The signature is simply passed through the re-signature function and goes largely unchanged. Further, the rights and content and content cannot be left unidentified for the same reason. They are matched with their identification signature which is a key generated using each of their identifiers.

DEVICE COMPLIANCY

Before any transaction or transfer can take place, it is necessary to verify that devices that synchronize are built to work with the formats supported by the DIM transcoder. Any updates in the formats being used by new content can be pushed as firmware updates or software updates for devices by manufacturers, so that they can continue to be compliant. Devices in turn must be allowed to sync only if they have the latest software running.
Offline attestation of devices will be periodical as updates will be as old as the last connection the DIM made with the server. During the time it waits before contacting the DIM operator for the next update, vulnerabilities may be exposed and made use of. To avoid this scenario, online attestation can ensure that all devices when synchronized have the latest version of software the DIM operator can push at that time. It will also be necessary to check the firmware checksum, to ensure that it runs an unmodified version of the device firmware. On a checksum failure, we revoke the device and prohibit transfer of content until it is updated to use approved firmware that may found on the device manufacturers website.

CONCLUSION

The demand for DMRS will continue to grow, as content providers and organizations realize the value and need for protecting their intellectual property or to increase the security and privacy of confidential or personal information. Digital Rights Management is a currently employed in a large array of different formats and the absence of a standard has resulted in the fragmentation of similar formats. Neither has any format emerged as a winner in the industry wide format war. Each company continues to support its own business model and hence the DRM format that supports it. Forcing users and DRM providers to switch to one format may not be a viable option which is why interoperability must be established as a layer between users and providers. It is also evident that this is possible while still supporting the features of the original format specification.DRM usage is going to continue to increase as more publishers discover its benefits. We use the suggested architecture to provide a method for the seamless conversion of content formats, DRM formats and Rights Expression Languages. Using this architecture it is possible to let consumers have the freedom to use the devices they like with all the content they own. The conversion is achieved by the use of a Device Interoperable Manager module present on the network. Clearly, DRM is a powerful

tool that can be used to protect owners of intellectual property from piracy by controlling devices remotely and by maintaining content in secure container that may be accessed only on successful authentication. This approach helps us in designing a protocol which efficiently manages the proper functioning of a DRM. It enables us to provide a structure for understanding and developing a protocol for efficient digital distribution of content in all forms - software and media - over any distribution channel.

REFERENCES

1. *Towards a Secure and Interoperable DRM Architecture:* Gelareh Taban, Alvaro A. Cárdenas and Virgil D. Gligor [2006]*;* ACM.
2. Present State and Emerging Scenarios of Digital Rights management Systems: Marc Fetscherin, University of Bern, Switzerland
3.Google
4.Wikipedia

Author

Priyanka Gupta, Bsc(Honours) Computer Science, Delhi University, MCA (GGSIPU University).Currently working in Teaching profession.

