Fine-Grained Access Control for Database Management Systems

By
Rahat Masood
2010-NUST-MS-CCS-09

Supervisor
Dr. Muhammad Awais Shibli
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS CCS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(May, 2013)
Abstract

The pervasive nature of computing paradigm has made Database Management Systems (DBMS) a predominate technology for business and enterprise applications. With the explosion of information in the computing world and the extensive use of information services, the role of database systems is continuously growing. These rapid technological advances require companies to adopt Database Management Systems that should not only be fast, scalable and reliable but also provide security from internal and external threats.

However, the proliferation of information systems in organizations worldwide (communication, transport, education, manufacturing, medicine, business etc.), has increased difficulty in controlling access to data which sometimes results in instigation of various security attacks. This increased reliance on information systems imposes different protection and privacy requirements on DBMSs. Moreover, the advancement in database technology (mainly including Object-Oriented and NoSQL) has made traditional security controls no longer adequate for providing effective security measures, since design and principles of such databases are completely different from those of traditional databases. These latest database paradigms invoke many provoking thoughts towards the security of data. The number of attacks including code injection, inference attacks, DoS attacks can be launched on these databases and basic database vulnerabilities such as unauthorized access, excessive privilege abuse, out-dated patches and misconfigurations may lead to avenues of attack on databases.

In this tip, sensitive data of an organization needs to be protected through various security controls primarily by practicing Authentication, Authorization, Encryption, Intrusion Detection System, Auditing and Availability mechanisms. Among these mechanisms, Access Control is considered one of the strong driving forces for protecting the data of an organization as well as preserving the privacy of individual users. In order to provide the strong shield of protection in Database Management Systems, a fine-grained access control scheme, to control access at the row and column level or even at cell-level, should be effectively implemented for the traditional and the latest
Abstract

There exists voluminous literature on specifying and modeling fine-grained access techniques for relational databases, however, very less or no work has been done to formalize the fine-grained access control model for unstructured databases (NoSQL and Object-Oriented). An effective FGAC approach is needed that can meet different protection and privacy requirements of databases for the guaranteed data integrity and authorized access. In addition, various FGAC techniques for relational databases have been proposed, however, suitability and adequacies of these techniques have not been explored yet. There is significant need to qualitatively evaluate the effectiveness of these techniques by proposing an assessment criterion that can measure the suitability of a FGAC technique from deployment, management and flexible access control policies perspective. Therefore, the aim of this thesis is to comprehensively investigate the Fine-Grained Access Control model for database management systems.

This thesis serves to improve the authorization issues within database management systems, particularly focusing on fine-grained access control model. Our research work specifically targets the three paramount approaches of database technology namely relational, object-oriented and NoSQL databases. We explore each of three database technologies from security perspective and pave the way to provide an effective fine-grained authorization solution for these databases. Therefore, the contribution of thesis is three-fold:

- **Benchmark for Relational FGAC Techniques:** In first part of research, we devise a benchmark based on partially ordered lattices for evaluating the effectiveness of FGAC techniques for various database deployment scenarios, each having different security requirements. The devised benchmark is based on NIST access control metrics and heavy scrutiny is performed based on which they are further classified into FGAC classes and security levels. Following the qualitative approach, we have also performed a comprehensive analysis on different FGAC techniques, given in literature and evaluated them according to our benchmark metrics. This research work details which particular FGAC technique to select that can match the security requirements of various organizations.

- **Annotation based Fine-Grained Authorization for Object-Oriented Databases (OODBs):** The second part of research serves to improve the authorization issues within OODBs, while exploring different access control techniques that have already been proposed. Our approach involves the realization of FGAC model in OODBs by
providing a solution based on annotations and Extensible Access Con-
trol Mark-up Language (XACML). Using the notion of meta-tagging,
we have provided customizable FGAC annotations which can be at-
tached to OODB platform for the executing the access control policies.
Our proposed approach has deduced that incorporation of FGAC with
OODBs reduces the security issues and could possibly be resulted as
an effective deployment in insecure computing paradigms.

- **Fine-Grained Encryption & Authorization for Unstructured
Databases:** Our last part of research deals with the security analysis
of NoSQL databases. Our analysis indicates that very basic level of
security features are provided in these databases since the main focus
is towards providing the high performance and scalable architecture.
In order to ensure the provable security features, we have provided
a fine-grained encryption and authorization system for unstructured
databases, particularly NoSQL databases. For the realization of the
proposed system, a FGAC model is implemented using XACML 2.0 and
an encryption mechanism is provided through cryptographic functions
using Java libraries. MongoDB, a document oriented database, is taken
as a test database for the verification of system.

In particular, this thesis intends to address and analyse the access con-
trol issues of database systems (relational, Object-Oriented, NoSQL) and
contributes towards providing a fine-grained access control by specifying ac-
cess rights at finer granularity.