Wuhan University
Journal of Natural Sciences

2008, Vol.13 No.4, 475-480

Article ID 1007-1202(2008)04-0475-06
DOI 10.1007/s11859-008-0419-3

A DRM System Based on Mobile Agent for Digital Rights Redistribution

□ **LI Ping, LU Zhengding†, ZOU Fuhao, LING Hefei**

College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China

Abstract: We propose a digital rights management (DRM) system based on mobile agent to protect the copyrights of content providers. In the system, the content provider creates a time limited blackbox out of an original agent and dispatches it to the user end to enforce DRM functions. The blackbox is an agent that can resist the attacks from the malicious user in a certain time interval. Owing to digital rights redistribution support, the user whose rights belong to redistribution category can transfer his rights to other users. Moreover, by introducing public key infrastructure (PKI) and certificate authority (CA) role, the security of the session can be ensured. An analysis of system security and performance and a comparison with traditional DRM system is given.

Key words: digital rights management; public key infrastructure; certificate authority; mobile agent; rights redistribution
CLC number: TP 309

0 Introduction

With the rapid development of digitization and Internet technology, it becomes more and more convenient to produce and distribute digital work. However, the copyright infringements of digital work on the Internet can not be neglected, especially in P2P networks. Thus an effective solution to protect digital rights[1] is in urgent need.

At present, DRM (digital rights management) is maybe the most popular technology to protect digital rights. The common process of the most DRM systems is described as follows: A user acquires encrypted content from the content provider, before he can render the content, the user must request a content rendering certificate from the content provider, and he will get the certificate to render the content after paying for it. So how to ensure the security of the certificate that comprises the content decryption key and other sensitive information, is a very important issue[2,3]. Usually, it is quite impractical for common users to construct a trusted execution platform module based on hardware. Then, as a common user, if he directly handled the content rendering certificate, it would lead to a security issue.

To solve this issue, we introduce mobile agent and time limited blackbox techniques. Mobile agent is a program which can migrate from one node to another and execute some specific task on the network, it decides freely when and where to migrate and returns to the original host with the result at last[4]. Time limited blackbox, which is presented by Hohl, is created out of the original mobile agent. The data and code in a blackbox can resist spying or corruption attacks from malicious

Received date: 2008-03-08
Foundation item: Supported by the National Natural Science Foundation of China (60502024); the Electronic Development Fund of Ministry of Information Industry of China ([2007]329) and the Natural Science Foundation of Hubei Province (2005ABA267)

Biography: LI Ping(1974-), male, Ph. D. candidate, research direction: multimedia security. E-mail:lpshome@sina.com
† To whom correspondence should be addressed. E-mail: zdlu@hust.edu.cn

users in a certain agent protection time interval[5,6].

Rights redistribution is a key technique of DRM system[7]. In fact, rights redistribution support can increase the motivation for common users to buy and use content, make the DRM system widely accepted by users and decrease the possibility for users to crack the DRM system[8]. However, S. H. Kwok proposes a scheme to redistribute rights by introducing a local DRM center, but it will seriously increase the complexity and terminal users' burden. Moreover, it would lead to a security issue[9]. S. K. Nair sets up a trusted platform module based on hardware on the mobile handset to enforce DRM functions and redistribute digital rights, but it is quite impractical for common computers[10].

PKI technique can be used for the security of communication sessions[11]. In fact, it uses certificates, which bind a user's public key and other information (e.g., name, E-mail) to verify user identity in the Internet and can be published by the third trusted party—CA to manage public key. CA is the kernel of the PKI, whose main functions are to dispatch, renew, revoke and verify certificates.

According to the introduction above, we propose a DRM system based on mobile agent for digital rights redistribution. In this system, a mobile agent is deployed on behalf of the content provider. It arrives at the user end to grant digital rights and enforce other DRM functions honestly. The system also provides rights redistribution support. User's rights information is managed by the content provider and saved in his local database. From the content provider, the common rights or redistribution rights of the content are bought freely by users. If a user has bought redistribution rights, he can transfer his rights to other user and benefit from it. Moreover, we adopt the PKI technique. Both the content provider and users need to acquire an identity certificate from CA. At the beginning of the session, they need to exchange their certificates and verify the identity of each other. The session between them will continue only if the certificates verification has passed.

1 Overview of the Proposed System

1.1 Structure of the System

As shown in Fig.1, there are three main roles in the system: content provider, user and CA.

● Content provider is generally responsible for digital content distribution and core DRM function, and deployed using high performance server.

● User is responsible for downloading digital content and rendering it after paying, and can redistribute his rights to other user as long as his acquired rights belong to redistribution category, which is usually deployed using ordinary computer.

● CA is responsible for certificate delivery and online certificate status query. Usually its hardware deployment is similar to content provider.

1.2 Description of Main Functional Modules of Each Role

The most important functional modules of each role are described as follows:

1) Content provider

① Identity certificate acquirement module: connect to CA, provide his information and request an identity certificate.

② User register module: accept user's register request and record user's related information in the database.

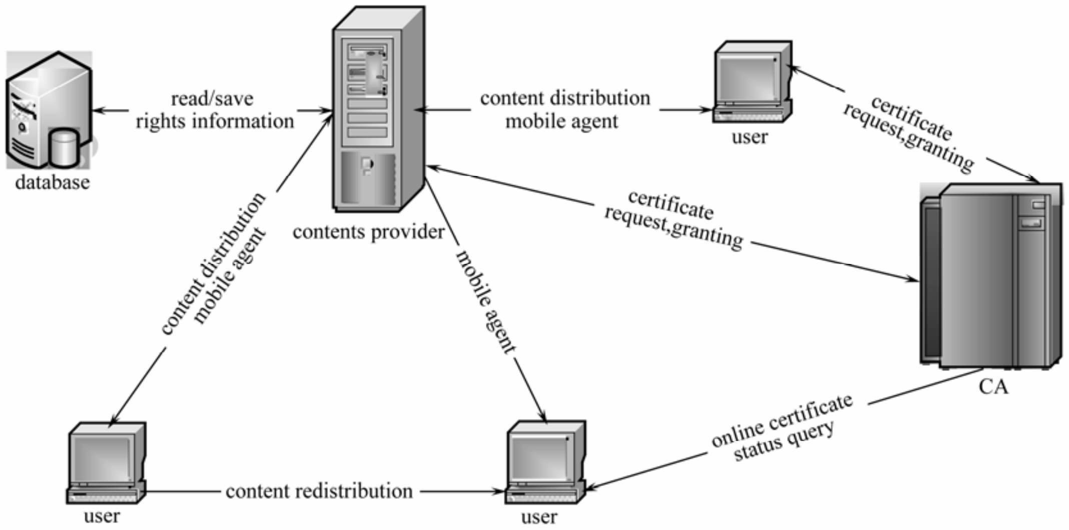

Fig.1 Structure of the system

③ Certificate status query module: connect to CA and check the user's certificate status.

④ Content management module: encrypt the contents (e.g., use AES algorithm).

⑤ Contents distribution module: distribute the encrypted content to the user.

⑥ Billing module: charge the fee according to the user's order (common rights or redistribution rights).

⑦ Time limited blackbox creation module: create a time limited blackbox out of an original mobile agent.

⑧ Mobile dispatching module: dispatch a mobile agent to the user end.

2) User

① Identity certificate acquirement module: connect to CA, provide his information and request an identity certificate.

② User register module: connect to the content provider, provide his information to register.

③ Certificate status query module: connect to CA and check the content provider's certificate status.

④ Content acquirement module: connect to the content provider and acquire content.

⑤ Content rendering certificate acquirement module: request a content rendering certificate from the content provider.

⑥ Content rendering module: interact with the mobile agent dispatched by the content provider, analyze the rights, decrypt and render the content (the decrypted content can not be saved but only be rendered at the user end).

3) CA:

① Register module: accept the request of the content provider or a user, verify the provided information.

② Certificate generating module: generate a certificate for a user or the content provider. The certificate should follow the X.509 certificate specification.

③ Certificate revoking module: revoke the certificate and add it to the revoked certificate list.

④ Online certificate status query module: provide online certificate status query service to the content provider and users.

2 System Implementation and Analysis

2.1 System Work Flow

This system enforces the DRM functions mainly by the communication between the content provider and users, so we emphasize the work flow of them. In the following, let us consider a scenario that Alice acquires content and redistribution rights from the content provider, and then redistributes her rights to Bob.

1) Alice acquires content from the content provider

① Alice connects to the content provider.

② Alice retrieves the content she needs from the content list provided by the content provider (in the form of web pages).

③ Alice exchanges and verifies the certificate with the content provider.

④ Alice requests the content from the content provider after verification.

⑤ The content provider distributes the encrypted content to Alice.

2) Alice requests a content rendering certificate, and the content provider dispatches a mobile agent to her

Alice can render the content only if she has acquired the content rendering certificate.

① Alice connects to the content provider.

② Alice exchanges and verifies the certificate with the content provider.

③ After verification, Alice requests a content rendering certificate and pays for it.

④ According to the rights request of Alice, the content provider generates a content rendering certificate, and records her rights information in the local database.

⑤ The content provider generates a mobile agent to carry the certificate, and then creates a time limited blackbox out of the agent.

⑥ The content provider dispatches the blackbox (also a mobile agent) to Alice.

⑦ The mobile agent, which carries the content rendering certificate, reaches Alice and starts to execute. It interacts with content rendering module of Alice and provides some information like content decryption key and rights information for it. The content rendering module decrypts the content to render.

⑧ The mobile agent records the rights information to Alice's computer and returns to the content provider.

3) Alice redistributes her rights to Bob

If Alice has bought redistribution rights of the content, she can transfer her rights to Bob.

① Bob connects to Alice if he needs her content.

② Bob exchanges and verifies the certificate with Alice.

③ After verification, Bob requests and pays for the content, Alice distributes the requested encrypted content to Bob.

④ Alice connects to the content provider.

⑤ Alice exchanges and verifies the certificate with the content provider.

⑥ After verification, Alice requests to redistribute her rights to Bob, and gives part of her profits (e.g., 50%) from Bob to the content provider.

⑦ According to the request of Alice, the content provider generates new rights information of Alice and Bob and records it to the local database.

Thus the content rights of Alice are redistributed to Bob, and Alice can't render the content any more. After that, if Bob wants to render the content or redistribute his rights, he will directly connect to the content provider instead of communication with Alice.

2.2 Security of the Mobile Agent

In this system, some information the mobile agent carries such as content decryption key is frequently attacked by malicious users. Thus how to ensure the security of the mobile agent is a key issue.

In fact, mobile agent system comprises mobile agent and mobile agent environment (MAE). Mobile agent can migrate from one MAE to another MAE and interact with the local server/resource to achieve the task. Thus, the security of mobile agent is composed of the security of the mobile agent itself and the security of the host. At present, according to current techniques, the security of the host can be implemented. So here we mainly discuss the security of the mobile agent itself.

The security threats to mobile agent from malicious users include spying attack and corruption attack. Corruption attack means that malicious users modify the sensitive data or code in the mobile agent, while spying attack means that malicious users read illegally the sensitive data or code in the mobile agent. In the system, the rights information is saved and managed by the content provider, malicious users usually have no reasons to corrupt the mobile agent because it can't bring them any profits. So we aim at spying attack here.

To address this issue, we propose a scheme which can creates a time limited blackbox out of an original mobile agent to confirm the agent's security. The term of time limited blackbox is presented by Hohl, who defines that a mobile agent is a time limited blackbox, if:

1) for a certain known time interval

2) code and data of the agent specification cannot be read

3) code and data of the agent specification cannot be modified

4) attacks after the protection interval are possible, but these attacks do not have effects

Hohl also presents some mess-up algorithms to convert a mobile agent to a time limited blackbox. The main ideas of these algorithms are as follows: variable recomposition, conversion of control flow elements into value-dependent jumps, depositing keys to the third trusted hosts.

However, we propose another algorithm that can efficiently create a time limited blackbox out of an original mobile agent (which is not discussed in detail here). Such a blackbox is an agent that performs the same work as the original agent, but is of a different structure. Thus it can resist the attacks from malicious users in a certain agent protection time interval. The content provider then dispatches the blackbox to the user end to enforce DRM functions.

2.3 Countermeasure to Copyrights Infringement

Although many methods have been adopted to protect digital rights, copyrights infringement still possibly exists. So we must adopt the following measures once the infringement behavior happens:

① Add the malicious user to the black list and no longer distribute content to him;

② Notify this information to CA, CA will revoke the user's certificate after confirmation. Once the certificate is revoked, the malicious user can't use the service of the system any more.

2.4 Analysis of System Performance

The mobile agent is designed as a lightweight level program. It doesn't involve lots of information, so it can migrate between the content provider and user quickly and efficiently. After arriving at the user end, the main function of the mobile agent is to interact with the content rendering module and provide some information to decrypt and render the content. Thus the implementation is rather simple and efficient.

Because of the rights redistribution support in this system, the user whose digital rights belong to redistribution category can transfer his rights to other users. In this process, the encrypted content is distributed directly between the two users, which can lighten the burden of the content provider in content distribution and balance the network load.

Commonly, at the beginning of a session, a user needs to exchange and verify the certificate with the content provider. However, the content provider is generally considered a trusted service party, so a user needn't verify the certificate each time, which relieves the communication burden of users.

2.5 Analysis of System Security

1) Security of the roles

At the beginning of a session, the content provider and a user need to verify the identity of each other according to the identity certificate. The certificate status can be confirmed its validity by querying CA. So, the introducing of PKI and CA role can help us to construct a trusted communication process and to ensure the security of the roles.

Moreover, the content provider can lower the credit level of the user who has illegal behaviors, or notify that information to CA. The CA then decides whether or not to revoke the certificate of the user. This can efficiently restrain users from copyrights infringement.

2) Security of contents and rights information

The contents to be distributed are encrypted by an algorithm named AES, which can protect the security of the content if the safety of the decryption key can be ensured. The encrypted content can be decrypted and rendered only in the specific contents rendering module at the user end. Moreover, the decrypted content can't be saved. So the security of the content can be ensured.

The rights information of users is saved in the local database of the content provider, and he manages the users' rights according to the rights saved in this database. The malicious users can't get any profits from changing the rights information saved in their computer, which ensures the security of the rights information.

3 Comparison with Traditional DRM System

3.1 Rights Redistribution

Most traditional DRM systems emphasize the distribution of rights between the rights holders and common uses, but pay very little attention to rights redistribution. However, S.H.Kwok achieves rights redistribution by introducing a local DRM center (database), but this mode increases the complexity and burden of users, and it will lead to a security issue for common computers because it manages rights redistribution and generates peer certificate at the user end. Furthermore, the user who has redistributed his rights can recover his rights and redistribute his rights again by taking some measures like hard disk clone. Srijith K. Nair proposes setting up a trusted platform module based on hardware on the mobile handset to enforce DRM and rights redistribution, but the requirement to the hardware is rather high and it is quite impractical for common computers.

In this system, user rights information is saved in the content provider's local database, which is the basis for the content provider to enforce the DRM functions. No extra hardware or software is required for users' computers. Though this mode may bring some more burdens to the content provider, it ensures the profits of the content provider and the security of the system. Moreover，in the process of rights redistribution, the digital content is distributed directly between the two users, while the content provider only dispatches a mobile agent with smaller size. As a result, the burden of the content provider is greatly relieved and the whole system load is rather balanced.

3.2 System Security

In most existing DRM systems, a user must acquire a content rendering certificate before he can render the content. However, the certificate, which includes content decryption key, would be cracked by the malicious user if it was saved at the user end all the time. Once he gets the content decryption key, the malicious user will decrypt the content and illegally distribute it to other users without paying. This will cause serious copyrights infringement. However, in this system, the dispatched mobile agent is also a time limited blackbox which is created out of an original mobile agent. It is very difficult for malicious users to spy the time limited blackbox and acquire content decryption key in the certain agent protection time interval.

Besides, this system introduces PKI and adds a CA role compared to traditional DRM system. Through the certificate verification we can ensure the security of the session between the content provider and a user. CA can revoke the identity certificate of malicious users to protect the justice and security of the system.

4 Conclusion

DRM systems are used by content provider to restrict the ways the users use the content. This paper proposes a DRM system based on mobile agent for digital rights redistribution. In the system, the mobile agent dispatched by the content provider can fully represent his benefit and enforce DRM functions flexibly and honestly. The dispatched mobile agent is a time limited blackbox which is created out of an original agent. This can prevent it from spying attacks by malicious users in a certain agent protection time interval. The rights redistribution support can decrease the copyrights infringement by users and increases the motivations of users to distribute content. With the introducing of PKI and CA role, the security of communication session between the content provider and a user can be ensured after the certificate verification. The analysis and the comparison with traditional DRM system show that the proposed system is secure, efficient and simple to implement.

References

[1] Iwata T, Abe T, Ueda K, *et al*. A DRM System Suitable for P2P Content Delivery and the Study on its Implementation[C] //*The 9th Asia-Pacific Conference on Communications*. Piscataway: IEEE, 2003:806-811.

[2] Dhamija R, Wallenberg F. A Framework for Evaluating Digital Rights Management Proposals[C]//*The 1st International Mobile IPR Workshop: Rights Management of Information Products on the Mobile Internet*. Helsinki: Helsinki Institute for Information Technology HIIT, 2003: 13-21.

[3] Lin E T, Lagendijk R L. Advances in Digital Video Content Protection [C]//*Proceedings of IEEE, Special Issue on Advances in Video Coding and Delivery.* Piscataway: Institute of Electrical and Electronics Engineers Inc, 2005: 171- 182.

[4] Langeand D B, Oshima M. Seven Good Reasons for Mobile Agents[J]. *Communications of the ACM*, 1999, **42**(3): 88-89.

[5] Hohl F. A Model of Attacks of Malicious Hosts against Mobile Agents[J].*Lecture Notes in Computer Science,*1998, **1543**: 593-608.

[6] Hohl F. Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts[J]. *Mobile Agents and Security*, 1998, **1419**: 92-113.

[7] Sekim A, Kameyama W. A Proposal on Open DRM System Coping with Both Benefits of Rights-Holders and Users[C]//*Conference Record IEEE Global Telecommunications Conference*. San Francisco: Institute of Electrical and Electronics Engineers Inc, 2003: 4111-4115.

[8] Cheung S C, Curreem H. Rights Protection for Digital Contents Redistribution over the Internet[C]//*Proceedings of the 26th Annual International Computer Software and Applications*. Los Alamitos: IEEE Comput Soc, 2002:105-110.

[9] Kwok S H, Lui S M. A License Management Model to Support B2C and C2C Music Sharing [EB/OL]. [2008-01-03]. *http://www*10*.org/cdrom/posters/*1008*.pdf*.

[10] Nair S K, Popescn B C, Gamage C, *et al*. DRM preserving Digital Content Redistribution[C] //*Proceedings - Seventh IEEE International Conference on E-Commerce Technology, CEC* 2005. Piscataway: Institute of Electrical and Electronics Engineers Computer Society, 2005: 151-159.

[11] Boldyreva A, Fischlin M, Palacio A, *et al*. A Closer Look at PKI: Security and Efficiency[C]//*Public Key Cryptography PKC* 2007 10*th International Conference on Practice and Theory in Public-Key Cryptography.* Berlin: Springer-Verlag, 2007: 459-475.

□