A Novel Role-Based-Access-Control(RBAC) Framework and Application

Yanjie Zhou[1,a], Min Wen[2,a]

[1]College of Mathematical and Computer Science Jiangxi Science & Technology Normal University
Nanchang, China 330031

[2] Department of Civil and Architectural Engineering Nanchang Institute of Technology
Nanchang, China 330099

[a] zhouyanjie1111@126.com

Keywords: RBAC; Access Control; Internet Security; Novel Framework and Application

Abstract. In recent time, RBAC has gained and kept a dominant stage of AC(access control) in the research area and industry, respectively. Over the time, needs for risk awareness in AC has paid special attention. Even though, role based access control conquers risk via inner features, a quantified method of risk awareness has been proposed as a leading and fascinating research topic due to its inherent flexibility. In this approach, risk-cost metrics are calculated for different entities involved in AC such as users and related objects and a risk threshold restricts the permissions which could be exercised. The quantified methodology arranges dynamism in access decisions procedure based on contexts-situations such as an worker accessing sensitive files through a work computer versus accessing using her own device. In this paper, we compare the difference between the traditional risk mitigation and the recent quantified risk-aware approaches in RBAC and propose a framework for introducing risk-awareness in RBAC models that incorporates quantified-risk. We also provide a formal specification of an adaptive risk-aware RBAC model by enhancing the NIST core RBAC model.

Introduction

The concept of constraints-based risk mitigation has been well-studied in role based access control (RBAC) models. For instance, separation of duty and role cardinality constraints of RBAC are all concerned about risk mitigation. Generally, constraints are static in nature as they are predefined policies that always give the same outcome regardless of the situation. Such a static risk mitigation approach fails to adapt to varied and changing circumstances under which access decisions are made in modern systems. We call the constraints-based risk mitigation approach as “traditional” risk-awareness approach.

Recently, a quantified approach to risk-awareness in access control has drawn much attention as the need for agile and dynamic access control has emerged. Several works have been published in this arena [1]–[3], mainly attempting to assess and utilize risk metrics in different access control systems. A quantified risk-aware access control system differs from the traditional ones in that it permits/denies access requests dynamically based on estimated risk instead of the predefined ones which always give the same outcome. In quantified risk-aware access control, risk is represented as a metric where, for example, the higher its value associated with a user, the higher the chances that the user will perform inappropriate actions. (Consequently, an access request involving a user or a resource with a higher risk-value poses more security threat/risk to the system than a request by a user or for a resource with a lower risk value.) Although a number of works have investigated quantified risk in RBAC [4].

In this paper, we propose a framework for risk-aware RBAC models. We identify the components of RBAC that can be made risk-aware and hence require changes in how they behave and interact with other components. We also analyze the basic distinction between traditional and quantified approach of risk-awareness in RBAC. We identify two types of quantified risk, i.e. non-adaptive and adaptive, and analyze the necessary functionalities for utilizing them in an RBAC system. Finally, we formalize the adaptive risk-aware RBAC by enhancing the NIST Core RBAC model.

Methodology of Our Proposed approach

Risk-Aware RBAC Components. The Fig.1 shows the model of our proposed method, it could be divided as the following parts(with detailed discussion). URA: In RBAC, a role is a collection of permissions and a user is assigned one or more roles so they can perform particular tasks. PRA: In RBAC, permissions are assigned to roles and roles to users. A combination of permissions can be very powerful, consequently, might pose a significant risk to the system. Session: In RBAC, users need to create a session and activate one or more of their assigned roles to exercise certain privileges. Hence, the access capability of a user at a particular time is determined by the activated roles in their sessions. Note that an organization might develop a particular risk-aware approach to one or more of these components based on their requirements.

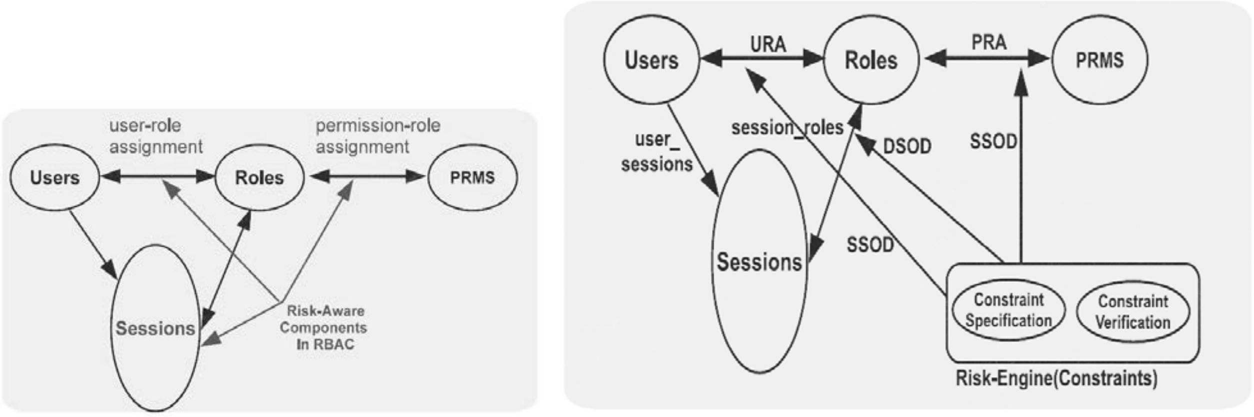

Fig. 1 Our Proposed model component

Types of Risk-Awareness in RBAC. As discussed earlier, in RBAC, risk-awareness can be categorized into two types. One is the traditional approach in which risk is basically mitigated by specifying and enforcing constraints on the above identified risk-aware components. The other is a quantified approach where the value of risk of a certain risk-aware component is estimated that dynamically restricts certain activities. In the following, we discuss both types of risk-awareness and also analyze their basic differences. (1) Traditional Risk-Awareness: Traditionally risk-awareness in access control systems are constraints driven. Fig 2 shows the components of the traditional risk-aware RBAC. Here, the functionality of the Risk-Engine is to specify and enforce constraints. Basically, the constraints are specified for each risk-aware component of the RBAC model, i.e. URA, PRA and sessions, and enforced. The purpose of the risk-engine is to specify and enforce the constraints to exercise certain policies dealing with risk, e.g. static separation of duty (SSOD), dynamic separation of duty (DSOD), etc. SSOD policies are specified for restricting certain conflicting roles to be assigned to a user, while the DSOD policies are specified for restricting certain roles to be simultaneously activated in one or more sessions of a user. (2) Quantified Risk-Awareness: In the quantified approach, risk is represented as a metric where, for example, a higher value is more risky than the lower one. An estimated risk value helps the system to dynamically make decisions for the operations of the risk-aware components of RBAC. Previous work shows the components of the risk-aware RBAC sessions. As shown, for each user session ‘risk-threshold’ is estimated. Each permission is assigned a risk value, consequently, risk of a role is determined by combining its assigned permission risks. The session ‘risk-threshold’ and the risk of the roles are then compared to make decisions on role activation/deactivation within a session. Several approaches [4] have been published in literature for calculating risk of roles and permissions. Similarly, the value of session ‘risk-threshold’ can be calculated and previous work shows examples of risk-factors that might influence the estimated value. (3) Adaptive Approach: the Fig.3 shows the approach.

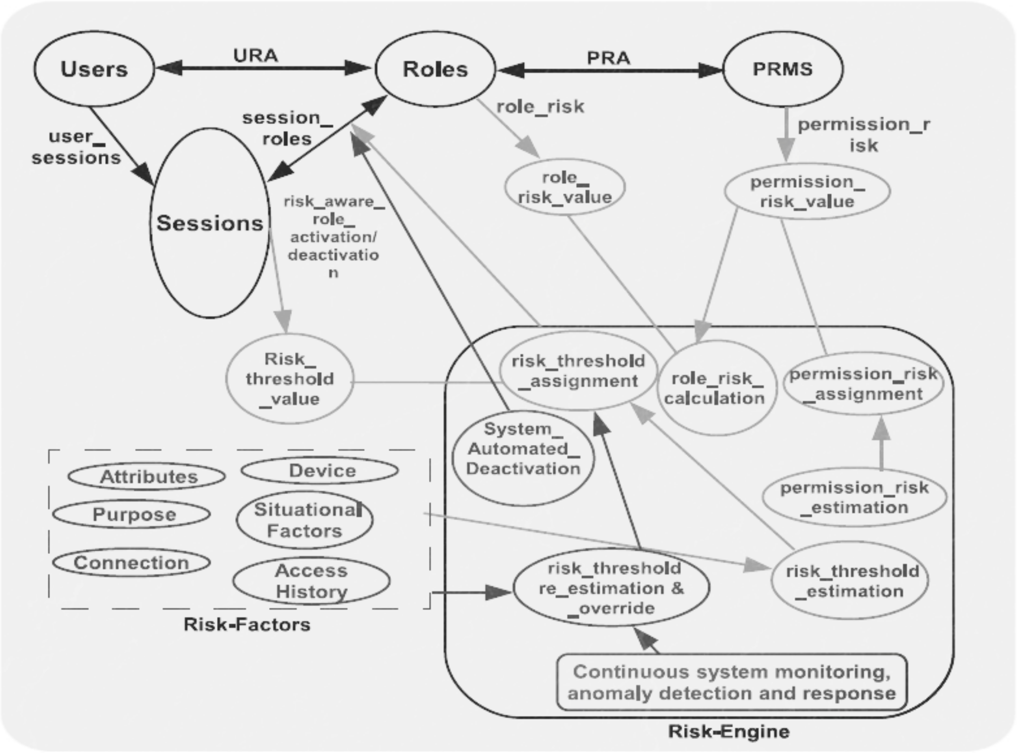

Fig. 3 Adaptive Quantified Risk-Aware RBAC

Formal Analysis of the Framework

AssignRisk: This administrative function assigns a risk value to a permission.

```
function $AssignRisk(ops, obj : NAME, risk : \mathbb{R}_{\geq 0})$
    if $ops \in OPS$ and $obj \in OBJ$ then
        $assigned\_risk'(ops, obj) \leftarrow risk$
    end if
end function
```

RoleRisk: This function returns estimated risk of a role. It takes role as an input and returns the sum of its assigned permissions' risk.

```
function $RoleRisk(role : NAME, result : \mathbb{R}_{\geq 0})$
    /*The value of $result$ is initially 0*/
    if $role \in ROLES$ then
        for all $ops \in OPS$ and $obj \in OBJ$ do
            if $((ops, obj) \mapsto role) \in PA$ then
                $result' \leftarrow result + assigned\_risk(ops, obj)$
            end if
        end for
    end if
end function
```

CreateSession: A user creates a session using this function. Initially the session does not contain any role. It utilizes an Eval RT function to calculate the risk threshold based on the user involved and system context. The functionality of Eval RT should be application specific, thus, we do not specify the details of this function. The session risk contains the sum of activated roles' risk in the session which is initially 0.

```
function $CreateSession(user : NAME, session : NAME)$
    if $user \in USERS$ and $session \notin SESSIONS$ then
        $SESSIONS' \leftarrow SESSIONS \cup \{session\}$
        $user\_sessions'(user) \leftarrow user\_sessions(user)$
                                   $\cup \{session\}$
        $risk\_threshold'(session) \leftarrow$ Eval_RT(session,user)
        $session\_risk'(session) \leftarrow 0$
    end if
end function
```

Related Work and Conclusion

Several approaches have been proposed for combining risk issues in different access control systems. Kandala et al [5] provide a framework that identifies different risk components for a dynamic access control environment. The Jason report proposes three core principles for a risk-aware access control system: measuring risk, identifying tolerance levels of risk and controlling information sharing. Cheng et al give a model to quantify risk for access control and provide an example for multilevel information sharing. Ni et al propose a model for estimating risk and induce fuzziness in the access control decision of the Bell-Lapadula model. Moloy et al propose a risk-benefit approach for avoiding communication overhead in distributed access control. All of these models mostly focus on how to estimate risk. In contrast, our work focusses on how to utilize such risk measures in different risk-aware RBAC components. Recently, a quantified risk-aware RBACsessions and role activation/deactivation framework have been proposed in [3]. There are also other approaches to achieve automated threat response in dynamically changing environments.

In this paper, we developed a framework for risk-aware role based access control (RBAC) models. There are two basic requirements for developing a risk-aware RBAC model: 1. Identify components which can be risk-aware and thereby utilize risk metrics for various purposes and 2. Select a particular risk-aware approach and its necessary functionalities. We identify that in RBAC sessions, user-role assignment and permission-role assignment processes are the main risk-aware components. We also showed that risk-awareness can be of two types: traditional and quantified approaches. The former is the conventional constraint driven approach, while the latter is a risk metric driven approach. Furthermore, the quantified approach are of two types: nonadaptive and adaptive and develop necessary functionalities for them. Finally, we formalized the functionalities of adaptive risk-aware RBAC sessions by extending NIST standard RBAC. In the future, we plan to investigate introducing quantified risk-awareness in more general models such as attribute-based access control and conduct some mathematical work using the [6,7] method.

References

[1] Gail-Joon Ahn and Ravi Sandhu. Role-based authorization constraints specification. ACM Trans. Inf. Syst. Secur., 3(4):207–226, November 2000.

[2] Richard T Simon and Mary Ellen Zurko. Separation of duty in rolebased environments. In CSFW, pages 183–194. IEEE, 1997.

[3] Khalid Zaman Bijon, Tahmina Ahmed, Ravi Sandhu, and Ram Krishnan. A lattice interpretation of group-centric collaboration with expedient insiders. In Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on, pages 200–209. IEEE, 2012

[4] Dechmi, F., Playán, E., Cavero, J., Martínez-Cob, A., Faci, J.M., 2004. A coupled crop and

solid-set sprinkler simulation model: I. Model development. J. Irrig. Drain. E-ASCE.

[5] Ravi S. Sandhu. Lattice-based access control models. IEEE Computer, 26(11), 1993.

[6] Xu B, Wang X H, Wei W, et al. On reverse Hilbert-type inequalities[J]. Journal of Inequalities and Applications, 2014, 2014(1): 198.

[7] Khalid Zaman Bijon, Ram Krishnan, and Ravi Sandhu. Risk-aware RBAC sessions. In Information Systems Security, pages 59–74. Springer, 2012.