An Efficient Wrapper-based Digital Rights Management

Wei-Chen Wu[1]*, Horng-Twu Liaw[2]
[1]*Computer Center, Hsin Sheng College of Medical Care and Management, Taoyuan County, Taiwan, R.O.C.*
wwu@hsc.edu.tw
[2]*Department of Information Management,Shih Hsin University, Taipei, Taiwan, R.O.C.*
htliaw@cc.shu.edu.tw

Abstract

In this paper, we propose a novel digital publication issuing mechanism, which supports business model, and implemented the system. In this mechanism, we adopted API-HOOK to avoid changing habits of customers. However, the properties of digital contents make themselves be easily copied and transferred if there is not any proper protection for them. Hence, it is a critical issue for publication provider to effectively control and distribute their digital publications. Digital Rights Management is a mechanism, which might congregate various techniques to protect the rights of digital publication from copyrights violations. Moreover, Wrapper-based Digital Rights Management technique applies encapsulating digital contents by packaging content and monitoring by API-Hook to control and protect them, which provide a way to authenticate users by users' machine serial number or smart card via network. Hence, users may use the digital contents without changing their digital content player. According to the definition of Digital Rights Management, this paper provides a digital publication issuing mechanism, which supports superdistribution for advertising digital publications effectively and improving development of digital contents.

Keywords:*Digital rights management; API-hook; Wrapper; Superdistributation; Business model.*

1 Introduction

With the rapid development of the Internet and computers, more and more digital documents and digital products weed through the old to bring forth the new unceasingly. It is essential to protect digital contents, which will improve the intention of digital contents providers to create new products and protect the rights of legal customers.
Digital Rights Management (DRM) is a mechanism, which congregates hardware and software to ensure the rights of digital publication providers against illegal usage [1]. The DRM could track and manages the usage of digital contents, such as the legality of copy or distribution. However, some prevailing systems, such as Windows Media Rights Manager, iTunes, and Adobe Systems, only support their own digital content types. These systems do not provide interoperability, which limits the usage of digital contents with many restrictions.

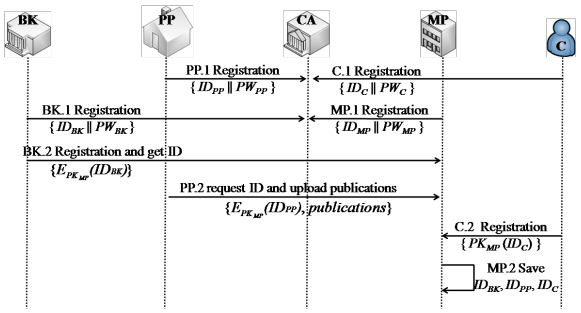

Figure 1. The processes of Certificate Requesting and Registration Phase

The concept and architecture of Superdistribution is proposed by Mori [2, 3] for building up a software service system in a P2P structure. Superdistribution could also be a business model, which distributes digital publications safely and effectively by combining some free methods [4, 1].

There are some advantages would be obtained if DRM supports superdistribution, such as progressing distribution channels, reducing distribution costs, and forming strong partner networks. In this paper, we will adopt Windows32 API hooking for it is more inexpensive than designing DRM system with expensive hardware. Under the assumption of payment flow has been well implemented, we implement the DMR system on Windows 32-bit platform. The rest of this paper is organized as follows. We propose a novel wrapper-based digital publication issuing mechanism in Section 2. In Section 3, Implementation is presented. Finally, a conclusion is presented in Section 4.

2 Our Scheme

We propose a secure, fair and effectively distributing digital publications issuing mechanism for the systems lacking of business models and charging mechanisms to solve the problems of digital publications being transacted on the Internet.

In our mechanism, we adopts Elliptic Curve Cryptography (ECC) [5], KryptoKnight authentication and key distribution system [6] to protect customers' personal information, and add a trusted third party call certificate authority to issue licenses and to support fair judgment in transactions if necessary. The original business mode of DRM is still kept in our mechanism for easily adapting the rights of new customers. The major five roles of this mechanism are described as follows: Customer(C),Certificate Authority (CA),Digital Publication Provider(PP),Digital Publication Rights Issuing Management Platform(MP) and Bank(BK). Our mechanism contains the following seven phases:

1. Certificate Requesting and Registration Phase: This phase is an initial phase, all roles of this mechanism must register to CA and request certificates. After registration, PP assigns the basic grants for superdistribution and transfers the grants of digital publications to XrML format. Then, PP sends digital publications and XrML to MP through a secure channel. Fig. 1 shows the detailed processes.
2. Superdistribution Phase: The potential customer C_N could receive a protected digital publication shared by original customer C_O through email, instant message, or P2P. C_N can use the publication with basic grants. Fig. 2 shows the detailed processes.

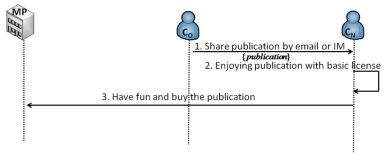

Figure 2. The processes of Superdistribution Phase

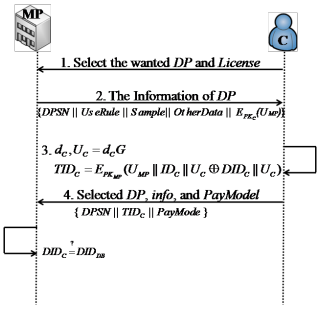

Figure 3. The processes of Publication Selecting and Authentication Phase

3. Publication Selecting and Authentication Phase: After the customer finishes registration and gets the certificate, the customer could get publications from the website of MP or by superdistribution. The Customer C sends request containing wanted publication identity and wanted grants to MP. Fig. 3 shows the detailed processes.
4. License Issuing Phase: After payment, the customer can request the license to enjoy the publication. The detailed processes are shown as Fig. 4. C sends $TradeOK_C$(a success message of X's transaction) to MP for requesting the license.
5. Tracking Phase: Regardless of online or offline patterns, DRM controller must record and trace the processes of how users enjoy publications for protecting the publications. Fig. 5 shows the detailed processes.
6. Customers' License Transferring Phase: In order to handle various modes of transactions, we support license transferring services for flexible use of valid licenses. Fig. 6 and 7 show the detailed processes.
7. Rights Transferring Phase: There are various business models in commercial circumstances. Considering the demands of providers, they may transfer their rights to others. For example, some enterprises may find business opportunities from some digital publications and then buy out them. Moreover, the transferred target must be the member of this mechanism. The detailed processes are shown as Fig. 8.

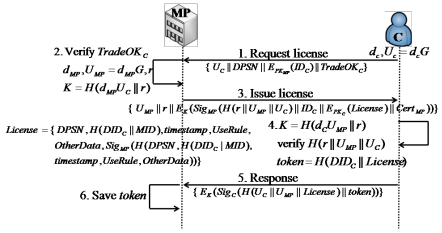

Figure 4. The processes of License Issuing Phase

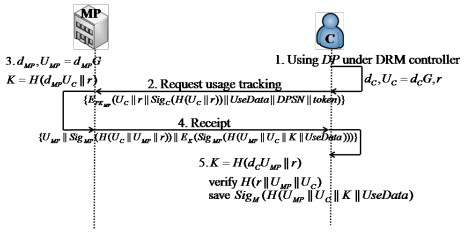

Figure 5. The processes of Tracking Phase

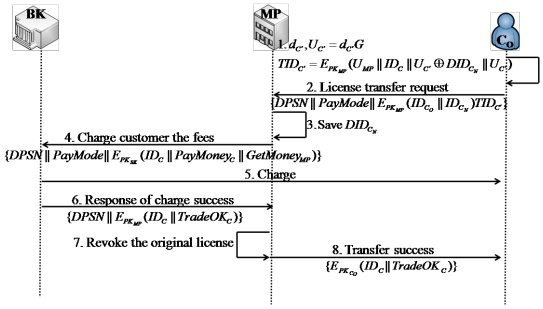

Figure 6. The processes of Customers' License Transferring Phase

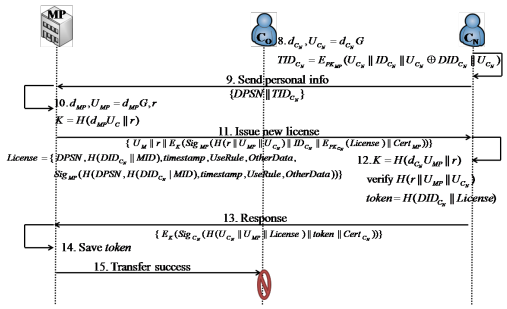

Figure 7. The processes of Customers' License Transferring Phase (Cont.)

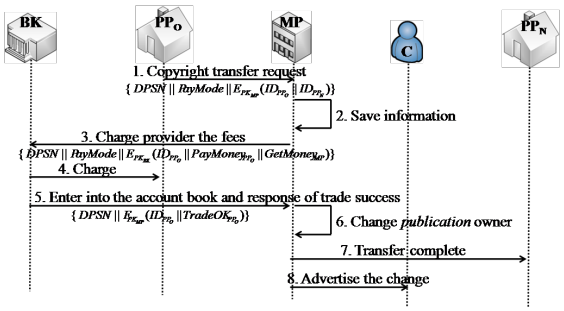

Figure 8. The processes of Rights Transferring Phase

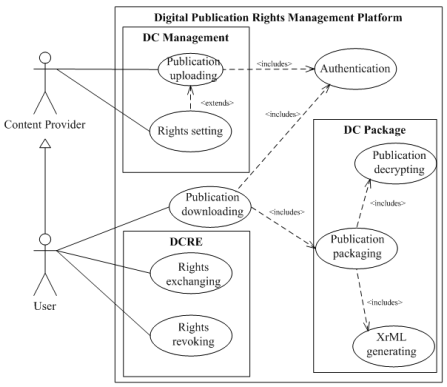

Figure 9. The modules and functions in digital publication rights management platform

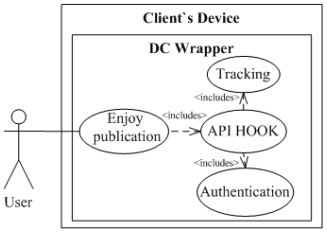

Figure 10. The functions of DC Wrapper

3 Implementation

This research implements a sample of DRM system for protecting digital publications. The implementation contains following features: reaching integrity and security by wrapping; monitoring processes by API HOOK; describing digital rights language with XrML. Moreover, this system allows various authentications, including both online and offline authentication with device identity of hardware or smart card. This section displays the architecture of this system.

There are four functional modules in this system shown as Fig. 9 and 10 , including Digital Content (DC) Management, DC Package, DC Wrapper, and DC Rights Exchange (DCRE). Furthermore, DC Management, DC Package, and DCRE are the modules of digital publication rights issuing management platform. DC Wrapper is the module of clients and it starts when they use the services of digital publications. The followings describe the functions of each module:

1. DC Management
   This module provides publication uploading and rights setting, such as the print right, use times, and use durations, etc.

2. DC Package
   What the providers hope are distributing their publications effectively and make money. Furthermore, customers must be authenticated and paid for their publications. This system decrypts digital publications for avoiding unauthorized use. Moreover, we package the contents to a new file, including decrypted publication,

copyright information, rights expression language, and API HOOK module. In addition, we support marketing grants and basic grants for supporting superdistribution. In addition, above makes rights exchanging and rights revoking more easily. Besides, this implementation provides convenience of user-friendly interface under API HOOK by adopting MFC.

3. DCRE
   This system supports rights exchanging and rights revoking. As mentioned above, this research allows providers think more about business models.

4. DC Wrapper
   We adopt API HOOK to monitor processes. Customers need not to install plug-in and change their habits.

4 Conclusion

In this paper, we proposed a novel digital publication issuing mechanism, which supports business model, and implemented the system. In this mechanism, we adopted API-HOOK to avoid changing habits of customers. The mechanism inherits all advantages of the research of Liaw et al. [7]. In addition, we proposed the concept of DRM controller, such that Digital publication could be distributed effectively and securely under such protection.

References

[1] Ku, W., Chi, C.: Survey on the technological aspects of digital rights management. Information Security (2004) 391–403

[2] Liu, Z., Wang, B., Lee, B., Han, M.: Security license distribution mechanism for rights delegation models of group distribution between consumers. In: Computational Science and its Applications, 2007. ICCSA 2007. International Conference on, IEEE (2007) 144–152

[3] Mori, R., Kawahara, M.: Superdistribution: the concept and the architecture. IEICE TRANSACTIONS **1976** (1990)

[4] Liu, Q., Safavi-Naini, R., Sheppard, N.: Digital rights management for content distribution. In: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21, Australian Computer Society, Inc. (2003) 49–58

[5] Barker, E., Johnson, D., Smid, M., of Standards, N.I., (US), T.: Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Cryptography:(revised). National Institute of Standards and Technology (2007)

[6] Molva, R., Tsudik, G., Van Herreweghen, E., Zatti, S.: Kryptoknight authentication and key distribution system. Computer SecurityESORICS 92 (1992) 155–174

[7] H.T. Liaw, J.F. Lin, W.L.S.L., Lin, C.: Digital publication right issuing management practice mechanism. Journal of e-Business **9** (2007) 321–352