Access Control Requirements for Content Management Systems

Author and co-authors

Andre Reyneke

Reinhardt A. Botha

Stephen Perelson

Author's affiliation

Faculty of Computer Studies

Port Elizabeth Technikon

Author's contact details

{areyneke, reinhard,stephen}@petech.ac.za

041-5043313

Faculty of Computer Studies

Port Elizabeth Technikon

Private Bag X6011

Port Elizabeth, 6000

Access Control Requirements for Content Management Systems

Abstract

Information has become important in today's organizations. The management of this information has therefore also become vital. Content management is seen as the overall process for collecting, managing and publishing information. In order to keep the content management system up to date, there must be a proper workflow system in place. The workflow system will ensure that important changes, not only in the content management system but also changes in the organization affecting the content management system, are brought under the attention of the content management system administrator. Due to the important nature of information stored in the content management system, security issues need to be addressed. One such security issue is access control.

Various access controls should be specified in order to effectively secure information throughout the phases of the content management process. This paper sets out to identify the access control requirements of content management systems. It contributes, therefore, by identifying a set of access control requirements that are vital for effectively controlling access within the content management system.

Keywords:

Content Management, Security, Access Controls, Permissions

Access Control Requirements for Content Management Systems

1 Introduction

Organizations have realized that information has become imperative. Warehouses of valuable information are contained within these organizations. This information has to be managed and secured properly and in so doing, an organization can effectively use this information advantageously against its competitors. In order for this information to be of value to the organization, it needs to be stored and maintained effectively. Content management systems provide this functionality to help organizations improve the quality of information.

The content management system collects information from the various sources (Boiko, 2002). These sources of information may include legacy systems, databases, or output from programs executed within the organization. The content management system then manages this information in such a way that it can be easily retrieved. The content management system will then be able to respond to requests from users by publishing quality assured information.

A content management system thus provides information to various employees within the organization. However, certain information may be sensitive to particular users of the content management system. It is thus of vital importance that certain security mechanisms are implemented to prevent users of the content management system from viewing information not meant for them (ISO, 1989).

Access controls are security mechanisms implemented to prevent users from accessing unauthorized information (Oppliger, 2001). By implementing access controls within a content management system, the risk of a user viewing sensitive information is drastically minimized.

2 Content Management Systems

Content management can be seen as the overall process for collecting, managing, and publishing information (Boiko, 2002; Pokorny, 2001). In order for the organization to build a content management system the organization has to realize what information an organization has and identify the information an organization needs (Boiko, 2002).

Content management systems enable not only the users within the information technology department to add information but also allows users throughout the organization to add information as well (Pokorny, 2001).

Collecting, managing and publishing of information, known as content components, is the responsibility of the content management system. As depicted in figure 1 the content management system has 3 distinct systems.

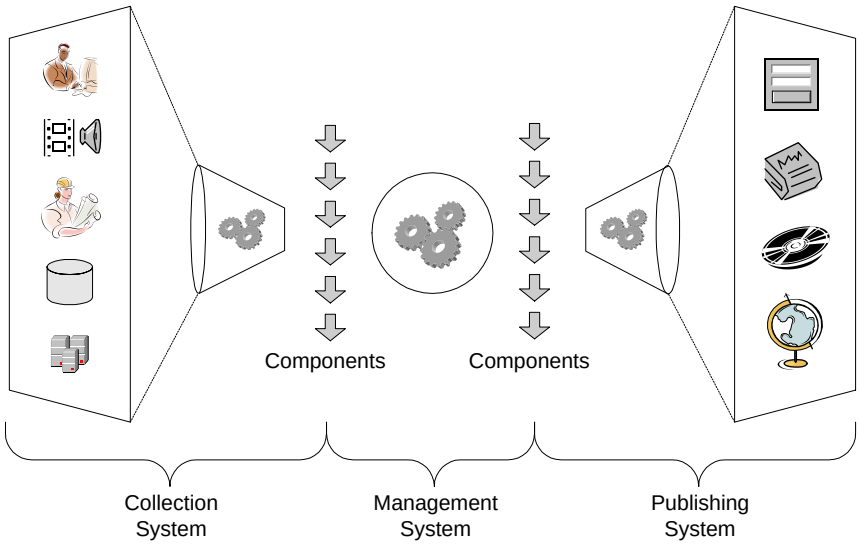

Figure 1: Content Management Responsibilities
(Boiko, 2002)

The first system is the collection system which collects raw information. The gathered raw information is then transformed into content components and placed in a data store known as the management system. The management system is the second system of the content management system. Content components are then obtained from the management system and transformed

into publications by the the third system of the content management system, the publication system.

The content components have to be stored in such a way that they can be easily retrieved by the publishing system and as such, the management system will transform the content components for publication. All of these transformation phases are collectively known as information staging.

The information staging phase of the content management system will operate upon sensitive information and as such information security should play an important role.

3 Information Security

Information security has become very important in organizations over the past few years. Organizations are forced to protect their information by maintaining a high level of information security (von Solms, 1998). In order to maintain this high level of information security, developers must ensure that a number of security objectives are met.

These security objectives are implemented by means of various security services, which are declared in a standards document known as ISO 7498-2. The ISO 7498-2 is a standard defined by the International Standards Organization (ISO). ISO 7498-2 is part of the ISO 7498 standard, which is a reference model for interconnecting open systems. An addition to the ISO 7498 standard, ISO 7498-2, describes the security services that can be used when interconnecting open systems.

Five main categories of security services are defined by the ISO 7498-2 standard. They are: Authentication, Access Control, Data Confidentiality, Data Integrity and Non-repudiation (ISO, 1989). These security services can be used to enforce various security objectives.

This paper focusses on the following security objectives: confidentiality, integrity and availability. Keeping the security objectives in mind, the main focus, concerning this article, is access control requirements within a content

management systems.

4 Access Control Requirements for Content Management Systems

According to Oppliger (2001) access controls prevent unauthorized access to the resources of a system. Thus, access controls are implemented to prevent users from gaining access to resources they are not permitted. These access controls are implemented as a result of certain access control requirements.

In content management systems it is imperative that access controls, resulting from the access control requirements, play a significant role.

In this paper we propose that access control requirements for content management systems can be divided into two categories. Firstly, there are access control requirements in line with the organization's policies and procedures. Secondly, there are access control requirements for when access control is enforced.

The following is the proposed list of access control requirements for content management systems:

- Specification in line with policies and procedures
  - Simple
  - Least Privileges
  - Temporal
  - Separation of Duties
  - Easy to maintain
- Enforcement
  - Changes according to business processes
  - Access history

– Unobtrusive

These access control requirements will now be described in more detail.

4.1 Specification in line with policies and procedures

Policies and procedures include various rules concerning the organization and encapsulates the goal/mission of the organization. There are various access control requirements as a direct result of the policies and procedures. The following sections explain these requirements in more detail.

4.1.1 Simple

Access controls as previously enlightened provide mechanisms to prevent users from gaining access to resources not meant for them. It is thus very important that access controls provide a fair amount of security. However, the access controls should not complicate user access to the content management system. The access controls should also be very simple to implement into the content management system (Bullock & Benford, 1999).

For example, the content management system administrator realizes that there might be a problem with inferred information. If he decides to implement several access controls to prevent users from inferring information, it could lead to employees not being able to gain access to information they require. It would also be an arduous job to implement these access controls to cater for this problem. As such, it is important to maintain simplicity in order to improve the ease of administration of the content management system.

4.1.2 Least Privileges

In order for users to do their job, it is imperative that they have the correct permissions in order to gain access to the information they require. However,

these permissions should not allow users to gain access to information that is not meant for them. Accordingly, users should receive a minimum set of permissions to perform a specific task (Botha & Eloff, 2001).

For example, a manager may only be able to change the salaries of staff members that report to him. He must not be able to change his own salary or the salaries of any other staff member other than those staff members that report to him.

4.1.3 Temporal Permissions

Certain users only need to gain access to information during specific times. Permissions thus need to be assigned to these users in order to restrict them from gaining access to information during unspecified times. These access permissions are called temporal access permissions. The assigning of temporal access permissions has been noted in many application security policies as a crucial requirement (Bertino, Bettini, Ferrari, & Samarati, 1998).

For example, Kurt is a part-time employee at an organization and uses the content management system to gain access to information tailored for his specific job function. However, Kurt only needs to have access to the information on Fridays between 15:00 and 18:00 and Saturdays between 09:00 and 13:00. It is thus important for the content management system administrator to assign Kurt temporal access to the information he needs. The permissions should only take effect at the times Kurt is working.

4.1.4 Separation of Duties

Fraud and major errors could have a significant effect on an organization. Therefore, separation of duties is implemented to reduce the possibility of these kinds of problems within an organization. The separation of duties divides tasks and associated privileges in such a way that more than one user is required to complete a specific task in order to prevent collusion (Ahn & Sandhu, 1999).

For example, Sue is the financial manager and a user of the content management system. Sue is able to submit information regarding the ordering of office equipment to the content management system. However, Sue must not be able to approve the addition if this information into the content management system. It is normally the system administrator or the system itself that adds the information to the content management system. This information is passed through various processes to ensure its integrity before being added to the content management system.

4.1.5 Easy to maintain

It is very important that changes of access permissions should be easy to examine and to modify. If changes need to occur within the systems, it is important that those changes are only necessary on the access control service and not on any other component of the system (Botha, 2001).

For example, John is promoted to assistant manager in the purchasing department. Human resources notify the content management system administrator of the change in the organization. It should be as easy as a few clicks of the mouse to reassign the new permissions in order for John to do his new job.

4.2 Enforcement

Certain access control requirements need to be enforced during the run-time of the content management system. These access control requirements are implemented at design time, but only take effect when the content management system is executing. These access control requirements that need to be enforced during the run-time of the content management system will now be described.

4.2.1 Changes according to business processes

From an organization's point of view the effective management of business processes is becoming increasingly important (Atluri, Huang, & Bertino, 1998). The reason for this being that according to Wells (2000) even small improvements to the business processes can have a substantial effect on the success of an organization. Furthermore, the access control requirements will have to change if one or more of the business processes change.

For example, in the past each department within the organization had a staff member purchasing articles for that department. The head of department only had to give his permission and the purchase could be made. The organization then decided that because of non-vital purchases a purchasing department was required. This new purchasing department became part of the finance department.

In order for articles to be purchased for a department an employee first had to get permission from the head of the department. Next, a purchase order would be send to the purchasing department. The purchasing department would then decide whether their purchase order was required or not.

4.2.2 Access history

Users often search for information that they require, but the information that gets returned tends to be insignificant. This is the result of most web structures being large and very complex. In order to improve the usability and user retention of a web site, the needs of users should be predicted (Eirinaki & Vazirgiannis, 2003). Furthermore, the access controls that a user needs should also be predicted. This can be done by keeping records of the user's activities.

For example, Sue is a user of the content management system. One of Sue's job functions is to calculate the inventory level of the organization's warehouses every Friday. She thus needs all the dispatch information of all the warehouses every Friday morning.

If a register is kept of each time Sue accesses the dispatch information, the system should realize that Sue uses the permission on a regular basis. The content management system should attempt to personalize the permission and make access to the information quicker.

4.2.3 Unobtrusive

When the access controls are implemented it must integrate with the system in such a way that it does not interfere or give extra overhead for the users of the system (Bullock & Benford, 1999). Thus, features currently used within the system must be used where possible.

For example, Ben logs onto a system with his username and password. Ben is then able to access all his necessary programs without entering his username and password again. The company decides to implement a content management system. Now Ben must first log into his machine and then when he wants to gain access to the content management system he will need to enter a username and password again. To complicate the whole situation, the username is different to the one Ben uses to log onto his machine. By integrating authentication throughout the disparate systems it will be possible to make security less obtrusive.

5 Conclusion

Organizations can definitely benefit from collecting and managing their information in a proper manner. Content management systems are specifically designed for this purpose. However, the problem of users of the content management system gaining access to information not meant for them can be addressed by implementing specific security mechanisms. Because access controls were specifically designed for preventing users from gaining access to unauthorized information, this paper focused on access control requirements for content management systems. Not only does access controls ensure that information is kept confidential, it also helps by assuring that the integrity of the information is maintained.

Various access control requirements were identified and discussed in more detail. These access control requirements could be divided into two parts. The first part was access control requirements in line with the policies and procedures of the organization. The second part was access control requirements that need to be enforced while the content management system is executing. Furthermore, the content management system administrator is responsible for implementing the various access controls resulting from the access control requirements. It is also the responsibility of the content management system administrator to maintain the content management system and ensure that maximum security is intact.

This paper concludes that although various access control requirements were identified, it is believed that many more other requirements exist. When implementing a content management system, it is of vital importance to have good security mechanisms in place. However, if there are too many security mechanisms, the content management system could contain certain flexibility issues. Finally, this paper has shown that access controls in a content management system is necessary and has described certain access control requirements for this purpose.

References

Ahn, G.-J., & Sandhu, R. (1999). The RSL99 language for role-based separation of duty constraints. In *Proceedings of the 4th ACM workshop on role-based access control* (pp. 43–54).

Atluri, V., Huang, W., & Bertino, E. (1998). An execution model for multilevel secure workflows. In *11th ifip working conference on database security, august 1997, and database security, xi: Status and prospects.*

Bertino, E., Bettini, C., Ferrari, E., & Samarati, P. (1998). An Access Control Model Supporting Periodicity Constraints and Temporal Reasoning. *ACM Transactions on Database Systems*, *23*(3), 231-285.

Boiko, B. (2002). *Why Content Management – A Content Management*

Domain White Paper (Tech. Rep.). www.metatorial.com: Metatorial Services Inc. and HungryMinds Inc.

Botha, R. (2001). *CoSAWoE : A Model for Context-sensitive Access Control in Workflow Environments.* Unpublished doctoral dissertation, Rand Afrikaans University, Pretoria, South Africa.

Botha, R., & Eloff, J. (2001). A framework for access control in workflow systems. *Information Management and Computer Security*, *9*(3), 126-133.

Bullock, A., & Benford, S. (1999). An access control framework for multi-user collaborative environments. In *Proceedings of group'99* (pp. 140–149). Phoenix, Arizona.

Eirinaki, M., & Vazirgiannis, M. (2003). Web Mining for Web Personalization. *ACM Transactions on Internet Technology*, *3*(1), 1-27.

ISO (Ed.). (1989). *Information processing systems Open Systems Interconnection Basic Reference Model Part 2: Security Architecture.* http://www.iso.org: ISO.

Oppliger, R. (2001). *Security Technologies for the World Wide Web.* 685 Canton Street Norwood, MA 02062: Artech House, INC.

Pokorny, J. (2001). Static Pages are Dead: How a Modular Approach is Changing Interaction Design. *Interactions*, 19-24.

von Solms, R. (1998). Information security management (1): why information security is so important. *Information Management and Computer Security*, *6*(4), 174-177.

Wells, M. (2000). Business process re-engineering implementations using Internet technology. *Business Process Management Journal*, *6*(2), 164-184.

Acknowledgement: We would like to thank the National Research Foundation for their financial support for research conducted towards this paper.