Position papers of the Federated Conference on Computer Science and Information Systems, pp. 107–112
DOI: 10.15439/2017F555
ISSN 2300-5963 ACSIS, Vol. 12

Risk Management in Access Control Policies

Pierrette Annie Evina, Faten Labbene Ayachi, Faouzi Jaidi
Higher School of Communications of Tunis (Sup'com),
University of Carthage, Tunis, Tunisia
Email: {pierrette.evina, faten.labbene, faouzi.jaidi}@supcom.tn

***Abstract*—The evolution of information systems and their openness to their socio-economic environment has led to new needs in terms of security. At the heart of information systems, Database Management Systems (DBMS) are increasingly exposed to specific intrusion types, including internal threats due to authorized users. In addition, the access control policy (ACP) defined on a database schema is stored at the same location as the data it protects and is thus highly prone to corruption attempts such as non-conformity of the roles or permissions assignment in the policy observation state compared to a reference state, especially in the case of the Role-based access Control (RBAC). We establish a correlation between the detected anomalies and we explore the log files and other audit mechanisms to propose a global and comprehensive risk management formal approach that mainly verifies the recommendations of the ISO 31000:2009 standard.**

I. Introduction

ACCESS Control is a technique used to grant access to any system by users. The authorization to access the system is usually synonymous of the user's authentication at the entry of the system and the attribution of some privileges or credentials to that user.

The access control is constantly evolving and the environment in which it is implemented is increasingly dynamic. For the Discretionary Access Control (DAC) especially designed for commercial applications, the permissions to access resources are granted by the owner of the data. For the Mandatory Access Control (MAC) specially designed for military applications, access to resources is controlled by an operator and therefore; a user does not have control on his own data [3]. Due to the complexity in the use of this two models, many other access control models have been developed. Role Based Access Control (RBAC), the famous one, uses role to group many users according to their function. It offers, compared to others, a high degree of flexibility when implementing access control policies. Many extensions of the RBAC model exist and aim to secure more the information systems.

Since years, the notion of risk and that of risk management have been introduced in the information security field and the risk-aware access control aims is to reduce the consequences occurring from granting access to a specific information for an unauthorized personnel who can misuse it. The risk is characterized by the potential event, the consequences of that event on the achievement of the objectives and the associated likelihood [2]. As far as its activities and tasks are concerned, each system or organization is exposed to risks which can be caused intentionally or not. Thus, the management of users in the access control system should receive a great attention. Also, the rules governing that access control should be consistent with those established for the access control policy at the designing phase or at a given reference moment.

We propose a system that will enable, indifferently, to thwart the threats related to the action of users on data and those inherent to the changes occurring during the evolution of the access control policy. The remainder of the paper comprises the following paragraphs: paragraph II gives the problem statement; paragraph III presents the main objectives; paragraphs IV discusses the related works; paragraph V presents our methodology; paragraph VI presents our proposed framework ; paragraph VII presents the expected results; paragraph VIII concludes the paper.

II. The Problem statement

The environment in which access control systems are implemented is dynamic and increasingly requires rapid and instant decision-making. Also, the ever-evolving technological development of information systems in general and that of access control in particular recommends careful consideration of security risks that could lead to malfunctioning of these systems. The exposure of these assets to threats is inherent to the manipulation of data by suspicious users and the management of the access control policy by wicked administrators.

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 and enable decisions to be made automatically based on the

needs related to the risk issues. This requires controlling this risk, and even quantifying it.

To carry out this task, many researchers have studied risk in access control by producing various methods of managing it. For the major part, they have been more interested in the risk associated with users actions on manipulated objects or, to a greater extent, they were interested in the risk associated with managing these users and the permissions assigned to them. Visibly, they were considering that the access control policy was reliable and valid. Thus policies are in fact exposed to various threats and the literature provides very little works that address the technical problems derived from the implementation of the access control policy [1].

Operating an access control policy requires a certain degree of compliance with the specifications defined at its design phase or at an initial phase. We propose to explore this aspect by deeply studying the risk of non-conformity of the rules established for the management of access control.

III. OBJECTIVES

The objective of our work is to develop a system capable of detecting and correcting 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. 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 ACP 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.

IV. THE 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.

Authors in [6] 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 [6]. 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 [18] proceed as in [6]. The difference is just that while the late decide to allow access only and only if the trustworthiness is more than the clearance, in [18] 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 [17] 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 [15] evaluate the risk occurred when managing users and permissions through the Role based access control (RBAC) during the pre-mining phase [15]. 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 [16], 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.

J. Ma, K. Adi, M. Mejri, L. Logrippo in [7] and [8] 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 [7], [8] highlights the notion of the importance of objects associated with that of criticality of actions of users to those objects.

Authors in [9] 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 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.

Users queries are risky especially when there is a misapplication of the rules established in the access control policy. Thus, [13] 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 [13] 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.

V. Methodology

The intention of the present research started from a previous work. Indeed, anomalies of non compliance of access control policy have been defined. But we believed that there exist a correlation between two or more anomalies and that can lead to other threats. This threats have to be defined.

The first task consist in an analysis of the results of that previous work.

In order to get more information related to our work plan, the second task is the documentary research. An important number of publications have been identified and studied in order to precisely identify our subject. Some publications have enabled us to establish the state-of-the-art.

Another step is the one during which we explore the log files. this will allow us to collect information about recurrent attacks, i.e data that are regularly and improperly exploited, as well as anomalies of non-compliance (or revelations about users, hidden roles, and so one).

A simulation on a real database is done, with real schemes and tables created. This will enable us to verify our results, qualitatively and quantitatively..

We use the Markov chains to model the unauthorized accesses and thus to model the illegal behavior users.

Our expectation is to come out with new concepts that we believe will be adopted and will advance research in the security of information systems, the security of access controls and the security of databases.

VI. Our proposed framework

Unauthorized update of the access control policy is largely responsible of data corruption. This situation can be exploited by a criminal who wants to access the database. However, at the present stage of 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. 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.

Thereafter 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.

As a result, the recurrent targeted data is identified and a list of such sensitive data is established. At the end, we draw a resultant architecture which is based on international stan-

dards. Indeed, as recommended by the ISO 31000: 2009 standard, our Risk Management System (RMS) is composed by (i) a Risk Assessment Engine (RAE) and (ii) a Risk Treatment engine (RTE). (figure 1) The risk assessment phase is usually developed in 4 steps: Context assessment, Risk Identification, Risk Analysis and Risk Evaluation [19].

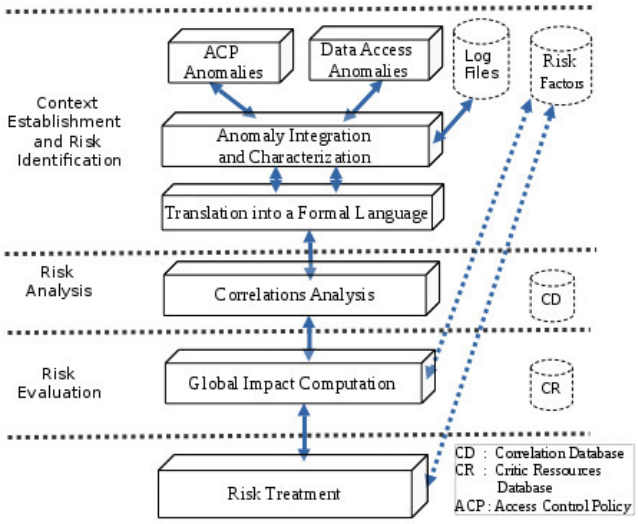

Fig. 1 : A framework for risk management

The risk contextualization concerns the identification of the assets in the database system that are to 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 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 **[1].** 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.**[1]**

The concrete process of our risk approach related to our framework is shown in the following (figure 2)

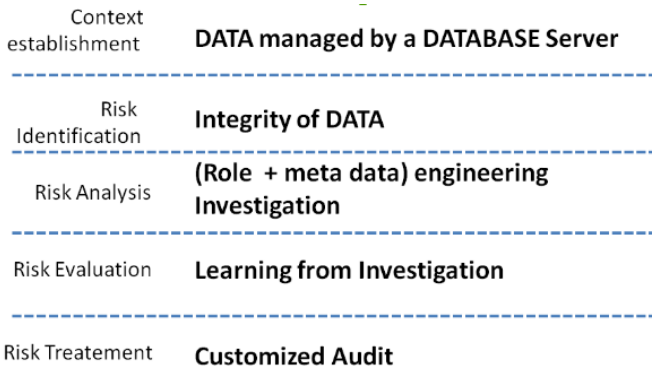

Fig. 2 : The approach process

VII. EXPECTED RESULTS

Before going into details, let us give the list of the main awaited results. This are:

- design of an intrusion detection system for unauthorized update of access control policy
- detection of induced faults by establishing a correlation between the detected anomalies
- list of the recurrent targeted and sensitive data
- detection and establishment of the intrusive user behavior and thus, reinforcement of the Intrusion Detection Systems
- production of a global and comprehensive system for risk management for access control systems

To illustrate this while considering the above framework, we should have a fairly complete list of anomalies and an evaluation of the related risk which is determined with our risk assessment approach.

This has been initiated by a previous work by F. Jaidi and F. Labbene Ayachi in [14]. Indeed, as stated in RBAC standard, ACP is defined as the set of all users, roles, permissions and assignments, i.e ACP = (USERS, ROLES, PERMS, AUR, ARR, APR) where AUR, ARR, APR represent respectively the user-role assignment, the role-role assignment, and the permission-role assignment.

ACP is the formal specification of the policy and ACP' is the formal representation of the implemented policy. ACP contains the elements as specified in the early stage of the policy engineering. Within the framework of the RBAC, these elements ideally reflect the concepts related to the

definition of users, roles and permissions, the allocation of roles to users, the allocation of roles to roles, the assignment of roles.

On the other hand, the elements of the ACP' contain concepts that are also related to the definition of users, roles and permissions, the allocation of roles to users, the allocation of roles to roles, the assignment of roles . This concerns the implementation of the policy by the managers, taking into account the access of malicious users to the data and also taking into account possible accidental corruption of the policy.

Things could be perfect if ACP' was conform to ACP. Unfortunately, this is not always the case. So, to verify that ACP' is conform to ACP, their elements are compared. In [1], this comparison has been done and among others, the following anomalies have been defined :

- hidden users which are visible when new users, not initially defined, are injected in the concrete instance ACP'
- hidden roles are observable when new roles, not initially planned, are introduced in the concrete policy ACP'.
- hidden access flow (HiddenACF) is perceptible in the case of illegal assignments of roles to roles, roles to users or permissions to roles.

To go further in the interpretation of corruption attempts, we consider the correlation between these anomalies, we come out with some new anomalies definitions expressing unauthorized accesses.

Considering the frequency of occurrence of each of these events that constitute an anomaly, random variables are thus defined. A relationships of dependencies can be established between them. Hence, a statistical link can be established between these variables since the increase or decrease of one variable is related to the increase of the other variable.

Concretely, a hidden role implies action. This presupposes permissions, delegations and users that were not considered in the policy as initially defined (these are for example, hidden users, hidden roles, hidden assignments). An analysis of the correlations makes it possible to identify critical anomalies that lead to high risks of corruption of the policy. We thus define, notions such as suspicious users or altered roles. This is done in the following way:

Definition 1: (Suspicious users)

We define in (2) a suspicious user as:

$$SuspiciousUsers = \{u \in USERS \mid r \in (HiddenRoles \cup AlteredRoles)\ (u, r) \in AUR'\}. \quad (1)$$

where USERS is the set of the users of the access control policy.

Definition 1: (Altered Roles)

We define in (1) an altered role as:

$$AlteredRoles = \{r \in ROLES \mid r' \in HiddenRoles\ (r',r) \in AUR'\} \cup \{r \in ROLES \mid p' \in PERMS'\ (r , p') \in APR'\}. \quad (2)$$

where ROLES is the set of roles defined in access control policy and PERMS is the set of permissions to be granted in the access control policy.

We intend to use the Markov chains to model these unauthorized accesses and thus to model the illegal behavior of a user. We try to ameliorate in an incremental manner the model obtained and to attribute a weighting according to the frequency of occurrence of a given unauthorized access. For risk assessment, risk factors will be assessed taking into account the correlation coefficients for those events or anomalies identified.

VIII. Conclusion

Information systems, including database systems, are exposed to threats of any kind arising out of the use of malicious users. This is submitting the data to the risk of alteration and destruction. Since the access to these systems are filtered by access control systems, insiders threats are certainly responsible for loss of integrity, confidentiality, data availability. But, the access control policies that regulate these accesses are also source of danger to the information systems as far as their evolution is concerned although they are generally considered valid and reliable. Indeed, from the design phase to the implementation phase, these policies are not always conform to the initial phase or to an intermediate phase taken as reference. Anomalies of non-conformity in the ACP have been the subject of the work of F. Jaidi and F. Labbene Ayachi, who defined some of them.

By studying the correlation between these anomalies and using the log files that are intrinsic to the system, we think we can detect other anomalies whose risk is also evaluated by faithfully applying the recommendations of the international standards, such as the recommendations of ISO 31000. So, We propose a system to detect and mitigate risks for access control policies. This system will take into account other intrusions detection systems (IDS) in order to produce a global and comprehensive system for risk management in access control systems.

References

[1] F. Jaidi and F. Labbene Ayachi. "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). DOI: 10.5220/0005577304540459

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

[3] 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). *DOI*: 10.1109/2.485845

[4] 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. DOI: 10.1109/CNS.2013.6682761

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

[6] 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). DOI: 10.1109/SP.2007.21

[7] J. Ma, (2012). "A formal approach for risk assessment in RBAC systems". Journal of Universal Computer Science, vol. 18, pp. 2432-2451. DOI: 10.3217/jucs-018-17-2432.

[8] 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. DOI: 10.1109/PST.2010.5593248.

[9] N. Baracaldo, J. Joshi, (2013). "An adaptive risk management and access control framework to mitigate insider threats", Computers & Security. DOI: 10.1016/j.cose.2013.08.001.

[10] 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. DOI: 10.1109/HPCC. 2008.37

[11] L. Chen, J. Crampton, (2011). "Risk-aware role-based access control". In Proc. of the 7th International Workshop on Security and Trust Management. DOI : 10.1007/978-3-642-29963-6_11

[12] 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. DOI : 10.1007/978-3-642-13739-6.

[13] Ebru Celikel, Murat Kantarcioglu, Bhavani Thuraisingham and Elisa Bertino. A risk management approach to RBAC". Risk and Decision Analysis 1 (2009) 21–33. DOI 10.3233/RDA-2008-0002. IOS Press.

[14] 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. DOI: 10.1007/978-3-319-19713-5_5.

[15] Alessandro Colantonio, Roberto Di Pietro, Alberto Ocello, and Nino Vincenzo Verde, "Evaluating the Risk of Adopting RBAC Roles", ara Foresti; Sushil Jajodia. Data and Applications Security and Privacy XXIV, 6166, Springer, pp.303-310, 2010. DOI: 10.1016/j.dss. 2010.08.022.

[16] Chris Burnett, Liang Chen, Peter Edwards and Timothy J. Norman, "TRAAC: Trust and Risk Aware Access Control", 2014, Twelfth Annual International Conference on Privacy, Security and Trust (PST). DOI: 10.1109/PST.2014.6890962.

[17] Nguyen Ngoc Diep, Le Xuan Hung, Yonil Zhung, Sungyoung Lee, Young-Koo Lee, and Heejo Lee. "Enforcing Access Control Using Risk Assessment", Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07) 0-7695-2768-X/07 $20.00 © 2007. DOI: 10.1109/ECUMN.2007.19

[18] Hemanth Khambhammettu, Sofiene Boulares, Kamel Adi, Luigi Logrippo. "A framework for threat assessment in access control systems" that appeared in Proceedings of 27th IFIP TC 11 Information Security and Privacy Conference (SEC 2012), 2012. DOI: 10.1007/ 978-3-642-30436-1_16

[19] Pierrette Annie Evina, Faten Labbene Ayachi, Faouzi Jaidi and Adel Bouhoula, "Towards a Reliable Formal Framework for Enhancing Risk Assessment in Access Control Systems", EPiC Series in Computing Volume 45, 2017, Pages 77–82 SCSS 2017. The 8th International Symposium on Symbolic Computation in Software Science 2017