Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Digital Rights Management (DRM) and RSS (Rich Site Summary)

Swapna D.Lokhande, Mr.Girish Agrawal , Ms.Pragati Patil
Department of CSE, RTMNU
India

Abstract — In the proposed system an Rich Site Summary (RSS) feed is create and is protected internet by using Digital Rights Management (DRM) techniques. This RSS feed is like an application that is to be purchased by the required user. Without subscription and password the user is unable to access the feed. This is done by DRM technique that without password the feed cannot be accessed. A software re-encryption scheme is implemented to protect the RSS feed from unauthorized user. The proposed system combines secret sharing and encryption scheme. DRM constitutes an incentive for software providers to take part in a future networking scenario

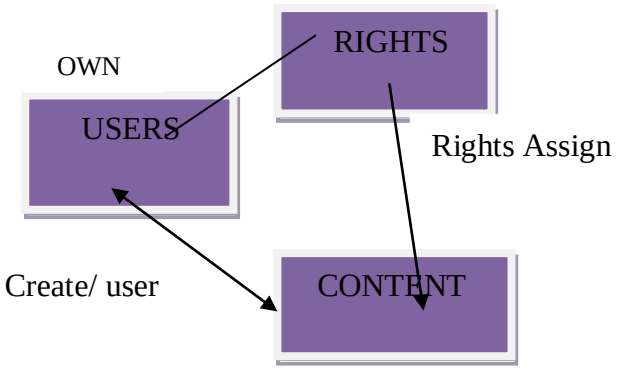
Keywords — DRM, Privacy, Multiple Keys, Encryption, RSS, Security

I. INTRODUCTION

Digital networks have profoundly transformed how we distribute different products and the ways that individual's access and enjoy such works. Digital networks have changed all of this. Many copyright holders are keen to make their works available digitally in order to exploit the efficiencies of digital distribution. Everyone is also interested to explore new ways of accessing and enjoying creative works, for example by purchasing one song at a time rather than a whole album. However, many copyright holders have expressed reluctance to make their works available in digital format without a means to control the work, ostensibly to protect it against copyright infringement. Many of these copyright holders have turned to technological tools in search of a means to control access and use of creative works in the digital environment. Known as "Digital Rights Management," or "DRM," these technological tools are changing the ways individuals interact with digital content. In this paper we are concern with creating an RSS feed and protecting it in internet by using DRM techniques.

1.1 Digital Rights Management (DRM):

Digital rights management (DRM) is a class of access control technologies that are used by hardware manufacturers, publishers, copyright holders and individuals with the intent to limit the use of digital content and devices after sale. The term Digital Rights Management (DRM) broadly refers to a set of policies, techniques and tools that guide the proper use of digital content. DRM is the "digital administration of privileges" and not the "administration of digital privileges". DRM manages all rights, not only the rights applicable to permissions over digital content but also on its security and privacy.



1.2 DRM Framework.

The overall DRM framework suited to building digital rights-enabled systems can be modelled in three areas:

- How to manage the creation of content so it can be easily traded.
- How to manage and enable the trade of content.
- How to manage the usage of content once it has been traded. This includes supporting constraints over traded content in specific desktop systems/software.

© 2013, IJARCSSE All Rights Reserved

1.3 Security Supporting Techniques of DRM.

There are various techniques of DRM through which security of the digital content is done on internet, these are as follows:

1) **Cryptography Methods**: Cryptography is used to protect the content from access and to secure communications between the user and the distributor. There are various encryption and decryption techniques used to secure the digital content.
2) **ID techniques**: Content owners can use content identification (for example) to detect theft, whilst users could use this to and content which they have seen or heard but which they have not yet acquired.
3) **Digital Object Identification (DOI):** This scheme works similar to a bar code given a cryptic identifier, a server looks up the current location of the content and redirects you there [DOI].
4) **Trusted Computing Base:** A Trusted Computing Base (TCB) assures others that the owner (of the TCB) can execute computations faithfully inside the TCB without exposing secrets to the owner.

2.1 Rich Site Summary (RSS):

RSS (Rich Site Summary) is an arrangement for delivering frequently changing web content. Many news-associated sites, weblogs and other online publishers organise their content as an RSS Feed to whoever wants it. Benefits and Reasons for using RSS solve a problem for people who regularly use the in internet. It allows every individual to easily stay informed by recovering the latest content from the sites you are interested in. Anyone can save time by not needing to visit each site separately. You ensure your privacy, by not needing to join each site's email newsletter. Many sites display a small icon with the acronyms RSS, XML, or RDF to let you know a feed is available. RSS is catching on as one of the most widely used XML formats on the Web. RSS is a technology that is being used by infinite web lovers around the world to keep track of their favourite websites. In the 'old days' of the web to keep track of updates on a website you had to 'bookmark' websites in your browser and manually return to them on a regular basis to see what had been added.RSS flips things around a little and is a technology that provides you with a method of getting relevant and up to date information sent to you for you to read in your own time. It saves an individual time and helps them to get the information you want quickly after it was published.

2.2 How RSS feed is created:

Rich site summary (RSS) is a technology that is being used by millions of web users around the world to keep track of their favourite websites or news blogs etc. In this proposed scheme an RSS feed is created which is based on different engineering courses offered by any engineering college. When any branch is selected it gives details of students of that particular branch. This feed is designed using MYSQL and XML. Steps to create the algorithm are as follows:

- **Identify the items for your RSS feed** :

  Items are stories, articles, or other pieces of online content that you have created. Each item should be connected or similar in some way, meaning they should be about the same topic or theme.

- **Insert XML and RSS tags at the beginning and end of the file** :

  You will need to designate your RSS feed as an XML file, and include the version. Use version 1.0 for your original feed. You may update your feed on a regular basis, which will require you to create new files with version 2.0, 3.0, etc.

- **Create a channel for the RSS feed :**

  Think of the channel of your feed the way you think about television channels. Name the channel something general that describes what is similar about all of your items. It alerts Internet users that all of the items are related, the same way the Food Channel alerts viewers that the content will be on the subject of food. The channel appears at the top of the file.

- **Add <item> before each place on your list** :

  Use brackets to enclose the tags identifying the title, description and link. The XML file necessary for an RSS feed requires you to use open and close tags in these brackets: < >. A forward slash is also required at the closing tag after each line. Make sure to close the item tag after you finish the link like this: </item>

© 2013, IJARCSSE All Rights Reserved

2.3 Security Implemented through DRM on created RSS Feed:

DRM is the technology used to secure the digital content on internet. So RSS feed is protected using DRM techniques on internet. When the product of RSS feed is purchased by any user, and then the user is provided a product code. These product key acts as a password without that product key the product cannot be accessed. This product key is implemented as encryption technique. In this proposed work re-encryption technique is used. Each time the user subscribe the feed product code is to be inserted. This product key will be same but internally each time product code encryption method will be different. In this system three types of techniques are used they are as follows:

1) **Message Digest Algorithm (MD5 ()):** It calculates the md5 hash of a string.

Syntax:

String md5 (string $str [, bool $raw_output = false])

Calculates the MD5 hash of str using the RSA Data Security, Inc. MD5 Message-Digest Algorithm, and returns that hash.

2) **Secure Hash Algorithm SHA1():** Calculate the sha1 hash of a string

Syntax:

tring sha1 (string $str [, bool $raw_output = false])

Calculates the sha1 hash of str using the US Secure Hash Algorithm 1.

3) Crypt():

crypt () will return a hashed string using the standard Unix DES-based algorithm or alternative algorithms that may be available on the system

Syntax:

string crypt (string $str [, string $salt])

PHP sets a constant named CRYPT_SALT_LENGTH which indicates the longest valid salt allowed by the available hashes.

II. CONCLUSIONS

Therefore we reached to a conclusion that we have created any RSS feed and protected it on internet by using DRM techniques .IN this paper we have described three techniques MD5, SHA1, CRYPT().SO whenever the authorized user subscribe the RSS feed each time the security process changes . Therefore by using only one product key three times protection is provided.

ACKNOWLEDGMENT

I would like to take this opportunity to express my sincerest thanks to all the people who have contributed towards the successful completion of my paper. I sincerely acknowledge the invaluable support and guidance extended to me by Prof. Girish Agrawal, Prof. Pragati Patil, Head of Department of M.Tech, and Computer Science & Engineering.

REFERENCES

[1] Eindhoven University of Technology, Department of Mathematics and Computer Science.

[2] DRM_Basics_01649008 MARCH/APRIL 2006 027- 6648©2006 IEEE.

[3] "Privacy-Preserving DRM for Cloud Computing" Ronald Petrlic Department of Computer Science University of Paderborn 33098 Paderborn, Germany ronald.petrlic@upb.de

[4] Perlman, C. Kaufman, and R. Perlner, "Privacy- Preserving DRM," in Proceedings of the 9th Symposium on Identity and Trust on the Interested. IDTRUST'10. New York, NY, USA: ACM, 2010, pp. 69–83. [Online]. Available: http://doi.acm.org/10.1145/1750389.1750399

[5] J. E. Cohen, "DRM AND PRIVACY," Berkeley Technology Law Journal, vol. 18, pp.575– 617, 2003, Georgetown Public Law Research Paper No.372741.

[6] C.Conrado, M. Petkovic, and W. Jonker, "Privacy- preserving digital rights management," in Secure Data Management, ser. Lecture Notes in Computer Science, vol. 3178. Springer, 2004, pp. 83–99.R.

[7] Iannella (2001, June). "Digital rights management Architectures" D-Lib R. L. Rivest, A. Shamir, and L. Adleman.

© 2013, IJARCSSE All Rights Reserved