EPiC Series in Computing

Volume 45, 2017, Pages 77–82

SCSS 2017. The 8th International Symposium on Symbolic Computation in Software Science 2017

Towards a Reliable Formal Framework for Enhancing Risk Assessment in Access Control Systems

Pierrette Annie Evina, Faten Labbene Ayachi, Faouzi Jaidi and Adel Bouhula

Higher School of Communications of Tunis (Sup'com), University of Carthage, Tunis, Tunisia.

Pierrette.evina@supcom.tn, faten.labbene@supcom.tn, faouzi.jaidi@supcom.tn, adel.bouhoula@supcom.tn

Abstract

The constant evolution of access control requirements and the dynamic environment in which they evolve require nowadays quick and instant decision-making related to risk of illegitimate access in Information Systems. Various contributions defined in the literature aim to overcome or to mitigate related risks and paradoxically adopted the hypothesis of reliability and validity of access control policies. However, the corruption of these policies is a security aspect of great importance and should be handled actively because (i) an access control policy is also exposed to the same threats as the managed data is and (ii) properties and parameters of the concrete policy at a given stage may differ, in a critical manner, from a reference stage. We define a reliable and complete solution for risk management in the context of Database Servers. We intend to define a rigorous risk management approach that mainly verifies recommendations of the standard ISO 31000:2009. Our approach takes into consideration all identified threats on a Database Server and provides an environment for the analysis of the correlation between the threats detected in particular by different security devices. To ensure a high level of surety, we opt for defining a formal framework that allows to efficiently address this problematic and to formally represent and verify our risk management processes.

1 Introduction

Although corruption of Access Control Policies (ACP) is a serious security aspect, it remains not enough discussed in literature and almost all research works adopted the hypothesis of reliability and validity of ACP. In a database context, the ACP is closed to the data it protects and is also exposed to

attempts of corruptions. Hence, the validation of ACP has emerged in a crucial practice to ensure the conformity of an implemented policy with the specified one. Validation is a nonstop step in the lifecycle of the ACP. The Security Architect has to be helped with adequate tools to perform this step and detect anomalies, if they do exist, in the expression of implemented ACP.

Consequently, it becomes appropriate to strengthen the validation process by an automatic decision maker each time anomalies of non-compliance are detected. We propose to analyze the validation process output through a reliable Risk Management System (RMS) that allows (i) identifying actual risks (ii) minimizing their effects always they occur in future (iii) learning from the history of detected anomalies and (iv) predicting future threats on the database.

Our contribution includes risk assessment and risk treatment processes specifications according to the ISO 31000: 2009 standard. From the analysis of the history of the non-compliance anomalies detected during the ACP evolution, an evaluation and a quantification of the exposure of a given database schema to risks will be carried out.

The remainder of this paper comprises the following paragraphs. Paragraph 2 discusses about related works, paragraph 3 presents our proposed framework and paragraph 4 concludes the paper.

2 Related works

Researchers have investigated risks in access control systems and have produced various approaches to risk management. We classify different efforts in three trends: (i) A quantified risk assessment approach which allows to calculate the risks associated with the actions of users (Cheng 2007) (Ma 2010) (Ma 2012) (ii) An approach based on the concept of the confidence level assigned to each user separately and thus to calculate the risks associated with the allocation of authorizations to users (Baracaldo 2013) (iii) A mitigation approach that proposes techniques and measures to reduce identified risks (Feng 2008). All these proposals are either access-granted based or user-confidence based approaches.

Authors in (Jaidi 2015-a) proposed a policy-evolution based approach which is a dynamic risk-aware approach that evaluates the risks related to the non-compliance anomalies detected on the ACP. The authors qualify the state of evolution of the policy by estimating rating and thresholds to bind each rate. Authors do not go deeper in the risk management process specifications as their proposal was not fine-grained. Our contribution takes up the results of this work to specify an overall risk management system. To be more effective, our system must take into account the output of other intrusion detection mechanisms activated on the server such as the log files and the audit mechanisms.

In (Jaidi 2015-b) authors introduce basic formal definitions that help detecting and discussing non-compliance anomalies in RBAC-based policy. The V&V process requires putting in duality two different notations. To do so, they consider that **ACP** denotes the formal specification of the policy and $\mathbf{ACP_{\_IMP}}$ is the formal representation of implemented policy.

Anomalies of inconsistency belong to access control rules that are syntactically conform to the RBAC model, but not initially foreseen during the specification of the policy. It includes hidden users, hidden roles and hidden access flow. Hidden users are visible when new users, not initially defined, are injected in the concrete instance. Hidden roles are observable when new roles, not initially planned, are introduced in the concrete policy. Hidden access flow is perceptible in the case of illegal assignments of: roles to roles, roles to users or permissions to roles. Authors go further to formally define concepts of missed users, missed roles, missed access control flows, renamed roles, renamed users and redundancy in AC Policy. Outputs of the validation process detailed in (Jaidi 2016) constitute an input of our risk management system. We detail our approach in what follows.

3 Our proposed framework

An unauthorized updating of the access control policy reflects the exposure of data to the risk of corruption. The exploitation of this anomaly by an usurper to achieve illegal access to the database resources cannot be detected by other intrusion detection mechanisms. However, one solution is to use the outputs of the trace tools to reconstruct the accesses made.

We rely on the following three scenarios to justify our remarks. (i) For any hidden user it is possible to retrieve from the log files all the accesses that he has made to the data and to detect possible vulnerabilities not covered by the security system. (ii) The existence of a Hidden role is an indicator which makes it possible to identify all the target data and intervene for example to raise their degree of criticality and to update the risk factors. (iii) The correlation between two or more anomalies makes it possible to go further in the interpretation of corruption attempts in complex organizations. i.e. the existence of a hidden role attributed to a hidden user.

In following we develop these three aspects and we rely on formal definitions to go further in our reasoning and demonstration.

3.1 Tracking of hidden users

A definitively hidden user may have already used his privileges to access data, or execute stored procedures. The audit mechanism, if activated, allows retrieving the scenarios of the accesses made by the hidden user on the data.

We define then as *Unauthorized Access* of a hidden user the sequence of elementary SQL actions performed on the data during a session initiated for this user. An *Unauthorized Access* consists of a set of N nodes and a set of directed edges between nodes. Each node represents an SQL statement.

We define the *Tracking of a user* the set of all *unauthorized accesses* performed by the user on the database. The analysis of the trace of a user makes it possible to detect the recurrent unauthorized accesses, identify the target elementary data, or to replay the attempts of fraud if necessary.

A similar concept to *Unauthorized Access* is the concept of *Application Profile* introduced in approaches dealing with intrusion detection solutions. In (Bouchahda 2010) authors enhances that protecting the database from insider threats requires sophisticated techniques able to build profiles of normal access and detect anomalous access with respect to those profiles.

3.2 Correlation of anomalies

The discovery of hidden users is a conductor that makes it possible to go further in the analysis of fraud attempts. It is therefore relevant to identify the roles attributed to him, the data he has had access to, etc. We consider that assigning a hidden role to a hidden user is an elaborate level of fraud. An *Unauthorized Access* is called critical if the access is partially or totally protected by a hidden role. Also, we call *suspicious user* any user associated directly or indirectly with a hidden role. It may be useful to analyze previous accesses to data of a suspicious user or assign it to a customized audit.

3.3 Target Data

According to (6), the set of permissions associated to a given hidden role allows to compute the set of objects of the database referenced by the hidden role. *Tracking* a hidden user or a suspicious user makes it possible to identify the elementary data targeted by the unauthorized access. It is relevant at this level to identify the following classification of sensitive data:

Conceptually Sensitive Data: are database objects identified as critical by the administrator of the database schema. The definition of access control to these objects is the responsibility of the security architect.

Strategically sensitive data: objects that are referenced in hidden roles or data referenced in unauthorized access scenarios.

4 Architecture of the Risk Management System

As recommended by the ISO 31000: 2009 standard we enhance our Risk Management System (RMS) by (i) a Risk Assessment Engine (RAE) which is downstream of the Risk Treatment engine (RTE) in figure 1 below. The risk assessment phase is usually developed in 4 steps: Context assessment, Risk Identification, Risk Analysis and Risk Evaluation.

In the following, we detail step by step functionalities of our RAE engine.

- The Context Assessment step consists in identifying relevant outputs incoming from other security mechanisms activated on the Database Server.
- The Risk Identification step deals with the integration of the security data with regard to a given database schema, and target security mechanisms. This integration step includes the transformation of these data into a single formal notation.
- Risk Analysis step go further in the exploration of illegal access scenarios. It is based on a formal analysis of integrated security data to calculate relevant correlations.
- Risk Evaluation step uses the previous results to adjust the parameters and risk factors. It is a phase of self-adaptation that allows our system to correct its estimate of the risk incurred.

Risk Treatment Engine (RTE) implements several reaction mechanisms or security barriers. We cite, for example, the need for a customized audit that is the activation of monitoring on the activities of a given user, the adaptation of the security policy to new needs, etc.

We verify that the implementation of a Risk Monitoring Engine will strengthen the capacity of RMS by a monitoring and warning functionality crucial for the Security Architect.

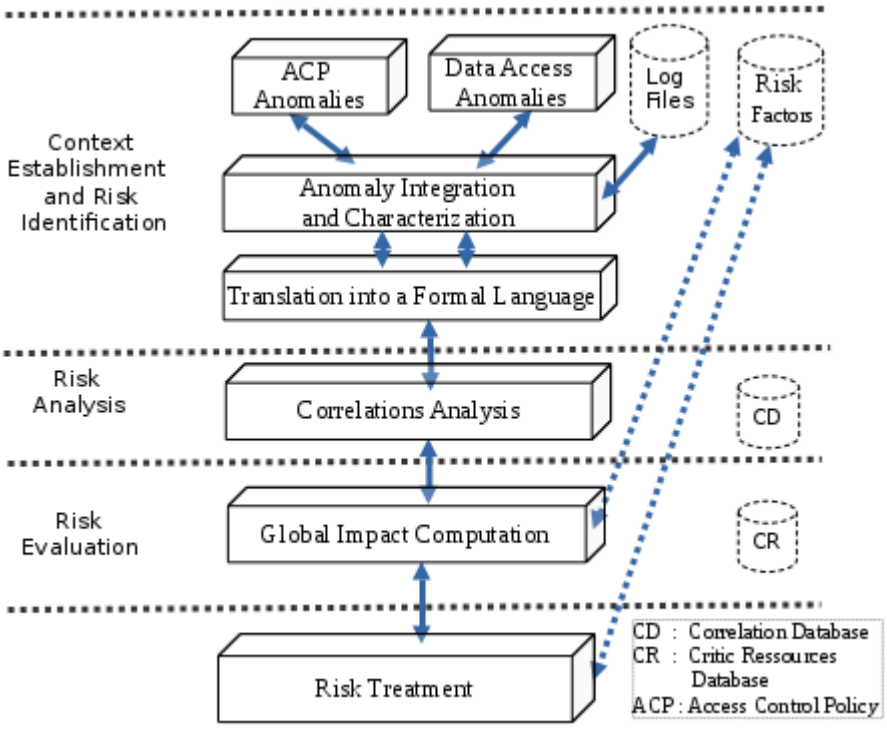

Figure 1: Risk assessment approach.

5 Conclusion

The deployment of an effective risk management approach is based on a good identification of the problems encountered. The exploitation of output of the formal validation process on database AC Policies has enabled us to achieve this objective. Furthermore, the establishment of a relevant Risk Management System for DBMS will better protect these critical resources, measure the risk encountered and intercept it.

RMS is a necessarily customized solution for a personalized security solution. Our approach makes it possible to integrate outputs coming from different security mechanisms such as log files, audit mechanism, validation process, and so on. This first step allows going further in the analysis and interpretation of the risks incurred by the DBMS.

Data managed by the RMS system such as unauthorized access, tracking, etc. are relevant information whose lifetime will be longer than the lifetime of the initial data used for their calculation. For example, the content of log files has a limited lifetime because these files are regularly reset by the database administrator. The RMS solution is also the memory of the architect security.

References

R. Sandhu, E. J. Coynek, H. L. Feinsteink, and C. E. Youmank. (1996) Role-Based Access Control Models", IEEE Computer, vol. 29, no. 2, (pp. 38-47).

K. Z. Bijon , R. Krishnan and R. Sandhu. (2013). A Framework for Risk-Aware Role Based Access Control. 6th Symposium on Security Analytics and Automation.

F. Jaidi and F. Labbene Ayachi. (2015). A Risk Awareness Approach for Monitoring the Compliance of RBAC-based Policies. In Proceedings of the 12th International Conference on Security and Cryptography (SECRYPT-2015), (pp 454-459)

International Electrotechnical Commission, International Standard, ISO/IEC 31010:2009, First Edition, 2009.

P.-C. Cheng, P. Rohatgi, C. Keser, P.A.Karger, G.M. Wagner, A.S. Reninger, (2007). Fuzzy MLS: An Experiment on Quantified Risk–Adaptive Access Control, In Security and Privacy, (pp.222 –230).

F. Feng, C. Lin, D. Peng, J. Li, (2008). A trust and context based access control model for distributed systems. In Proc. of the 10th IEEE International Conference on High Performance Computing and Communications, HPCC '08, pp. 629-634.

L. Chen, J. Crampton, (2011). Risk-aware role-based access control. In Proc. of the 7th International Workshop on Security and Trust Management.

J. Ma, (2012). A formal approach for risk assessment in RBAC systems. Journal of Universal Computer Science, vol. 18, pp. 2432-2451.

J. Ma, K. Adi, M. Mejri, L. Logrippo, (2010). Risk analysis in access control systems. In Eighth Annual International Conference on Privacy Security and Trust (PST), pp. 160-166

N. Baracaldo, J. Joshi, (2013). An adaptive risk management and access control framework to mitigate insider threats, Computers & Security.

A. Bouchahda-Ben Tekaya, N. LeThanh, A. Bouhoula, F. Labbene Ayachi, (2010). An Access Control model for Web Databases. 24th Annual IFIP WG 11.3 Working Conference on Data and Applications Security; DBsec 287-294.

F. Jaidi and F. Labbene Ayachi. (2015). A formal approach based on verification and validation techniques for enhancing the integrity of concrete role based access control policies. In International Joint Conference (pp. 53-64). Springer International Publishing.

F. Jaidi. (2016). Spécification, Analyse et Vérification Formelle des Implémentations des Politiques de Contrôle d'Accès dans les SGBDs. (in french). Phd Thesis, SUP'