CONCEPTUAL MODEL AND SECURITY REQUIREMENTS FOR DRM TECHNIQUES USED FOR E-LEARNING OBJECTS PROTECTION

Maria Nickolova, Eugene Nickolov

Abstract: This paper deals with the security problems of DRM protected e-learning content. After a short review of the main DRM systems and methods used in e-learning, an examination is made of participators in DRM schemes (e-learning object author, content creator, content publisher, license creator and end user). Then a conceptual model of security related processes of DRM implementation is proposed which is improved afterwards to reflect some particularities in DRM protection of e-learning objects. A methodical way is used to describe the security related motives, responsibilities and goals of the main participators involved in the DRM system. Taken together with the process model, these security properties are used to establish a list of requirements to fulfill and a possibility for formal verification of real DRM systems compliance with these requirements.

Keywords: Security, DRM protection, e-learning.

ACM Classification Keywords: D.4.6 Security and Protection.

Introduction

Over the past few years, the world of educational material publishing has been marked by the process of innovation and integration, caused by the advent of digital technologies. As a result of these changes, a new digital educational content market is emerging with a new commercial approach: from the distribution and sale of tangible products to the distribution and licensing of intangible products. This commercial change also has a very strong impact on educational content rights management (copyright and licensing, etc.). In the light of these factors, DRM (Digital Rights Management) becomes a need that cannot be delayed. Since the 1980s, the software and entertainment industry have sought technologies that can somehow limit copying or redistribution. While DRM has been most frequently used for movies, it is gaining more widespread use in educational media as well. Many audio files, such as Apple's iTunes files, have various built-in DRM schemes to limit the number of devices they may be played on. Many producers of e-books also use a similar DRM implementation to limit how many computers a book may be viewed on, and even how many times it may be viewed. In mid-2005, a number of content producers for television began also requesting DRM of their shows via the popular TiVo system.

Main Systems and Methods Used for DRM in E-Learning

Since the mid-1990s, the major technology companies have rapidly developed sophisticated, proprietary content protection schemes (DTCP, used to protect content within the home, was developed by Hitachi, Intel, Matsushita, Sony and Toshiba; HDCP, protecting digital video content across buses to PC monitors and to other display devices was promoted by Intel, etc.). Nowadays more sophisticated digital rights enforcement mechanisms are created executing specified user rights, coming as part of the content code, within the end user device. Protection mechanisms are being built into software such as Adobe Acrobat™, Apple iTunes™, Windows Media Player™, Microsoft Office™, etc. There are four different approaches for the creator of a document to assign certain rights only to persons in possession of legal rights. The first one is the “strong DRM” - some DRM technologies are designed to set and automatically enforce limits on user behavior, so that the user is unable to act illegally (e.g. copyright mechanisms which could not be overcome). The second method encourages learners to use learning objects only in legal way. In Potato system, for example, where the users play an active distribution part, they are motivated to re-distribute learning content they have paid for and earn money with it. The third method does not prohibit students to use illegally e-learning materials, but personalizes products to identify their origin in illegal environment (e.g. LWDRM technology). The forth method consists in disabling access to content upon detecting an attempt at unauthorized use. Such “self-help” technologies is often directed and controlled externally upon detection of the prohibited activity and therefore, implemented in tandem with some sort of monitoring functionality.

All these DRM technologies use two kinds of anti-copying measures - passive and active. Passive measures change the e-learning object's contents in the hope of confusing most illegitimate users' computer drives and software, or simply block access to it. Active measures, in contrast, rely on software on the computer that actively intervenes to block access to the e-learning content by programs other than the DRM vendor's own software. Passive measures don't pose security problems, but they are relatively easy to overcome. The method of active protection is working much better but is linked to some serious security problems, that depend on the parties involved in DRM schemes and their disobedience to the main security requirements.

In recent years, there have been proposed different models of DRM systems with specific properties [1, 2, 3, 4]. These proposals incorporate various security requirements. Some of them are related to the principal DRM functionality, whereas other requirements realize the specific properties for which that architecture was constructed [4]. DRM systems are designed to provide a solution for a security problem and the understanding of the core security requirements is crucial for fundamental comprehension of the security of DRM systems.

Examination of Participators in DRM Schemes

The main DRM participators are: the e-learning object author, the content creator, the content publisher, the license creator and the end user (student). They all must be present for a DRM system to function.

E-learning object author is the person(s) who creates the e-learning object and owns the copyrights. His/her impact on the DRM security is the least, but often it is the author alone who selects the used DRM technology.

The content creator is the person(s) or the media company that creates the e-learning content on the base of e-learning objects, submitted by one or more authors. He/she is responsible not only for the practical secure realization of the e-learning site but also for putting together all e-learning objects and the use of additional elements. Besides the implementation of DRM protection of learning objects, the content creator could use DRM technology to offer a revenue-generating alternative for traditional downloading. This means that the content creator plays a key role in DRM security.

The content publisher is the second most important participator from a security point of view. Generally he/she is responsible for the authentication of potential users, for the verification of their legitimacy and for ensuring their confidentiality and privacy. He/she also enables and tracks the content traffic. He/she works in close relation with the license creator.

License creator binds the content of the e-learning object to a license. He/she can use DRM technology to offer to the users a tailor-made access to content. By offering a clearly legitimate and known-quality alternative for downloading or acquiring a legal copy, license creator can stimulate the legitimate use of e-learning content. Also, as the content is bound to a license created by the license creator, most content distributed in this way will not spread beyond the license creator's control.

End user (student). To acquire a license, the end user accessing the protected content must contact the *license creator's server* specified in the metadata packaged with the protected content. Users are mainly drawn to DRM systems since they offer a legitimate, known-quality alternative to more dubious sources of content. Another advantage that DRM systems could offer to students, is the possibility to restrict the access to (and thus the cost of) e-learning content to precisely what the user wishes.

Conceptual Model of Security Related Processes of DRM Implementation in E-Learning

In order to derive a generic model, we start with one component for the four main roles in a DRM system security: the content creator, the content publisher, the license creator and the end user (student). The content creator and the content publisher are linked to the license creator and the license creator in his turn is linked to the end user.

This model is very simple and doesn't reflect some particularities of DRM protected e-learning content, so it needs some improvements. The first improvement is caused by the need to distinguish two types of content: protected e-learning content (which DRM is to protect), and free content (which a user can access without license and permissions). These results in dividing the end user's component in two: one communicating with the content publisher and another, communicating with the license creator. A second improvement is bound to the two possibilities for delivering the protected e-learning content – the "predelivery" and the "postdelivery". The concept of "predelivery" assumes that access is provided to the requesting end user prior to the media itself being transferred (acquired) or as part of the normal downloading process. The "postdelivery" presumes the widest possible dispersion of e-learning content. This approach, known as *superdistribution,* embraces students who have received the e-learning content from some source other than the main delivery channel (the e-learning site, the licensed shops, etc.). But to utilize this content, the recipient would have to contact the license creator and to provide the needed information and payment before receiving the right to access it. To reflect this particularity we shall split the distribution in two parts – one realizing content “predelivery” (content publisher) and another – for content “postdelivery” (other source). The last improvement is bounded to the main inherent characteristic of all DRM protected content: legal access to all protected content is granted only under a license, but DRM offers possibilities for different kinds of licenses. This results in splitting the license creator's component in two parts: one reflecting the temporary licenses, allowing access to a part of the e-learning content or to all the content but for a limited time or numbers of use, and another for the permanent license granting permanent access to the e-learning content.

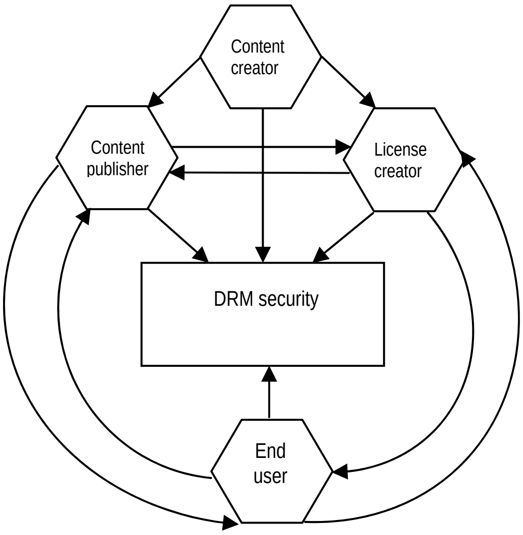

Fig.1 Conceptual model of DRM security

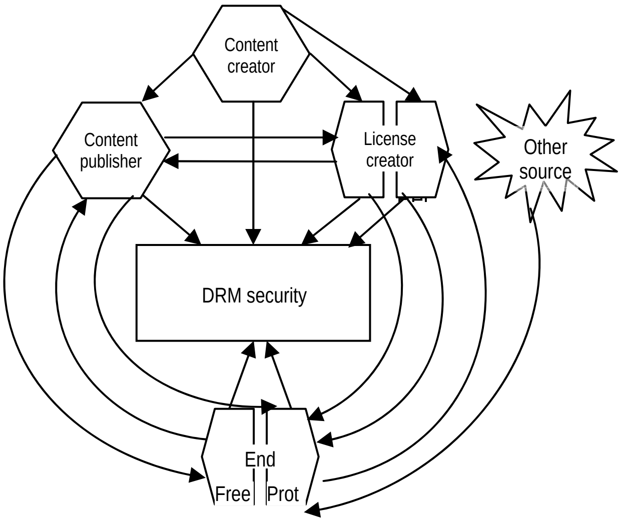

Fig.2 Improved conceptual model of DRM security

The content creator creates the content, which is published in the web (or company/university LAN/WAN) or distributed in some physical form (CD, DVD, etc.) by the content publisher and bound to a license by a license creator. If “predelivery” concept is used the content distribution is not obligatory bound or limited to the respective e-learning site/official channel of distribution. If the scheme of “postdelivery” is chosen, the content publisher is responsible for the legal content dissemination.

Motives, Responsibilities and Goals of the Main Participators in DRM Schemes

Let’s now draw a list of the general Motives (M), Responsibilities (R) and Goals (G) of the content creator, the content publisher, the license creator and the end user in using DRM protection.

Content creator

M-I: Could use the same DRM to protect his own copyrights.

R-I: Separates technically the learning objects (or parts of them) which will be DRM protected, based on author’s copyrights and desires.

R-II: Selects the DRM technology to be used, based on such criteria as robustness, viability, security and price.

R-III: Implements the selected DRM scheme (appending it in the OS core components or binding it to specific applications used to access the protected content).

R-IV: Is responsible for the limiting of the impact of possible system breaking.

G-I: The site structure (or physical media) should use advanced technological methods (encryption, scrambling, etc.) to deny access to protected content to all illegitimate users, even to technically experienced.

G-II: The site structure (or physical media) should not use any potentially harmful methods of content protection (active protection measures as ActiveX controls, backdoors capabilities, etc.) which could put at risk the security of end users’ systems.

Content publisher

M-I: Could get some profit by using DRM to offer more content to end users (not obligatory linked to the main e-learning site content).

R-I: Should ensure the right and secure functioning and accessibility of the e-learning site/physical media.

R-II: Should verify the rights of all users trying to get access to protected e-learning objects.

R-III: Should guarantee together with the license creator that the content used and the way of its use are not linked directly to the personal data of the end user.

G-I: Protected content should be accessible only by owners of a valid license issued by the license creator and under the conditions of this license.

G-II: All users that have not got such a license should be redirected to license creator without downloading and installing additional software to their systems.

License creator

M-I: Could use a DRM scheme to offer object-based or time-based licenses to end users.

R-I: Should deliver precisely the kind of license that has been requested, at the desired time for the licensee.

R-II: Should define clearly in the license agreements the end user’s rights and responsibilities and should see to their observation.

G-I: To stimulate the legitimate use of e-learning content by offering affordable personalized access to different groups of users.

G-II: To keep the user aware of all agreements between the license creator and the end user.

End user

M-I: Is guaranteed a legal functional copy by buying a license for DRM protected e-learning content.

M-II: Won’t be persecuted for illegal dissemination and use of e-learning content.

R-I: Order licenses or content on the user's behalf requires his intentional participation.

R-II: Must not share the licensed content he/she received legally free or against payment.

G-I: To acquire a consumable form of the content that he/she desires, at the moment he/she desires it.

G-II: Not to allow a decrease in computer’s security caused by DRM protected content.

Conclusions from the Conceptual Model and the Analysis of Principal Participators

The proposed model of the DRM system security and the analysis of the motives, responsibilities and goals of principal participators in DRM allow us to establish the principal security properties of DRM technologies. Taken together, these results could be used as a basis for the determination of security requirements of a DRM system, based on proven security components and protecting the integrity of usage rights. The methods we used support some derivation from the general security requirements, but due to the systematic approach, the descriptions are sufficiently exhaustive for our goals.

Main Security Requirements to Principal Participators in DRM Scheme

Understanding and defining security requirements is a fundamental part of establishing effective DRM standards and technologies. Here we will apply the considerations expressed above as security requirements in the model of Fig. 2. Each responsibility and goal described previously will be translated into security property for the model.

Security requirements to content creator

R-I leads to the following requirements for the content creator:

(1) (security) Neither the whole protected object nor part of it should in any state or conditions threaten the end user system’s security.

(2) (efficiency) The separation of DRM protected object must meet end user demands and expectations for convenience, performance and ability to deal with content.

R-II leads to the following requirements for the selected DRM technology:

(1) (usability) It must not be too restrictive for consumers who legitimately paid for content and want to share it on several devices.

(2) (privacy) It must allow a user to interact with it in an anonymous/pseudonymous way.

(3) (privacy) It must give the user more control and privacy as regards to domain-based protected content without sacrificing content owner's control.

(4) (universality) It must work with disconnected, multiplatform and multi-business end user's systems.

(5) (usability, transparency) It must provide ease of use, be transparent and visible.

R-III leads to the following requirements to the DRM implementation:

(1) (independence) The implementation can't rely on a software component on the user's device to perform integrity checking, decrypt the content or enforce the usage rights.

(2) (authentication) No DRM component sends the protected content to another component, unless the receiving component is authenticated as an official component and allowed to receive the content from the sending component.

(3) (self-protection) DRM software must preserve its integrity and efficiency even in extremely hostile environment.

(4) (self-protection) Besides the basic requirements valid for secure software the DRM implementation must be reverse-engineering-proof and temper-resistant.

R-IV leads to the following requirements for the long-term DRM security:

(1) (damages limitation) The possibility for "break once, run always" should be prevented.

(2) (updatability) The DRM system components should allow updates of new or altered system protective measures preventing security breaches during their installation.

G-I leads to the following requirements for the degree of DRM security:

(1) (secrecy) It must be neither possible to discover nor to alter the function that the DRM software performs and it must be also impossible to impersonate it.

(2) (constraint) The selected DRM solution must force the user to fulfill the obligations previously established by the license before granting the rights and access to these contents.

G-II leads to the following requirements for the relation between the used DRM system and end user protection:

(1) (safety) The DRM solution must correspond to the end user security point of view.

(2) (priority) In case of contradiction between the requirements for illegitimate access prevention and these for end user security, the last must prevail.

Security requirements to content publisher

R-I leads to the following requirements for DRM system efficacy:

(1) (proportionality) The end user should pay only what he gets and should get only what he paid in a form and under conditions corresponding to his license.

(2) (completeness) E-learning content must be available to the end user at any time and with quality, conformable to the license terms and conditions.

R-II leads to the following requirements for DRM license scope:

(1) (efficiency) The adherence to license terms must be strictly observed regardless of the location and the device from which the end user tries to access e-learning content.

(2) (completeness) The license must be bound to the user, not to the device used.

R-III leads to the following requirements for the user personal data security:

(1) (confidentiality) Personal data must be bound to the purpose of the service; they may be used only by consent of the end user or by a legal obligation.

(2) (secrecy) Together with the license creator the content publisher must ensure the confidentiality of the personal data.

(3) (protection) Together with the license creator the content publisher must protect the personal data against loss, distortion, and correctness with respect to the intended use.

G-I leads to the following requirements for DRM efficacy and secrecy:

(1) (secrecy) The content is only accessible by the end user specified in the license and all information remains secret until it has been converted into an analogue form.

(2) (trust) The end user is able to use the content only if all terms of any one valid license governing this content are met.

(3) (robustness) The internal parameters of the content/licensed user pair cannot be influenced or disrupted by the license creator, the user nor any third party.

(4) (secrecy) No secret information, necessary for the operation of the components or pertaining to content (e.g. cryptographic keys, content, etc.); can be discerned from the content creator - licensed user pair, nor from the communication channel between them.

(5) (constraint) The DRM system protection ends at the end user.

G-II leads to the following requirements for no-forced use of DRM protected content:

(1) (knowledge-ability) All potential users of e-learning content should dispose of reliable complete and exact information about the possibilities, the conditions and the way of acquiring a license.

(2) (undependability) The advertising of license acquiring must not be linked to modifications in end user system and the license acquisition must be realized in an absolutely voluntary and conscious way.

(3) (safety) The used DRM technology must guarantee that attempts to access DRM protected content will not modify the end user's system nor threaten its security.

Security requirements to license creator

R-I leads to the following requirements for DRM technologies' precision and completeness:

(1) (integrity) The request for licensing should be received correctly.

(2) (availability) The user should be able to immediately contact the license creator.

(3) (availability) The user should always be able to receive license and content.

(4) (integrity) The content/license should be received fully and correctly.

(5) (authentication) Only authenticated users with whom an agreement has been reached will receive licenses for the content for which that agreement was reached.

R-II: leads to the following requirements for honesty in DRM use:

(1) (lifetime care) License agreements should include control over content after delivery.

(2) (limitation) Content providers can not make offers that violate the rights of end users.

(3) (transparency) The responsibilities for observation of rights and obligations of end user must be clearly separated between the content publisher and license creator.

(4) (knowledge-ability) User must be well informed about restrictions for content transportation and exchange between devices.

G-I leads to the following requirements for collaboration among participators in DRM scheme:

(1) (completeness) License creator should offer licenses covering all possible combinations of individual and collective, limited and unlimited access to a part or the whole content of e-learning object.

(2) (accessibility) The license price should be specified together with the author(s) and the content creator according to the target audience.

G-II leads to the following requirements for transparency for e-learning content protection:

(1) (freedom) Personal data protection functions must be transparent so that users can at all times exercise their right of information confidentiality and deactivate these functions for the information and files that they "own".

(2) (participation) If personal data is transmitted in conjunction with the use of the DRM, the user must have the possibility to consent to such transmission in every case.

(3) (knowledge-ability) The user must be informed of the type and extent of data transmitted to the content publisher or any third party related to the protected content.

Security requirements to end user

R-I leads to the following requirements for end user's involvement in DRM scheme:

(1) (knowledge-ability) End user must indicate what he wants to obtain.

(2) (compliance) End user must strictly observe the limitations of the acquired license.

R-II leads to the following requirements for end user engagements:

(1) (awareness) He must not let intentionally or unintentionally let others get access to DRM protected e-learning content unless this is not expressly indicated in the license.

(2) (safety) He must keep his system free of malware and protected from exposure.

G-I leads to the following requirements for clearness in DRM participators' relationships:

(1) (availability) The license creator services should be available at any time for the user.

(2) (trust) The content publisher sends what has been agreed upon with license creator.

(3) (authentication) The license creator must authenticate itself to the user.

G-II leads to the following requirements for end user commitment:

(1) (trust) End user must not use in illegitimate way the DRM protected e-learning content.

(2) (safety) End user must not allow the e-learning content he acquired legitimately to be distributed by illegitimate channels which could threaten his system' security (e.g. P2P networks).

Conclusion

In this paper we analyzed and described the key roles taking part in a DRM system as well as desired security properties. Then we built a generic conceptual model of security related processes of DRM implementation in e-learning and used a methodical way to describe the security related motives, responsibilities and goals of all participators involved in the DRM system. Taken together with the process model, these security properties allowed us to establish the core security requirements of DRM systems which lead to an improved understanding of the DRM security aspects.

This paper takes a practical stance towards security: it presents a list of requirements to be fulfilled and a possibility for formal verification of real DRM systems compliance with these requirements. Further developments can lead to the establishing of a theoretical basis in which it is possible to verify that a trusted DRM system complies with the requirements upon it. The process model used for establishing the requirements can be refined to include more details for a more thorough analysis of a particular system. However, such a requirement refinement requires some loss of the generic nature and therefore may result in confining the applicability of the resulting findings to systems exhibiting specific characteristics.

References

[1] S. Guth, A Sample DRM System - Digital Rights Management, Volume 2320 of LNCS, pages 32 – 50, Springer-Verlag GmbH, November 2003.

[2] Open Mobile Alliance (OMA), DRM Architecture, OMA-DRM-ARCH-V2 0-20040715-C.

[3] B.C. Popescu, F.L.A.J. Kamperman, B. Crispo, and A. S. Tanenbaum, A DRM Security Architecture for Home Networks, DRM '04, Proceedings of the 4th ACM Workshop on Digital Rights Management, pages 1 – 10, ACM Press, 2004.

[4] C. Serrao, D. Naves, T. Barker, M. Balestri, and P. Kudumakis, Open SDRM - An Open and Secure Digital Rights Management Solution, Proceedings of the International Association for Development of the Information Society (IADIS'03), International Conference on e-Society, Lisbon, Portugal, June 3-6, 2003.

Authors' Information

Maria Nickolova – National Laboratory of Computer Virology, BAS, Acad. G.Bonthev St., Bl.8, Sofia 1113, Bulgaria, e-mail: maria@nlcv.bas.bg.

Eugene Nickolov – National Laboratory of Computer Virology, BAS, Acad. G.Bonthev St., Bl.8, Sofia 1113, Bulgaria, e-mail: eugene@nlcv.bas.bg.