Digital Rights Protection Management of Web Portals Content

Theodoros Evdoridis
University of the Aegean, Greece

Theodoros Tzouramanis
University of the Aegean, Greece

INTRODUCTION

Without doubt one of the most important factors that contributed to the wide acceptance and popularity of Web portals is the potential for users to access a broad spectrum of information from a single access point, the Web portal itself. A Web portal, in such a way, aggregates information from multiple sources and makes that information available to various users. Regardless of whether the offered assets are hosted within the Web portal or whether the latter serves as a gateway to information services and resources located on the rest of the Internet, a Web portal is simultaneously an all-in-one Web site and a browsing guide to all available Internet information worldwide. Even though there is no definite taxonomy of portals, relevant labels such as government, community, enterprise, general and others are offered aiming at defining the Web portal with respect to its content and its target group. Summarizing, it could be assumed that a Web portal offers centralized access to all relevant content and applications (Tatnall, 2005).

On the other hand, the ability to create, host and distribute digital material, one of the key features of digital technology that a Web portal utilizes and derives its huge success from, proved to be a double edged sword since it allowed zero cost reproduction of the digital material for purposes of piracy. Piracy of relevant digital material offered by a Web portal is common today and it has posed significant problems in terms of financial losses to the owners of digital content that is offered through it. This explains why the owners of digital content hesitate to place their work on a Web portal where they may be illegally copied and distributed.

Nonetheless, the advantages of adopting this idea and applying it securely in practice are considerable from both customer and owner perspectives. That is why effective copyright protection techniques must be employed in order to convince the owners of digital material to allow their assets to be hosted on the Internet and especially on Web portals. The latter are highly attractive to the new world and are considered to be the meeting point for all technologically oriented people with a mind to purchase something.

This is where digital rights management (DRM) comes into play, employing a set of technical means to control illegal distribution of the aforementioned material and to protect the intellectual property of the original owners (Guenette, Gussin, & Trippe, 2001). Furthermore DRM aims to protect the rights of the users who legitimately purchased the digital material from the original owners.

This article surveys the most effective watermarking techniques available for every multimedia and database entry that requires copyright protection within a Web portal. Subsequently, the most commonly encountered code obfuscation methods for software objects will be discussed. The conclusion will present views for the future of DRM in the territory of Web portal applications.

BACKGROUND

While copyright infringement existed in the predigital era, the digital age may have increased the ease and scope with which copyright material can be copied.

DRM is often confused with the term access control. The difference lies into the domain where the content is being protected. Access control techniques apply when the content resides in the copyright owner's space and DRM techniques apply when the content is located in the customer's space where it can be freely accessed and examined extensively. This is why copyright protection through DRM is considered much more complicated and hard to achieve.

Apple Computers on April 28, 2003 introduced the iTunes Music Store, an online music service that, by January 2006, has sold over 850 million songs worldwide, which accounts for over 80% of digital music sales (Drmwatch.com, 2005). The service has attracted the interest of many companies with respective Web portals which either included it as part of their array of services such as America Online, or which designed a service of their own, such as Microsoft's MSN music service (Music.msn.com, 2006) to counter the former. America Online's music service through the iTunes music store utilizes a technique called FairPlay (Music.aol.com,

2006). FairPlay will allow a protected track to be copied exclusively onto Apple Computer's iPod, portable music players. In addition, the protected track may be played on up to five authorized computers simultaneously and may be copied onto a standard CD audio track any number of times.

This raises another question related to the DRM issue concerning the boundaries between the content owner rights and customer rights, when they trample on each other. This is due to the fact that the respective parties interpret the term "rights" as conditional. As a result, some DRM techniques employed by content owners, such as limiting the number of times a sound track can be duplicated, even for backup purposes or to restrain the portable multimedia players on which the content may be played, have caused serious protests on the part of customers, with the latter arguing that these few technical measures seriously threaten end user rights and stifle productivity and innovation. These open disagreements were taken under consideration and, as a result, some of the respective DRM techniques were recently (Drmwatch.com, 2005) declared illegal in France whereas the European Community is expected to rule a ban on these methods.

DIGITAL RIGHTS PROTECTION

From an evaluation of the resulting situation, it is certain that the intellectual property of content owners who deposit their work in a Web portal must not be left unprotected and the end user rights should be simultaneously preserved. A correct approach to fulfilling this end implies designing effective DRM techniques and examining any immediately following possible conflicts with the customer. Consequently, methods that simultaneously offer copyright protection and do not apply usability restrictions on the objects they aim to protect should be adopted.

Taking the first step into this end, it is observed that the digital content provided by Web portals can be divided into two broad categories: data and software (Atallah, Prabhakar, Frikken, & Sion, 2004). The first one consists of all possible forms of multimedia, including images, videos and digital sounds as well as digital documents, e-books and text structured information. Moreover this specific category includes data hosted in a database that are either queried out or exported in large chunks. The second category features software only, as indicated by the division of categories above.

Due to the fact that the above classification is decided according to the digital object's data properties, DRM techniques follow the same path and implement different techniques when trying to protect the specific objects. Two approaches are offered by DRM in order to protect the digital material hosted in Web portals: digital watermarking and code obfuscation. The first one aims to protect objects provided by Web portals that fall into the first category, whereas the second one involves exclusively software objects.

Digital Watermarking

Digital watermarking ("watermarking" for short) as well as its relevant information hiding techniques are not products that characterize our age but, on the contrary, are inherently related to the habits and tendencies of every time period (Rosenblatt, Trippe, & Mooney, 2001). However, the hazards mentioned above in combination with the adoption of digital technology from the modern world at the individual and social levels were considered a significant factor that hastened the transport of watermarking techniques in the digital world (Cox, Miller, & Bloom, 2002). This leads to the term *digital watermarking* which, in the present context, will be considered equivalent to the term *watermarking*. The latter is employed in order to protect the digital rights of various contents by enabling provable ownership over it. This is accomplished by performing relatively minor modifications on the object which designate the identification information (Watermarkingworld.org, 2005). The embedding procedure regarding these modifications, which is called marks, is determined by a publicly known algorithm and a secret key. This combination defines deterministically the segments of the object that will be altered as well as the alteration itself. The watermarking procedure is considered symmetric considering that the detection—verification process uses the same, most of the time, combination of algorithm and key to locate the alterations that were applied during the embedding process.

With respect to the perceptibility (visual or audible) of the watermark, there are two categories: visible and invisible. Even though in most of the cases a visually undetectable watermarked is preferred, there are some cases where a detectable watermarking is used. For instance in a situation where the content owner desires an ownership mark that is visually apparent but does not prevent the object from being used for some purposes such as scholarly research, a visible watermarking scheme could be employed. An example of a watermarked image with a visible watermark is depicted in Figure 1.

A crucial feature of any watermarking procedure is that it modifies the object it aims to protect. Taking this for granted, it is of utmost importance that the modifications enforced by the watermark not only comply with the initial requirement of being detectable but also have a marginal impact on the object, with respect to its usage. A member of the information hiding family and a really close relative of digital watermarking is digital fingerprinting (Li, Swarup, & Jajodia, 2005; Petitcolas, Anderson, & Kuhn, 1998). Many domain experts claim that these two share many features