Enabling Secure Digital Marketplace

Hongxia Jin
IBM Almaden Research Center
jin@us.ibm.com

Vladimir Zbarsky
IBM Almaden Research Center
zbarsky@us.ibm.com

ABSTRACT

The fast development of the Web provides new ways for effective distribution of network-based digital goods. A digital marketplace provides a platform to enable Web users to effectively acquire, share, market and distribute digital content. However, the success of the digital marketplace business models hinges on securely managing the digital rights and usage of the digital content. For example, the digital content should be only consumable by paid users. This paper describes a Web-based system that enables the secure exchange of digital content between Web users and prevents users from illegally re-sell of the digital content. Part of our solution is based on broadcast encryption technology.

Categories and Subject Descriptors:K.6.5 [Management of Computing and Information Systems][Security and Protection]

General Terms: Security, digital content, marketplace

Keywords: DRM, content protection, security, download

1. INTRODUCTION

The fast development of the Web provides new ways for people to exchange goods. Web 2.0 companies like Ebay provide platforms that enable Web users to become a buyer/seller and exchange their goods. It provides an online marketplace for people. In this type of business model, the marketplace provider derives most of its revenue by charging a service fee for each buy/sell transaction that is done through its Website. On the other hand, more and more people are producing and consuming content in digital form, for example, software, digital document or video/audio. Unfortunately different from a physical good that can be sold to only one buyer, digital good can be easily copied and sold to many buyers. While it helps driving more legitimate sales, it also allows potential illegal re-sells of the copies of the digital goods. So a digital marketplace must provide security features that ensure only the paid buyers can acquire and consume the digital content. Only then people can be motivated to produce and sell their digital content online.

As a concrete example, one can imagine a web user who produces a video clip teaching how to do a certain thing. Another Web user might be looking for ways to learn how to do that. A digital marketplace would provide secure and effective exchange of digital learning content.

We classify the marketplace scenarios into two different cases. In one case the acquired content is restricted to only display on one particular device. In the other case the acquired digital content can be displayed/rendered on multiple and maybe different type of devices. For example, a user wants to run the purchased software on multiple machines, or playback the purchased video content on different types of devices. In this paper we will show a system that can enable secure digital marketplace in both cases. The main design goal is to prevent people from making copies and resell copies illegally.

2. OUR SYSTEM

Our system mainly involves three parties, the marketplace provider (the server), web users as content producers/sellers (client) and web users as content consumers/buyers (client). Figure 1 illustrates a transaction process at high level.

As a first step of the transaction process, the selling client uploads his content to the server where the content will be encrypted and packaged. The uploaded content will be encrypted with a randomly picked key called title key. The title key will also be encrypted and reside together with the encrypted content. Once the content and its title key are encrypted, it can be stored securely in the backend repository. Of course storing the content and the title key in their encrypted form does not require special storage. In the meanwhile, the preview or introduction of the digital content is displayed and advertised on the server web site.

When the buying client identifies the content he wants to purchase from the server website, he will connect to the repository to download the encrypted content together with its encrypted title keys (step 2). In our system we will rebind the title key to the buying client (step 3 and 4). This will prevent people from illegally re-sell the content. The calculation that binds the title key to the client is performed on the server side, not on the client side. We call the server that performs this function the clearing house. The marketplace provider can also function as the clearing house.

How does the clearing house learn the title key in order to bind the title key? Well, when the content is packaged and encrypted, the title key is encrypted with a key that is agreed upon between the clearing house and the server who packages the content. Different ways may be used to encrypt the title key. A simple way would be encrypting the title key with the server's public key. After the buying client downloads the packaged content, it extracts the encrypted title key from the packaged content.

In the case that only one machine is allowed to playback

WWW 2008, April 21–25, 2008, Beijing, China.
ACM 978-1-60558-085-2/08/04.

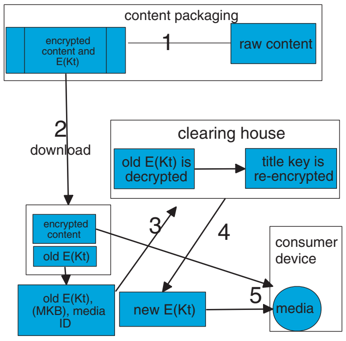

Figure 1: High level overview

the purchased content, the buying client will first make the payment, then send the encrypted title key together with its machine specific information (e.g., ID) to the clearing house (step 3). The payment could be made to the clearing house or directly to the selling client. In either case, once the payment is confirmed, the clearing house will decrypt the encrypted title key using the key that was initially agreed upon with the content packaging server. The clearing house then derives a machine unique key based on the machine specific information using an one-way function and re-encrypts the title key using the machine unique key. The re-encrypted title key is sent back to the buying client (step 4). Only on the specified playback machine the buying client can derive the machine unique key and decrypt the title key to decrypt the content.

In a more generic case, the purchased content can be consumed on multiple devices. Those devices may not be even known when the content is purchased. In order to enable this, we utilize a technology called broadcast encryption [1].

2.1 Broadcast Encryption

A broadcast encryption scheme is a key management technology that allows a piece of content to be accessible only by a subset of privileged/enabled users and not the revoked/disabled users. When a user is found non-compliant he/she will be excluded from future content access. The structure that enables exclusion/revocation of users is called Media Key Block (MKB). MKB can enable very compliant device to calculate a key that ultimately derives the title key to decrypt the content. Any non-compliant device will not be able to process MKB and derive the key to access content. Unlike a public key system, a broadcast encryption system is not identity based. As long as a device is compliant, he can process MKB and ultimately access content. It has been used in Content Protection for Recordable Media [2].

2.2 Binding title key to the media

We believe it is possible to use broadcast encryption scheme to enable purchased content be consumable by multiple devices. We burn the purchased content onto a physical recordable media and bind the title key to the media. The media contains in it a MKB created by the clearing house, and each playback device is a user in a broadcast encryption scheme.

In order to bind the title key to the media, the buying client not only needs to send to the clearing house the initially encrypted title key but also the MKB and media ID information extracted from the recordable media (step 3). The clearing house will calculate the media key out of the MKB and derive a media unique key from the media key and the media ID. The clearing house will re-encrypt the title key with the media unique key (step 4). The buying client will burn the downloaded encrypted content and the new encrypted title key to the recordable media (step 5). This media can be played back at any compliant device because any compliant device can process MKB and decrypt the title key to decrypt the content. But any copies of the media will not work because the content encrypting key (the title key) is bound to the particular media.

3. KEY FEATURES AND CONCLUSIONS

In this paper we described a system that provides a marketplace that enables web users to exchange digital content securely. The first main feature in our system is that the content is stored encrypted; and the content encrypting key (title key) itself is stored encrypted together with the content. Second, it provides ways to prevent illegal re-sale of the content. We achieve this by binding the title key to a particular machine or a piece of physical media. Third, in our system, the clearing house which does the title key binding can be placed anywhere that the client can access. It does not have to be tied to the repository that stores the content. The clearing house does not have to interact with the content server and does not have to know the content. This simplifies the design of the clearing house. The clearing house and the content server can even be two independent entities. Moreover, in order to prevent illegal reselling of the decrypted content which is of course more bandwidth-consuming for attackers but might allow them stay anonymous, we can easily add a feature similar to [4]. Basically different devices will be bound to the different variations embedded in the content. Those variations allow identification of which copy of the content has been re-distributed.

We discussed two business scenarios. In one scenario the acquired content is bound to a particular machine/device. In another scenario the acquired content is bound to a physical media but can be consumed in multiple devices. In later scenario we used broadcast encryption technology which has been used in traditional settings to protect the large amount of content produced by small number of producers [3].

As future work we want to improve the system by taking into considerations of the unique setting of the new Web paradigm in which there exist large number of content producers (e.g., web users) each producing small number of content (e.g., video clips). While our preliminary system design shows some similarities with traditional content protection system setting. We believe the uniqueness of the new Web setting may deserve a different system design.

4. REFERENCES

[1] A. Fiat and M. Naor, “Broadcast Encryption,” *Crypto'93*, LNCS Vol. 773, pp480-491. Springer, 1993.

[2] www.4centity.com

[3] CPRM Specification, CPRM Network Download

[4] H. Jin, J.Lotspiech and S.Nusser, ”Traitor tracing for prerecorded and recordable media”, *ACM DRM workshop*, pp.83-90, Washington.DC.2004.