Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp186-189)

The Design and the Implementation of Web Service Security System for the Secured Distribution of Digital Contents

SEUNG-BAE YUN, HYUNK-JIN KO, UNG-MO KIM
Dept of Computer Engineering
Sung-Kyun-Kwan University
1459-7, Gwanyang 2-dong, Dongan-gu, Anyang-si, Gyeonggi-do, Korea
KOREA

Abstract: - With the development of multi media technology, the demand on digital contents distribution is increasing. However, it is very difficult to guarantee the integrity of digital contents and to protect the copyrights of the contents. Accordingly, in this article, the system applying DRM technology, the digital copyright technology for web security was designed and implemented. To protect digital music sources, PKI, SEED encryption algorithm and XrML, which explicitly specifies copyright, were used to implement an upgraded system to serve digital contents. It will be a sample model to enforce web security technology.

Key-Words: - DRM, XrML, Web service, authentication, Security, Digital content

1 Introduction

With the development of information and communication technology, the establishment of high-speed network and the rapid development of multi media technology, demands on Digital Contents (animation, static images, MP3) were rapidly increasing. While Digital Content has advantages such as easy mass distribution through digital communication, and the simple and easy use, it cannot guarantee the integrity of the data. As digital data is widely applied to various media, it cannot guarantee the copyright of the contents owner because of the mass copy by unauthorized access and the unauthorized modification without the permission of the owner. Therefore, the Digital Content provider wants to have technological and instrumental environments that prevent copyright infringement so that he can be paid for his efforts for the content. The composition of these environments is mandatory. Among the copyright protection technologies, DRM (Digital Right Management) has been known to protect digital contents from illegal distribution because it allows the authorized users to deliver and use the digital content such as MP3 file. [1]

In this article, DRM was introduced to MP3 file, one of digital contents. We designed and implemented DRM based web security system where only authorized users who acquire the right from E-commerce only can use music source file on and off line.

The composition of this article is as follows. In the second chapter, we learn about conventional DRM technology. In the third chapter, the design and implementation of DRM based system that this article proposes are described. Finally, in the fourth chapter, the conclusion is made and future research tasks are described.

"This paper was supported by Faculty Research Fund, Sungkyunkwan University, 2004"

2 Related Researches

2.1 Status of DRM Research

As Digital Contents can be copied without damaging the quality, we need to develop digital copyright protection system to protect the contents from copyright infringement. Therefore many researches on DRM system are under progress and solutions using DRM technology are being developed [2, 3,10]

DRM is a technology that protects and manages the right and benefits of the copyrighter by protecting the digital contents from the use of unauthorized users using copyright protection technology [1].

It has been developed focusing on encryption technology to ensure the secrecy and integrity. To specify the copyright explicitly, standardization process is being made based on XrML (eXtensible

rights Markup Language). To give identifier, DOI (Digital Object Identifier) is being actively adopted [4].
Additionally many other solutions that can provide digital contents distribution in an integrated way by combining with E-commerce system according to various conditions are emerging.

2.2 Conventional DRM System

2.2.1 DRM System of InterTrust

The special feature of DRM solution of InterTrust is to perform the collection of use details, recording and billing by using encryption and watermarking and specifying copyright use regulations. It runs an agent program in the user computer and deal with license, billing and running the digital content through agent. As the content is distributed pre-encrypted, the license agent will check the license, transfer billing information and make the transaction when the user's computer is using the digital content. [1, 5].

2.2.2 DRM System of Microsoft

DRM System of Microsoft is end-to-end DRM system, which securely distributes digital medial files to the digital content provider and consumers [6]. The core control part is WMRM(Windows Media Rights Manager). The rights manager of WMRM delivers media such as music and video that are protected as encrypted files on Internet. In WMRM, each server or client instance will get key pairs through individualization process. For the instances deemed cracked or unsafe, it will cancel the certificate and they will be excluded from the service list.

2.2.3 Analysis of the conventional DRM System and Comparison with the Proposed System

When defining the use regulations, we need to control the use regulations variably. Most of current technologies define the use regulations allowing the running of the content according to the number of use, the period of use (initiation and expiry date) and the age of the user.
Regarding the packaging the content, both systems use inserting copyright information in the original content. The disadvantage of the conventional systems is that they are subject to be used in the dedicated player only. The limitation of the player restricts the use of the contents because DRM is used to treat the content.
However, the system proposed in this article does not have this kind of restriction because it performs decryption and license management through the user's agent. We enhanced the speed of encryption and decryption applying SEED encryption algorithm.[7]

3 Proposed System Structure and Implementation

3.1 System Architecture

The proposed system is operating with the configuration of client/server as shown in the figure 1.
The server comprises with external interface, music source monitor, encryption processor, packaging processor, monitor interface and database.[10]

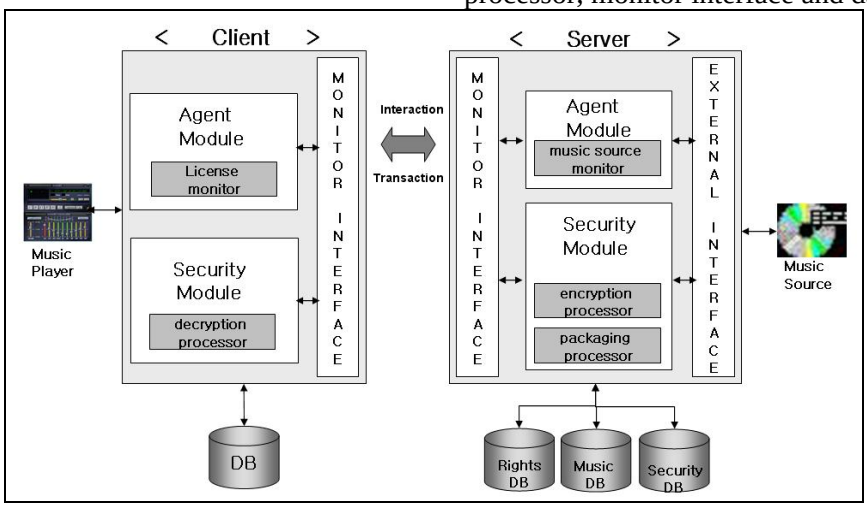

Fig.1. System Architecture

The client comprises with user agent program with license monitor and decryption processor and database. When digital content is registered in system server through external interface, the content is monitored according to the use regulations allowing the running of the music source according to the number of use or period of use (initiation and expiry date) according to the agent module of the music source monitor. And then the music sources are encrypted.

3.2 User Authentication

Users will perform user authentication based on the PKI certificate. The left of figure 3 shows the web site implementation, which will be responsible for web service of the server.

The user should install the user program in his or her system and be authenticated before listening the music.

3.3 Encryption and License File Creation

The content provider transfers the music source to the server and the server encrypts the content using SEED algorithm. It stores M (encrypted music) with ks (Secret Key) in the music database in the server.

SEED algorithm is a block encryption algorithm that deals with message by block.

M=Eks[Music Source]

As it is a symmetric encryption, file size is not very big and can be decrypted very quickly. When the user buys the source after authentication, access control list is created in XrML with Ks reflecting the purchase level of the user. The created XrML file is encrypted with the public key(pk) of the user and the file is protected against the unauthorized users. [8, 9] The figure2 below shows M(encrypted music source) and L(encrypted XrML file) creation and packaging process in the server.

3.4 Decryption and Music Source Listening Process

The encrypted source file M and encrypted XrML file will be delivered to the user in package. The user get authentication through user agent program and can listen to the music he or she bought. The primary key used for the user authentication will be used for the decryption of XrML and the agent program will judge if he or she has the right to use the file through the decrypted XrML. If it judges that he or she is the rightful user, it decrypts M using Ks (secret key) recorded in XrML. Client agent program will call the executor(Music Player) registered in the user system. The right of figure3 shows the Client Agent execution.

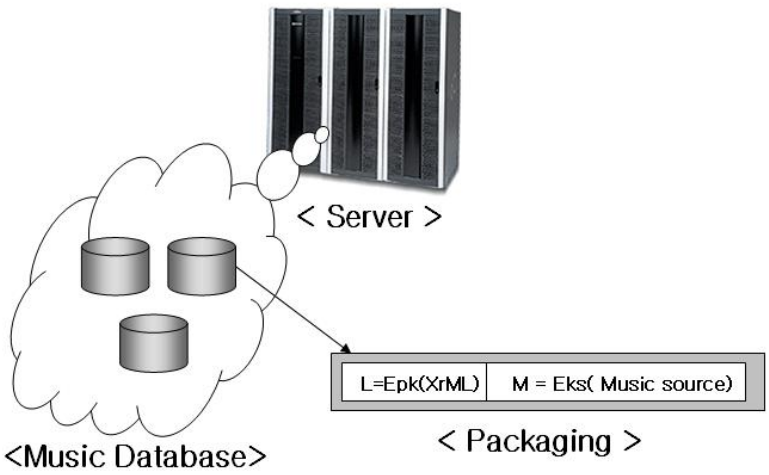

Fig. 2 M(encrypted music) and L(encrypted XrML file) creation and packaging process in the server

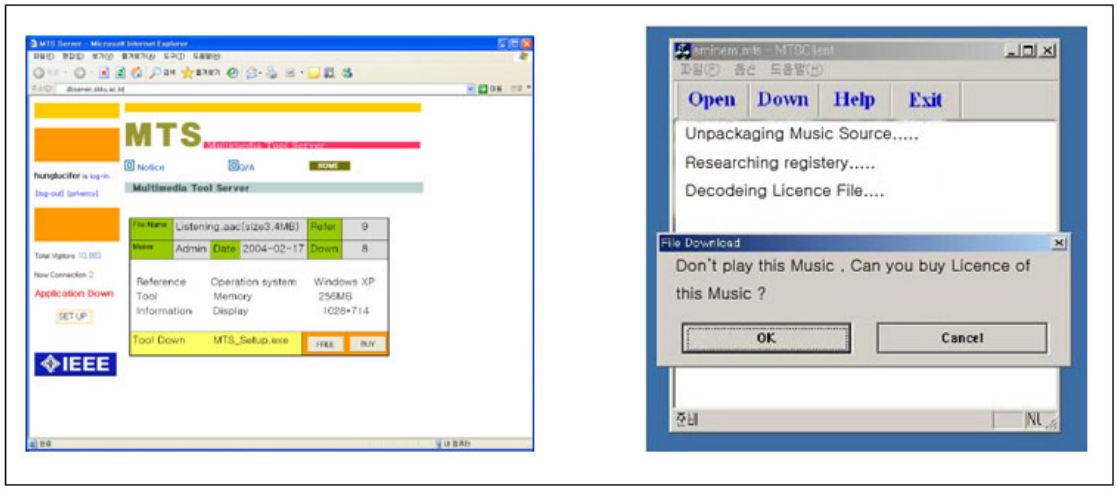

Fig. 3 shows the web site implementation, which will be responsible for web service of the server and Client Agent implementation, which will be responsible for license monitor of the client

4. Conclusion and Future Studies

In this article, DRM, the digital contents copyright protection technology, was introduced to design and implement web security system that allows only rightful users to use digital music (MP3 file), one of the digital contents. This study has many restrictions and improvement points to generalize to all the digital contents. First of all, this system encrypts the whole music. This method can be used for restricted digital contents only and it cannot be used for high volume multimedia files. Additionally the packaging of music and license file is ineffective, because it should be repackaged if the license file is upgraded. Currently, a research is under progress to improve license file packaging technology and to identify the best security technology that can be applied to most digital contents by encrypting specific frame only rather than the whole file and by reducing the time for decryption.

References:

[1] Joshua Duhl, Susan Kevokian, "Understanding DRM System.", *An IDC White Paper*, 2001.

[2] Sung, J Park, "Copyrights Protection Tech niques," *Proceedings International Digital Content Conference*, Seoul, Korea, Nov., 28-29, 2000.

[3] V.K. Gupta, "Technological Measures of Protection," *Proceedings of International Comference on WIPO*, Seoul

[4] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transac tion on Information Theory*,Vol.IT-22, No.6, pp.644-654, November, 1976.

[5] Joshua Duhl, "Digital Rights Management : A Definition," *IDC 2001*.

[6]Microsoft: http://www.microsoft.com/windows/windows media/drm.asp

[7] Korea Information Security Agency, 128bit block encryption algorism standard

[8] Takeshi Imamura, Blair Dillaway, Ed Simson, "XML Encryption Syntax and processing", *W3C*, December, 2002

[9] Content Guard, "XrML 2.0 Technical Overview version 1.0" March, 2002

[10] F.hartung, F.Ramme, "Digital Rights Management and Watermarking of Multimedia content for M-commerce Applications", *IEEE com. Magazine*, Vol. 38, pp78~84, Nov. 2000