Risk-based Decision Method for Access Control Systems

Riaz Ahmed Shaikh, Kamel Adi, Luigi Logrippo
Department of Computer Science and Engineering,
Université du Québec en Outaouais,
Quebec, Canada
Email: {riaz.shaikh, kamel.adi, luigi.logrippo}@uqo.ca

Serge Mankovski
CA Technologies,
125 Commerce Valley DR W, Thornhill,
Ontario, Canada.
Email: serge.mankovski@ca.com

***Abstract*—Traditional security and access control systems, such as MLS/Bell-LaPadula, RBAC are rigid and do not contain automatic mechanisms through which a system can increase or decrease users' access to classified information. Therefore, in this paper, we propose a risk-based decision method for an access control system. Firstly, we dynamically calculate the trust and risk values for each subject-object pair. Both values are adaptive, reflecting the past behavior of the users with particular objects. The past behavior is evaluated based on the history of reward and penalty points. These are assigned by the system after the completion of every transaction. Secondly, based on the trust and risk values, an access decision is made.**

I. Introduction

Commonly used security and access control systems, such as MLS/Bell-LaPadula [1], RBAC [2] are not very suitable for dynamic environments, like healthcare, emergency services and the military. These systems are rigid and require establishing clearance of a requester, which is a manual and time consuming procedure [3], [4], [5]. This happens because, in these systems, security policies are typically hard coded into decision logic [6]. Also, these relatively static policies are the result of pre-computed trade-off analysis between various organizational objectives [7]. Furthermore, in these systems, "there is no way to turn up or down the knob that governs the trade-off between security and operational needs" [8]. For example, in an organization, release of certain types of information may be revealed to people having shown a responsible attitude towards information they acquired in the past.

In this context, we can informally state the problem in the following fashion: *Traditional access control systems do not consider uncertainty and risk in access control decisions, and this makes them inflexible and difficult to adapt to changing circumstances*. Therefore, new dynamic risk-based access control decision methods are needed through which we can increase or decrease users' access to classified information based on the past behavior.

In this paper, we propose a risk-based decision method for access control systems. One of the novelties of this work is that we dynamically calculate the trust and risk values for each subject-object pair. Based on these values, an access decision is made. Furthermore, both values are adaptive, reflecting the past behavior of the users with particular objects. In this work, we evaluate past behavior based on the history of reward and penalty points. After completion of every transaction, reward or penalty points are assigned to the user with respect to specific objects.

The rest of the paper is organized as follows. Section II contains related work. Section III presents proposed risk-based decision method. Finally, Section IV concludes the paper and discusses future work.

II. Related Work

Incorporating consideration of risk in access control systems has recently gained the attention of researchers [4], [5], [6], [9], [10]. A brief overview of some of the existing work is given below.

McGraw [6] has proposed a Risk-Adaptable Access Control (RAdAC) mechanism. Firstly, the system determines a security risk associated with granting access. Secondly, the system will compare the measured risk with the access control policy that identifies the acceptable level of risk for the object being accessed. Thirdly, the system will verify the operational need. If all the requirements for operational need, as specified in the policy, are met then access is granted. RAdAC furnishes high-level infrastructure for the granting of exceptions, but it does not itself contain a risk model. The author has not provided details about how to quantitatively measure risk and operational need.

Zhang *et al.* [4] have proposed a Benefit and Risk-based Access Control (BARAC) model. In this model, transactions are associated with risk and benefit vectors. Based on the configuration, an allowed transactions (AT) graph is constructed. Transactions are allowed if the total system benefit outweighs the total system risk and certain properties of the graph are satisfied. The state is largely static and updating a state leads to intractable problems [10].

Cheng *et al.* [9] have proposed a Fuzzy MLS access control model. It quantifies the risk associated with an access. The system will dynamically control risky information flows based on its current operational needs, risk tolerance and environment. They calculate risk based on a value of information and probability of unauthorized disclosure. Similarly, Qun Ni *et al.* [5] have proposed risk-based access control systems based on fuzzy inferences. They shows that the fuzzy inference is

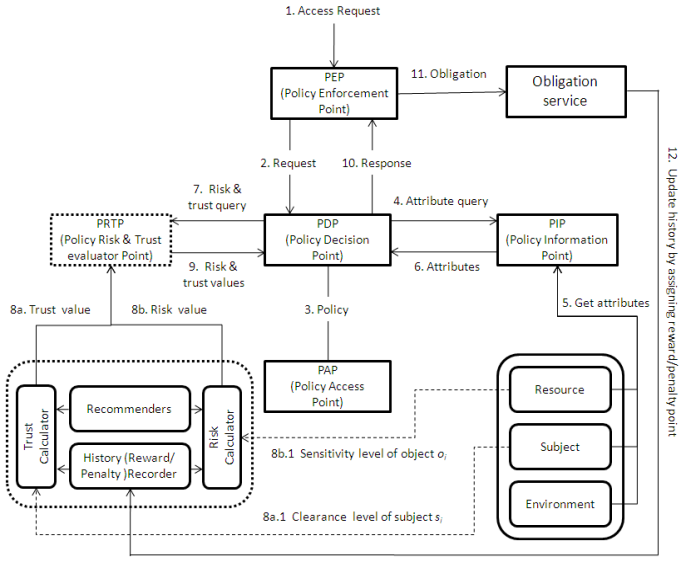

Fig. 1. Process flow of Risk-based Decision Method

a good approach for estimating access risks. They introduce fuzzy membership functions for subjects and objects. In order to implement risk-based BLP systems to satisfy simple security properties, they introduce pre-defined "if antecedent then consequent" rules. For example, if the subject security label is *not unclassified* and the object security label is *classified*, then the access risk is low. In both these works, the authors have not incorporated the past behavior of users to measure risk.

III. Risk-based Decision Method

Traditionally, whenever a Policy Decision Point (PDP) receives an access request from the requester, it first requests the additional information from the Policy Access Point (PAP) and Policy Information Point (PIP) and then makes a decision. In our proposed method, the PDP also requests information about the trust and risk values associated with the particular subject and object and then takes the decision. These trust and risk values are calculated based on three main factors:

1) history of reward and penalty points,
2) clearance level of the subject, and
3) sensitivity level of the object.

The process flow of the proposed risk-based decision method is shown in Figure 1. This framework is a modification of the standard XACML framework. All the new components that we have added are highlighted with dotted lines.

Details about assignment of reward and penalty points, calculation of trust and risk values, and how trust and risk values are used in decision making are given below.

A. Step 1: Awarding Reward and Penalty Points

After access is given, an obligation service is executed in the system that will decide whether to assign rewards or penalty points to users. In practice, the obligation service (Obl) is application dependent. Therefore it is very hard to devise generic mechanisms through which a system can decide whether to assign reward or penalty points to users. For example, in the e-purse scenario [11], validation of an e-cash process is the obligation service. If e-cash is successfully redeemed then the system will assign reward point(s) to the subject s with respect to object o and vice versa.

B. Step 2: Trust Calculation

Our method of dynamically calculating trust values will be designed to satisfy the following requirements:

- **Property 1**: If the reward points increase then the trust value also increases.
- **Property 2**: If the penalty points increase then the trust value decreases.
- **Property 3**: If neither penalties nor rewards are available, or only penalties are available, then the trust value is set to a minimum / default value, which is l_s .
- **Property 4**: If only reward points are available, then the trust value is set to a maximum value, which is $2 \times l_s$.

For each subject object pair, we calculate a trust value ($T_v(s,o)$). Trust is calculated based on two factors:

1) Clearance level of the subject (l_s), and
2) Reward points history ($H^+(s,o)$).

Based on the clearance, subjects can be classified in numerous ways. For example, in case of a military classification method, one of the following clearance levels is assigned to the subject.

$$\text{Security labels} = \{\text{Top Secret, Secret, Confidential,} \\ \text{Sensitive but unclassified, Unclassified}\}.$$

Let $L_S : S \rightarrow L$ be the maximum clearance level each subject can have. Let $l_s : s \rightarrow l$ be the current clearance level of a subject s, which must be $l_s \leq L_S$ (i.e. L_S must dominate l_s).

At the beginning, when there is no adequate local history for the subject, the system will use the advice of recommenders to calculate the reward point history ($H^+(s,o)$). Recommenders can also be used when additional information for the subject is required. The reward points history ($H^+(s,o)$) factor simply represents the percentage of reward points among the total points. The $H(s,o)^+$ is calculated in the following manner.

$$H^+(s,o) = \begin{cases} w_0 \left(\frac{R^I}{R^I+P^I}\right) + \sum_{k=1}^{m} w_k \left(\frac{R_k^E}{R_k^E+P_k^E}\right) & \text{if history is available} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where R^I and P^I represents the total number of reward and penalty points respectively, which the system stores locally. R^E and P^E represent the total number of reward and penalty points respectively, which are sent by the recommenders. The m represents the total number of the recommenders. Each recommender may have different weight w values. However, the sum of all weight values ($w_0 + \sum_{k=1}^{m} w_k$) is 1. When recommendations are not needed nor available, then the value of w_0 is set to 1.

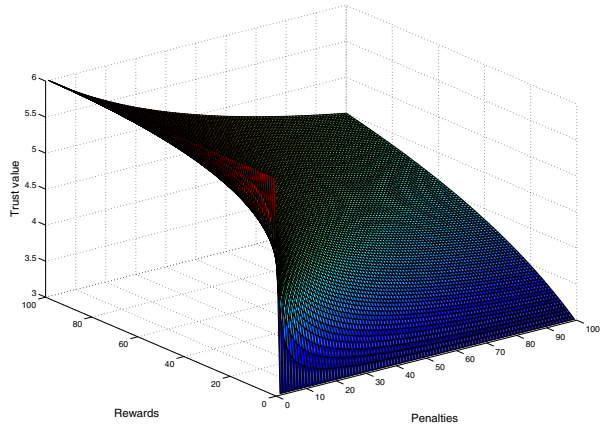

Fig. 2. Trust behavior: l_s=3

After measuring the clearance level of the subject and the reward points history, we calculate the trust value for the subject-object pair ($T_v(s,o)$) in the following manner.

$$T_v(s,o) = l_s \times \left[1 + H^+(s,o)\right] \tag{2}$$

In this equation we multiply the subject sensitivity level (l_s) with the factor $1 + H^+(s,o)$. We have added 1 in $H^+(s,o)$ because whenever the system does not have the record of reward points ($H^+(s,o)$), then it sets the trust value to the default value which is l_s.

The graph shown in Figure 2 is obtained by equation 2. This illustrates that the required characteristics are retained in equation 2. Property 1 can be verified by checking the right most side of Figure 2. Property 2 can be verified by checking the left most side of Figure 2. Property 3 can be verified by checking the right side of Figure 2. Property 4 can be verified by checking the left side of Figure 2.

Proposition 1: The range of trust values is always between $[l_s, 2 \times l_s]$.

Proof: From equation 2, we have

$$T_v(s,o) = l_s \times \left[1 + H^+(s,o)\right]$$

$$= l_s \times \left[1 + w_0 \left(\frac{R^I}{R^I + P^I}\right) + \sum_{k=1}^{m} w_k \left(\frac{R^{E_i}}{R^{E_i} + P^{E_i}}\right)\right] \tag{3}$$

In a worst case, when the subject s does not have any reward points, then the subject s will get minimum trust value. Since there are no rewards points, the values of R^I and R^E become 0 in equation 3. Therefore, we get

$$= l_s \times \left[1 + w_0 \left(\frac{0}{0 + P^I}\right) + \sum_{k=1}^{m} w_k \left(\frac{0}{0 + P^{E_k}}\right)\right]$$

So, the minimum trust value a subject s can get is:

$$T_v(s,o) = l_s \times [1 + 0] = l_s. \tag{4}$$

In a best case, when the subject s does not have penalty points then the subject will get a maximum trust value. In these cases, the values of P^I and P^E become 0 in equation 3. Therefore, we get

$$= l_s \times \left[1 + w_0 \left(\frac{R^I}{R^I + 0}\right) + \sum_{k=1}^{m} w_k \left(\frac{R^{E_k}}{R^{E_k} + 0}\right)\right]$$

$$= l_s \times \left[1 + w_0 + \sum_{k=1}^{m} w_k\right]$$

Since as we mentioned earlier, the sum of all weight values ($w_0 + \sum_{k=1}^{m} w_k$) is 1. Therefore, the maximum trust value a subject s can get is:

$$T_v(s,o) = l_s \times [1 + 1] = 2 \times l_s. \tag{5}$$

■

C. Step 3: Risk Calculation

Our method of dynamically calculating risk values will be designed to satisfy the following requirements:

- **Property 5**: If the penalty points increase then the risk value also increases.
- **Property 6**: If the reward points increase, then the risk value decreases.
- **Property 7**: If penalty points are not available, then the risk value is set to a minimum / default value, which is l_o.
- **Property 8**: If only penalty points are available, then the value of risk is set to a maximum value, which is $2 \times l_o$.

For each subject object pair, we calculate a risk value ($R_v(s,o)$). Risk is calculated based on the following two factors:

1) Sensitivity level of the object (l_o), and
2) Penalty points history ($H^-(s,o)$).

Based on the sensitivity, objects can be classified in numerous ways. For example, in case of a business, one of the following sensitivity labels can be assigned to an object.

$$\text{Security labels} = \{\text{External}, \text{Private}, \text{Sensitive}, \text{Public}\}.$$

Let $L_O : O \rightarrow L$ give the maximum sensitivity level each object can have. Let $L_o : o \rightarrow l$ give the current sensitivity level of an object o, which must be $L_o \leq L_O$ (i.e. L_O must dominate L_o).

The penalty history ($H^-(s,o)$) factor simply represents the percentage of penalty points among the total points of a pair (s,o). The $H^-(s,o)$ is calculated in the following manner.

$$H^-(s,o) = \begin{cases} w_0 \left(\frac{P^I}{R^I + P^I}\right) + \sum_{k=1}^{m} w_k \left(\frac{P_k^E}{R_k^E + P_k^E}\right) & \text{if history is available} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

where R^I and P^I represents total number of reward and penalty points respectively, which the system stores locally. R^E and P^E represent the total number of reward and penalty points respectively, which are sent by the recommenders. The w represents the weight value and the sum of all weight values ($w_0 + \sum_{k=1}^{m} w_k$) is 1.

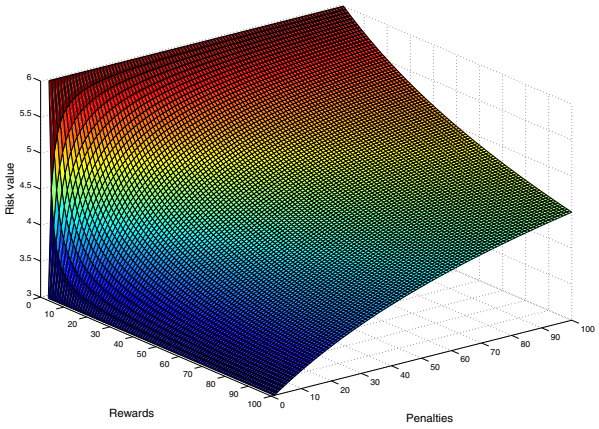

Fig. 3. Risk behavior: l_o=3

After measuring the sensitivity level of an object and the penalty point history, we calculate the risk value for the subject-object pair ($T_v(s,o)$) in the following manner.

$$R_v(s,o) = l_o \times \left[1 + H^-(s,o)\right] \tag{7}$$

In this equation we have multiplied the object sensitivity level (l_o) with the factor $1 + H^-(s,o)$. We have added 1 in the $H^-(s,o)$ because whenever a system does not have a record of penalty points ($H^-(s,o)$), then it will set the risk value to the default value, which is l_o.

The graph shown in Figure 3 is obtained by equation 7. This illustrates that the required characteristics are retained in equation 7. Property 5 can be verified by checking the right side of Figure 3. Property 6 can be verified by checking the right most side of Figure 3. Property 7 can be verified by checking the left side of Figure 3. Property 8 can be verified by checking the left most side of Figure 3.

Proposition 2: The range of risk values is always between $[l_o, 2 \times l_o]$.

Proof: Similar to *proof* 1. ■

D. Step 4: Decision Mechanism

Once the trust and risk values are calculated, the system will make a decision based the equation below.

$$D(T_v(s,o), R_v(s,o)) = \begin{cases} \text{Permit} & \text{if } T_v(s,o) \geq R_v(s,o) \\ \text{Deny} & \text{otherwise} \end{cases} \tag{8}$$

If the trust value $T_v(s,o)$ is greater or equal to the risk value $R_v(s,o)$ then the system will permit access, otherwise the access request will be denied.

IV. Conclusion and Future work

In this paper, we have proposed a dynamic risk-based decision method for access control systems. First, we have introduced the concept of assigning rewards and penalty points for a subject with respect to particular objects. These rewards and penalties reflect the past behavior of the subject. Based on the past behavior and current security levels of a subject and an object, we calculate the trust and risk values that are associated with each subject-object pair. Based on these values, an access decision is made.

In the future, first, we plan to extend this work by incorporating tunable flexibility parameters in the trust and risk calculation methods. Second, we would like to analyze the impacts of these parameters on security resiliency.

Acknowledgment

The work reported in this article was partially supported by the Natural Sciences and Engineering Research Council of Canada, PROMPT Quebec, and CA Technologies.

References

[1] D. E. Bell and L. J. LaPadula, "Secure computer system: Unified exposition and multics interpretation," The Mitre Corporation, Tech. Rep. ESD-TR-75-306, Mar 1976.

[2] D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*. Artech House Publishers, 2003.

[3] L. Dickens, A. Russo, P.-C. Cheng, and J. Lob, "Towards learning risk estimation functions for access control," in *In Snowbird Learning Workshop*, 2010.

[4] L. Zhang, A. Brodsky, and S. Jajodia, "Toward information sharing: Benefit and risk access control (barac)," in *Proceedings of the Seventh IEEE International Workshop on Policies for Distributed Systems and Networks*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 45–53.

[5] Q. Ni, E. Bertino, and J. Lobo, "Risk-based access control systems built on fuzzy inferences," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 250–260.

[6] R. McGraw, "Risk-adaptable access control (RADAC)," in *Privilege (Access) Management Workshop. NIST–National Institute of Standards and Technology–Information Technology Laboratory*, 2009.

[7] F. Salim, J. Reid, and E. Dawson, "Authorization models for secure information sharing: A survey and research agenda," *The ISC International Journal of Information Security*, vol. 2, no. 2, pp. 69–87, 2010.

[8] J. P. Office, "Horizontal integration: Broader access models for realizing information dominance," The Mitre Corporation, Tech. Rep. JSR-04-132, Dec 2004.

[9] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger, "Fuzzy multi-level security: An experiment on quantified risk-adaptive access control," in *IEEE Symposium on Security and Privacy*. Los Alamitos, CA, USA: IEEE Computer Society, 2007, pp. 222–230.

[10] I. Molloy, P.-C. Cheng, and P. Rohatgi, "Trading in risk: using markets to improve access control," in *Proceedings of the 2008 workshop on New security paradigms*, ser. NSPW '08. New York, NY, USA: ACM, 2008, pp. 107–125. [Online]. Available: http://doi.acm.org/10.1145/1595676.1595694

[11] C. L. Clark, "Shopping without cash: The emergence of the e-purse," *Economic Perspectives*, vol. 29, no. 4, pp. 34–51, 2005.