A Formal Approach for Risk Evaluation and Risk Analysis in Access Control Policy Management

Pierrette Annie Evina[1], Faten Labbene Ayachi[1], Faouzi Jaidi[1,2] and Adel Bouhoula[1]
[1]*Higher School of Communications of Tunis (Sup'com), University of Carthage, Tunis, Tunisia*
[2]*ESPRIT School of Engineering, Tunis, Tunisia*

1 INTRODUCTION

In information systems (IS) and especially in database management systems (DBMS), a good knowledge of the threats impacting the proper functioning of these systems, is essential in order to ensure protection and also to ensure the confidentiality and integrity of the data they contain. Several mechanisms are regularly put in place to remedy or to minimize the harmful effects related to the theft or misuse of data by authorized or unauthorized users. It is in this context that the access control (AC) and the risks related to its exploitation are the subject of numerous scientific papers. But, in this trend, the access control policy is somehow neglected because, a priori, most researchers hypothesize its reliability and validity. Though the access control policy (ACP) is exposed to many irregularities throughout its evolution. During its existence there are changes in its expression compared to rules established during its conception. In our research, we present a risk management approach for database access control systems, with particular emphasis on non-compliance anomalies in the access control policy. The correlation between the various anomalies mentioned is also taken into account in order to optimize the solution we propose. For this, a correlation management subsystem is proposed upstream in order to provide input data to a global and comprehensive risk management system whose framework is based on the ISO 31000 and ISO 27000 international standards for risk management. Our system will also integrate a sub-system that detect all other forms of anomalies related to the interaction between users and the other access control system resources.

The correlation management subsystem must detect and analyze the correlation between anomalies. It also produces the necessary input for a new risk management approach that will consider and overcome the effects induced by the correlation between anomalies found in the ACP expression since we believe that handling correlations between anomalies can reveal sophisticated intrusion scenarios in DBMS.

Finally, our contribution will include, in addition to assessment and risk treatment, the identification of safety barriers to prevent or minimize the hazardous occurrences. From the analysis of the history of the non-compliance anomalies detected during the access control policy evolution, an evaluation and a quantification of the exposure of that policy to risks will be carried out.

2 RESEARCH PROBLEM

The continuous technological development of the Information Systems in general, and that of Access Control in particular recommends the consideration of security risks that may lead to the malfunctioning of these systems. Unlike traditional Access Control systems whose policies were based on static decisions, new systems must adapt to the dynamic environment in which the technology evolves. That enables a quick and instant decision-making related to risk of illegitimate access. Some researchers have studied risks in Access Control by producing various approaches of risk management. However, these contributions are mostly focused either on the risks associated with user actions on the manipulated objects, or on the risks associated with managing the users and the permissions assigned to them.

The literature provides very little work to address the technical problems that may arise from the implementation of the access policy. Indeed, corruption of policy is a security aspect that is not discussed enough because almost all research works adopted the hypothesis of reliability and validity of policies. However, the operation of an access control policy requires its prior conformity with the specifications defined either at its conception stage or referring to a validate state. Works in this area recently resulted in identification of a set of critical non-compliance anomalies, when the implemented

Evina, P., Ayachi, F., Jaidi, F. and Bouhoula, A.
A Formal Approach for Risk Evaluation and Risk Analysis in Access Control Policy Management.
In *Doctoral Consortium (ENASE 2018)*, pages 17-22

policy was not conform with its original specifications. Consequently, it becomes appropriate to implement a reliable system that enables to avoid the occurrence of the identified risks related to these anomalies of non-compliance. Eventually, the effects should be managed when these risks are present.

Data corruption is mostly the consequence of Unauthorized updates of the access control policy especially when there are illicit actions of some users who want to access the database. At the current stage of our research, we could not find an intrusion detection system that can detect this type of anomaly. But, it is possible to trace the action of users on the database. Thus, suspicious and unauthorized users are detected using the log files of the database system (Evina et al., 2017).

A correlation is defined and established between these different anomalies in order to detect the induced faults. Thus, a user who fraudulently accesses a protected data is an usurper who has certainly benefited from the privileges that have been attributed to a role that is not reserved for him. (Evina et al., 2017). One of the objectives in our work is to make use of subsequent effects derived from the correlation of anomalies to minimize the risks of degradation of access control policies. To the best of our knowledge, access control policy has never been scrutinized from that point of view.

3 OUTLINE OF OBJECTIVES

The objective of our work is to develop a system capable of mitigating the negative effects of anomalies that occur in the access control policies management cycle, through an assessment and analysis of the risks linked to the evolution of these policies. This system integrates a sub-system that detect all other forms of anomalies related to the interaction between users and the other access control system resources (Evina et al., 2017). Our contribution integrates previous approaches and allows to go beyond the phase of detection of the anomalies towards a complete solution of:

(a) Recovery on anomaly

(b) Calculation of the impact of critical anomalies coupled with the logging mechanisms underlying the DBMS

(c) Specification of a learning and expertise approach on anomalies exploration and the discovery of correlations between those anomalies

(d) Specification of new mitigation approaches with adequate barriers to reduce the exposure of the PCA and data to subsequent attempts at corruption.

The above points will ultimately leads to a global and comprehensive system for detecting and dealing with anomalies that impede the proper functioning of access control systems.

4 OUR APPROACH

In this section, we describe the framework of the proposed risk management overall system which is presented in figure1 below. Indeed, our Risk Management System (RMS) which is in accordance with the process described in the ISO 31000 standard, comprises two main components, namely (i) a Risk Assessment Engine (RAE) and (ii) a Risk Treatment engine (RTE).

According to the ISO 31000 standard, the risk assessment phase is usually developed in following steps: Context assessment, Risk Identification, Risk Analysis and Risk Evaluation

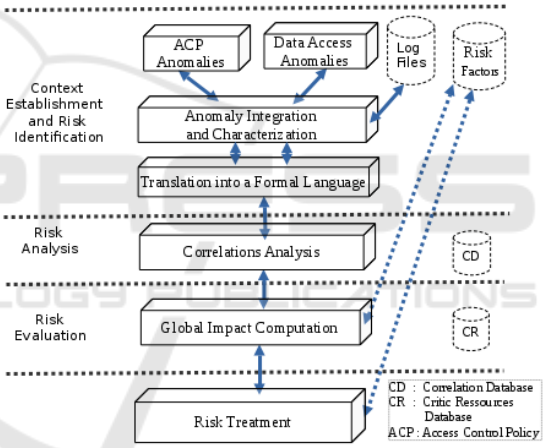

Figure 1: The proposed risk management framework.

The risk contextualization concerns the identification of the assets in the database system that should be protected. It is at this stage that the scope of the risk management is defined as well as the risk criteria to be used later on in the risk management process.

The tracking of these users is therefore the first step in our anomaly identification process, which allows us to identify unauthorized access as well as the recurrent targeted data (Evina et al., 2016). The risk identification concerns the identification of vulnerabilities that threaten data. It consists in computing the set of suspicious users and targeted data. The aim of risk identification is to make a complete list of risk that will be the object of the further steps of the risk assessment process.

The risk analysis that will confirm or deny the corruption of the data and the criticality of the vulnerability as it explores the authorized access scenarios based on data from log and audit security mechanisms activated on the database server. This enables to detect and establish the intrusive user

Behavior and thus, to reinforce the Intrusion Detection Systems (IDS)

The risk evaluation is a phase of self-adaptation that allows our system to correct its estimate of the risk incurred. It uses the results of the analysis phase to adjust the risk factors.

The risk treatment consist mainly in avoiding risk, mitigating it, and removing its source or changing the likelihood of it occurrence as recommend in (Evina et al, 2016).

A risk treatment plan is usually put in place and shows the procedure. That treatment plan precise the different actions to be taken, the persons responsible of applying the plan, the resource requirements, the performance measures and constraints, the reporting and monitoring requirements and the timing and schedule.[Evina et al, 2016].

5 METHODOLOGY AND EXPECTED RESULTS

In our approach of risk management, we focus on anomalies of non compliance of access control policy which have been defined in (Jaidi et al., 2016). But we believed that there exist a correlation between two or more anomalies and that can lead to subsequent threats. These threats have to be defined and the related risk can be evaluated. To accomplish that task, the methodology shown in figure2 has been defined.

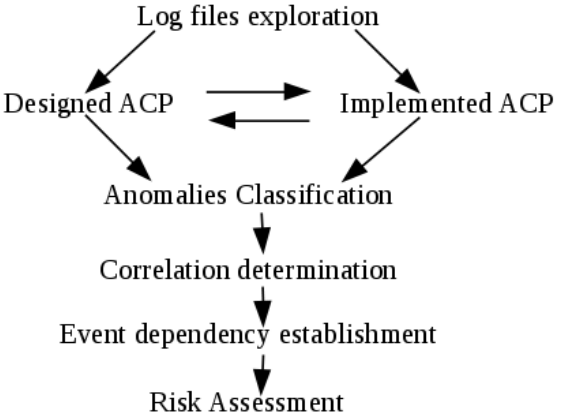

Figure 2: Our research process.

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 as far as its expression is concerned. Also, a comparison is done between two states of the ACP and lead to the establishment of a list of the various anomalies of non conformity and their frequency of occurrence. Then, a formal description of the correlation definition and evaluation procedure is produced. This shall be done with the correlation management module which supplies a risk management module. That will furthermore lead to the analysis and the evaluation of the risk related to the correlated identified threats associated to the direct effect from the anomalies by the same 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.

The main awaited results as listed in (Evina et al., 2017) are as follow:

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 as:

- 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 comprehensive system for risk management in access control systems.

6 STAGE OF THE RESEARCH

At the present stage of our research work, the following task have already been accomplished:

1. The above framework of figure 1 has been defined and described in a paper titled « Towards a Reliable Formal Framework for Enhancing Risk Assessment in Access Control Systems » by Evina et al. published in the EpiC Series in Computing, volume 45. In this paper, it is a question of defining the architecture of our system

which fits well with the specifications of the ISO 31000 standard and that we establish in two main parts namely: the first block in which are implemented the various mechanisms contributing to the risk assessment linked to the evolution of security control policies and the second block in which security barriers and any other necessary mechanism are implemented For security risks.

2. Our corrective and deductive approach has been explicitly described in the paper titled "Risk Management in Access Control Policies » presented in INSERT'17 (International Conference on Security, Privacy and Trust, 2017). the paper present our system for the management of anomalies of non-compliance rising during the evolution cycle of access control policies without neglecting the risks related to the direct access of the users and analyzing the risks related to the correlation between the various anomalies.

The developpement of anomalies correlation framework for risk-aware access control enhancement is under process as well as the proper evaluation of the correlation and the risk.

7 STATE OF THE ART

The research on risk management in access control can be classified into two main categories: the access-based approaches and the policy management based approaches. For the access based approach authors calculate the risks associated to access requests. Some authors integrate into their model, the trust and/or the context parameters in order to evaluate that risk. The second category of authors evaluate the risk that is related to the access control policy. None of the authors produces a fine grained risk management that is related to the changes occurring during the evolution of the access control policy.

7.1 Risk Management in Access Control

Authors in (Cheng et al., 2007) provide a solution to overcome the risk related to unauthorized access of users in an access control system. They use the Bell et Lapadula's access control model. This one is made up of security labels on the objects and the clearance on the subject (Cheng et al., 2007). They evaluate the trustworthiness of a user and the sensitivity of the evaluated object. It is a matter of determining the risk related to unauthorized access of a user on an object/data. To address this risk, the authors evaluate user confidence and the object sensitivity. The risk associated with unauthorized access is thus quantified in order to dynamically control the actions of the users on data.

Authors in (Khambhammettu et al., 2012) proceed as in (Cheng et al., 2007). The difference is just that while the late decide to allow access only and only if the trustworthiness is more than the clearance, in (Khambhammettu et al., 2012) authors treat the problem of unauthorized access by identifying different cases : they consider the level of the object sensitivity score compared to that of the subject trustworthiness score and vice versa. Then, a decision is taken in order to deny or to allow the access to the system.

The risk is evaluated according to the threat assessment approach used. But the risk caused by sudden and anticipated threat is not taken into consideration as the trustworthiness of the subject and the sensitivity of the objects are established a priori.

As security problems are much more complex in ubiquitous computing compared with traditional environment, authors in (Diep et al., 2007) plan to make the access control management more dynamic and precise. 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.

Authors in (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 permissions creation, modification, or deletion in the access control system. The creation, modification or deletion actions are causes of many mistakes and role misuses. Therefore, they establish a ranking of the users and permissions based on the degree of importance of the risk induced for future mitigation.

In (Burnett et al., 2014), the authors provide a solution to avoid unwanted disclosure of information by corrupted users. They consider the risk occurred when a user manage his own data, granting permission to other users and determine the trustworthiness of users. They also consider the case where access is inappropriately denied to some users by the owner. They exploit and compute the opinion of a user onto another user to evaluate the loss function due to unwanted disclosure of information through an access control system.

Authors in (J. Ma et al., 2010) and (J. Ma et al., 2012) mainly consider the role delegation issue. Indeed, for a user to delegate his rights to another one, there should be among the two users a trusted

relationship. The authors extend the access control architecture in which they incorporate the trust based reasoning. In the case of role delegation, and according to the authors, related risk is computed based on the levels of confidence of the delegate. The risk assessment proposed in (J. Ma et al., 2010) and (J. Ma et al., 2012) highlights the notion of the importance of objects associated with that of criticality of actions of users to those objects.

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 behavior are osculated in order to maintain the trust of each at an appreciable level and above a certain threshold. Below that threshold, authors think that the privileges of this kind of users should be removed. For the purpose, they propose an algorithm that reduces the exposure of the access control to risk. They also propose a methodology to help the system administrator in managing inference threats due to the changes of the users behavior.

7.2 Risk Management in Access Control Policy

Users queries are risky especially when there is a misapplication of the rules established in the access control policy. Thus, (Celikel et al., 2009) deal with the risk management in the access control policy, notably the RBAC in distributed databases. The users queries are the main elements observed and considered while assessing risk. Thus, in order to allow an early detection and control of probable negative consequences in the system, the authors in (Celikel et al., 2009) handle and define user risks. Those risks include the bad utilization of users credentials. As far as the access control policy evolves, it is exposed to various corruption attempts. There can be abnormal elements like missed, renamed, hidden users or hidden roles. After they slightly evaluate the risk of having such abnormal elements, the authors plan an assessment module that defines a response monitor.

Our contribution is to produce a comprehensive and global system that addresses risk management in access control policies during its evolution. It is necessary to identify the anomalies. Specifically, we study the correlations that may exist between one or more detected anomalies. This will make it easier to interpret the corruption risks to which the policy of access control is subjected.

7.3 Anomalies Correlation for Risk Enhancement

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 automation 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 behavior 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. There exist another difference between our work and theirs. Indeed, they provide a ranking alerts system that enables to prioritize anomalies according to their importance. While we consider the correlation existing between these anomalies in order to adjust the risk factors through sophisticated scenarios and prevent ACP expression from degradation.

8 CONCLUSION

The research work we present is about risk management in access control policies for database management systems. Rather than the user-data interaction, we focus on the policy expression and on the impact due to the non-compliance anomalies observed on the expression of two different states of the same policy. The non-compliance anomalies are generally caused by the irregular updates of the ACP due to malicious users or vicious database administrators. The correlation of such anomalies is valuable. None of the authors encountered in the literature work on that aspect of the expression of ACP expression neither they do not take into consideration the consequences of the correlation that might exist between two or more such anomalies.

Our contribution aims to produce a risk management framework that consequently takes into

consideration the subsequent effects of the correlated anomalies, in addition to the direct impact caused by the same anomalies on the whole database access control system. For that reason, our system is designed to be as global and comprehensive as possible.

At the present stage of our work, we have already furnished in a recent publication, the description of the proposed framework for the overall risk management system for our approach. The paper that presents in details the correlation management subsystem is also under process.

In a close future, we intend to concretely and practically evaluate the correlated risk and the overall risk with real case studies with real database.

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.