Chapter 19
A Software Engineering Approach for Access Control to Multi-Level-Security Documents

Muneer Ahmad
King Faisal University, Saudi Arabia

Low Tang Jung
University Technology PETRONAS, Malaysia

Noor Zaman
King Faisal University, Saudi Arabia

Fausto Pedro García Márquez
University of Castilla-La Mancha, Spain

ABSTRACT

Access control to multi level security documents is very important and challenging issue. Millions of organizations around the globe intend to apply security levels over their confidential documents to protect from unauthorized use. Some numbered access control approaches have been proposed and an optimal solution is the need of the time. This chapter presents an overview of a robust software engineering approach for access control to multi-level security documents. The access control system incorporates stages including data refinement, text comprehension, and understanding of multi-stage protection and application levels. It will scan the document, tag the sections of certain text, understand the meaning of various levels, group-up the text using bottom-up approach, and then classify the levels as per protection norms (set as organization wise) defined. This approach will be very helpful for multi-level protection of precious information. Only authorized users would be able to access the information relevant to them as defined by the authorities.

INTRODUCTION

The information which is tagged can be termed as sensitive information (restricted by a group of people or government, agencies as per rules defined for its protection). The defined system must provide the check and balance to deal with tagged documents (identified as secure), e.g. the demands to secure particular information set under prescribed norms (to make it protected by unlawful use). It is worth mentioning that classified information passes through a series of steps to make it in a form that is secure.

DOI: 10.4018/978-1-4666-3679-8.ch019

The institutions may take benefits by relying over usefulness of precious document handling that include the way to share, collect, functionalize, feedback, associate and provide the fair and secure means for its protection. Gupta (1996) narrated that such multi level processing leads us to a fact that relevant information should be provided to relevant authority at specified time employing secure means. The only possibility that provide the state of the art methodology is to adopt certain criteria's that govern the security classification. All these efforts to protect the documents from unauthorized use are to judge the importance of documents travelling from one hand to another hand passing through different unsecure levels. The classification phenomenon reflects that all documents can't be treated with one norm of security. Different documents must possess different security levels. As an analogy, in an office environment, the documents arriving and departing the top management have different security requirements against the normal documents.

The series of channels that may describe the said phenomenon is to look for potential contributors that claim the ownership of this information, one the ownership is identified, the documents can be assigned different labels (as per policies defied to protect the information). The labeled information is further passed through security checks (security controls) as per some defined criteria. Finally the security controls can be listed against each classification as explained by Murata (2003).

Another very important aspect to protect this information depends over the factors that relevant institute demands the importance under which the information should be handled. So before implementing the security policies, the organization should review the levels of security tags set for protecting specified information. It is also mandatory that information in how much old? In the case, protection levels are rarely used, some latest information important for the organization should be made protected (Wikipedia, 2012). Legislation and development of security norms also vary from organization to organization.

Some Common protection levels that could be used by organizations are termed as public, trusty, confidential and private. The government institutes may incorporate classification labels as Sensitive and Unclassified, confidential, Normal Secret and Top Secret. It is mandatory to mention the relationship between these tags for confirming the best product.

Secondly, once the security levels are implemented under organization policies and norms, the people working in such institutes must be given some basic and advanced training to get a clear picture for securing information. They must also understand and focus the need to protect their information. Likewise, different places may incorporate different security levels as per need (WikiPedia (Wiki), 2012).

A very little work has been done and being researched in the area of documents protection from unauthorized use. Current, state of the art research done by Alhammouri (2008) depicts piece wise security classification (may incorporate some approaches like TOP-BOTTOM approach).

Another current approach proposed by Damiani (2000) for document protection is utilization of access control model (using XML). This model has been implemented with a restriction to process it up to DTD (Data type definition) level only. It makes each data type definition to be pertained with specified information wrapped in the document (deciding which part can be accessed by user and which can't be).

The document protection can also be made by fragmenting the security levels into different security classes, as an analogy, the University of Auckland (New Zeeland) developed a tool for security protection of local documents. The tool implemented the security level as described the norms set by the institute. Another institute NIST