Anomalies Correlation for Risk-Aware Access Control Enhancement

Pierrette Annie Evina, Faten Labbene Ayachi, Faouzi Jaidi and Adel Bouhoula
Higher School of Communications of Tunis (Sup'com), University of Carthage, Tunis, Tunisia

Keywords: Anomalies, Correlation, Access Control Policy, Database, Risk Management.

Abstract: In the context of database management systems (DBMS), the integrity of access control policies (ACP) is a constantly neglected aspect. However, throughout its evolution, ACP is not valid and free from irregularities due to users and administrators actions, intentionally or not. So, considering regular ACP updating activities, we pay a particular attention on anomalies in ACP expression. Taking into account the correlation that exists between two or more of such anomalies, we present the "correlated threats management system" (CORMSYS). This system must detect and analyze the correlation between anomalies since we believe that handling correlations between anomalies can reveal sophisticated intrusion scenarios in DBMS. The presented system also produces the necessary input for new risk management approach that will consider and overcome the effects induced by the correlation between anomalies found in the ACP expression. CORMSYS is composed of four main parts: (i) the Correlation Definition and Analysis subsystem; (ii) the Users Tracking subsystem; (iii) the Intrusion Scenario Identification subsystem and (iv) the Illegal Behavior Modeling subsystem.

1 INTRODUCTION

For access control, the detection and the analysis of anomalies and intrusions are widely discussed in the field of information systems (IS) and particularly in database management systems (Bertino et al., 2010).

Actually, the integrity of ACP is a neglected aspect in the literature as many authors spontaneously think about the reliability of the access control policies expression. Although, policies that govern access control in IS or DBMS are also subjected to anomalies that make them vulnerable at one stage or another in their lifetime.

Focused on anomalies in ACP expression, we then propose to assess regular ACP updating activities. This action can inevitably lead to a variety of anomalies such as those stated in (Jaidi et al., 2017). These anomalies are sometimes due to a partial implementation or they are just anomalies of non conformity, redundancy, inconsistency and contradiction in the expression of policies. So, in this context, what is the induced impact of this correlation when these anomalies are correlated with each other? Can the assessment of this impact have positive consequences on the overall risk management of ACP?

Our intention is to implement a "correlated threats management system" (CORMSYS). This system uses identified anomalies found in the ACP expression, analyzes the correlation existing between them in order to produce a database of risk factors related to the effects induced by the anomalies correlation.

Of course, the study of correlation is nowadays increasingly used for the risk analysis. But, to the best of our knowledge, the correlation between anomalies in ACP has never been discussed and we think that if this is done, it can enhance the well-functioning of ACP in DBMS. Our contribution aims to design a system that detect and report correlations between anomalies in ACP expression, for the revelation of sophisticated intrusion scenarios that constitute a major threat in systems. Our system will furnish inputs for a new risk management approach that will precisely consider the effects induced by the anomalies correlation in ACP expression.

The remainder of the paper comprises the following sections: section 2 gives the problem statement; section 3 proposes the basic representation of the topic related terms; section 4 presents our proposed framework; section 5 gives the methodology used; section 6 discusses the related works; section 7 concludes the paper.

Evina, P., Labbene Ayachi, F., Jaidi, F. and Bouhoula, A.
Anomalies Correlation for Risk-Aware Access Control Enhancement.
DOI: 10.5220/0006766802990304
In *Proceedings of the 13th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2018)*, pages 299-304
ISBN: 978-989-758-300-1

2 PROBLEM STATEMENT

ACP is a set of access control statements materializing the association between user, action and object. In ISS and particularly in DBMS, ACP are subject to attacks of various types as well as the access control systems they govern and the impact of these attacks often has considerable effects. Thus, ACP is said to be corrupt if an access control statement is illegally added, modified or suppressed in that ACP. The identification of these statements or anomalies is carried out in a validation phase which consists in analyzing two consecutive versions of the policy: a reference version and an active current version.

The syntax analysis of the anomalies makes it possible to identify the correlations that may exist between them. A correlation between anomalies underlies an elaborate scenario of policy corruption and therefore an elaborate scenario of intrusion. We presume that the harness of the statistical link existing between two anomalies or more can considerably improve the treatment of the risk of degradation of the information systems, precisely, that of the DBMS. Moreover, in order to alleviate or remedy the effects of these anomalies, it is appropriate to set up a risk management system. We believe that it is necessary to deeply carry out the analysis of anomalies in ACP by the establishment of a learning system for the management of incidents or attacks and to perform the assessment of the risks arising from the correlation between these anomalies of non-conformity.

Taking into account the attacks on AC in DBMS as well as the discrepancies that may exist between a concrete ACP and the initial version of the same policy, we plan to produce a formal approach for the risk management in the case of policies degradation in DBMSs. Our approach takes into account the recommendations of the ISO 31000 standard and will be able to analyze and evaluate the risk induced by the correlation of ACP anomalies. A "correlated threat management system" (CORMSYS) is designed to enhance the presented risk management approach by producing the necessary input. Thus the present paper aim to present the CORMSYS framework situated upstream on the overall risk management system proposed for the future.

3 BASIC REPRESENTATIONS

As ACP (access control policy) defines the authorized access of users to database objects, an access control statement can be represented by the triplet (U_i, A_j, O_k) where U_i designates a given *authorized user and* (A_j, O_k) designates the permission to execute an *authorized action* A_j on a *visible object* O_k .

An *authorized user* is any user identified in the DBMS by a login and a password and being authorized to connect the database server.

An authorized action is any action being specified in the ACP i.e. insert, select, update, delete, execute, etc.

A *visible database object* is any object being specified in the ACP i.e. a table, a view, a procedure, etc.

We introduce in the following the syntax that we adopt to materialize the possible alterations of an access control statement.

(a)	(U_i, $\bar{A}_j$, $\bar{O}_k$).	Authorized user assigned not specified permission.
(b)	($\bar{U}_i$, A_j, O_k).	Unauthorized user assigned authorized permission.
(c)	(U_i, $\bar{A}_j$, O_k).	Authorized user assigned unauthorized action on visible database object.
(d)	($\bar{U}_i$, $\bar{A}_j$, $\bar{O}_k$).	Not specified access control statement.
(e)	($\bar{U}_i$, $\bar{A}_j$, O_k).	Unauthorized user assigned unauthorized action on visible database object.

Users referenced in (a), and (c) are authorized users being however corrupted.

Users referenced in (b), (d) and (e) are definitively intruders.

4 PROPOSED FRAMEWORK

CORMSYS framework is shown in figure 1 and is composed by the following four subsystems: (1) Correlation Analysis subsystem; (2) Users Tracking subsystem; (3) Intrusion Scenario Identification subsystem; (4) Illegal Behavior Modeling subsystem.

Correlation Analysis Subsystem (CAS) operates the analysis of anomalies and detects correlation between them. These anomalies are irregularities or differences visible when comparing the ACP at different stages. The anomalies, listed and located in a specified database, are scrutinized and some characteristics are determined in order to establish the statistical links existing between these anomalies. They are then translated into formal language allowing inference and deduction. This subsystem provides two kinds of outputs. (1) The set of database objects referenced in the anomalies. This set is relevant for the Risk Management subsystem for updating risk factors. (2) Set of users to be revoked and set of users to be closely supervised.

Users Tracking Subsystem (UTS) provides an investigation phase where log files are scanned to retrieve accesses made by revoked and/or supervised users. For each access, this phase extracts the four following properties: session identifier, user login, user actions on database objects. Indeed, to access data in the DBMS, a user needs to have been granted some authorizations and privileges. So, in this stage, the granted privileges are examined as well as the authorization to log into the system

Intrusion Scenario Identification Subsystem (ISIS) builds the intrusion scenarios for each user identified in the previous session. A scenario is a sequence of elementary accesses achieved on the database during a user session. So a sequence of events is described to characterize the effects involved. For example, it will be necessary to describe the user's intrusion process or the type of requests commonly used by an alleged user who wants to make use of unauthorized privilege on a given object.

Illegal Behavior Modeling Subsystem (IBMS) provides two main functions. (1) It compares intrusion scenarios and identifies their similarities. (2) It classifies scenarios according to a predefined resemblance function. By classifying the wicked actions of the DBMS users, this subsystem determines the actions that are harmful to the DBMS. At this stage, risk factors are sorted and constitute the main entries to the further risk management process. Although risk factors are constantly changing, we can contemplate a general view of these factors as there may be a constant identification of new threats and new vulnerabilities. The quantity and quality of threats are evaluated, as well as their frequency. Dangerous users are determined, listed and ranked in order of danger. That allows having a precise representation of illegal access.

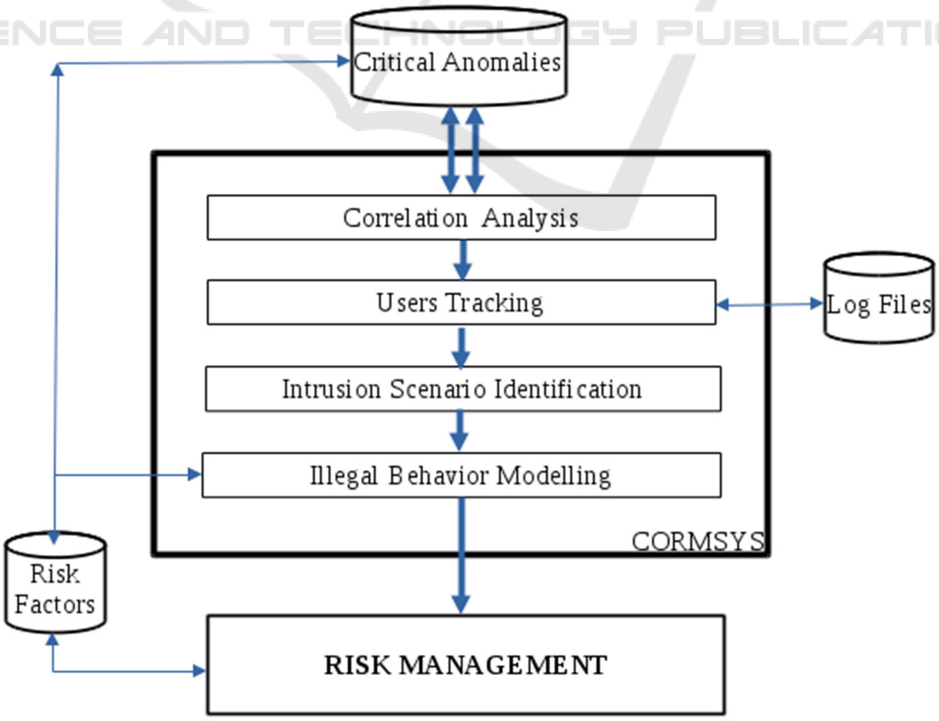

Figure 1: the proposed framework.

Risk Management Subsystem (RMS) evaluates risk. A threshold is established for the regulation of exposure of DBMS to risk. Critical anomalies are registered as they are source of high level risk in DBMS.

Indeed, these anomalies have important impact over confidentiality, integrity and availability of data in the system. Also, they have a significant impact on the integrity of the policy.

Inside the risk management module, there is a correction phase that intervenes to mitigate or to eliminate the risk of degradation of the DBMS. It is associated to a testing and control phases in order to constantly keep the system safe.

5 METHODOLOGY

In order to get more information related to our work plan, the documentary research is performed. An important number of publications have been identified and studied in order to precisely identify our contribution.

We will then formally describe our learning approach and explore the DBMS's log files in order to collect information about recurrent attacks, i.e data that are regularly and improperly exploited, as well as all the defections occurring in the ACP.

Also, a comparison is done between two states of the ACP and lead to the establishment of a list of all the anomalies and their frequency of occurrence.

Then, a formal description of the correlation definition and evaluation procedure is produced. For that purpose, a correlated threats management system (CORMSYS) is designed. CORMSYS supplies a risk management module and that will furthermore lead to the analysis and the evaluation of the risk related to the correlated identified threats.

We will adapt the features of our system to work with a real database, with real schemes and tables created. It will then be possible to confirm the results, qualitatively and quantitatively.

We expect to reach the following results:

1. Listing anomalies related to unauthorized update of access control policy.
2. Detecting induced faults through analysis of correlation between detected anomalies with more specific results:
   - Definition of the list of the recurrent targeted and sensitive data.
   - Detection and establishment of intrusive user behavior and thus, reinforcement of the Intrusion Detection Systems.
   - Production of a global and comprehendsive system for risk management in access control systems.

6 RELATED WORKS

Several works exist in the literature, leading to the detection of anomalies in access control systems including those in databases. Elisa Bertino et al had done a recap of such works in (Bertino et al., 2007). From that work, we learn that, Anomalies Detection Systems (ADS) designed in DBMS are generally intended to counter attacks related to the use of data by users.

The ADS allow detecting abnormal activities of users or applications. It doesn't take into account anomalies related to alteration of ACP specifications. In the present paper, we are especially concerned with the ACP defections caused intentionally by authorized users or database administrators.

Concerning risk management, several works deal with risk assessment techniques but generally concern the risk related to the user-data relationship. Very few works linger on the rules governing this relationship, i.e the ACP.

In (Cheng et al., 2007) and in (Khambhammettu et al., 2012), authors provide a solution to overcome the risk related to unauthorized access of users on an object in an access control system. To address this risk, the authors evaluate user confidence and the object sensitivity. Authors in (Diep et al., 2007) plan to make the access control management more dynamic and precised. They evaluate the action of users or processes on the system and take into account the context parameters. These parameters are also considered as input in the risk assessment process. (Colantonio et al., 2010) evaluate the risk occurred when managing users and permissions through the Role based access control (RBAC) during the pre-mining phase (Colantonio et al., 2010). They consider the constant modification due to the users or access permissions creation, modification, or deletion in the access control system. In (Burnett et al., 2014), the authors provide a solution to avoid unwanted disclosure information by corrupted users. They consider the risk occurred when a user manage his own data. In (Ma et al., 2010), authors mainly consider the role delegation issue which is source of risk. Authors in (Baracaldo et al., 2013) propose an access control framework to mitigate insider threats with a risk management process which is adaptive. The changes in users behaviour are osculated.

Regarding risk in ACP, few authors are concerned. (Celikel et al., 2008) deal with the risk management in the access control policy, notably the RBAC in distributed databases. They think that user's queries are risky especially when there is a misapplication of the rules established in the access control policy. Thus, in (Celikel et al., 2008) the user's queries are the main elements observed and considered while assessing risk. Some authors also sort out non-compliance defaults that occur in a role-based ACP during its lifecycle and evaluate the risk associated to the identified attacks and alterations that corrupt the ACP. They intended to ensure a high surety to that ACP.

In AC as well as in ACP, authors do not worry about the correlation that can exist between the anomalies detected. To the best of our knowledge, none of these works evokes the notion of correlation in attacks analysis. In addition to the in-depth study of the threats in ACP, we plan to explore the correlation between these threats.

Many authors already adopted machine learning techniques for the automatization of procedures of detection of anomalies and intrusions in IS and precisely in DBMS. So, authors in (Costante et al., 2013) for example, developed a machine-learning-based system that automatically acquires knowledge related to the normal behaviour of users during the database activities. Their system compares the user's sql queries exchanged with the database server and also it evaluates the sensitivity of the manipulated data in order to avoid the data leakage in DBMS. In (Darwish, 2016) the author proposes to detect anomalies using the correlation among queries in DBMS transactions with log-records. We do not use machine learning for the anomalies detection as authors in (Grushka-Cohen, 2016) do. But there exist a difference between our work and theirs. Indeed, they use detected anomalies and produce a ranking alerts system that enables to prioritize anomalies according to their importance. While we use identified anomalies and study the correlation existing between these anomalies in order to identify sophisticated scenarios and be able to adjust the risk factors when preventing ACP expression from degradation.

7 CONCLUSIONS

Over its life cycle, an access control policy faces some irregularities or anomalies in its expression. This is source of vulnerabilities for information systems (IS), especially for database management systems (DBMS).

In the current paper, we presented the CORrelated threats Management SYStem (CORMSYS) that takes into consideration the critical anomalies that threatens the ACP and analyses the correlation between these anomalies.

Our contribution aims to enhance the proper functioning of ACP by considering a wide range of anomalies for which the correlation is identified and handle for the purpose. To the best of our knowledge, the analysis of such correlations has never been carried out. We are convinced that the handling of these correlations and that of the induced effects can (1) reveal some subtle scenarios during the exploitation of data in DBMS, (2) leads to the supervision of the illegal behaviour of some DBMS users and (3) contributes to overcome anomalies that undermine the integrity of access control policies in DBMS. In a nearest future, we intend to develop the CORMSYS by explicitly formalizing each subsystem in order to produce, upstream, the necessary inputs for a new risk management approach.

REFERENCES

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

International Electrotechnical Commission, *International Standard, ISO/IEC 27000:2014.*

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

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

Bertino, E., Ghinita, G., Kamra, A., 2011. “Access Control for Databases: Concepts and Systems” *Foundations and Trends in Databases Vol. 3*, http://dx.doi.org/10.1561/1900000014.

Khambhammettu, H., Boulares, B., Adi, A., Logrippo, L., 2012. “A framework for threat assessment in access control systems” that appeared in *Proceedings of 27th IFIP TC 11 Information Security and Privacy Conference.* http://dx.doi.org/10.1007/978-3-642-30436-1_16.

Diep, N. N., Hung, L. X., Zhung, Y., Lee, S., Lee, Y. K., Lee, H., 2007. “Enforcing Access Control Using Risk Assessment”, *Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07).* http://dx.doi.org/10.1109/ECUMN.2007.19.

Colantonio, A., Di Pietro, R., Ocello, A., Verde, N.V., 2010. “Evaluating the Risk of Adopting RBAC Roles”, ara Foresti; Sushil Jajodia. Data and Applications Security and Privacy XXIV, 6166, *Springer*. http://dx.doi.org/10.1016/j.dss.2010.08.022.

Burnett, C., Chen, L., Edwards, P., Norman, T. J., “TRAAC: Trust and Risk Aware Access Control”, *2014. Twelfth Annual International Conference on Privacy, Security and Trust (PST)*. http://dx.doi.org/ 10.1109/PST.2014.6890962.

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

Baracaldo, N., Joshi, J., 2013. “An adaptive risk management and access control framework to mitigate insider threats”, *Computers & Security*. http://dx.doi. org/ 10.1016/j.cose.2013.08.001.

Celikel, E., Kantarcioglu, M., Thuraisingham; D., Bertino, E., 2009. A risk management approach to RBAC”. Risk and Decision Analysis 1 (2009) 21–33. DOI 10.3233/RDA-2008-0002. *IOS Press*.

Costante, E., Vavilis, S., Etalle, S., Petkovic M., Zannone, N., 2013. Database Anomalous Activities: Detection and Quantification, *SECRYPT 2013: 603-608*.

Grushka-Cohen, H., Sofer, O., Biller, O., Shapira, B., Rokach, L., 2016. CyberRank-Knowledge Elicitation for Risk Assessment of Database Security, *2016 ACM.* DOI: http://dx.doi.org/10.1145/2983323.2983896.

Darwish, S. M., 2015. Machine learning approach to detect intruders in database based on hexplet data structure. *Journal of Electrical Systems and Information Technology 3 (2016) 261–269,* http://dx.doi.org/10.1016/j.jesit.2015.12.001.

Jaidi, F., Ayachi, F. L., Bouhoula, A., 2017, A Comprehensive Formal Solution for Access Control Policies Management: Defect Detection, Analysis and Risk, SCSS 2017. *The 8th International Symposium on Symbolic Computation in Software Science 2017, Volume 45, 2017, Pages 120–132*.

Boulares, S., Adi, K., Logrippo, L., 2017, Insider Threats Likelihood Assessment for Flexible Access control, *International Conference on e-technologies.* DOI-10.1007/978-3-319-59041-7_5.

Boulares, S., Adi, K., Logrippo, L., 2017, Insider Threats Likelihood Assessment for Access control: quantitative approach, *International Symposium on foundation and precice of security*. DOI-10.1007/978-3-319-51966-1_9.