LICENSE MANAGEMENT SCHEME WITH ANONYMOUS TRUST FOR DIGITAL RIGHTS MANAGEMENT*

Jiang Zhang, Bin Li, Li Zhao, Shi-Qiang Yang

Department of Computer Science , Tsinghua University, Beijing China
{zhang-jiang03, libin98, zhaoli}@mails.tsinghua.edu.cn, yangshq@tsinghua.edu.cn

ABSTRACT

One of the major issues raised by Digital Rights Management systems concerns the protection of the user's privacy and anonymous consumption of content. However, most existing license management schemes for DRM systems do not support the protection of user privacy. Moreover, some other schemes such as PrecePt can only bind the license with a specified device though they concern privacy protection. In this paper, we propose a license management scheme named LMSAT (License Management Scheme with Anonymous Trust) which provides a more powerful and flexible license acquisition and usage tracking scheme to allow the user access the contents anytime, anywhere, and on any compliant devices anonymously.

1. INTRODUCTION

Digital Rights Management (DRM) is the technology to distribute digital contents in a secure manner that can protect and manage the rights for all participants in contents distribution value-chain including producers, providers, distributors, and consumers [1]. Most existing DRM systems such as MS DRM [2] and InterTrust DRM [3] focus on protecting copyrights of digital contents to prohibit illegal copy and illegal distribution of digital contents and to let only authorized users use the contents. However, these DRM systems have not concern the protection of user's privacy because it is not necessary for fraud prevention. The user's private information is easily revealed through user authentication in license acquisition and usage tracing for fraud prevention [4]. Thus, user's privacy has been compromised. To be successful among the users whose privacy awareness is growing rapidly, DRM systems need to protect the user's privacy along with the rights of content providers. A license management protocol named PrecePt [5] which provides the user's privacy protection has been proposed. But in PrecePt, the license is bound to a specified device, which does not conform to the requirements of some users to use digital contents anytime, anywhere, and on any device.

Privacy enforcement technique in DRM includes encryption and anonymity. In this paper, we propose a license management scheme with anonymous trust named LMSAT which provides a powerful license acquisition and usage tracking scheme to allow the user access the contents anytime, anywhere, and on any compliant devices anonymously. The user buys a token with a secret Anonymity ID (AnonymityID) and corresponding password on it anonymously from the provider through a mechanism such as the pre-payment scheme in advance, and then the user can request a license bound to the Anonymity ID. The Anonymity ID is a string of random binary digit which represents an anonymous account. When the user requests the license of the digital contents, he can input the Anonymity ID and corresponding password according to the requirements of DRM system, and then the DRM system will charge the anonymous account for the corresponding contents. In the usage tracking phase, Anonymity ID, rather than user's private information, is needed. Moreover, the user can use the contents anytime, anywhere, and on any compliant devices using the token with the Anonymity ID, which enhances the use convenience and flexibility. In the present context, the compliant device is a device which complies with a given standard and can identify the Anonymity ID in the token.

The rest of this paper is organized as follows: In Section 2, we introduce the DRM system model for the LMSAT scheme. In Section 3, we propose the LMSAT scheme. In Section 4, we present the performance analysis of the LMSAT scheme and draw a comparison analysis with previous work. Finally, in Section 5, we conclude the paper.

2. DRM SYSTEM MODEL FOR THE LMSAT SCHEME

The DRM system model (shown in Fig.1) for the LMSAT scheme contains four main participants: Content

* Supported by the National Natural Science Foundation of China under Grant No.60432030

Producer, Content Provider, Clearing House (CH) and Client. Each participant has authenticated public-private key pair and public key certificate through DRM Certification Authority (CA) [6]. Content Producer delivers protected contents to Content Provider. A user requests one favorite content from Content Provider's server, and then Content Provider delivers the protected content to Client. The content received by Client can not be used without a valid license because of encryption. When the user pays money and starts a license acquisition protocol with CH for the content through DRM Agent (DA) in the Client, the client can get the corresponding license for the content from CH, and then the content can be rendered according to the usage rules in the license.

DA is an agent loaded in the Client device which pays for the content, acquires a license from CH, authenticates the license and the content, decrypts the protected content, enforces the rights, and reports to CH for usage. DA works in a trusted DRM environment which ensures the authenticity, integrity, and confidentiality of the content and the usage rules [7].

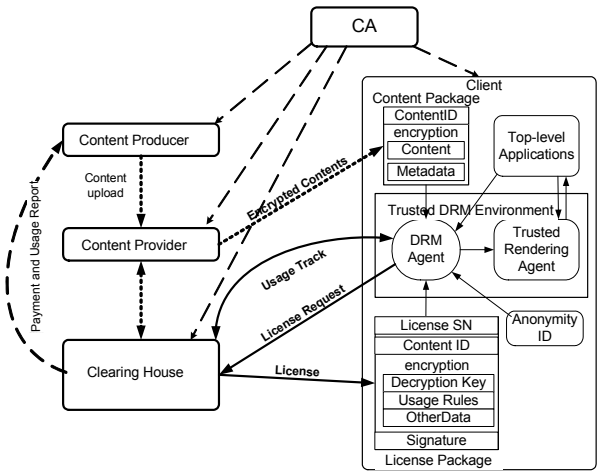

Fig.1 DRM system model for the LMSAT protocol

3. LMSAT: LICENSE MANAGEMENT SCHEME WITH ANONYMOUS TRUST

The proposed license management scheme comprises two parts which are license acquisition phase and usage tracking phase. In the license acquisition phase, DA acquires a license through running license acquisition protocol. In the usage tracking phase, CH receives the report of the content usage from DA.

3.1. Basic Assumptions

The paper makes the following assumptions for LMSAT:

- Every participant in the DRM system model knows all cryptography algorithms used in this scheme.
- Every participant has an authenticated public-private key pair and the public key certificate through DRM Certification Authority (CA).
- The user has paid for the content, and the user gets a Anonymity ID (AnonymityID) through the payment phase.
- Anonymity ID can only be read and identified by DA securely, and attackers can not get the information.
- The license stored in Client can be only authenticated and manipulated by DA. DA works in a trusted DRM environment which ensures the authenticity, integrity, and confidentiality of the contents and the license.

3.2. License Structure

The license has the following parameter: the license sequence number (SN), the requested content ID (ContentID), the encryption result of the information including the decryption key for the protected contents (DecryptionKey), the usage rules (UsageRules) which is chosen from a number of offered usage possibilities by the user, and the other information (OtherData) using K_B as the key, and the signature of CH which ensures the authenticity and integrity of the license. K_B which acts as the symmetric private key for encrypting the important information in the license is defined as H(AnonymityID || ContentID), where H is the hash function, the symbol || indicates concatenation of strings.

$$License = \{SN, ContentID, [DecryptionKey, UsageRules, OtherData]_{K_B},$$
$$Sig_{CH}(H(SN, ContentID, [DecryptionKey, UsageRules, OtherData]_{K_B}))\}$$

3.3. Elliptic Curve Diffie-Hellman (ECDH)

Elliptic curve cryptography is a relatively new family of public-key algorithms which offers similar security to other public key algorithms in use today such as RSA but with smaller key sizes and memory requirements [8] [9]. Elliptic curve Diffie-Hellman (ECDH) is popular key agreement method which transforms DH algorithm into an elliptic curve . In the elliptic curve Diffie-Hellman (ECDH) key agreement, the two communication parties server S and client C agree beforehand to use the same curve parameters set T={p, a, b, G, n, h}. They each generate their temporal private keys S_S and S_C , respectively, and the corresponding temporal public keys $Q_S = S_S$ G and $Q_C = S_C$ G. Both the client and server exchange their temporal public keys, and each multiplies its private key with other party's public key to compute a common session key K= S_S $Q_C = S_C$ $Q_S = S_S$ S_C G. An

attacker cannot determine this session key from the curve parameters.

3.4. License Acquisition Phase

Fig.2 shows that DA acquires a valid license bound to AnonymityID from CH.

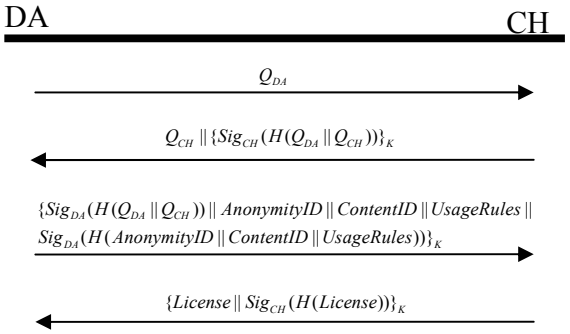

Fig.2 License Acquisition Protocol

In the first step, DA generates a temporal private key S_{DA} and computes the corresponding temporal public key as $Q_{DA} = S_{DA}G$. Next, DA sends Q_{DA} to CH.

In the second step, CH generates a temporal private key S_{CH}, computes $Q_{CH} = S_{CH}G$, and computes the session key $K = S_{CH}Q_{DA}$. Next, CH signs $H(Q_{DA} \| Q_{CH})$ and encrypts $Sig_{CH}(H(Q_{DA} \| Q_{CH}))$ using K as key, and sends Q_{CH} with the encryption result to DA.

In the third step, DA computes the session key as $K = S_{DA}Q_{CH}$, decrypts the message, verifies the signature Sig_{CH} by using $Cert_{CH}$, and verifies $H(Q_{DA} \| Q_{CH})$. If the verification is successful, DA signs $H(Q_{DA} \| Q_{CH})$, gets the information such as the Anonymity ID(AnonymityID), the requested content ID (ContentID), and the requested usage rules (UsageRules), and signs *H(AnonymityID || ContentID || UsageRules)*. They are encrypted by *K* as key, and then DA sends the result to CH.

In the last step, CH decrypts the message and verifies $Sig_{DA}(H(Q_{DA} \| Q_{CH}))$. If the verification is successful, CH verifies Sig_{DA}(H(AnonymityID||ContentID||RightsInfo)) and checks whether the user is legal or not according to AnonymityID. If the authentication is successful, CH generates a license including the license sequence number (SN), ContentID, and the encryption result of important information such as the corresponding decryption key (DecryptionKey) for the protected content and the usage rules (UsageRules) that indicates the rights the user has concerning usage of the content using K_B = *H(AnonymityID || ContentID)* as key, and signs *H(License)*. Next, CH encrypts the license and the signature using *K* as key, and sends the result to DA.

When the message including the license is received by DA, DA decrypts the message and verifies $Sig_{CH}(H(License))$. If the verification is successful, DA then gets the license sequence number, the content ID, and decrypts the information including DecryptionKey and UsageRules in the license using K_B = *H(AnonymityID || ContentID)* as key. Thus, DA gets the corresponding decryption key of the protected content specified by ContentID, and can decrypt the protected content and send the decrypted content to the trusted rendering agent for rendering.

3.5. Usage Tracking Phase

In many business models such as ownership, rental, subscription, pay-per-view, and promotion, it is necessary to collect the content usage information for fraud prevention. In LMSAT scheme, CH receives the report of the content usage information from DA in Client. The usage information should be protected by encryption to avoid revealing user's privacy. Fig.3 shows the usage tracking protocol between CH and DA.

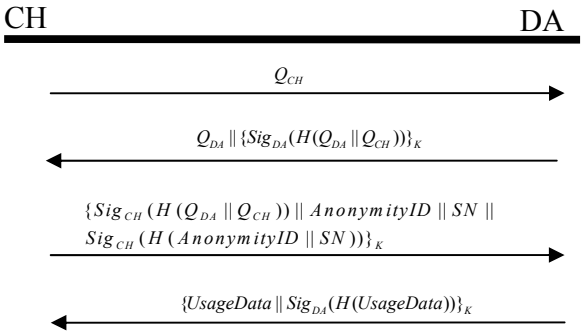

Fig.3 Usage Tracking Protocol

In the first step, CH generates a temporal private key S_{CH} and computes the corresponding temporal public key as $Q_{CH} = S_{CH}G$. Next, CH sends Q_{CH} to DA.

In the second step, DA generates a temporal private S_{DA}, computes $Q_{DA} = S_{DA}G$, and computes the session key $K = S_{DA}Q_{CH}$. Next, DA signs $H(Q_{DA} \| Q_{CH})$ and encrypts $Sig_{DA}(H(Q_{DA} \| Q_{CH}))$ using *K* as key, and sends Q_{DA} with the encryption result to CH.

In the third step, CH computes the session key as $K = S_{CH}Q_{DA}$, decrypts the message, verifies the signature $Sig_{DA}(H(Q_{DA} \| Q_{CH}))$. If the verification is successful, CH signs $H(Q_{DA} \| Q_{CH})$, gets the information including

the Anonymity ID(AnonymityID) and the license sequence number (SN) which CH wants to track, and signs *H(AnonymityID || SN)*. They are encrypted by *K* as key, and then CH sends the result to DA.

In the last step, DA decrypts the message and verifies $Sig_{CH}(H(Q_{DA} \| Q_{CH}))$ and Sig_{CH}(H(AnonymityID||SN)) . If the verification is successful, DA collects the usage information (UsageData) according to AnonymityID and SN, and signs *H(UsageData)*. Next, DA encrypts the UsageData and the signature using *K* as key, and sends the result to CH.

4. SCHEME ANALYSIS AND COMPARISON

The goal of LMSAT is to provide a powerful license acquisition and usage tracking scheme to protect user's privacy and allow the user access the contents anytime, anywhere, and on any compliant devices. The proposed scheme achieves user privacy towards the content provider through anonymous buying of the User Rights. The user can access his contents anytime, anywhere, on any compliant device using his token with Anonymity ID because the licenses are bound to the Anonymity ID.

The important information including DecryptionKey, UsageRules, and OtherData in the license is encrypted by K_B , $K_B = H(AnonymityID \| ContentID)$. So only the user with a correct AnonymityID can compute the correct key according to his AnonymityID and the ContentID. An attacker can not decrypt the important information in the license and render the corresponding content even if he gets the content and the license.

LMSAT can prevent a user to share his Anonymity ID and licenses with other unauthorized users. The license is bound to the Anonymity ID which represents an anonymous account, so when the user distribute his Anonymity ID to let others consume the protected contents, the DRM system will charge the anonymous account bound to the Anonymity ID for the consumed contents.

LMSAT uses the ECDH key agreement scheme to establish a secure communication channel between DA and CH, which ensures the security of data transferred between DA and CH. Thus, LMSAT can defense against a malicious attacker and protect user's privacy.

In Table.1, we compare the analysis results of our proposed scheme (LMSAT) with those of other DRM systems, such as PrecePt, MS DRM, and InterTrust DRM. Key distribution of the above schemes uses public key cryptography except InterTrust DRM which uses both public and secret key cryptography. InterTrust DRM uses server-based key management, however, LMSAT, PrecePt, and MS DRM use the distributed key management which can cause more stabilization. All of the schemes support copyright protection, but only LMSAT and PrecePt provide user privacy protection. Furthermore, LMSAT allow the user access the contents anytime, anywhere, and on any compliant devices using the token with the Anonymity ID, which enhances the use convenience and flexibility.

Table.1 Comparison with Other DRM Schemes

	LMSAT	**PrecePt**	**MS DRM**	**InterTrust DRM**
License Form	separately	separately	separately	with content
Key Distribution	Public Key	Public Key	Public Key	Hybrid
Key Management	distributed	distributed	distributed	server based
Copyright Protection	high	high	high	high
User Privacy	high	high	low	low
Use Convenience	high	low	high	high

5. CONCLUSION

The present DRM systems and frameworks are vulnerable in user privacy infringement or short of use convenience. In this paper, we propose a powerful license management scheme with anonymous trust, LMSAT, which provides a license acquisition and usage tracking scheme to protect user's privacy and allow the user access the contents anytime, anywhere, and on any compliant devices.

6. REFERENCES

[1] J. Dubl and S. Kevorkian, "Understanding DRM System: An IDC White Paper", IDC, 2001.

[2] Microsoft: http://www.microsoft.com/windows/windowsmedia/drm/default.aspx.

[3] InterTrust: http://www.intertrust.com.

[4] P. Vora, D. Reynolds, L.Dickinson, J.Erickson, and D.Banks, "Privacy and Digital Rights Management", Proceedings of the W3C Workshop on Digital Rights Management, January. 2001, pp.22-23.

[5] B. Park, J. Kim, and W. Lee, "PrecePt: A Privacy-Enhancing License Management Protocol for Digital Rights Management", Proceedings of AINA'04, 2004.

[6] S. Brands, "Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy", MIT Press, August. 2000.

[7] Thomas S. Messerges and Ezzat A. Dabbish, "Digital Rights Management in a 3G Mobile Phone and Beyond", Proceedings of the 2003 ACM workshop on Digital rights management, Washington DC, USA, October. 2003, pp.27-38.

[8] S. Kumar, M. Girimondo, and A. Weimerskirch, "Embedded End-to-End Wireless Security with ECDH Key Exchange", 46th IEEE Midwest International Symposium on Circuits and Systems, 2003.

[9] Torii. Naoya, Yokoyama. Kazuhiro, "Elliptic curve cryptosystems", Fujitsu Scientific and Technical Journal, v36, n2, 2000, pp. 140-146.