the proceedings of International Workshop on Secure and Ubiquitous Networks-SUN05; Part of DEXA 2005 - 16th International Conference on Database and Expert Systems Applications, Copenhagen, Denmark, 22 - 26 August 2005. Applied Research Group, Satyam Computer Services Ltd.

DMW- A Middleware for Digital Rights Management in Peer-to-Peer Networks

Praveen Kumar, Sridhar G, Sridhar V, and Gadh R*.
Applied Research Group, Satyam Computer Services Limited
SID Block, IISc Campus, Bangalore, India 560 012
Email: {Praveenkumar_GS, Sridhar_Gangadharpalli, Sridhar}@satyam.com
** UCLA, Los Angeles, USA, E-mail: gadh@ucla.edu*

Abstract

Enforcing DRM in collaborative, Peer-to-Peer (P2P) networks comprising different types of user devices is a challenging task as it is difficult to monitor the network operations in a P2P network that is not governed by any rules. In such a scenario, efficient revenue generation for the content service providers for distributed content, prevention of unauthorized copying and distribution, and maintaining anonymity of the peers are some of the main challenges. In this paper, we present a middleware for DRM enforcement in P2P like network comprising mobile and static devices that exchange content among themselves. Most of the middleware modules discussed in the literature address the issues of content management. The proposed middleware provides a trusted environment for DRM enforcement in P2P like network.

1. Introduction

Recent advances in wireless communication are characterized by enhanced handset capabilities on one hand and ever increasing bandwidth availability on the other. These advances have opened up new avenues of revenue generation for service providers and at the same time triggered a huge demand for value added services in mobile networks. Telecom operators are increasingly providing mobile users with value added multimedia services such as digital music, ring tones, games, and video on demand (VOD). VOD is poised to be a value added service with huge potential for revenue generation [1]. The iTunes Music Store has set a new milestone by demonstrating a successful business model for online music business which provides protected music content on Mac or PC [9]. The success of iTunes, VOD, and other multimedia services highly depends on how effectively digital rights can be managed over the content's lifecycle. In such a scenario, Digital Rights Management (DRM) allows a content provider to enhance revenue by secure encryption of media content, and efficient tracking of media delivery and usage, thereby preventing any unauthorized usage and revenue loss.

In this paper, we present architecture for DRM middleware (DMW) to enforce DRM in mobile handsets that form a P2P like network for content exchange through super-distribution. DMW is a network oriented middleware that resides in each peer device. DMW acts as a facilitator for value-added services by ensuring controlled content distribution and DRM rights enforcement with access control and copy control during content rendering and distribution. By providing these services, DMW enables the realization of a trusted system for secure content exchange between peers. In the following sections, we describe DMW assisted P2P communication architecture along with its main components, and scenarios highlighting DRM enforcement in P2P networks.

2. Background and Related Work

Multiple parties are involved along the value chain of content creation, management, delivery, and usage. Proper revenue distribution along this value chain calls for a comprehensive approach towards DRM and content download standards. Several organizations in this value chain have formed the Open Mobile Alliance (OMA) [8] that has contributed significantly to the evolving DRM mobile architecture standards.

Content providers see a lot of value in super distribution [8] that boosts the demand for content among the mobile user groups. For example, a user who acquired an interesting content would want to share the same with a peer. This unrestricted sharing of content might lead to revenue loss to the content provider. In this paper, we are visualizing super-distribution of content among mobile users as a peer-to-peer like phenomenon. We further expand the P2P network to different devices a user may own in addition to the mobile handset, and to which he may transfer the content for purpose of either rendering or storage.

In a decentralized environment like a P2P network where peers join and leave the network randomly, DRM enforcement posses a serious challenge. Fenkam et al [3] present a study on access control for mobile P2P collaborative environments and describe architecture for mobile teamwork providing access control support for various devices. They highlight the importance of distributedness in access control enforcement and rely on a P2P middleware to enforce offline access control. In this paper, we extend this idea to copy control to prevent illegal copying of protected content. Pearson in [6] describes trusted computing platforms as the next security solution for secure content consumption. These are of particular interest for Content Service Providers (CSPs) to enforce DRM. Garfinkel et al [4] describe a flexible OS architecture to support trusted computing and to establish a trusted system to improve security and robustness in distributed systems. They design a OS architecture based on the idea of Trusted Virtual Machine Monitor (T-VMM) that provide backward compatibility allowing existing applications and OS to realize benefits of trusted platforms with little or no modifications. However, there are issues that arise in implementing such VMMs for trusted computing in heterogeneous peer devices with different OS. Messerges et.al [5] provide a framework for protecting digital content in the embedded environment of a 3G mobile phone and introduces a “Family Domain” approach that uses key sharing between members of the domain for content management. They extend a generic OS by adding DRM/Security extensions to form a trusted system. Eskicioglu et.al in [2] proposes new channels for protected distribution of usage rights and provides a method for content copy control. However, protection of content in local storage (hard disk) still remains an open issue that needs to be addressed to provide end-to-end security solutions. In our previous work [7], we proposed a Network-Centric DRM for DRM enforcement in mobile devices by monitoring multimedia content delivery through a DRM server and by forcing the execution of embedded codes in the multimedia content using enhanced device capabilities.

3. DRM Middleware (DMW) for P2P Content Sharing

Content providers can greatly benefit by allowing super distribution of content among user groups. However, unrestricted content sharing among the users can drastically diminish the possible revenues to content providers. Therefore, a balanced approach that facilitates content sharing among users with reasonable amount of restrictions is required to meet the objectives of P2P content sharing and revenue generation.

In this paper, a decentralized approach for rights enforcement system in the form of network oriented middleware is proposed. This middleware is based on a multi-tier architecture comprising of the following (as shown in Figure 2):

- Upper Tier: Application level Middleware tier which liaisons between the application and OS. The middleware at this tier provides services to an application for interpreting the rights and rendering the secure content.
- Middle Tier: OS level middleware tier provides DMW specific extensions to OS to help track illegal use of content.
- Lower Tier: Hardware level middleware tier for rights enforcement.

The proposed middleware addresses the following:

- Interoperability: Multiple formats interpretation and enforcement of rights objects..
- Compatibility: Content, Rendering Device and Rendering Application compatibility.
- Trustworthiness: Identification of device capabilities for DRM enforcement/content sharing.
- Content manageability: Analysis of Meta data for authorization, access control, and copy control.
- Support for protected Content distribution.

We consider a wireless network consisting of mobile and static devices with different OS that form a heterogeneous P2P like network for content sharing as illustrated in Figure 1. Establishment of a trusted system requires support from OS to provide trusted services such as digital rights management. A generic OS has limited capabilities to detect and handle all types of access and copy violation attempts made by a user through rendering application and hardware. This necessitates the need for additional services from the DMW to plug the security gaps left by the OS, rendering application, and hardware to establish a trusted system.

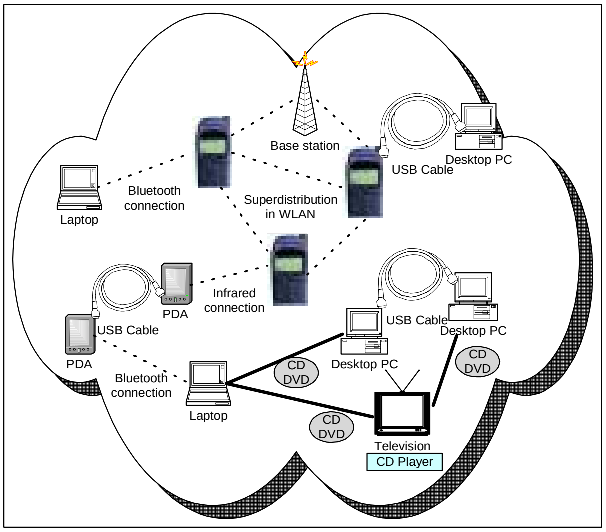

Figure 1. Architecture of DMW assisted P2P like network

4. Layered Middleware Services for DRM enforcement

In a network which consists of heterogeneous devices and P2P like self administrating character, effective enforcement of DRM can be achieved only by a multi-tier approach wherein the DRM is addressed at application, OS and hardware levels. Therefore we propose a multi-tier middleware which spreads over these three layers. The proposed middleware is based on a multi-tiered, multi- layered architecture consisting of different service–oriented layers which address content sharing and DRM enforcement aspects in a P2P network. Figure 2 illustrates the layered architecture of the proposed middleware, DMW. DMW provides a range of services from content negotiation and acquisition as part of topmost layer, DRM enforcement and super-distribution as part of intermediate layers to rendering as part of the bottommost layer. These service layers are explained below:

User Services layer: This layer provides user services, namely, User Authentication, Content Information Exchange, and Device/Content compatibility checking.
User Authentication: DMW authenticates a user device that is downloading the content. The DMW of receiver device determines the unique device identifier and transmits the same to the DMW of the sender. The DMW of the sender then ensures that the content is downloaded only onto the permitted device by requesting the receiver for a unique identifier before initiation of download. During content rendering, DMW authenticates user based on the content key on behalf of the application
Content Information Exchange: DMW propagates content availability information to the peers and performs negotiations with peers during content exchange. DMW propagates meta-data associated with the content such as content ID, format, device requirements, and DRM security specifications.
Compatibility Analysis: This module checks the compatibility of user device with respect to the Device type, Device model, OS, rendering application, and support hardware compatibility for successful content rendering and DRM enforcement during content processing and distribution. It ensures that the receiver obtains only those content formats that can be rendered on his/her device. Content provider can also check the compatibility of the receiving device in enforcing DRM for the content that is to be delivered.

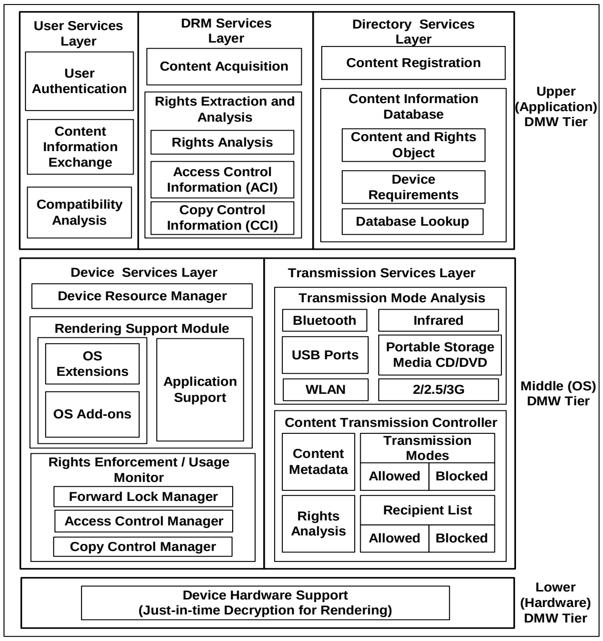

Figure 2. DMW Multi-Tiered, Multi-Layered architecture

DRM Services layer: This layer provides DRM services like Content Acquisition, Rights Analysis, Access Control, and Copy Control Information.
*Content Acquisition**:*** This module downloads the DRM protected content package into the device local memory. The content download is performed after downloading device is authenticated by “User services layer” and device compatibility requirements are met.
Rights Analysis: This module analyses the rights object. In the case of combined delivery, the rights are extracted from the rights object that form part of the

DRM package that also contains the content object. In the case of separate delivery, this interacts with "Content Information Exchange" module to obtain the necessary rights object.

Access Control Information: This module administers access control based on the rights analysis and allows access to content for rendering, allowed time duration of rendering, and maximum number of views allowed for the content.

Copy Control Information: This module extracts the copy control information embedded in the rights object, and interprets the level of copying allowed and the limitations in the number of generated copies. This approach tries to address the issue of copy control of digital content which is a major source for DRM violation. However the issues such as how to generate and manage rights objects for the content copies remains to addressed.

Directory Services layer: This layer provides directory services, like maintaining the content availability list and authorizing the content for processing such as rendering, through the Content Registration Manager.

Content Registration Manager: This module registers downloaded content before making it available for rendering. DMW ensures that the rendering application renders only the content that is registered with the Content Registration Manager. It acts like a centralized content management authority during rendering and during content exchange.

Content Information Database: This database contains details of the Content Object, Rights Object, Content Owner ID, Content Format, and Cost of Content. It also maintains the Device compatibility requirements like Device Type, Device Model, OS, and Application and Support Hardware details.

Device Services layer: This layer is responsible for the implementation of DRM on the protected content based on information provided by upper "DRM Services layer." The Device Resource Manager, Rendering Support Module, and the Rights Enforcement/Usage Monitor provide the functionality related to digital rights enforcement.

Device Resource Manager: This module checks whether the device has enough resources like memory, cache, and CPU to render the content. It also checks whether the application can be loaded into the memory for execution.

Rendering Support Module: This module provides a set of extensions and add-ons to OS to enforce DRM. These are provided based on access control and CCI analyses in the upper "DRM Services Layer." With these extensions and add-ons, OS can support access control and copy control.

Rights Enforcement/Usage Monitor: This module checks for proper enforcement of the rights and monitors the adherence to the rights during rendering. It enforces device-specific forward lock mechanism for forward lock protected contents through Forward Lock Manager. In the case of combined delivery and Separate delivery, this module checks for the enforcement of access control and copy control on the DRM protected content through Access Control Manager and Copy Control Manager.

Transmission Services layer: This layer analyses the various communication channels for content exchange and controls content transmission among peers.

Transmission Mode Analysis: This module checks for the possible transmission channels available for distribution of the content to different types of peer devices. Further, the devices that can be reached through these channels could be defined to form a personal area network. Sometimes, the best possible channel to reach a peer could be decided based on the availability of multiple channels. For instance if two peer devices are connected to each other by two different channels say a WLAN and a Bluetooth , this module would check both the channel conditions vis-à-vis the content characteristics, just at the time of transmission and makes appropriate channel selection for content transmission. Further this module also checks for possible violation of rights for transmission. For instance a user is allowed to transmit within a WLAN but not allowed to transmit to storage media such as a CD writer.

Content Transmission Controller: This module controls the transmission of copy-protected content based on the transmission mode analysis. The rights associated with content are analyzed and any violation of rights would result in content not being accessible. Realizing the content control at a lower level would help enforce DRM in most of the situations. Content Transmission Controller checks for allowed/blocked recipient list since certain content providers allow re-distribution of their content only among selected recipients. Finally, it checks for allowed/blocked transmission channels and allows content to be transmitted only through the allowed transmission channels. Especially in P2P like networks, contents could be released with group licenses which allow a user to share the content with peers in a specific group; in such a scenario this module would facilitate to control transmission of content to authorized recipients.

5. Scenarios of DMW DRM enforcement

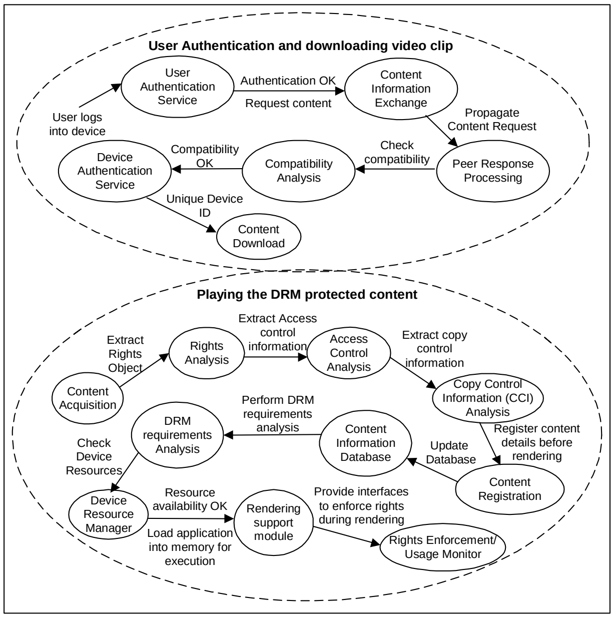
User Authentication and downloading video clip
User logs into device
User Authentication Service
Authentication OK
Request content
Content Information Exchange
Propagate Content Request
Peer Response Processing
Check compatibility
Compatibility Analysis
Compatibility OK
Device Authentication Service
Unique Device ID
Content Download
Playing the DRM protected content
Content Acquisition
Extract Rights Object
Rights Analysis
Extract Access control information
Access Control Analysis
Extract copy control information
Copy Control Information (CCI) Analysis
Register content details before rendering
Content Registration
Update Database
Content Information Database
Perform DRM requirements analysis
DRM requirements Analysis
Check Device Resources
Device Resource Manager
Resource availability OK
Load application into memory for execution
Rendering support module
Provide interfaces to enforce rights during rendering
Rights Enforcement/ Usage Monitor

Figure 3. Scenario of User authentication, downloading, and playing video content.

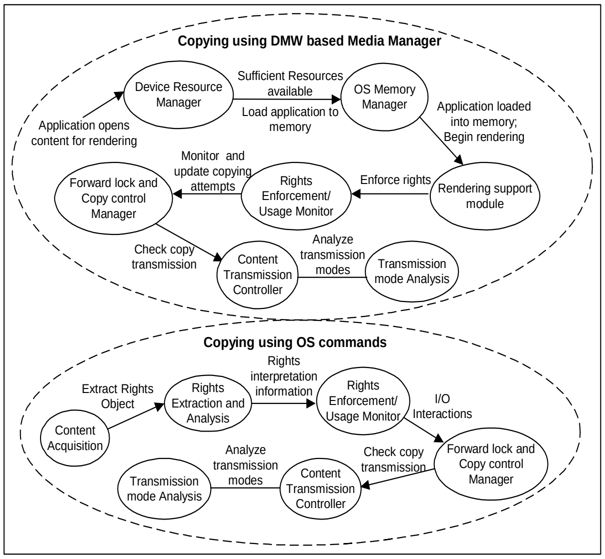
Copying using DMW based Media Manager
Application opens content for rendering
Device Resource Manager
Sufficient Resources available
Load application to memory
OS Memory Manager
Application loaded into memory; Begin rendering
Rendering support module
Enforce rights
Rights Enforcement/ Usage Monitor
Monitor and update copying attempts
Forward lock and Copy control Manager
Check copy transmission
Content Transmission Controller
Analyze transmission modes
Transmission mode Analysis
Copying using OS commands
Content Acquisition
Extract Rights Object
Rights Extraction and Analysis
Rights interpretation information
Rights Enforcement/ Usage Monitor
I/O Interactions
Forward lock and Copy control Manager
Check copy transmission
Content Transmission Controller
Analyze transmission modes
Transmission mode Analysis

Figure 4. Scenario of Copy control enforcement on protected content

In Figure 3, Content Information Exchange module enquires about availability of video clip. It receives responses from various peers regarding content availability, cost, DRM requirements, and device compatibility requirements. The rights and access control information is analyzed, resource requirements are ensured before initiating the rendering. User interactions with the downloaded content are monitored for any violation against the DRM requirements.

In Figure 4, a user would like to copy a downloaded content onto a storage medium using a media manager application. In this case, the rights associated with the content is analyzed and enforced by DMW Media Manager. If the user uses OS commands to copy, Rights Enforcement/Usage monitor that constantly monitors all I/O activities and Copy Control Manager together enforces the rights.

6. Summary and Discussion

Our proposal in this paper is to address the DRM at different levels namely at application level, OS level, and hardware level. By this, we intend to spread the trustworthiness across these layers. We have proposed a multi-tier and multi layered middleware to enforce DRM in P2P like networks. The proposed middleware resides in user devices and provides trusted environment to enforce DRM.

7. References

[1] S. Byers et.al, “Analysis of Security Vulnerabilities in the Movie Production and Distribution Process”, In *Proc. of ACM Workshop DRM’03*, Oct 27, 2003, Washington, USA.

[2] A.M. Eskicioglu et.al, “New Channels for carrying copyright and usage rights data in Digital Multimedia Distribution”, In *International Conference on Information Technology: Research and Education (ITRE 2003)*, August 11-13, 2003, Newark, NJ.

[3] P. Fenkam et.al, “Towards an Access Control System for Mobile Peer-to-Peer Collaborative Environments”, Appeared in *Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02)*, June 10-12, 2002, Pittsburgh.

[4] T. Garfinkel et.al, “Flexible OS Support and Applications for Trusted Computing”, In *9th Workshop on Hot Topics in Operating Systems (HotOS IX)*, May 18-21, 2003, Hawaii.

[5] T. S. Messerges and E.A. Dabbish, “Digital Rights Management in a 3G Mobile Phone and Beyond”, Appeared in *Proc. of 2003 ACM Workshop on Digital Rights Management (DRM’03)*, October 2003, Washington, USA.

[6] S. Pearson, “Trusted Computing Platforms, the Next Security Solution”, *Technical Report, Trusted Systems Lab*, HP Labs, UK.

[7] Sridhar G. et.al, “DRM Enforcement in Mobile Devices”, I*n 2nd Wireless Telecommunication Symposium (WTS2004)*, May 2004.

[8] “OMA DRM Requirements Version 2.0”, Released 15-May-2003, http://www.openmobilealliance.org/.

[9] “iPod + iTunes for Mac and Windows”, http://www.apple.com/itunes/