Analyzing the Content Protection Mechanisms in Open Source Web Content Management Systems

Fatma Al-Terkestany, Samir El-Masri
Information Systems Department
College of Computer & Information Sciences
King Saud University, Riyadh, Saudi Arabia

Abstract - As the web content management system contains sensitive information, the quest for web content protection is extremely important. This paper reviews some of the popular web content management systems and analyzes the available protection solutions. However, these solutions have some limitations in protecting the web content from unauthorized access. The research aims to propose some improvements to protect the content through the mean of digital rights management. Finally, the paper discusses the impact of using the suggested advanced protection mechanisms.

1. Introduction
Web content management system is the most widespread and frequently used types of content management systems. It consists of applications used to create, manage, store and deploy content on the web, including text, graphics, video or audio, and application code. [4] Essentially, the web content management systems support common processes such as authoring, repository, workflow and publishing. One of the most important elements of complexity in the content processes is content protection. The quest for web content protection during the last few years has been very critical issue. Therefore some researches in developing content protection technologies have been proposed. Digital rights management adopted protection technologies to safeguard the content, manage it and enforce the rule of the digital content usage and distribution.

As a content protection mechanism, the access control system has been integrated to web content management systems. It is the process of limiting access to the web content only to authorized users, programs, or other systems on a need-to basis. In general, access control is defined as the mechanism by which users are permitted access to resources according to the authentication of their identities and the associated privileges authorization.

This paper is organized as the following: section 2 reviews some of the content protection solutions as well as the popular open source web content management systems. Section 3 states the limitations of the previous protection solutions. In section 4, some improvements to protect the content through the mean of digital rights management are proposed.

2. Content Protection
Content protection is the general term used to include mechanisms and technologies designed to protect content by controlling its use, in order to give content providers control over access and redistribution of protected material. Typically, the term "content" is widely defined to include, but not be limited to, all materials, information, text, graphics, images, audio, video materials available on the web site.

Several protection solutions have been developed to protect web content. Localized, [17] the company that specialized in digital rights management, developed many products like HTML protection software to protect the web content and images. The software provides many control functions such as viewing, copying, modifying, saving, and printing content and more. In addition, the company offers a valuable web content security solution for publishers who need to
control the dissemination of their web based content to specific users. It uses encryption and digital rights management as an alternative to the existing access control system which relies on password mechanisms.

CopySafe, [18] is copy protection software for web pages and images which can be employed in any existing web solution. It allows the web pages author to control access to the web content by enable or disable the use of print, keyboard, menu and browser toolbar options. In addition, the software encrypted images to ensure that they can only be viewed from a certain web site.

Furthermore, a variety of protection software available in the market and some of them are used to protect the content from all copying and saving techniques (copy protection), as well as the web browsers grabbers. Whereas, the sophisticated solutions include mechanisms to encrypt and decrypt the web content and the decryption keys are distributed to authorized persons only.

In the context of web content management systems, content protection solutions have been provided in term of access control system and as extensions:

1. **Joomla** protects the web content through the utilization of two important features which is user management and access management. [8] Joomla manages users by defining a set of user groups and assigning permissions to each of them. Dividing users among groups help to restrict access to the web content and allow only authorized user to access web content. Moreover, it is useful in accountability and traceability. Moreover, most content on a Joomla website can be optionally restricted to users at or above a given access level. An article might be restricted to registered users so that public will not see it. Users who have previously been registered and who log in to the site front-end will see this article. Administrators have the ability to restrict user access to particular content. In addition, Joomla provides more advanced access control like prevent printing or saving of the content.

2. **WordPress** has a feature called "content visibility". It is to control the access of posts and pages on an individual basis. Three authorization permission levels are available: public, private, password protected. Private access control means to hide the content from the public completely whereas; in password protected, the content appears to website visitors but they should provide the password in order to view this content. Thus, private permission can be used to protect paid content on the website and decide who can access it. However, the access control system in WordPress is very basic and simple. It cannot protect very specific content from being accessed by a specific user.

3. Lastly, **Drupal**, protects content in creation, modification and administration from unauthorized access, Drupal uses permissions. Administrators assign permissions to roles and then assign roles to users. Each user role has its own set of permissions. Since the content in Drupal is placed within modules, each module has a set of access controls to protect content. Moreover, there are some content protection modules that can be used inDrupal, like content access module [13]. This module allow user to manage permissions for content by role and author as well as to specify custom view, edit and delete permissions for each content type.
3. The Limitations of the Content Protection Solutions

After investigating three of the most popular open source web content management systems, Joomla, WordPress and Drupal, we conclude the following:

4. Although major improvements were applied on managing users and controlling their access to website resources, content protection requires more attention!

5. The current systems focus on protecting content after publishing by specifying authorized users and controlling their access using simple controls like disable printing, copying and saving.

6. The systems didn't have secure content distribution methods that deal with offering content for the user. No advanced techniques are used to protect published content like tracking content or copyrights technologies.

7. Usually, the web content management systems include default workflow that can be used or modified. In certain web content management systems, you can design an unlimited number of workflows. Protecting content during workflow often is not addressed.

8. Protecting content by using of copyrights is not sufficient! Since law isn’t a preventive measure, copyright law does not prevent authorized users from copying the published content and distribute it. Authorized users can make dozens of copies of the web content almost as easily as they can make one. Moreover, they can email it to everyone in their address book. Thus, the need for technological based protection is necessary.

To address the above limitations, content protection needs to be addressed beyond the current usage of user management and access control. Content protection has two parts: copy protection technologies to prevent the direct copying of protected content, and rights management technologies to tag content with information about what permissions the owner has granted for its use. As more sensitive content enters the web content management systems, the desire to protect that content grows. This research focuses on the integration of the major existing content protection technology, digital rights management, into the web content management systems. [14]

4. Suggested Improvements

The digital rights management is an alternate term for content protection mechanisms. It is about defining, protecting, and tracking the rights associated with accessing protected content. Therefore, combining the digital rights technologies in the web content management systems adds an extra layer of content protection by providing the following features: [15].

1. Copy protection: it encompasses mechanisms and technologies to protect content from being copied. The content owner can use the integrated copy protection technology to prevent unauthorized copying of content.

2. Advanced usage control: it allows the content owner to control content viewing, printing, editing, copying and execution.

3. Advanced access control: it defines roles and permissions according to the customized workflow and allow for permission inheritance.

4. Content accountability and auditing so the web content management system should record the date, time and user for every access to the web content. This feature will assist in tracking content and protect it from unauthorized access.
It is important to emphasize that content protection must be addressed during content workflow and after publishing. The workflow of the web content management system represents the different stages or phases through which the content passes from its initial creation to its final distribution and publishing. During the content lifecycle, several users and processes may be involved. Applying protection content technologies ensure that content is protected once it is created. The content owner can set access rights of the content to specify how it can be accessed at the next stage in the workflow. For example, in a publishing workflow, content author may want to prohibit editing of a specific part of the content like preventing editor from the modifying author's contact information. By integrating content protection technologies to all phases in workflow, protected content is created and protected content is published.

[6] Usually, the web content management systems provide the workflow customization capability which allows the website administrator to customize workflow according to business needs. In this case, it is required to adapt the new lists of permissions and roles. As a result, no one technology achieves all of the content protection functions required. Thus, a series of digital rights technologies are needed to protect content once it has been created and during its workflow until it has been published.

5. Conclusion

The open source web content management systems utilize some mechanisms to protect their web content from unauthorized access. The integrated access control system used the concept of roles and permissions to restrict access to the content. However, there is a demand to have more advanced and flexible content protection solutions. As the suggested solution, digital right management technologies can be combined with the web content management systems and provide an extra layer of protection.

6. References


