Dynamic Risk-based Decision Methods for Access Control Systems

Riaz Ahmed Shaikh, Kamel Adi, Luigi Logrippo
Université du Québec en Outaouais, Gatineau, Québec, Canada.

Abstract

In traditional multi-level security systems, trust and risk values are pre-computed. Any change in these values requires manual intervention of an administrator. In many dynamic environments, however, these values should be auto-adaptive, and auto-tunable according to the usage history of the users. Moreover, occasional exceptions on resource needs, which are common in dynamic environments like healthcare, should be allowed if the subjects show a positive record of use towards resources they acquired in the past. Conversely, access of authorized users, who have negative record, should be restricted. These requirements are not taken into consideration in existing risk-based access control systems. In order to overcome these shortcomings and to meet different sensitivity requirements of various applications, we propose two dynamic risk-based decision methods for access control systems. We provide theoretical and simulation-based analysis and evaluation of both schemes. Also, we analytically prove that the proposed methods, not only allow exceptions under certain controlled conditions, but uniquely restrict legitimate access of *bad authorized* users.

Key words: Access Control, Policy, Risk, Security, Trust

1. Introduction

Commonly used access control systems, e.g., Role-based Access Control (RBAC) [1] systems, and multi-level security systems, e.g., Bell-LaPadula (BLP) [2] are rigid and require establishing the clearance of a requester, which is a manual and time consuming procedure [3–5]. In these systems, security policies are typically hard coded into decision logic [6] and are the result of pre-computed trade-off analysis between various organizational objectives [7]. Furthermore, these traditional systems do not consider uncertainty and risk in access control decisions, and this makes them inflexible and difficult to adapt to changing circumstances. Due to these limitations, these systems are not very suitable for dynamic environments, like healthcare, emergency services and the military. This motivates us to work in the area of dynamic risk-based decision methods for security and access control systems.

Consider a hospital environment, with various levels of clearance for technicians and doctors and various levels of sensitivity for resources (drugs, equipment, type of treatment). A newly hired technician may be assigned to a low clearance level. As she asks for access to resources, initially access is allowed taking into consideration her clearance level and the sensitivity classification of the resources, as well as possibly recommendations coming from

Corresponding Author: Riaz Ahmed Shaikh, Email: riaz.shaikh@uqo.ca, Tel: +1-819-595-3900 Ext:1656.
This paper is an extended version of our short paper (4 pages) entitled “Risk-based Decision Method for Access Control Systems” published in the proceeding of the 9th Annual Conference on Privacy, Security and Trust (PST2011), Montreal, Canada, July 2011.

previous experiences with her. After each resource access, her performance in using the resource is evaluated by a supervisor. Her history of performance with respect to each resource is recorded: a technician may be very good in dispensing drugs, less good in dispensing certain specialized treatment. In consideration of this history, her access rights with respect to specific resources may be raised or lowered, but remain bound to maximum and minimum values determined by her initial clearance (e.g., a junior technician can never be allowed to handle a resource reserved to a senior technician or to a doctor). After some experience with her, her clearance level may be adjusted, for example she may be promoted to a senior role, but this will be done by administrators.

In more general terms, a flexible risk-based access control decision system should keep track of the outcomes of allowing access of users to resources, and determine future access decisions on the basis of these outcomes. For each user and resource, access of the user to the resource should be respectively relaxed or restricted if the user has shown a positive or negative record of use towards the resource. Recently proposed risk-based access control methods such as [4–6,8,9] do not take into consideration such variability. The objective of this work is to incorporate such variability in the access control decision systems.

In our proposed method, we consider two values, for a given (subject, resource) pair, one that represents how much can we trust the subject towards the resource, and another one that represents the risk of assigning the resource to the subject. A positive record of use of the subject for the resource at the same time increases the trust and decreases the risk of the subject towards the resource; a negative record of use has the opposite effect. We show in Section 3 that the 'record of use' can be implemented by maintaining a history variable which records reward and penalty points for each (subject, resource) pair. Each time a subject requests access to a resource, the history variable is used to determine risk and trust values associated with the request, and these in turn are used to determine whether access should be granted. If access is granted, an obligation service is executed to decide whether the outcome of the action of the subject on the object was positive or negative, resulting in the assignment of new reward or penalty points. These points are used to update the history variable, and the process continues. As defined here, the method is conceived to be implemented in a Multi-Level Security system (MLS)[2].

In a dynamic, highly responsive environment, it may be desired to change access rights quickly in response to recent changes in evaluations; in more conservative environments, it may be desired that these changes be more gradual. To this effect, in a refinement of this technique we propose a EWMA (Exponentially Weighted Moving Average)-based dynamic risk-based decision method for access control systems (See Sec. 4). In this method, we show that it is possible to give more or less importance to recent history with respect to older history.

The rest of the paper is organized as follows. Section 2 presents related work and we briefly highlights the methodology, pros and cons of existing approaches. Section 3 presents our first proposed dynamic risk-based decision method. This section presents the process flow, the mathematical formulation of trust and risk concepts, and decision mechanism. Section 4 presents the EWMA-based dynamic risk-based decision method. In this section, we have not only provided the mathematical formulation of trust and risk concepts but also provided a comparison of the two approaches. Section 5 presents a theoretical and simulation-based analysis and evaluation of the two proposed methods. This section also includes the security resiliency analysis of both risk-based decision methods against threats of allowing illegitimate accesses and restricting legitimate accesses. Finally, Section 6 concludes the paper.

2. Related Work

Incorporating consideration of risk in access control systems has recently gained the attention of researchers [4–6,8–10]. 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 compares the measured risk with the access control policy that identifies the acceptable level of risk for the object being accessed. Thirdly, the system verifies the operational need. If all the requirements for operational need, as specified in the policy, are met then access is granted. RAdAC provides a high-level infrastructure for the granting of exceptions, but it does not itself contain a risk model. The author does not provide 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 [9].

Cheng *et al.* [8] 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 show that fuzzy inference is 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 past behavior of users is not considered to measure risk.

Wang and Jin [10] have proposed a quantified risk-adaptive access control method to protect patient privacy in health information systems. In their model, accessing information (irrespective of whether it is public or highly confidential) that is not required for one's job leads to a high risk score, while accessing relevant information results in a low one. In their model, relevance between medical record and a purpose is determined with a relevance-relation function θ. The authors have mentioned in their paper that the concrete form of the function θ is never known, which makes their approach less generic.

As compared to the state-of-the-art work, including [4–6,8,9], our proposed methods have the following three unique features:

(i) In our methods, trust and risk values are auto-tunable according to the past behavior of the users (Section 3).
(ii) The proposed EWMA-based method is suitable for both conservative and highly responsive environments as compared to the methods that we have cited, that only work in conservative environments (Section 4).
(iii) Our methods, not only allow exceptions under certain controlled conditions, but uniquely restrict legitimate access of bad authorized users (Section 5) .

We provide theoretical and simulation-based analyses and evaluation of both methods (See Sec. 5). These analyses show that indeed our methods have the characteristics we have described.

3. Risk-based Decision Method

Traditionally, whenever a Policy Decision Point (PDP) receives an access request from a requester, it first requests additional information from the Policy Access Point (PAP) and Policy Information Point (PIP) and then makes a decision. In our proposed method, the PDP requests information about the trust and risk values associated with the particular subject and object and then takes the decision. The process flow of the proposed risk-based decision method is shown in Figure 1. This framework is a modification of the standard eXtensible Access Control Markup Language (XACML) framework [11]. All the new components that we have added are highlighted with dotted lines. When the Policy Enforcement Point (PEP) receives an access request from the subject (Step 1), it forwards it to the PDP for an evaluation (Step 2). The PDP first checks the organizational policy (Step 3), e.g., for the current request, should the system make a decision based on the trust and risk values? After that the PDP fetches attributes relevant to the access request from the PIP (Steps 4 to 6). Once all required information is received, the PDP sends a query to the policy risk and trust evaluator point (PRTP) (Step 7). The PRTP evaluates the trust and risk values based on the past behavior of the user (Step 8). The past behavior is evaluated based on the history of reward and penalty points. If the system does not have an adequate history then the PRTP evaluates both values based on recommendations. The current trust and risk values associated with the particular subject-object pair are returned to the PDP (Step 9). Based on the trust and risk values, the PDP makes the decision. This decision is forwarded to the PEP, which enforces it (Step 10). If the access is granted, the PEP informs (Step 11) the obligation service that will decide whether to assign reward or penalty points to the user (Step 12).

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.

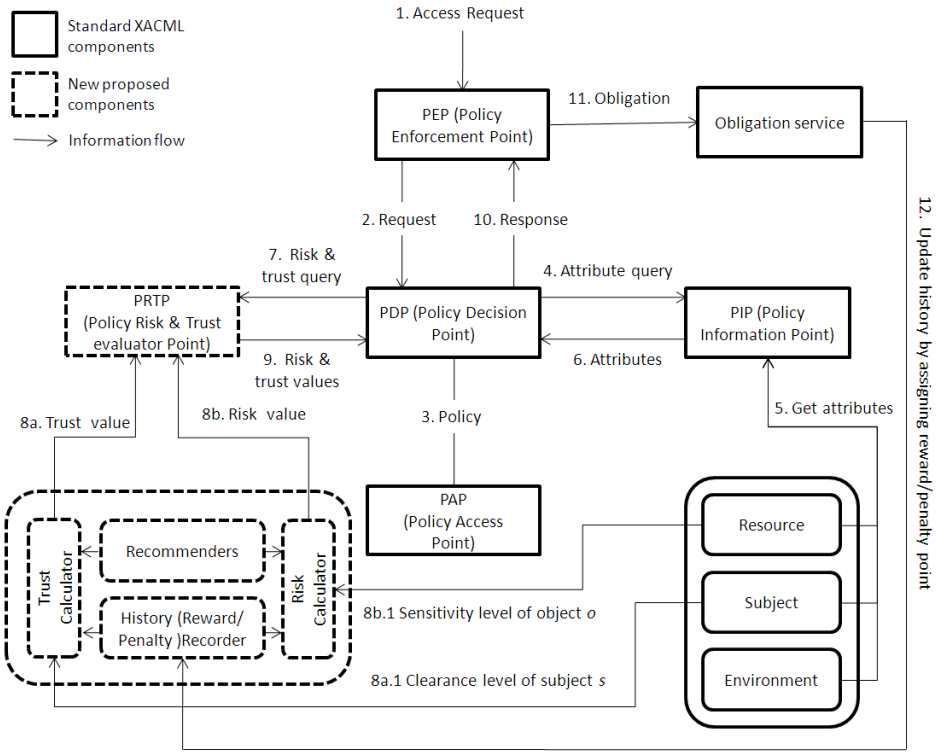


Fig. 1. Process flow of Risk-based Decision Method

3.1. *Step 1: Awarding Reward and Penalty Points*

After access is given, an obligation service is executed in the system that will decide (based on the evaluation of the context) whether to assign reward or penalty points to users as shown in Figure 2. If the result of an evaluation is good then the system will assign reward points, and if the result of an evaluation is bad then the system will assign penalty points. In practice, the obligation service is application dependent. Therefore we will not attempt to describe generic mechanisms through which a system can decide whether to assign reward or penalty points to users.

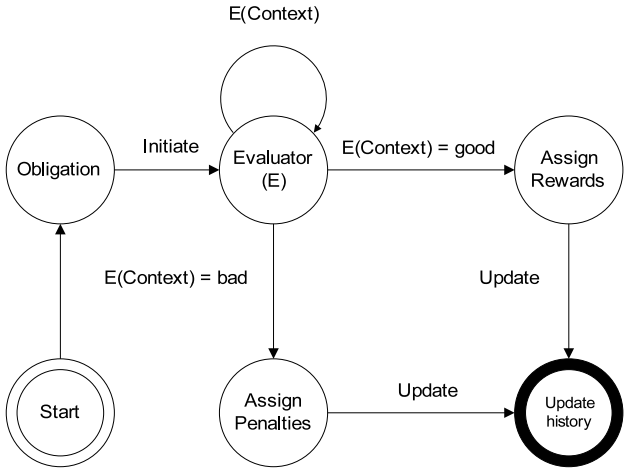


Fig. 2. Data flow for assignment of reward / penalty points

Let us take an example of an e-purse scenario [12,13], where users pay e-cash for using some service such as a subway. Assume that a person wants to use the subway for traveling from one station to another. In this case, the subway registers users when they board, and charges the users' e-purse when they disembark. In this scenario, the validation of the e-cash process can be the obligation service. If e-cash is successfully redeemed, then the system will assign reward point(s) to the subject with respect to the service. If e-cash is not successfully redeemed due to insufficient funds or any other reason, then the system will assign penalty point(s).

3.2. *Step 2: Trust Calculation*

Our method of dynamically calculating trust values has been designed to satisfy the following intuitively described requirements:

- **Property 1**: If neither penalties nor rewards are available then the trust value is set to a default value.
- **Property 2**: Reward points increase the trust value.
- **Property 3**: Penalty points decrease the trust value.
- **Property 4**: In the presence of both rewards and penalties, the trust value is always bound between minimum and maximum values.
- **Property 5**: If only penalties are available then the trust value is set to a minimum value.
- **Property 6**: If only reward points are available then the trust value increases more quickly with the increase in reward points but never exceeds a maximum value.

These properties of trust are inspired by the observation of real world examples such as the following one, presenting a scenario of trust relationship evolution between a client and a credit card company.

(i) If client is new then credit card company sets default credit limit for the client. From this observation we derived property 1.
(ii) If client pays bills on time, then his credit limit may be increased. From this observation we derived property 2.
(iii) If client misses some payment deadlines, then his credit limit may decrease. From this observation we derived property 3.
(iv) Based on the type of credit card (e.g., gold, silver), maximum and minimum credit limits are set. Based on the bill payment history, the credit limit is set, but always bound between minimum and maximum credit limits. From this observation we derived property 4.
(v) If client always pays bills late then his credit limit is set to the minimum value according to the type of the credit card. From this observation we derived property 5.
(vi) If client *A* has been paying bills on time for the last 12 months and client *B* has been paying bills on time for the last 24 months, then the credit limit of client *B* should be higher than the credit limit of the client *A*. From this observation we derived property 6.

Note that these properties are generic and are not limited to this example.

Mayer *et. al.* [14] have defined trust as a function of trustee's behaviour that includes its ability, benevolence and integrity and of the trustor's propensity to trust. In this paper, we determined trustee's behaviour with the help of a reward point history $H^+(s,o)$, and trustor's propensity to trust with a subject clearance level l_s. Based on these two factors, we calculate the trust value T_v for the subject-object pair (s,o) in the following manner.

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

In this equation we multiply the subject clearance level l_s by 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.

Let us first discuss the derivation of parameters used in the calculation of trust value, and then we will discuss whether the required properties are retained in this equation.

Our method of calculating the reward points history $H^+(s,o)$ attempts to mimic the way trust builds up in real life: we use a measurement based on rewards and penalties, which we call the Local Reward History (LRH), and possibly a measurement based on positive and negative recommendations, which we call the External Reward History (ERH). The LRH for a pair (s,o) is calculated in the following manner:

$$\text{LRH}(s,o) = \left(\frac{R}{R+P}\right)\alpha^{\frac{1}{R+1}}; 0 < \alpha < 1. \tag{2}$$

where R and P represent the total number of reward and penalty points respectively for the pair (s, o), which the system stores locally. The expression $\frac{R}{R+P}$ simply represents the percentage of reward points among the total points. This expression is enough when we have both reward and penalty points. To make the LRH value grow gradually in the absence of penalty points, we have multiplied the $\frac{R}{R+P}$ expression with $\alpha^{1/(R+1)}$, where α represents the rate at which the trust value increases with the increase in reward points.

The External Reward History (ERH) is obtained via recommendation of trusted peers. Getting recommendations is an optional step. These can be considered only when the system does not have an adequate local history. The ERH for a pair (s, o) is calculated in exactly same manner as the LRH(s, o), the only difference is that the values of R and P are obtained from the recommenders:

$$\text{ERH}(s,o)_k = \left(\frac{R_k}{R_k+P_k}\right)\alpha^{\frac{1}{R_k+1}}; 0 < \alpha < 1. \tag{3}$$

where R_k and P_k represent the total number of reward and penalty points respectively for the pair (s, o), which are sent by the recommender k.

In general, the $H^+(s, o)$ is calculated in the following manner:

$$H^+(s,o) = \begin{cases} w_0\text{LRH}(s,o) + \sum_{k=1}^{m} w_k\text{ERH}(s,o)_k & \text{if history is available} \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

where 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 or not available, then the value of w_0 is set to 1. In the absence of local and external reward histories the value of $H^+(s, o)$ is set to zero.

Based on the clearance, subjects can be classified in numerous ways. For example, many organizations employ a hierarchical range of classifications, and one of the following clearance levels can be assigned to a subject.

$$\text{Security levels} = \{\text{Top Secret, Secret, Confidential, Unclassified}\}.$$

Other security labels may also be used. Whatever labels are used, we first sort them according to their sensitivity level and we map them on in ordered sequence of numbers. For example, we can assign numbers to the above mentioned security labels in the following manner.

$$\text{Security levels} = \{\text{Top Secret=4, Secret=3, Confidential=2, Unclassified=1}\}.$$

Let $L_S : S \rightarrow L$ be the maximum clearance level each subject can have. Here S represents a set of subjects and L represents a set of security levels. 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).

The graph shown in Figure 3 is obtained by equation 1. This illustrates that the required properties are retained in equation 1. For example, the index (0,0) of Figure 3 shows that in absence of both reward and penalty points, the trust value is set to the default value, which in this example is 4. This satisfies property 1. The right most side of Figure 3 shows that with the increase in reward points the trust value also increases. This satisfies property 2. The left most side of Figure 3 shows that with the increase in penalty points the trust value decreases. This satisfies property 3. The values between the index (1,1) to (100,100) of Figure 3 show that when both rewards and penalty points are available, the trust value is bound between minimum and maximum values, which in this example are 4 and 8 respectively. This satisfies property 4. The right side of Figure 3 shows that in the presence of only penalty points, the trust value is set to a minimum value, which in this example is 4. This satisfies property 5. The left side of Figure 3 shows that in the presence of only reward points, the trust value increases more quickly with the increase in rewards points but never exceeds the maximum value, which in this example is 8. This satisfies property 6.

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

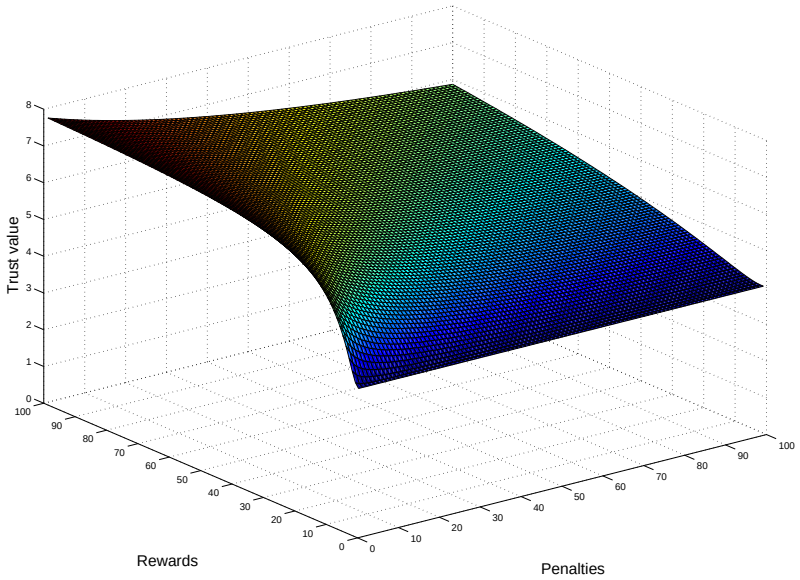


Fig. 3. Trust behavior: l_s=4

Proof: See *Appendix* A.1. ■

Proposition 2: The default trust value $T_v^{def}(s, o)$ is l_s.
Proof: See *Appendix* A.2. ■

Note that in our approach, the minimum and default trust values are the same. We keep them the same for simplicity. However, different values could also be used with minor tuning in equation 1. Tuning can be performed in many ways but the following condition must be kept:

$$T_v^{min}(s, o) \leq T_v^{def}(s, o) \leq T_v^{max}(s, o).$$

3.3. *Step 3: Risk Calculation*

Our method of dynamically calculating risk values has been designed to satisfy the following requirements:

- **Property 7**: If neither reward nor penalty points are available then the risk value is set to a default value.
- **Property 8**: Penalty points increase the risk value.
- **Property 9**: Reward points decrease the risk value.
- **Property 10**: In the presence of both rewards and penalties, the risk value is always bound between minimum and maximum values.
- **Property 11**: If only reward points are available then the risk value is set to a minimum value.
- **Property 12**: If only penalty points are available then the risk value increases more quickly with the increase in penalty points but never exceeds a maximum value.

The USA National Institute of Standards and Technology (NIST) [15] has defined risk as a function of threat likelihood and impact. At a high-level, we adopt the same definition. We determine the threat likelihood based on the penalty point history and the impact based on the object sensitivity level. If the sensitivity level of the object is high then the impact will be high also. For example, impact of disclosure of top secret information can range from jeopardizing national security to disclosure of privacy act data [15].

Based on the penalty point history $H^-(s, o)$, and sensitivity level of the object l_o, we calculate the risk value R_v for the subject-object pair (s, o) in the following manner:

$$R_v(s,o) = l_o \times \left[1 + H^-(s,o)\right]. \tag{5}$$

Let us first discuss the derivation of the parameters used in the calculation of risk value, and then we will discuss whether the required properties are retained in Equation 5 or not.

As in case of the reward point history, the penalty points history $H^-(s,o)$ factor is also composed of two sub-factors: 1) Local Penalty History (LPH) and 2) External Penalty History (EPH). The LPH for a pair (s,o) is calculated in the following manner:

$$\text{LPH}(s,o) = \left(\frac{P}{R+P}\right)\alpha^{\frac{1}{P+1}}; 0 < \alpha < 1. \tag{6}$$

Note that we have used the expression $\frac{P}{R+P}$ that represents the percentage of penalty points among the total points, whereas in LRH we used the expression $\frac{R}{R+P}$ which represents the percentage of reward points among the total points.

The EPH is obtained via recommendation of trusted peers and is calculated in the following manner:

$$\text{EPH}(s,o)_k = \left(\frac{P_k}{R_k+P_k}\right)\alpha^{1/(P_k+1)}; 0 < \alpha < 1. \tag{7}$$

In general, the $H^-(s,o)$ is calculated in the following manner:

$$H^-(s,o) = \begin{cases} w_0\text{LPH}(s,o) + \sum_{k=1}^{m} w_k\text{EPH}(s,o)_k & \text{if history is available} \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

Based on the sensitivity, objects can also be classified in numerous ways. It is the responsibility of the owner of an object to assign an appropriate level to it. Note that subjects and objects should be labeled according to the same classification method. For example, if subjects are classified into four categories: 1) Top secret, 2) Secret, 3) Confidential, and 4) Unclassified, then objects should also be classified into the same four categories.

Let $L_O : O \rightarrow L$ be the maximum sensitivity level an object can have. Here O represents a set of objects and L represents a set of security levels. Let $l_o : O \rightarrow L$ be 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 graph shown in Figure 4 is obtained by equation 5. This illustrates that the required characteristics are retained in equation 5. For example, the index (0,0) in Figure 4 shows that in absence of both rewards and penalty points, the trust value is set to the default value, which in this example is 4. This satisfies property 7. The right side of Figure 4 shows that with the increase in penalty points the risk value also increases. This satisfies property 8. The right most side of Figure 4 shows that with the increase in reward points the risk value decreases. This satisfies property 9. The values between the index (1,1) to (100,100) of Figure 4 show that when both rewards and penalty points are available, the risk value is bound between minimum and maximum values, which in this example are 4 and 8 respectively. This satisfies property 10. The left side of Figure 4 shows that in the presence of only rewards points, the risk value is set to a minimum value. This satisfies property 11. The left most side of Figure 4 shows that in the presence of only penalty points, the risk value increases more quickly with the increase in penalty points but never exceeds the maximum value, which in this example is 8. This satisfies property 12.

Proposition 3: The range of risk value is always between $[l_o, 2 \times l_o]$.

Proof: See *Appendix* A.3. ■

Proposition 4: The default risk value $R_v^{def}(s,o)$ is l_o.

Proof: See *Appendix* A.4. ■

As in the case of trust, the minimum and default risk values are the same. In order to use different values the following condition must be kept:

$$R_v^{min}(s,o) \leq R_v^{def}(s,o) \leq R_v^{max}(s,o).$$

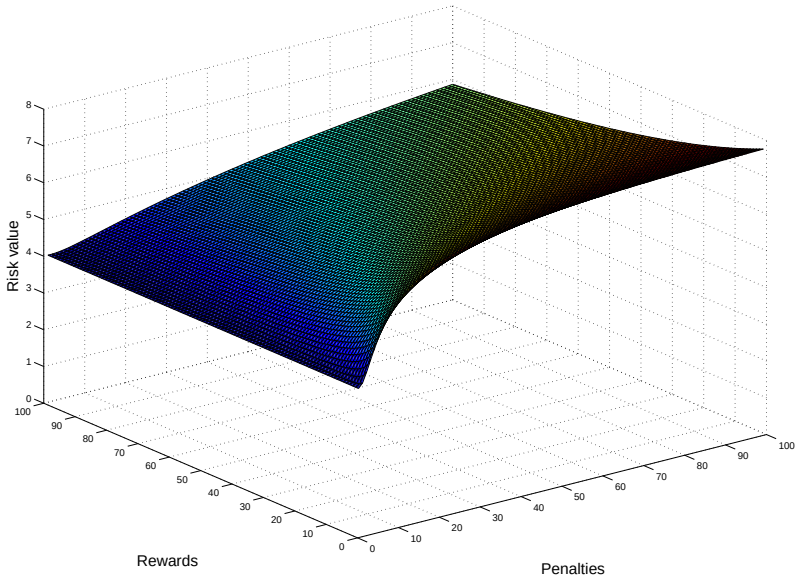


Fig. 4. Risk behavior: l_o=4

3.4. *Step 4: Decision Mechanism*

Conceptually, trust and risk zones are created for each subject-object pair (s, o) as shown in Figure 5. Both trust and risk values always fall inside their respective zones. Once the trust and risk values are calculated, the system will make a decision based on the equation below.

$$D(T_v(s,o), R_v(s,o)) = \begin{cases} \text{Permit if } T_v(s,o) \geq R_v(s,o) \\ \text{Deny otherwise} \end{cases} \tag{9}$$

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

Let us assume that the system will assign rewards and penalty points to users according to the policies specified in Table 1: if the user accesses an object from a secure public network, then the system will assign one reward point, and so on. Assume that Joe with clearance level 3 has accessed a level 3 object in the following sequence:
– from secure public network,
– from insecure public network,
– from secure private network, and
– from insecure private network.
In total Joe receives 2.5, and 3 reward and penalty points respectively. Assume that $\alpha = 0.2$. When the system receives a new read access request from Joe, it computes the trust and risk values, which are 3.86 and 3.95 respectively. The current trust value is less than the risk value, so the system will deny read access. Note that in a traditional MLS security system, Joe would always get read access to the object because his clearance level is equal to the sensitivity level of the object.

4. Second Proposed Method

So far, our proposed method of calculating reward and penalty histories has been based on the assumption that the recent and old history have equal weight. The consequence of this assumption is that the method may be unable to detect small changes in recent behavior of a subject in a timely manner. One of the approaches to solve this problem is

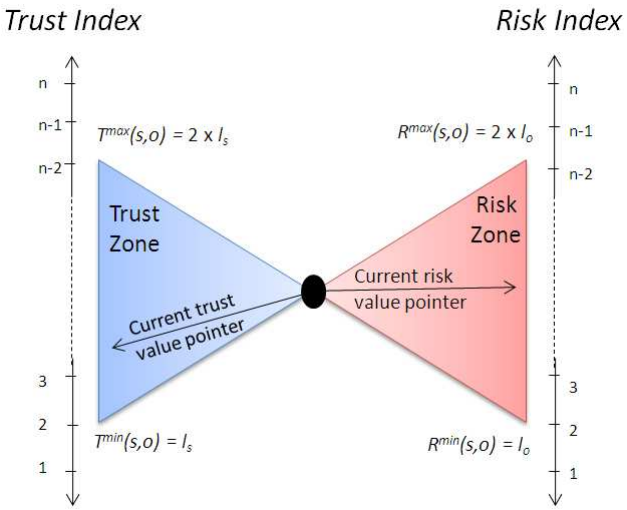


Fig. 5. Trust and Risk zones

Table 1
Sample reward and penalty assignment policy

	Secure network	Insecure network
Public network	1 reward	2 penalties
Private network	1.5 reward	1 penalty

to assign different weight values to the recent and past behavior. This can be done in many ways. One of the common methods used in statistics is *Exponentially Weighted Moving Average* (EWMA) [16]. In the EWMA approach, the weighting for older data points decreases exponentially, but never reaches zero. The EWMA is calculated as follows:

$$Z_t = \lambda X_t + (1 - \lambda) Z_{t-1} \tag{10}$$

where Z_t represents the EWMA at time t, X_t represents the most recent data point, Z_{t-1} represents the immediate preceding point, and λ is a weighting factor 0 to 1 (exclusive). Setting $\lambda = 0$ means that we are completely ignoring the most-recent transaction, and setting $\lambda = 1$ means that we are not considering old transactions at all. Therefore, the value of λ should be between 0 and 1. If the value of λ is high (close to 1), then we are giving more importance to recent transactions as compared to the old ones. If the value of λ is low (close to 0), then we are giving more importance to old transactions as compared to the most-recent ones.

We can apply the EWMA in our method for calculating rewards point history $H^+(s,o)$ in the following manner:

$$H_t^+(s,o) = \begin{cases} \lambda(X_t) + (1-\lambda)\left[w_0 \mathrm{LRH}(s,o) + \sum_{k=1}^{m} w_k \mathrm{ERH}(s,o)_k\right] & \text{if } t \geq 2 \\ w_0 \mathrm{LRH}(s,o) + \sum_{k=1}^{m} w_k \mathrm{ERH}(s,o)_k & \text{if } t = 1 \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

where $H_t^+(s,o)$ represents the rewards point history at time t for the subject-object pair (s,o), and X_t represents the result of the most recent transaction. Note that we can use this approach only when we have more than one historical instance available. In other cases, the reward point history will be calculated in exactly same manner as discussed in the previous section. In order to calculate a trust value, we only need to replace $H^+(s,o)$ with $H_t^+(s,o)$ in equation 1, as shown below.

$$T_v(s,o) = l_s \times \left[1 + H_t^+(s,o)\right] \tag{12}$$

Similarly, the concept of EWMA can easily be integrated in our penalty history $H^-(s,o)$ method in the following manner.

$$H_t^-(s,o) = \begin{cases} \lambda(X_t) + (1-\lambda)\left[w_0 \text{LPH}(s,o) + \sum_{k=1}^{m} w_k \text{EPH}(s,o)_k\right] & \text{if } t \geq 2 \\ w_0 \text{LPH}(s,o) + \sum_{k=1}^{m} w_k \text{EPH}(s,o)_k & \text{if } t = 1 \\ 0 & \text{otherwise} \end{cases} \tag{13}$$

A risk value is calculated by replacing $H^-(s,o)$ with $H_t^-(s,o)$ in equation 5, as shown below.

$$R_v(s,o) = l_o \times \left[1 + H_t^-(s,o)\right] \tag{14}$$

Note that when we calculate $H_t^+(s,o)$ in a situation where the penalty was assigned in the most-recent transaction, then the value of X_t could either be set to zero or a negative sign should be added with the number of penalties received in the last transaction. This is required because penalty points should not play a role in increasing the value of the reward point history $H_t^+(s,o)$. The same procedure should be adopted for calculating $H_t^-(s,o)$.

In order to analyze the differences of simple and EWMA based approaches, let us take again the example of Section 3.4. When the new access request comes, then according to the EWMA-based method ($\lambda = 0.2$), the trust and risk values are 3.24 and 4.22 respectively. In the simple risk-based decision method, the trust and risk values were 3.86 and 3.95 respectively. Note that in the last transaction, Joe gets a penalty. Due to this, the risk value increases more quickly in the EWMA-based approach as compared to the simple method. These values indicate that the EWMA-based approach responds more quickly to the recent change as compared to the simple method.

For detailed analysis, we have performed numerical simulations. The results of the simulation are shown in Figure 6. In this figure, the history of reward and penalty points are shown with bars. If the direction of the bar is positive, a reward point is assigned. If the direction of the bar is negative, a penalty is assigned. One can see that the EWMA-based approach reflects abrupt and recent changes in the behavior more quickly (depending on the value of λ) as compared to the simple approach. For example, in Figure 6(a), only penalty points are assigned during the period between 16 and 19. In this period, the EWMA based approach decreases the trust value more quickly as compared to the simple approach. Similarly, in Figure 6(b), for the same period, the EWMA based approach increases the risk value much faster than the simple approach.

Proposition 5: In the EWMA approach, the range of trust value is always between $[l_s\,(1 + \lambda(X_t))\,,\ l_s\,(2 + \lambda(X_t - 1))]$.

Proof: See *Appendix* A.5. ■

Proposition 6: In the EWMA approach, the range of risk value is always between $[l_o\,(1 + \lambda(X_t))\,,\ l_o\,(2 + \lambda(X_t - 1))]$.

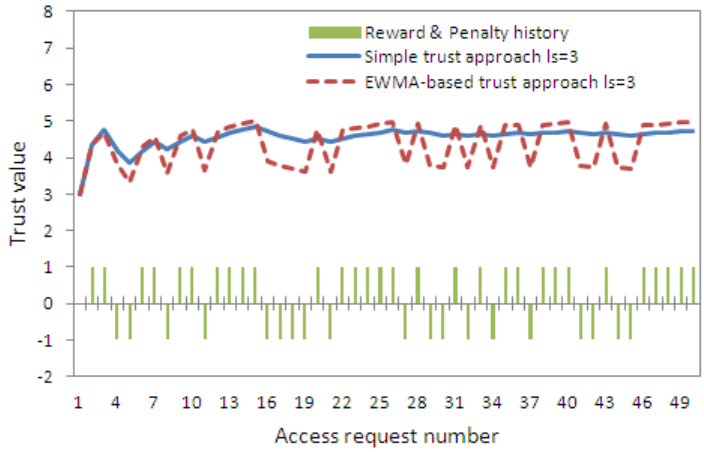
Proof: See *Appendix* A.6. ■

In the EWMA approach, the default values of trust and risk will remain same as in the simple approach.

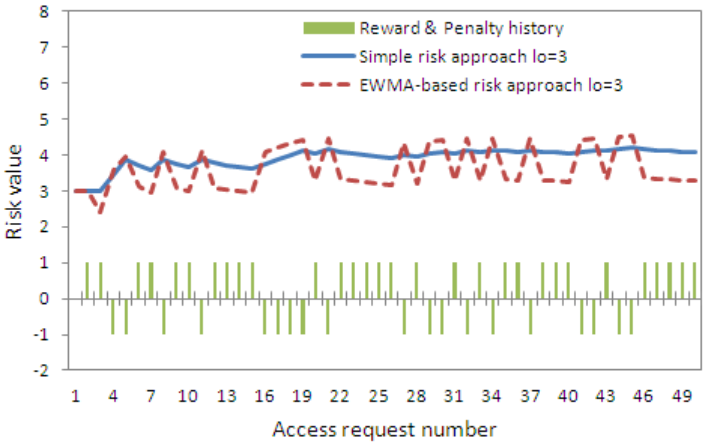
5. Analysis and Evaluation

5.1. *Security Resiliency Analysis*

In this section, we analyze the resiliency of both risk-based decision methods against threats of allowing illegitimate accesses and restricting legitimate accesses. Depending on the underlying multi-level security systems (MLS), access means read only or write only. As we have mentioned earlier, our proposed methods are loosely based on multi-level security systems (MLS). If the underlying MLS system is based on the Bell-LaPadula (BLP) confidentiality



(a) Trust



(b) Risk

Fig. 6. Comparison: $\lambda = 0.2$

model [2] then access means read only. If the underlying MLS system is based on the BiBa integrity model [17] then access means write only. Note that if we are assuming the Biba model, then the terms clearance level of a subject and sensitivity level of a object are replaced with the terms integrity level of a subject and integrity level of a object respectively.

We begin with the definition of *illegitimate* accesses.

Definition 1: Access is considered to be illegitimate if
(i) $l_s < l_o$, and
(ii) Subject s is permitted to access object o.
where, l_s represents the clearance level of the subject and l_o represents the sensitivity level of the object.

As we have mentioned earlier, the general objective of risk-based access control systems is to achieve flexibility. This is achieved by allowing exceptions in situations when regular conditions are not satisfied, for example when a subject with low clearance level is granted access to an object of high sensitivity level. Such exceptions should be allowed under controlled conditions. In this section, we will identify these conditions.

There are four possible scenarios:
(i) There are neither rewards nor penalties ($H^+(s,o) = 0$ and $H^-(s,o) = 0$).
(ii) There are only penalties ($H^+(s,o) = 0$ and $H^-(s,o) \neq 0$).

(iii) There are only rewards ($H^+(s,o) \neq 0$ and $H^-(s,o) = 0$).
(iv) There are both rewards and penalties ($H^+(s,o) \neq 0$ and $H^-(s,o) \neq 0$).

Claim 1: The proposed risk-based decision method does not allow illegitimate accesses if no reward and penalty histories are available.

Proof: See *Appendix* B.1.

In this scenario, the control condition for granting access is $l_s \geq l_o$. This satisfies the simple security property of the BLP confidentiality model which states that a subject at a given security level may not read an object at a higher security level. Also, it satisfies the $\star$(star)-property of the Biba integrity model that states that a subject at a given level of integrity must not write to any object at a higher level of integrity.

Claim 2: The proposed risk-based decision method does not allow illegitimate access if only penalty history is available.

Proof: See *Appendix* B.2.

In this scenario, the control condition for granting access is $l_s \geq 2 \times l_o$. One can note that in the presence of only penalty points, our proposed system will tighten the security control by increasing the control condition from $l_s \geq l_o$ to $l_s \geq 2 \times l_o$. Like scenario 1, our proposed method satisfies the simple security property of the BLP confidentiality model and the $\star$-property of the Biba integrity model.

Claim 3: If only the reward history is available then the proposed risk-based decision method allows illegitimate access only when $l_s \geq \frac{l_o}{2}$.

Proof: See *Appendix* B.3.

In this scenario, the control condition for granting an access is $l_s \geq \frac{l_o}{2}$. This shows that if the user's behavior is positive then system will grant access to the subject by relaxing the security control condition from $l_s \geq l_o$ to $l_s \geq \frac{l_o}{2}$.

Claim 4: If both reward and penalty histories are available then the proposed risk-based decision method allows illegitimate accesses only when

$$l_s \geq l_o \left(\frac{H^-(s,o)}{H^+(s,o)} \right).$$

Proof: See *Appendix* B.4.

In this scenario, the control condition for granting an access is $l_s \geq l_o \left(\frac{H^-(s,o)}{H^+(s,o)} \right)$. From this condition, we conclude that if the number of penalties is higher than the rewards then the system will tighten the security control as compared to the default condition, whereas if the number of rewards is more than the penalties then the system will slightly relax the security control condition.

Definition 2: Access is considered to be legitimate if
(i) $l_s \geq l_o$, and
(ii) Subject s is permitted to access object o.

Users having legitimate access can be broadly categorized into two types: *good* users and *bad* users. Authorized users are classified into these two categories based on the history.

Definition 3: An authorized user is considered to be *good* if

$$H^+(s,o) \geq H^-(s,o).$$

Definition 4: An authorized user is considered to be *bad* if

$$H^+(s,o) < H^-(s,o).$$

Claim 5: The proposed Risk-based decision method restricts legitimate accesses of bad users and allows legitimate access of good users.

Proof: Access is granted only when

$$T_v(s,o) \geq R_v(s,o).$$

From equation 1 and 5, we replace the values of T_v and R_v in the following manner

$$l_s \times \left[1 + H^+(s,o)\right] \geq l_o \times \left[1 + H^-(s,o)\right].$$

According to definition 2, a user is authorized if $l_s \geq l_o$. Therefore, in order to get to the lower limit, we can replace l_s with l_o or vice versa. We get the following result.

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

$$= \left[1 + H^{+}(s,o)\right] \geq \left[1 + H^{-}(s,o)\right]$$
$$= H^{+}(s,o) \geq H^{-}(s,o).$$

According to definition 4, for a bad authorized user, $H^{+}(s,o)$ should be less than $H^{-}(s,o)$. But this is not possible in this case. This shows that, in order to get access, $H^{+}(s,o)$ must be at least equal to $H^{-}(s,o)$. This proves that the legitimate access of the bad user is always restricted. The above result also confirms that the legitimate access of the good user (Definition 3) is always allowed.

■

Note: All the above mentioned five claims that are presented for the *simple* risk-based decision method also hold for the EWMA-based method. We only need to replace the formulas of $H^{+}(s,o)$ and $H^{-}(s,o)$ with $H_t^{+}(s,o)$ and $H_t^{+}(s,o)$ respectively. We prove here scenario 2 and we leave the other scenarios as an exercise for the reader.

Claim 6: The proposed EWMA-based decision method does not allow illegitimate access if only the penalty history is available.

Proof: Access is granted if

$$T_v(s,o) \geq R_v(s,o).$$

This can be written as:

$$l_s \times \left[1 + H_t^{+}(s,o)\right] \geq l_o \times \left[1 + H_t^{-}(s,o)\right].$$

Since no reward history is available, $H_t^{+}(s,o) = 0$, and we get:

$$l_s \geq l_o \times \left[1 + H_t^{-}(s,o)\right].$$

With the help of equation 13, the above equation is transformed into the following:

$$l_s \geq l_o \times \left[1 + \left\{\lambda(X_t) + (1-\lambda)\left[w_0\left(\frac{P}{R+P}\right)\alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k\left(\frac{P_k}{R_k+P_k}\right)\alpha^{\frac{1}{P_k+1}}\right]\right\}\right].$$

Since the reward history is not available, the value of R become 0. So we get:

$$l_s \geq l_o \times \left[1 + \left\{\lambda(X_t) + (1-\lambda)\left[w_0\left(\frac{P}{0+P}\right)\alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k\left(\frac{P_k}{0+P_k}\right)\alpha^{\frac{1}{P_k+1}}\right]\right\}\right]$$

$$l_s \geq l_o \times \left[1 + \lambda(X_t) + (1-\lambda)\left(w_0\alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k\alpha^{\frac{1}{P_k+1}}\right)\right].$$

As we know that $\lim_{P\to\infty}\left(\frac{1}{P+1}\right) = 0$. So, $\alpha^0 = 1$. Therefore, we get:

$$l_s \geq l_o \times \left[1 + \left\{\lambda(X_t) + (1-\lambda)\left[w_0 + \sum_{k=1}^{m} w_k\right]\right\}\right].$$

Since as we mentioned earlier, the sum of all weight values $w_0 + \sum_{k=1}^{m} w_k$ is 1, we get:

$$l_s \geq l_o \times [1 + \{\lambda(X_t) + (1-\lambda)\}]$$

$$l_s \geq l_o \times [2 + \lambda(X_t - 1)].$$

Here, X_t represents the most recent penalty point. Let us assume that the single penalty point is represented with 1, then we get:

$$l_s \geq 2 \times l_o.$$

Again, we get $l_s \geq 2 \times l_o$. Hence in the absence of reward points, illegitimate access is not possible.

■

5.2. *Simulation*

In this section, we will see how trust and risk values increase or decrease with the change in user past behavior. After that, we will see how such changes in trust and risk values will affect the access rights of the users.

For this purpose, we have performed a numerical simulation in Microsoft Excel for a single user *s* who periodically tries to access the same object *o*. After the completion of every transaction, we randomly assign reward and penalty points. Based on the total number of reward and penalty points, user *s* may be categorized as *good* (**Definition** 3) or *bad* (**Definition** 4) user. This setup is executed in the following three scenarios for both proposed approaches:

(i) Scenario 1: The subject clearance level (l_s) is equal to the object sensitivity level (l_o).
(ii) Scenario 2: The subject clearance level (l_s) is less than the object sensitivity level (l_o).
(iii) Scenario 3: The subject clearance level (l_s) is greater than the object sensitivity level (l_o).

In Figure 7 the history of reward and penalty points is shown with bars. If the direction of the bar is positive, a reward point is assigned. If the direction of the bar is negative, a penalty is assigned. Figure 7 shows that in each scenario, trust and risk values gradually increase or decrease with respect to the number of reward and penalty points. Figure 7(a), Figure 7(b) and Figure 7(f) show that access of users having proper clearance level may be restricted if the behavior of the user was *bad* in the past. Figure 7(c) and Figure 7(d) show that a user having lower clearance level may get access to an object of high sensitivity level if his past behavior was *good*. Note that the behavior of the two curves is complementary, when one moves up, the other moves down. However, the rate of change at both ends is mainly dependent on the values of l_s and l_o.

The results of numerical simulation prove that our proposed risk-based access control decision methods are adaptive and moderately increase or decrease all users' access rights to resources based on their past behavior.

6. Conclusion and Future Work

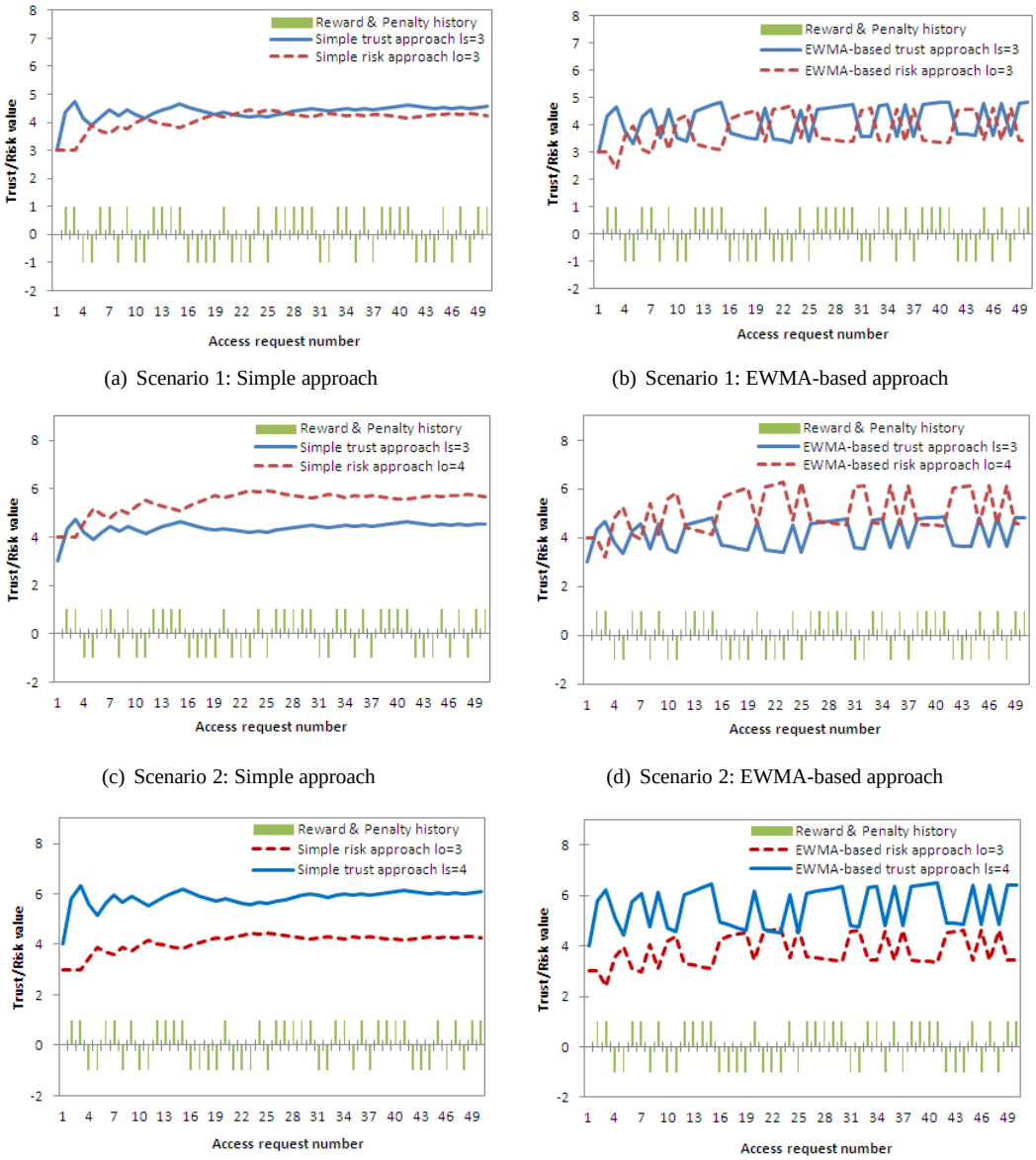
In traditional access control systems, policies are typically hard coded and are the result of pre-computed trust and risk values associated with subjects and objects respectively. Such approach is rigid and inflexible for dynamic environments. In order to overcome this limitation, researchers have started developing dynamic risk-based access control systems. However, recently proposed risk-based schemes have two major limitations: they do not consider the past behavior of users in dynamic decision making, which is necessary to differentiate good and bad authorized users, and they are not very suitable for highly responsive environments.

The goal of this work was to overcome both limitations. Our methods are based on the history of reward and penalty points, which are assigned to users after the completion of transactions. First, we have presented a simple risk-based decision method, which overcomes the first limitation (Section 3). To address the second limitation, we have proposed a method based on an Exponentially Weighted Moving Average (Section 4). In both methods, trust and risk values are dynamically calculated for each subject-object pair, and reflect the past behavior of users.

We have provided a security resiliency analysis of our proposed methods. Results show that they may allow occasional exceptions under certain controlled conditions which are described below.

(i) When no history is available then our proposed methods grant access only if the subject's clearance level dominates the object's sensitivity level (Appendix B.1). This condition is consistent with similar conditions defined in Multi-Level Security systems such as the simple security property of the BLP model.
(ii) When only the penalty history is available then our proposed methods will tighten the default security control condition. In order to get access, a subject's clearance should be at least twice the object's sensitivity level (Appendix B.2). This condition helps restrict illegitimate accesses, and also provides some degree of protection against bad authorized users.
(iii) When only the reward history is available then our proposed methods will grant access to subjects by relaxing the default security control condition up to a certain degree (Appendix B.3). This condition will help achieve flexibility in the access decisions.
(iv) When both reward and penalty histories are available then our proposed methods will grant access only if the ratio of rewards and penalties is greater than the ratio of the object's sensitivity level and the subject's clearance level (Appendix B.4). This condition provides all the benefits listed in the above mentioned scenarios.

Our methods can be modified and adapted to different needs, by choosing appropriate parameters or changing



(a) Scenario 1: Simple approach

(b) Scenario 1: EWMA-based approach

(c) Scenario 2: Simple approach

(d) Scenario 2: EWMA-based approach

(e) Scenario 3: Simple approach

(f) Scenario 3: EWMA-based approach

Fig. 7. Numerical simulations: $\lambda = 0.2$

the formulas in various ways. However such changes should be carefully introduced and in each case the desired properties should be checked. In the current formulation, the methods can be used to control upward accesses such as *no read up* (simple property of the BLP model) or *no write up* ($\star$-property of the Biba model). For controlling downward direction accesses like *no write down* ($\star$-property of the BLP model) or *no read down* (simple property of the Biba model) modifications are required in the decision mechanism (Section 3.4). This will be left to future research.

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. We thank Hemanth Khambhammettu, and Serge Serge

Mankovski for useful discussions. We are also thankful to the anonymous referees for comments that have led to improvements in the paper

References

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

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

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

[4] L. Zhang, A. Brodsky, 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, IEEE Computer Society, Washington, DC, USA, 2006, pp. 45–53. doi:10.1109/POLICY.2006.36.

[5] Q. Ni, E. Bertino, J. Lobo, Risk-based access control systems built on fuzzy inferences, in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS '10, ACM, New York, NY, USA, 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, E. Dawson, Authorization models for secure information sharing: A survey and research agenda, The ISC International Journal of Information Security 2 (2) (2010) 69–87.

[8] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, A. S. Reninger, Fuzzy multi-level security: An experiment on quantified risk-adaptive access control, in: IEEE Symposium on Security and Privacy, IEEE Computer Society, Los Alamitos, CA, USA, 2007, pp. 222–230. doi:http://doi.ieeecomputersociety.org/10.1109/SP.2007.21.

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

[10] Q. Wang, H. Jin, Quantified risk-adaptive access control for patient privacy protection in health information systems, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), ACM, New York, NY, USA, 2011, pp. 406–410. doi:http://doi.acm.org/10.1145/1966913.1966969.

[11] M. Verma, Xml security: Control information access with XACML (Oct 2004).
URL `http://www.ibm.com/developerworks/xml/library/x-xacml/`

[12] C. L. Clark, Shopping without cash: The emergence of the e-purse, Economic Perspectives 29 (4) (2005) 34–51.

[13] N. E. Dimmock, Using trust and risk for access control in global computing, Tech. Rep. UCAM-CL-TR-643, University of Cambridge, Computer Laboratory (Aug 2005).

[14] R. C. Mayer, J. H. Davis, F. D. Schoorman, An integrative model of organizational trust, The Academy of Management Review 20 (3) (1995) 709–734.

[15] G. Stoneburner, A. Goguen, A. Feringa, Risk management guide for information technology systems, Tech. Rep. SP 800-30, NIST (July 2002).

[16] M. L. Crossley, The desk reference of statistical quality methods, Amer Society for Quality, 2007.

[17] K. J. Biba, Integrity considerations for secure computer systems, Tech. Rep. MTR-3153, The Mitre Corporation (Apr 1977).

Appendix A. Proof of Propositions

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

Proof: From equation 1, we have:

$$\begin{aligned} T_v(s,o) &= l_s \left[1 + H^+(s,o)\right] \\ &= l_s \left[1 + w_0 \text{LRH}(s,o) + \sum_{k=1}^{m} w_k \text{ERH}(s,o)_k\right] \\ &= l_s \left[1 + w_0 \left(\frac{R}{R+P}\right) \alpha^{\frac{1}{R+1}} + \sum_{k=1}^{m} w_k \left(\frac{R_k}{R_k+P_k}\right) \alpha^{\frac{1}{R_k+1}}\right]. \end{aligned} \tag{A.1}$$

In the worst case, when a subject s does not have any reward points, then s will get minimum trust value. Since there are no reward points, the values of R and R_k become 0 in equation A.1. Therefore, we get:

$$= l_s \left[1 + w_0 \left(\frac{0}{0+P}\right) \alpha^{\frac{1}{0+1}} + \sum_{k=1}^{m} w_k \left(\frac{0}{0+P_k}\right) \alpha^{\frac{1}{0+1}}\right].$$

So, the minimum trust value $T_v^{min}(s,o)$ a subject s can get is:

$$T_v^{min}(s,o) = l_s\,[1+0] = l_s. \tag{A.2}$$

In the best case, when the subject s does not have penalty points then the subject will get a maximum trust value. In this case, the values of P and P_k become 0 in equation A.1. Therefore, we get:

$$= l_s \left[1 + w_0 \left(\frac{R}{R+0}\right) \alpha^{\frac{1}{R+1}} + \sum_{k=1}^{m} w_k \left(\frac{R_k}{R_k+0}\right) \alpha^{\frac{1}{R_k+1}}\right]$$
$$= l_s \left[1 + w_0 \alpha^{\frac{1}{R+1}} + \sum_{k=1}^{m} w_k \alpha^{\frac{1}{R_k+1}}\right].$$

Since we know that $\lim_{R\to\infty}\left(\frac{1}{R+1}\right) = 0$, then $\alpha^0 = 1$. Therefore, we get:

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

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

$$T_v^{max}(s,o) = l_s \times [1+1] = 2 \times l_s. \tag{A.3}$$

■

A.2. ***Proposition 2:*** The default trust value $T_v^{def}(s,o)$ is l_s.

Proof: In order to obtain default trust value $T_v^{def}(s,o)$ (when the subject s has neither reward nor penalty points) we need to replace the value of $H^+(s,o)$ with zero in equation 1. Therefore, we get:

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

■

A.3. ***Proposition 3:*** The range of risk value is always between $[l_o, 2 \times l_o]$.

Proof: From equation 5, we have:

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

This can also be written as:

$$= l_o \left[1 + w_0 \mathrm{LPH}(s,o) + \sum_{k=1}^{m} w_k \mathrm{EPH}(s,o)_k\right]$$
$$= l_o \left[1 + w_0 \left(\frac{P}{R+P}\right) \alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k \left(\frac{P_k}{R_k+P_k}\right) \alpha^{\frac{1}{P_k+1}}\right]. \tag{A.4}$$

In the best case, when a subject s does not have any penalty point for an object o, then the minimum risk value will be associated with o. Since there are no penalty points, the value of P and P_k become 0 in equation A.4. Therefore, we get:

$$= l_o \times \left[1 + w_0 \left(\frac{0}{R+0}\right) \alpha^{\frac{1}{0+1}} + \sum_{k=1}^{m} w_k \left(\frac{0}{R_k+0}\right) \alpha^{\frac{1}{0+1}}\right].$$

So, the minimum risk value $R_v^{min}(s,o)$ for an object o will be:

$$R_v^{min}(s,o) = l_o \times [1+0] = l_o. \tag{A.5}$$

In the worst case, when a subject s does not have any reward points for an object o then the maximum risk value will be associated with an object o. Since there are no reward points, the value of R and R_k become 0 in equation A.4. Therefore, we get:

$$= l_o \times \left[1 + w_0 \left(\frac{P}{0+P}\right) \alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k \left(\frac{P_k}{0+P_k}\right) \alpha^{\frac{1}{P_k+1}}\right]$$
$$= l_o \times \left[1 + w_0 \alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k \alpha^{\frac{1}{P_k+1}}\right].$$

Since we know that $\lim_{P\to\infty}\left(\frac{1}{P+1}\right) = 0$, then $\alpha^0 = 1$. Therefore, we get:

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

Since as we mentioned earlier, the sum of all weight values ($w_0 + \sum_{k=1}^{m} w_k$) is 1, the maximum risk value $R_v^{max}(s,o)$ that can be associated with an object o is:

$$R_v^{max}(s,o) = l_o \times [1+1] = 2 \times l_o. \tag{A.6}$$

■

A.4. ***Proposition 4:*** The default risk value $R_v^{def}(s,o)$ is l_o.

Proof: In order to obtain the default risk value $R_v^{def}(s,o)$ (when the subject s has neither reward nor penalty points) we need to replace the value of $H^-(s,o)$ with zero in equation 5. Therefore, we get:

$$R_v^{def}(s,o) = l_o \times [1+0] = l_o.$$

■

A.5. ***Proposition 5:*** In the EWMA approach, the range of trust values is always between $[l_s\,(1+\lambda(X_t))\,,\ l_s\,(2+\lambda(X_t-1))]$.

Proof: From equation 12, we have:

$$T_v(s,o) = l_s\left[1 + H_t^+(s,o)\right]$$
$$= l_s\left[1 + \left\{\lambda(X_t) + (1-\lambda)\left(w_0 \text{LRH}(s,o) + \sum_{k=1}^{m} w_k \text{ERH}(s,o)_k\right)\right\}\right]$$
$$T_v(s,o) = l_s\left[1 + \left\{\lambda(X_t) + (1-\lambda)\left(w_0 \left(\frac{R}{R+P}\right) \alpha^{\frac{1}{R+1}} + \sum_{k=1}^{m} w_k \left(\frac{R_k}{R_k+P_k}\right) \alpha^{\frac{1}{R_k+1}}\right)\right\}\right]. \tag{A.7}$$

In the worst case, when the subject s does not have any reward points, then s will get minimum trust value. Since there are no reward points, the values of R and R_k become 0 in equation A.7. Therefore, we get:

$$T_v(s,o) = l_s\left[1 + \left\{\lambda(X_t) + (1-\lambda)\left(w_0 \left(\frac{0}{0+P}\right) \alpha^{\frac{1}{0+1}} + \sum_{k=1}^{m} w_k \left(\frac{0}{0+P_k}\right) \alpha^{\frac{1}{0+1}}\right)\right\}\right]$$

So, in the EWMA method, the minimum trust value $T_v^{min}(s,o)$ a subject s can get is:

$$T_v^{min}(s,o) = l_s\left[1+\lambda(X_t)\right] \tag{A.8}$$

In this case, X_t represents the most-recent penalty point(s). As we mentioned in Section 4, when we calculate a trust value in a situation where penalties were assigned in the most-recent transaction, a negative sign will be added to the number of penalties received in this transaction.

In the best case, when the subject s does not have penalty points then the subject will get a maximum trust value. In this case, the values of P and P_k become 0 in equation A.7. Therefore, we get:

$$\begin{aligned} T_v(s,o) &= l_s\left[1+\left\{\lambda(X_t)+(1-\lambda)\Big(w_0\left(\frac{R}{R+0}\right)\alpha^{\frac{1}{R+1}}+\sum_{k=1}^{m}w_k\left(\frac{R_k}{R_k+0}\right)\alpha^{\frac{1}{R_k+1}}\Big)\right\}\right] \\ &= l_s\left[1+\left\{\lambda(X_t)+(1-\lambda)\left(w_0\alpha^{\frac{1}{R+1}}+\sum_{k=1}^{m}w_k\alpha^{\frac{1}{R_k+1}}\right)\right\}\right]. \end{aligned}$$

Since we know that $\lim_{R\to\infty}\left(\frac{1}{R+1}\right)=0$, then $\alpha^0=1$. Therefore, we get:

$$T_v(s,o) = l_s\left[1+\lambda(X_t)+(1-\lambda)\left(w_0+\sum_{k=1}^{m}w_k\right)\right].$$

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

$$\begin{aligned} T_v^{max}(s,o) &= l_s\left[1+\lambda(X_t)+(1-\lambda)\right] \\ T_v^{max}(s,o) &= l_s\times\left[2+\lambda(X_t-1)\right]. \end{aligned}$$

■

A.6. ***Proposition 6:*** In the EWMA approach, the range of risk values is always between $[l_o\left(1+\lambda(X_t)\right),$ $l_o\left(2+\lambda(X_t-1)\right)]$.

Proof: From equation 14, we have:

$$\begin{aligned} R_v(s,o) &= l_o\left[1+H_t^-(s,o)\right] \\ &= l_o\left[1+\left\{\lambda(X_t)+(1-\lambda)\Big(w_0\text{LPH}(s,o)+\sum_{k=1}^{m}w_k\text{EPH}(s,o)_k\Big)\right\}\right] \\ R_v(s,o) &= l_o\left[1+\left\{\lambda(X_t)+(1-\lambda)\Big(w_0\left(\frac{P}{R+P}\right)\alpha^{\frac{1}{P+1}}+\sum_{k=1}^{m}w_k\left(\frac{P_k}{R_k+P_k}\right)\alpha^{\frac{1}{P_k+1}}\Big)\right\}\right]. \end{aligned} \tag{A.9}$$

In the best case, when a subject s only received rewards for an object o, then the minimum risk value will be associated with o. Since there are no penalty points, the values of P and P_k become 0 in equation A.9. Therefore, we get:

$$R_v(s,o) = l_o\left[1+\left\{\lambda(X_t)+(1-\lambda)\Big(w_0\left(\frac{0}{R+0}\right)\alpha^{\frac{1}{P+1}}+\sum_{k=1}^{m}w_k\left(\frac{0}{R_k+0}\right)\alpha^{\frac{1}{P+1}}\Big)\right\}\right]$$

So, in the EWMA method, the minimum risk value $R_v^{min}(s,o)$ that an object o can get is:

$$R_v^{min}(s,o) = l_o\left[1+\lambda(X_t)\right] \tag{A.10}$$

In this case, X_t represents the most-recent rewards point(s). As we mentioned in Section 4, when we calculate a risk value in a situation where rewards were assigned in the most-recent transaction, then a negative sign is added with the

number of rewards received in this transaction. In this way, the risk value will decrease with the increase in reward points.

In the worst case, when a subject s only received penalties for an object o then the maximum risk value will be associated with o. Since there are no reward points, the value of R and R_k become 0 in equation A.9. Therefore, we get:

$$R_v(s,o) = l_o\left[1 + \left\{\lambda(X_t) + (1-\lambda)\Big(w_0\left(\frac{P}{0+P}\right)\alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k\left(\frac{P_k}{0+P_k}\right)\alpha^{\frac{1}{P_k+1}}\Big)\right\}\right]$$
$$= l_o\left[1 + \left\{\lambda(X_t) + (1-\lambda)\left(w_0\alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k\alpha^{\frac{1}{P_k+1}}\right)\right\}\right].$$

Since we know that $\lim_{P\to\infty}\left(\frac{1}{P+1}\right) = 0$, then $\alpha^0 = 1$. Therefore, we get:

$$R_v(s,o) = l_o\left[1 + \lambda(X_t) + (1-\lambda)\left(w_0 + \sum_{k=1}^{m} w_k\right)\right].$$

Since as we mentioned earlier, the sum of all weight values ($w_0 + \sum_{k=1}^{m} w_k$) is 1, the maximum trust value $R_v^{max}(s,o)$ that can be associated with an object o is:

$$R_v^{max}(s,o) = l_o\left[1 + \lambda(X_t) + (1-\lambda)\right]$$
$$R_v^{max}(s,o) = l_o \times \left[2 + \lambda(X_t - 1)\right].$$

■

Appendix B. Proofs of Claims

B.1. ***Claim 1:*** *The proposed risk-based decision method does not allow illegitimate accesses if no reward and penalty histories are available.*

Proof: Access is granted if:

$$T_v(s,o) \geq R_v(s,o).$$

From equation 1 and 5, we replace the values of T_v and R_v in the following manner:

$$l_s \times \left[1 + H^+(s,o)\right] \geq l_o \times \left[1 + H^-(s,o)\right].$$

According to the equations 4 and 8, if reward and penalty histories are not available then $H^+(s,o)$ and $H^-(s,o)$ are zero. Therefore, we get:

$$l_s \times 1 \geq l_o \times 1 \Leftrightarrow l_s \geq l_o.$$

Here, note that the subject clearance level should be greater than equal to the object sensitivity level. Therefore, in the absence of reward and penalty points, illegitimate access is not possible.

■

B.2. ***Claim 2:*** *The proposed risk-based decision method does not allow illegitimate access if only penalty history is available.*

Proof: Access is granted if:

$$T_v(s,o) \geq R_v(s,o).$$

This can be written as:

$$l_s \times \left[1 + H^+(s,o)\right] \geq l_o \times \left[1 + H^-(s,o)\right].$$

Since no reward history is available, $H^+(s,o) = 0$, and we get:

$$l_s \geq l_o \times \left[1 + H^-(s,o)\right].$$

With the help of equation 8, the above equation is transformed into the following:

$$l_s \geq l_o \times \left[1 + w_0 \text{LPH}(s,o) + \sum_{k=1}^{m} w_k \text{EPH}(s,o)\right]$$

$$l_s \geq l_o \times \left[1 + w_0 \left(\frac{P}{R+P}\right) \alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k \left(\frac{P_k}{R_k+P_k}\right) \alpha^{\frac{1}{P_k+1}}\right]$$

Since the reward history is not available, the value of R and R_k become 0. So we get:

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

$$l_s \geq l_o \times \left[1 + w_0 \alpha^{\frac{1}{P+1}} + \sum_{k=1}^{m} w_k \alpha^{\frac{1}{P_k+1}}\right].$$

Since we know that $\lim_{P \to \infty} \left(\frac{1}{P+1}\right) = 0$, then $\alpha^0 = 1$. Therefore, we get:

$$l_s \geq l_o \times \left[1 + w_0 + \sum_{k=0}^{m} w_k\right].$$

Since as we mentioned earlier, the sum of all weight values $w_0 + \sum_{k=1}^{m} w_k$ is 1, we get:

$$l_s \geq l_o \times [1 + 1]$$

$$l_s \geq 2 \times l_o.$$

Again, we get $l_s \geq 2 \times l_o$. Hence in the absence of reward points, illegitimate access is not possible.

■

B.3. ***Claim 3:*** *If only reward history is available then the proposed risk-based decision method allows illegitimate access only when* $l_s \geq \frac{l_o}{2}$.

Proof: Access is granted if:

$$T_v(s,o) \geq R_v(s,o).$$

This can be written as:

$$l_s \times \left[1 + H^+(s,o)\right] \geq l_o \times \left[1 + H^-(s,o)\right].$$

Since no penalty history is available, so $H^-(s,o) = 0$ and we get:

$$l_s \times \left[1 + H^+(s,o)\right] \geq l_o.$$

With the help of equation 4, the above equation is transformed into the following:

$$l_s \times \left[1 + w_0 \text{LRH}(s,o) + \sum_{k=1}^{m} w_k \text{ERH}(s,o)\right] \geq l_o$$

$$l_s \times \left[1 + w_0 \left(\frac{R}{R+P}\right) \alpha^{\frac{1}{R+1}} + \sum_{k=1}^{m} w_k \left(\frac{R_k}{R_k+P_k}\right) \alpha^{\frac{1}{R_k+1}}\right] \geq l_o.$$

Since the penalty history is not available, P and P_k are 0. So, we get:

$$\begin{aligned} l_s \times \left[1 + w_0 \left(\frac{R}{R+0}\right) \alpha^{\frac{1}{R+1}} + \sum_{k=1}^{m} w_k \left(\frac{R_k}{R_k+0}\right) \alpha^{\frac{1}{R_k+1}}\right] &\geq l_o \\ = l_s \times \left[1 + w_0 \alpha^{\frac{1}{R+1}} + \sum_{k=1}^{m} w_k \alpha^{\frac{1}{R_k+1}}\right] &\geq l_o. \end{aligned}$$

Since we know that $\lim_{R \to \infty} \left(\frac{1}{R+1}\right) = 0$, then $\alpha^0 = 1$. Therefore, we get:

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

Since as we mentioned earlier, the sum of all weight values ($w_0 + \sum_{k=1}^{m} w_k$) is 1, we get:

$$= l_s \times [1 + 1] \geq l_o$$

$$= l_s \geq \frac{l_o}{2}.$$

This implies that, in the presence of only reward history, the system will allow access to the resource if $l_s \geq \frac{l_o}{2}$.

■

B.4. ***Claim 4:*** *If both reward and penalty histories are available then the proposed risk-based decision method allows illegitimate accesses only when*

$$l_s \geq l_o \left(\frac{H^-(s,o)}{H^+(s,o)}\right).$$

Proof: This proof is straightforward. According to definition 1, an illegitimate access is only possible when $l_s < l_o$ and s is permitted to access object o. In our proposed method, this is only possible when $T_v(s,o) \geq R_v(s,o)$. This can also be written as:

$$\begin{aligned} l_s \times \left[1 + H^+(s,o)\right] &\geq l_o \times \left[1 + H^-(s,o)\right] \\ = \frac{1 + H^+(s,o)}{1 + H^-(s,o)} &\geq \frac{l_o}{l_s} \\ \approx \frac{H^+(s,o)}{H^-(s,o)} \geq \frac{l_o}{l_s} = l_s &\geq l_o \left(\frac{H^-(s,o)}{H^+(s,o)}\right). \end{aligned}$$

■