Future Generation Computer Systems 55 (2016) 321–335

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Dynamic counter-measures for risk-based access control systems: An evolutive approach

Daniel Díaz-López [a,*], Ginés Dólera-Tormo [a], Félix Gómez-Mármol [b], Gregorio Martínez-Pérez [a]

[a] Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia, 30.100, Murcia, Spain
[b] NEC Laboratories Europe, Kurfürsten Anlage 36, 69115, Heidelberg, Germany

HIGHLIGHTS

- Finding of best sets of counter-measures to protect resources.
- Dynamic countermeasures to face variations in the Risk Level (*RL*).
- Access depending on the fulfillment of a set of specific security controls.
- Method based on genetic algorithms with applicability in a real scenario.
- Resource protection according to the risk level (not under or overestimated).

ARTICLE INFO

Article history:
Received 20 November 2013
Received in revised form
29 August 2014
Accepted 9 October 2014
Available online 13 November 2014

Keywords:
ISO 27001
ISMS
Risk management
Access control systems
Genetic algorithms
Counter-measures

ABSTRACT

Risk-based access control systems are a new element in access control categories, incorporating risk analysis as part of the inputs to consider when taking an authorization decision. A risk analysis over a resource leads generally to temporal allocation of the resource in a risk level (e.g. high, medium, low). Ideally, for each risk level and kind of resource, the access control system should take an authorization decision (expressed like a permit or deny) and the system administrator should also trigger specific counter-measures to protect resources according to their risk level. In a small access control system with few resources it is possible for an administrator to follow the risk level changes and react promptly with counter-measures; but in medium/large access control systems it is almost unfeasible to react in a customized way to thousands of risk level emergencies asking for attention. In this paper we propose the adoption of dynamic counter-measures (which can be integrated within access control policies) changing along time to face variations in the risk level of every resource, bringing two main benefits, namely: (i) a suitable resource protection according to the risk level (not under or over estimated) and (ii) an access control system granting/denying access depending on the fulfillment of a set of security controls applicable in an authorization access request. To define the most appropriate set of counter-measures applicable for a specific situation we define a method based on genetic algorithms, which allows to find a solution in a reasonable time frame satisfying different required conditions. Finally, the conducted experiments show the applicability of our proposal in a real scenario.

1. Introduction

Access control systems are used in a wide variety of scenarios to manage privileges over resources, being the following the most conventional access control models: ACL (Access Control List) [1,2], RBAC (Role-Based Access Control) [3,4], ABAC (Attribute-Based Access Control) [5,6] and PBAC (Policy-Based Access Control) [7,8]. Risk-based access control systems [9,10] are the last evolution in access control systems as they incorporate a risk level analysis as main input for the authorization decision process. In typical risk-based access control systems, the risk level calculation is usually focused on the protection of assets, being an asset anything that has a value for the organization, i.e. information, equipment, software, services, etc.

* Corresponding author. Tel.: +34 868 887 646.
E-mail addresses: danielorlando.diaz@um.es (D. Díaz-López), ginesdt@um.es (G. Dólera-Tormo), felix.gomez-marmol@neclab.eu (F. Gómez-Mármol), gregorio@um.es (G. Martínez-Pérez).

http://dx.doi.org/10.1016/j.future.2014.10.012
0167-739X/

Asset protection is achieved through counter-measures, security controls or safeguards that are deployed by an organization in order to avoid that intentional or no-intentional actions affect its information assets. In this paper, a counter-measure *cm* will consist of a specific security control category *scc*, plus an associated effectiveness of such security control category $E(scc)$, as we will see later.

The risk level value, which can be estimated for an asset or a group of assets, must be under a well defined maximum threshold (acceptable risk) which is defined by the organization and represents the maximum risk level that such organization is willing to accept [11] (either for each particular asset, or overall for the whole organization).

The risk level can be measured using different risk analysis methodologies, which are a core element in Information Security Management Systems (ISMS), like the ones defined by ISO 27001 and ISO 17799 [12,13]. As shown in Eq. (1), the risk analysis methodologies commonly include the following elements to compute the risk level of a particular asset $\mathcal{A}$, given a specific threat $\mathcal{T}$, $RL(\mathcal{A}, \mathcal{T})$: (i) a factor related to the relevance of the asset $\mathcal{A}$ for the organization (impact $I(\mathcal{A})$), (ii) a factor associated to the probability that a specific threat $\mathcal{T}$ can be truly materialized over the asset $\mathcal{A}$ (probability of occurrence $P(\mathcal{T}, \mathcal{A})$) and (iii) a factor regarding the effectiveness of the security controls implemented in the organization to protect such asset $\mathcal{A}$, $E(\mathcal{A})$.

$$RL(\mathcal{A}, \mathcal{T}) = \frac{P(\mathcal{T}, \mathcal{A}) \cdot I(\mathcal{A})}{E(\mathcal{A})}. \quad (1)$$

As we can observe, whenever the probability of occurrence of a given threat $\mathcal{T}$ over a specific asset $\mathcal{A}$, $P(\mathcal{T}, \mathcal{A})$, and the impact of such asset $\mathcal{A}$, $I(\mathcal{A})$, are not negligible, there will always exist an associated risk level $RL(\mathcal{A}, \mathcal{T})$ (from now on, for simplicity, also noted just as RL), even if this is quite small due to a high security control effectiveness $E(\mathcal{A})$. According to the standard ISO/IEC 27001 [14], in the risk level evaluation and treatment process every organization evaluates the risk level of its assets and implements security controls to reduce that risk level (by decreasing the probability of occurrence of a threat $\mathcal{T}$, $P(\mathcal{T}, \mathcal{A})$, and/or increasing the effectiveness of the security controls over each of its assets $\mathcal{A}$, $E(\mathcal{A})$). However, after the corresponding risk level treatment, there is always a residual risk level which is remaining.

Additionally, according to the widely applied standard ISO/IEC 27005 [11], every organization should define the risk acceptance criteria, which determines how much an organization is willing to accept risks. A level of risk acceptance ($\widehat{RL}(\mathcal{A}, \mathcal{T})$ or, for simplicity, just $\widehat{RL}$) can be defined for all the assets or for specific groups of assets, and considers organization policies, objectives and interests of the different stakeholders. The levels of risk acceptance are determined and approved by the managers of the organization and require regular revision. As the context changes, the risks do and therefore it is necessary to adjust the levels of risk acceptance. In a continual improvement cycle for an Information Security Management Systems (ISMS), it is normal to observe a gradual decrement in the levels of risk acceptance (acceptable risk values).

1.1. Motivation and contribution

The model previously introduced for risk-based access control systems is in some way static, since it does not take into account the fact that the impact of an asset $\mathcal{A}$, $I(\mathcal{A})$, the probability of occurrence of a particular threat $\mathcal{T}$ over such given asset $\mathcal{A}$, $P(\mathcal{T}, \mathcal{A})$, and the security control effectiveness for that specific asset $\mathcal{A}$, $E(\mathcal{A})$, can change dynamically in short periods of time so that the risk level $RL(\mathcal{A}, \mathcal{T})$ can become remarkably variable. Besides, these systems use a set of static access control policies to process authorization requests over the assets $\mathcal{A}$ of an organization; but due to the dynamism of the aforementioned variables, it is reasonable to think that a static access control policy does not apply to every situation, since the response of the system (authorization decision) has to change and adapt to the current risk level of asset $\mathcal{A}$, $RL(\mathcal{A}, \mathcal{T})$, when a user is trying to access or manipulate it.

Current risk-based access control systems will use the risk level computed for each asset $\mathcal{A}$ within an organization, $RL(\mathcal{A}, \mathcal{T})$, to make their authorization decisions and, in the case of a high risk level, every authorization request toward such asset $\mathcal{A}$ has a high probability of being denied. Unless the risk level $RL(\mathcal{A}, \mathcal{T})$ decreases (actually, the probability of occurrence $P(\mathcal{T}, \mathcal{A})$ or impact $I(\mathcal{A})$), the authorization decision will not change, since the security controls are static and so their effectiveness $E(\mathcal{A})$ is not adapting to the changing conditions.

Denying access is a way of protecting assets in a risky situation, but it is rather not the most effective one for its blocking consequences on the service delivery. On the other hand, defining static security controls with an excessively high effectiveness $E(\mathcal{A})$ in order to keep the risk level low, becomes self-defeating since this can produce an overestimated protection for an asset $\mathcal{A}$ which does not really need it, or at least, not all the time. Furthermore, when a risk level variation occurs, the system administrator should trigger specific counter-measures to protect every asset $\mathcal{A}$ according to the current risk level $RL(\mathcal{A}, \mathcal{T})$. Yet, if the risk level rapidly varies in short periods of time for many assets (e.g. in medium large infrastructures) it is a cumbersome task for a system administrator to manually handle each risk level variation in a proper and timely fashion.

Thus, the main contribution of this paper lies in the definition, implementation and evaluation of a method inspired on evolutive algorithms to assist risk-based access control systems by dynamically finding a catalog of the best set of counter-measures describing how to adapt the access control policies related to a specific asset $\mathcal{A}$, in order to effectively and efficiently protect such asset according to its current risk level $RL(\mathcal{A}, \mathcal{T})$.

In particular, these optimal counter-measures are devoted to adapt the effectiveness $E(\mathcal{A})$ of the applied security controls and, in turn, the measured risk level for such specific asset $\mathcal{A}$, $RL(\mathcal{A}, \mathcal{T})$, to meet the pre-defined acceptable risk level $\widehat{RL}(\mathcal{A}, \mathcal{T})$.

The following main features and benefits can be named:

- In contrast to traditional risk-based access control systems, where the access control policies remain static regardless the variation in the risk level of the assets belonging to an organization, with this method inspired on evolutive algorithms the access control policies are dynamically re-shaped, adapting this way the effectiveness of the security controls over a specific asset $\mathcal{A}$, $E(\mathcal{A})$, and consequently modifying its current risk level $RL(\mathcal{A}, \mathcal{T})$.
- Such mechanism is able to promptly and accurately react to sudden and numerous variations of the risk level of several assets within an organization in an autonomous and automatic way, releasing human system administrators from the overwhelming task of manually adapting the security controls of each asset to protect them in such a dynamic environment.
- Instead of adopting the simplistic, but at the same time drastic and counter-productive remedy of denying access to an asset $\mathcal{A}$ when its current risk level $RL(\mathcal{A}, \mathcal{T})$ exceeds the acceptable risk $\widehat{RL}(\mathcal{A}, \mathcal{T})$, this method is able to find the optimal set of counter-measures specific for the current risk level of such asset $\mathcal{A}$, $RL(\mathcal{A}, \mathcal{T})$, not under or over estimating its protection, achieving the right balance between risk control and service denial.