2010 Fourth International Conference on Genetic and Evolutionary Computing

A DRM System for Home Network Based on RBAC and License Chain

Danmei Niu, Zhiyong Zhang, Lili Zhang
Electronic Information Engineering College
Henan University of Science and Technology
Luoyang, China
niudanmei@163.com, xidianzzy@126.com, lillyzh@126.com

***Abstract*—The purpose of DRM (Digital Rights Management) is to prevent from the illegal copy and distribution of digital contents. DRM technology could be used in home network, but in many situations, different users need different access rights to DRM contents in home network. The paper presented a DRM system for home network based on RBAC (Role-Based Access Control) and license chain. A DRM functional architecture for home network was shown, then the partition of roles and permissions for home network was made based on RBAC. Moreover, the working process of the system was put forward, and the system analysis was made. Finally, a conclusion was drawn and the future work was addressed.**

Keywords-digital rights managemen; home network; role-based access control; license chain

I. INTRODUCTION

The development of the network has made the distribution of the digitalized multimedia content easier. And the digitalized content provides much convenience like that it is easy to copy and the copied content is identical with the original. The other side of such convenience involves the illegal factor such as the copyright piracy and the illegal copy [1].

Recently, DRM (Digital Rights Management) has been used for preventing from the illegal copy and distribution [2][3][4]. Since a DRM content has the corresponding license and usage rule, and they are directly encrypted, the content obtained illegally cannot be played. Now, there are more and more digital devices in a home network, such as PC, digital TV, PDA, and MP3 Player. The user wants to play the DRM content freely on any of his multiple devices and realize the uniform management. The concept of AD (Authorized Domain) has been presented to resolve such problems [5][6]. Home network is the major applied form of AD. Each device has equivalent access right on the contents. However, certain contents such as adult contents, which are not allowed to children, are to be managed with access control [7]. That is in a home network, different users have different rights.

In this paper, we present a DRM system for home network based on RBAC (Role-Based Access Control) and license chain that controls the access rights of family members and devices.

II. RELATED WORK

There are several ways of allowing differentiations for rights within a domain. A straightforward solution would be to introduce differentiations during purchase of the rights when the user could immediately define different rights for different domain members and let the content provider encode this in the licenses. However, this is rather static, nonflexible, and privacy invasive approach.

Furthermore, introduce differentiations in the process of transcoding DRM licenses into domain DRM licenses [8]. Here, a person who bought the content (or domain administrator or a domain member who first accesses the license) will be allowed to add further restrictions on top of the original licenses specifically for domain members. However, a very strong requirement by the commercial content providers is that they want completely control over the content distribution and usage. Very often, content providers do not trust and do not allow transcoding of original licenses.

Another possibility is license chain, the domain administrator adds a chain for every license distributed to the domain, the chain records devices information of playing a DRM content [9]. This approach realizes tracing of a license in a domain, and does not change the original license. However, this could not provide appropriate rights to each member and device in a domain.

Therefore in this paper, an alternative solution is presented which supports combining RBAC and license chain, used for our DRM system, without transcoding of licenses.

III. A DRM SYSTEM FOR HOME NETWORK BASED ON RBAC AND LICENSE CHAIN

In this section, we propose a new DRM system based on RBAC and license chain for local domain management in home network environments. A home network is a good example of a localized domain.

A. A DRM Functional Architecture for Home Network

In Figure 1, we show a DRM functional architecture for home network.

978-0-7695-4281-2/10 $26.00 © 2010 IEEE
DOI 10.1109/ICGEC.2010.224

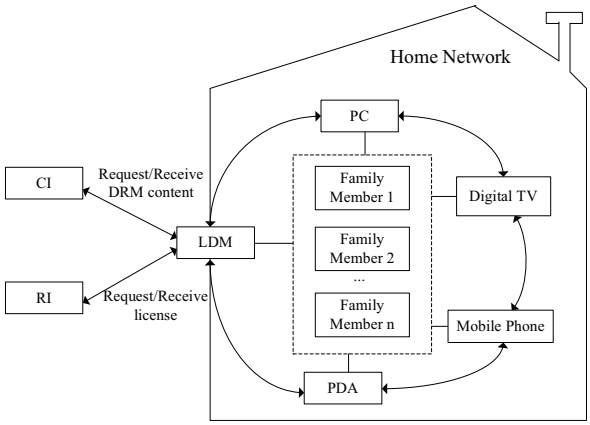

Figure 1. A DRM functional architecture for home network.

The following functional entities consist of the system:

- CI (Content Issuer): CI has a responsibility for providing digital content issue and download. The digital content which is requested by the user is packed and encrypted by CI (The encrypted content is called DRM content). Then CI sends DRM content to legal home network, CI also communicates with RI, and let RI create corresponding license.
- RI (Rights Issuer): RI has a responsibility for creating and distributing corresponding license of DRM content. According to the received information, RI creates corresponding license, then distributes the license to legal home network.
- LDM (Local Domain Manager): LDM is the core device of a home network, it has a responsibility for managing all the family members and devices of a home network. LDM requests DRM contents and corresponding licenses, then distributes acquired contents and licenses to the family members and devices. Maybe LDM is not a special device, it can be a PC or a notebook PC, and must have enough memory space and working capability.
- Devices(such as PC, digital TV, mobile phone and PDA)are connected in a home network, and the home network can be wired or wireless. Devices can access DRM contents through local or remote access approach.
- Family members are the users of the devices. They can read or play DRM contents on the devices.

B. The Introduction of RBAC

The core idea of RBAC is creating relations between permissions and roles, distributing appropriate roles to users, then users could have relations with permissions. Setting up roles is based on different tasks, and distributing roles to users is based on users' responsibility. About RBAC models, a famous model is Professor R. Sandhu's RBAC96 [10]. Our system is based on this model.

C. Partition of Roles for Home Network

According to the user classes and the relations of users, we design a hierarchical roles model for home network in Figure 2:

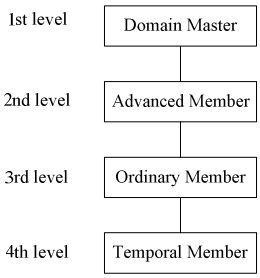

Figure 2. A hierarchical roles model.

- Domain Master: Only one family member can be domain master, who is the owner of a home network domain. Domain master is the principal and the highest manager, and manages LDM. Domain master has all the permissions.
- Advanced Member: Advanced member is managed by domain master. Advanced member's permissions are between domain master and ordinary member. Advanced member can realize part of domain master's permissions.
- Ordinary Member: Ordinary member is ordinary users of a home network, and can obtain domain license, then use DRM content.
- Temporal Member: A user who temporally share DRM content with the users of the home network, although he is not registered in the local domain. Temporal member has part permissions of using DRM content and has the lowest permission.

D. Partition of Permissions for Home Network

Role is an intermediary between a user and permissions. Endue users some roles, then endue permissions to roles, users could obtain corresponding permissions. There are many permission types for home network, such as creating and revoking domain, adding and deleting users or devices, obtaining and using license, using DRM content. Creating a table of relations for users, roles and permissions, domain master can quickly search for permissions of a role corresponding to a user. TABLE I shows a table of relations for users, roles and permissions.

TABLE I. A TABLE OF RELATIONS FOR USERS, ROLES AND PERMISSIONS

Users	**Roles**	**Permissions (realizing permissions of roles in a combined form)**
Family member 1 Family member 2 … Family member n	Domain master Advanced member Ordinary member Temporal member	Creating/revoking domain Adding/deleting users or devices Setting up maximal number of users/devices Purchasing DRM contents Requesting/using DRM contents Requesting/using licenses Distributing DRM contents/ licenses

This table is managed dynamically by domain master. When a family member registers or leaves the domain, or the role of a family member changes, or there is a new purchased DRM content, domain master dynamically determines the permissions of the role for the user and deals with the new DRM content.

E. Working Process

In this section, we explain the working process of the DRM System for home Network Based on RBAC and license chain.

- When a family member pays to the content provider for a DRM content, CI transfers a protected content to LDM. This content should be also played on other devices that are members of a home network. To support this capability, RI transfers a license for the purchased content, which is only accessible to LDM.

The license form follows ITUTX.509 international standard [11]. In this paper, the form of the license is shown in Figure 3.

License information: version number, serial number, signature algorithm;
License owner information: identity, public key;
Content information: ID, decrypting key;
Using permissions: using constraints of content, valid term;
Digital signature of RI.

Figure 3. The form of the license.

License information includes version number, serial number(a unique number for each license), signature algorithm(such as RSA algorithm). License owner information includes identity, public key. Content information includes ID, decrypting key. Using permissions includes using constraints of content, there are several types of constraints, such as using times of the content, devices number of using content at the same time, valid term of using content, etc. UTC time form is used for the valid term. Digital signature of RI is included in the license, this assures integrity. The DRM license is expressed in XML(Extensible Markup Language) form, mainly in XrML(Extensible rights Markup Language) and ODRL(Open Digital Rights Language). Once the license is purchased, it can not be modified.

In this paper, we add a chain for each license, the chain is used for recording the information of the family member using DRM content. The chain is only used in home network [9]. Current device which is using DRM content is identified in the chain, this assures the license is only on a device at the same time. Once the license is transferred to other users and devices, the original user and device can not use this license to play the corresponding content. This approach constrains some permissions, such as play times and term, and is more flexible. The chain structure is shown below:

Record 1: Content ID，
Sender(family member ID1, device ID1),
Receiver(family member ID1', device ID1'),
Timestamp1,
Digital signature of family member ID1.
Record 2:…
Record n:…
Current device n.

There are several records in a chain, each record includes content ID, sender information, receiver information, timestamp, digital signature of family member IDn.

- When a family member in the home network requests a DRM content and the corresponding license, he sends the LDM a message, including family member ID, device ID and requested content ID. The domain master checks if the family member and the device are legal, then queries the table of relations for users, roles and permissions, according to the table, decides if the family member has the using permission of the DRM content.
- If the family member has the using permission of the DRM content, the domain master sends the encrypted DRM content to the device which the family member is using. The encrypted DRM content can be stored in any device and be transferred freely in the home network.
- Suppose there is a information table of using license in the LDM, the table records the corresponding licenses of the DRM contents, including current family member ID and device ID using a DRM content, the serial number of corresponding license. The domain master checks the table, if the license is in the LDM, the domain master writes a record in the chain. Then the domain master sends the license and the attached chain to the device being used by the family member, and records the serial number of license, family member ID and device ID in the information table of using license.
- If the license in not in the LDM, the domain master checks the information table of using license, finds out current family member ID and device ID, and sends a message to them. The family member who is using the license writes a record in the corresponding chain, then sends the license and the attached chain to the receiver, and the sender can not play the content. The sender should also send the receiver information to the LDM, then the domain master can update the information table of using license.
- When the family member obtains the license, he can play the DRM content by using the decrypting key.
- When the permissions of a license is used up, that is the using times of the content becomes 0 or the valid term expires, the last family member who is using the license sends the license and the attached chain to the LDM, and the domain master will make a statistic and analysis according to the license and the chain.

IV. SYSTEM ANALYSIS

This system is based on RBAC and license chain, all the family members can share DRM contents according to the corresponding permissions of their roles. The license and the

attached chain assure DRM contents being used safely and legally. The performance of this system is analyzed below:

- The concept of AD has been adopted in home network, and the license of a DRM content is bound with a group of devices, not one device. The communication among RI, CI and the devices of home network is simplified greatly, the number of issuing licenses and the costing resource of managing licenses are reduced greatly, and the burden of RI is decreased [12].
- The license is bound with a home network, realizing sharing licenses in a home network. The family members transfer and use DRM contents freely, this is very convenient.
- DRM content is separated from the license, this increases the flexibility of management, that is if a DRM content is modified, the corresponding license is not influenced. The safe performance is also improved, even if an illegal user gets a DRM content, he could not play it without the license, preventing the illegal access.
- In the working process of this system, when a family member wants a license, the domain master will check if the family member ID and the device ID are legal, this working approach can identify the illegal users and devices, and prevent users from playing DRM contents in the unauthorized devices.
- The combination of RBAC and license chain is used in this system, realizing the tracing of licenses and the transferring permission of DRM contents, and the license is not modified. Every family member and device can be distributed the most appropriate permission based on RBAC [13]. The control of differentiation for rights is more flexible, and content provider can control over the content distribution and usage in home network.

V. CONCLUSION AND FUTURE WORK

In the typical DRM system, the license is bound with a device, the DRM content is only played on that device, this constrains the flexibility of using DRM contents. In this paper, we propose a DRM system for home network based on RBAC and license chain, this system satisfies the needs for the users, DRM contents can be transferred and used freely.

Our future work will concentrate on the distribution policy of specific permissions based on RBAC, how to make the working process of the system more efficient, etc.

ACKNOWLEDGMENT

The work was sponsored by National Natural Science Foundation of China Grant No.61003234 & No.60803150, China Postdoctoral Science Foundation Grant No.20100471611, Henan Province Key Technologies R & D Program Grant No.092102210295, and Henan University of Science & Technology Young Scholar Fund Grant No.2008QN010.

REFERENCES

[1] JungSoo Lee, Yeonjeong Jeong, Kisong Yoon, and Jihyun Park, ”DRM Applied Contents Share in Digital Home,” The 13th IEEE International Symposium on Consumer Electronics(ISCE2009), pp. 64-66, 2009.

[2] Z. Y. Zhang, Q. Q. Pei, J. F. Ma, and L. Yang, “Security and Trust in Digital Rights Management: A Survey,” International Journal of Network Security, Vol.9, No.3, 2009, pp. 247-263.

[3] INDICARE, “Consumer Survey on Digital Music and DRM,” http://www.indicare.org, May 2005.

[4] OMA (Open Mobile Alliance) 2.0, http://www.openmobilealliance.org, September 2007.

[5] S.A.F.A. van den Heuval, W. Jonker, F.L.A.J. Kamperman, and P.J. Lenoir, “Secure Content Management in Authorized Domains,” In Proc. IBC 2002, pp. 467–474, September 2002.

[6] S. Sovio, N. Asokan, and K. Nyberg, “Defining Authorization Domains Using Virtual Devices,” In SAINT Workshops 2003, pp. 331–336, 2003.

[7] Heeyoul Kim et al., ”Digital Rights Management with Right Delegation for Home Networks,” ICISC2006, LNCS 4296, pp. 233–245, 2006.

[8] Milan Petković, and R. Paul Koster, “User-Attributed Rights in DRM”, DRMTICS 2005, LNCS 3919, pp. 75–89, 2006.

[9] M. Li, S. L. Liu, and K. F. Chen., ” Study on the Integration of Home Network DRM and Typical DRM,” Computer Engineering, Vol.33, No.2, 2007, pp. 249-251.

[10] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman, ”Role-Based Access Control Models,” IEEE Computer, Vol. 29, No. 2, 1996, pp. 38-47.

[11] Y. P. Yu, and L. Xu, ”DRM technology based on domain user's rights,” Journal of Shenyang Institute of Aeronautical Engineering, Vol.26, No.5, 2009, pp. 87-90.

[12] Q. Q. Pei, “Research on Key Techniques and Applications of Digital Rights Management,” Xidian University, 2007.

[13] J. Yi, “RBAC-Based DRM Model and Implement,” Jilin University, 2007.