An Enhanced Access Control Model Based on Trusted Computing

Kuanmin Hu[1, a], Guoyang Cai[2, b], Chengsheng Shen[3, c]

[1, 2, 3]Guangdong Key Laboratory of Information Security Technology,

Sun Yat-sen University

[a, b, c]email: isscgy@mail.sysu.edu.cn

Keywords: Access Control; Trusted Computing; TPM; Operating System Security

Abstract. With the increasingly strict requirement for computer system security, access control models have become more complex. Existing models, such as discretionary access control (DAC) model, mandatory access control (MAC) model, role based access control (RBAC) model, and attribute based access control (ABAC) model, all have advantages and disadvantages regarding practicability and security. In addition, there is an inherent security risk in these access control models. The models merely control the access permission, but ignore the verification for the identity credibility of the entities involved in the access.

With the proposal of trusted computing and the application of trusted platform, it is possible to implement, on stand-alone computers, the verification of identity credibility for the entities involved in the access. In this paper, we analyze the authorization and access decision policy of the RBAC model and the ABAC model. The characteristics of the trusted computing, which can ensure the identity credibility of the entities involved in the access, is also considered. Based on the above analysis, we establish a trusted computing based enhanced access control (TCBEAC) model, which can be deployed on stand-alone computers for common users.

Introduction

The access control, as a vital point in the research of security, is mainly utilized to monitor and manage the entity behavior in the system based on the authorization and security policy to prevent the leakage and alteration of information [1]. In recent years we have seen frequent incidents that threaten the information security of enterprises and individuals. One of the important reasons is that system shows weak self-protection awareness when it is invaded by vicious procedures or users, failing to judge the validity of access behavior correctly. If the system can restrict the boundary of accessible resources based on access behavior [2], the private information in the system can be protected securely and effectively. From this perspective, the function of access control is to improve the system's resistance under attacks.

Existing research on access control model mainly focuses on the combination and extension of role based access control (RBAC) [3] and the attribute based access control (ABAC) [4]. The former is not flexible in permission control, while the latter is difficult to be configured which hinders extensive application. In this paper, a trusted computing based enhanced access control (TCBEAC) model is built by taking advantage of the authorization policy of RBAC and the permission control at attribute level of ABAC. Therefore, the established model presents the strengths of both RBAC and ABAC. Additionally, by utilizing the trusted computing function (mainly including the signature verification, abstract computing, etc.) of the USB-Key based trusted platform module (uTPM), the model ensures the credibility of the entities involved in the access control model.

The rest of the paper is organized as follows. Section 2 introduces the relevant access control models and trusted computing. Section 3 presents the TCBEAC model. The function of the uTPM in the TCBEAC model is explained in Section 4. Section 5 discusses the future work concerning the TCBEAC model and Section 6 concludes the paper.

Related Work

Access Control Model. TCBEAC model is proposed on the basis of the authorization policy of the RBAC model and the attribute concept of the ABAC model. RBAC model, as one of the most widely used models, was first proposed by Sandhu [3]. With the extensive application of this model, the disadvantages of the RBAC model emerge successively, as concluded below:

1. The sharp increase of roles
2. The inflexible permission control
3. The model is not fine-grained enough that the role cannot precisely identify an entity

ABAC model possesses favorable flexibility and dynamic decision-making ability, however, it cannot be widely utilized due to the complex policy design. In addition, some of the certificate authorities are un-trusted.

Numerous research progress have been made in the analysis and extension of RBAC and ABAC. For example, Xin Jin et al. [5] put forth the role-centric attribute-based access control (RABAC) model, in which the maximum permission is determined by a specific group of users. In this way, the issue of sharp increasing roles is resolved. To realize the reasonable assignment of the attributes in the ABAC model, Khalid Zaman Bijon et al. [6] propose an attributed-based constraints specification language (ABCL) and have proved that the language can be widely applied. To combine the advantages of RBAC and ABAC, D. Richard Kuhn et al. published Adding Attributes to Role-Based Access Control [7].

However, the above models and their extension cannot meet users' demands for security and easy use simultaneously. Therefore, by utilizing the authorization policy of the RBAC model and the attribute concept of the ABAC model, the TCBEAC model is constructed based on the trusted computing provided by the uTPM. The model is more secure and shows higher efficiency in attribute assignment.

Trusted Computing and TPM. The key to trusted computing is the concept of 'trusted'. According to the trusted computing group (TCG), trusted refers to an entity achieving the expected objective with the expected approach [8]. The trusted computing, as a hardware based security technology, enhances the security of the system by embedding trusted platform module (TPM), which provides nonvolatile storage and cryptographic algorithm on the mainboard [9, 10]. Similar to that of the third party in the asymmetric secret key system, TPM is able to signature and verify the certificates utilizing its cryptographic algorithm and integrity verification function. Trusted computing provides a feasible scheme for solving the absence of credibility verification for identities of the entities by utilizing hardware

uTPM. To apply trusted computing on stand-alone computers, the TCG have formulated a set of specification for TPM [11]. As the trust foundation of the trusted platform, TPM is designed to achieve the following goals:

1. TPM has to be secure, which is the base for proving the authenticity of the user identities and the foundation of TPM operation.
2. TPM needs to include all the functions required for establishing trusted platform and remote attestation, which are the core of the TPM.

However, the traditional TPM has a hidden danger of single sign-on failure, which is likely to cause the loss of secret key and result in an unstable system. The modifications of the mainboard due to system redesign may also affect the availability of TPM. To solve the above problems, uTPM is introduced. uTPM is a portable TPM based on USB KEY. It is issued by trusted institutions and connected with computers via USB. Each user can prove its identity using uTPM, and measure and report the state of the platform using the interface provided by the uTPM.

Design of the TCBEAC Model

Design Objectives. The access control model is applied on stand-alone computers. Stand-alone computers have been increasingly sophisticated nowadays, yet traditional access control models fail to meet users' demand for the security and the practicability of access control on stand-alone

computers.

Under such circumstances, we suggest that the access control model for stand-alone computers should meet the following objectives:

1. The entities involved need to be identified through the issued attribute certificate, so as to realize the access control at the level of attributes.
2. The attribute certificates of entities are signed using uTPM. In this way, the system can verify the credibility of the identities of the entities by verifying the integrity of the certificates.
3. With the application of the authorization policy of the RBAC model, the system guarantees the integrity and the easy configuration of the access control policy.
4. The users and the attributes should be graded, based on which invalid authorization is prevented. In addition, a flexible permission control scheme needs to be introduced in the system.

The framework of the TCBEAC model is illustrated in Fig.1.

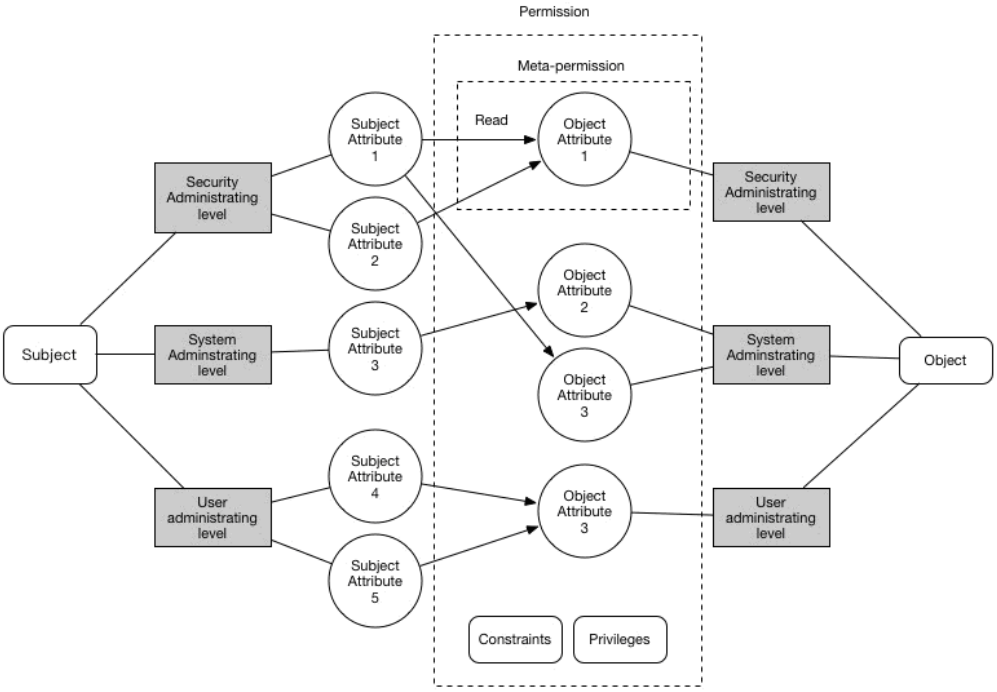


Fig.1 The framework of the TCBEAC model

The definitions of related concepts are as follows:

Trusted entity. The entity is the participant of access control and can be divided into two types, namely subject and object, according to the initiative in the access. An attribute certificate is issued to each entity in the TCBEAC model to identify the real identity of the entities. The relationship between the certificates and the entities is shown in Fig.2.

Attribute of the trusted entity. To simplify the authorization model of the access control, the users of the operation system are classified into following three grades:

1. Security administrators
2. System administrators
3. Non-privileged users

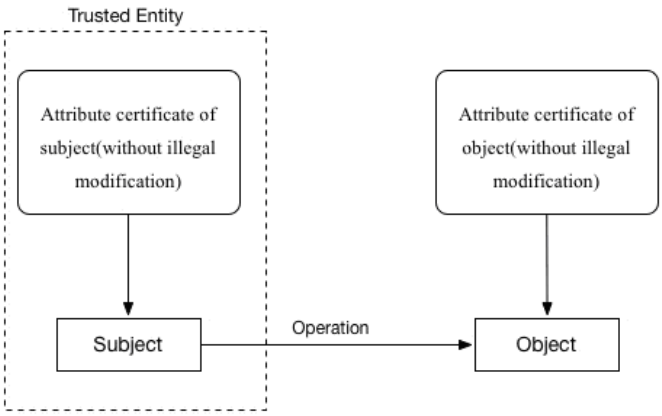


Fig.2 The trusted entities and the attribute certificates

The attribute of trusted entity is represented by an attribute set TA, in which the element ta refers to a quadruple (attrkey, attrtype, attrrange, attrrank). The definitions of the elements of the quadruple are

1. The attrkey is the key name and the only identifier of the attribute.
2. The attrtype represents the type of the value of the attribute and can be classified into atomic (single value) and set (set value).
3. The attrrange refers to the range of the value of the attribute.
4. The attrrank represents the administrating level of the attribute. According to the administration grade of the users, it is divided into the security administrating level, the system administrating level, and the non-privileged administrating level.

Attribute expression of trusted entity. The set of trusted entities' attribute expressions (TAE) contains all the attributes of an entity. Each element tae in the expression refers to that the concrete value of the attribute of an entity is constituted of a triple (attrkey, rop, attrvalue), in which the elements are defined as:

1. The attrkey is the key name of the attribute.
2. The rop is the relational operation symbol and
   rop $\in$ { $<$, $\leq$, $>$, $\geq$, $\neq$, $\in$, $\notin$ } if attrtype == *atomic*
   rop $\in$ { $\subset$, $\subseteq$, =, !=, $\supset$, $\supseteq$} if attrtype == *set*
3. The attrvaule is the concrete value of the attribute.

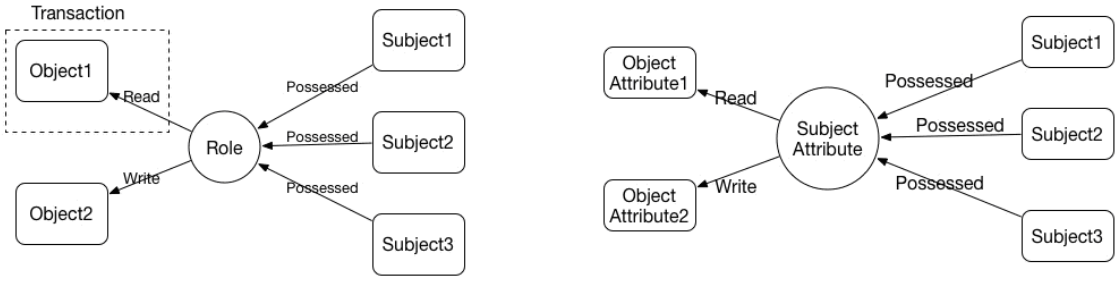
Attribute certificate. The attribute certificate is an important concept in the TCBEAC system. The assignment of the attribute expression of the entity is realized by issuing the attribute certificate to the target entity or modifying the certificate. Each attribute certificate needs to contain:

1. The expressions of the attributes presented by the entity.
2. The signature value obtained by encrypting the abstract value of the certificate using the RSA private key securely stored in the uTPM.

Meta-permission. The TCBEAC model takes advantages of and improves the permission management policy of the RBAC model and the attribute concept of the ABAC model. In the TCBEAC model, the permission of the access control is mapped as:

subject → attribute expression set of subject → meta-permission set of subject

The meta-permission in the model is bound to the attribute expression of an object. Therefore, while deciding the access authorization, the TCBEAC access control system needs to define a meta-permission set of the object meeting the accessible requirement. Only when the set is the subset of the meta-permission set of the subject, the subject is allowed to access the object. The authorization models of the RBAC and the TCBEAC are compared in Fig.3.



(*a*) *authorization models of the RBAC* (*b*) *authorization models of the TCBEAC*

Fig.3 Comparison between the authorization models of the RBAC and the TCBEAC

Permission constraints and privileges. A reasonable access control model needs to control the permission of the subject, so as to avoid the excess of authority. To realize this, the RABAC model is put forward by adding a permission filtering policy (PFP) module in the traditional RBAC model to reduce the permission of the subject according to the filtering policy[5]. However, the method is likely to excessively reduce the permission of the subject. The permission of the subject can be controlled by other methods [6, 12], however, all these methods fail to satisfactorily solve the problems in the permission control.

The TCBEAC model provides simple filtering policies, that is, the permission constraints, to the attribute expression of the object to reduce the permission of the subject. To avoid the excessive reduction of the permission due to the application of the permission constraints, privileges are introduced in the model to ignore certain permission constraints. The specific syntax of the permission constraints and the privileges are

< *permission constraints* > ::= *deny* < *tsae* > < *operation* > *on* < *toae* >

< *privileges* > ::= *ignore* < *key name of object attribute* > *constraints if* < *tsae* >

tsae: the attribute expression of the subject

toae: the attribute expression of the object

In the TCBEAC model, the permission of the subject is defined as the meta-permission set finally obtained from the union set of the meta-permission set corresponding to all the attribute expressions of the subject under the permission constraints and the privileges in the access control. When a subject accesses an object, the access control system first obtains all the attribute expressions of the subject and the object, and calculates the permission of the subject. In addition, the system acquires the accessible meta-permission set of the object in the actual access. Finally, the model determines the validity of the access by judging whether the accessible meta-permission set is the subset of the permission set of the subject.

Rules of the TCBEAC Model

The attribute management rule of the TCBEAC model. The attribute management rule is to restrict the attribute management ability of the users and the subjects. The following rules are formulated in the TCBEAC model according to the grading and classification of the users and the attributes:

1. The attributes can only be established and defined by the security administrators.
2. The attribute expressions of the subject and the object can only be assigned and managed by the users at the grades no lower than the corresponding attribute administrating level.
3. The assignment and the management of the attributes of the objects constructed by the subjects need to be limited by applying the constraints statement in the attribute expression of the subject. The syntax is defined as

   < *subject authorization constraints to object* > ::= *deny* < *tsae* > *assign* < *toae* >

The rule for authorizing meta-permissions in the TCBEAC model. The authorization of the meta-permission in the TCBEAC model is directly related to the security of the access control. Therefore, the authorization of the meta-permission is stipulated as follows:

1. When users authorize the meta-permission, the grade of the users needs to be equal to or higher than the administrating level of the attributes relating the meta-permission.
2. In the authorization of the meta-permission, the administrating level of the attributes of the object involved needs to be not higher than that of the attributes of the subject.
3. The authorization of the meta-permission has to follow the minimum principle.

The rule for managing the permission constraints and the privileges of the model. Considering the hidden risk of the permission constraints and the privileges in the TCBEAC model, the following management rules are formulated to avoid and reduce the influence:

1. For the attributes of the subjects and the objects involved in the permission constraints and the privileges, the administrating level of the attributes of the objects need to be equal to or lower than that of the subjects.
2. When users set the permission constraints, the grade of the users is expected to be not lower than that of the administrating level of the attributes involved in the permission constraints.
3. The privileges can only be assigned and revoked by the security administrators.

Performance Analysis

The section analyzes and compares the TCBEAC model with the RBAC and the ABAC models in terms of the complexity of permission assignment, the time complexity of the access decision, and the security. In this way, the authors attempt to theoretically verify the superiority of the TCBEAC model.

The complexity of permission assignment. The complexity of permission assignment refers to the number of the rules of the permission or access control when the permissions are designed to cover all the subjects and the objects, or the attributes of the subjects and objects.

For the three models, their complexities of permission assignment are

1. For the TCBEAC model, the complete permission set is defined as TSAE×OP×TOAE, where the TSAE and the TOAE refer to the attribute expression sets of the subjects and the objects respectively, and the OP represents the operation set. According to the definition, it is known that the complexity of permission assignment of the model is O(|TSAE| * |TOAE| * |OP |).
2. The complexity of permission assignment of the RBAC model is O(|ROLE|* |OBJ| * |OP|), where ROLE, OP, and OBJ are the role set, the operation set, and the object set, respectively.
3. Considering the combination of the attribute expressions, the complexity of permission assignment of the ABAC model is $O(2^{|SAE|} * 2^{|OAE|} * |OP|)$. In which, the SAE and the OAE are the attribute expression sets of the subjects and the objects separately, and the OP is the operation set.

The time complexity of the access decision. The time complexity of the access decision refers to that for obtaining the decision result through inquiring and computing the relevant permissions in the access control process.

1. The time complexity of the access decision of the TCBEAC model can be regarded as the judgment process of a subset. The optimal complexity of the subset judgment algorithm is O(nlog(n)), where n represents the number of the elements satisfying the accessible meta-permission set.
2. As the time complexity of the access decision of the RBAC model is basically the process for searching a certain element in the set, its time complexity is O(n), where n is the number of the transactions of the subjects.
3. The time complexity of the access decision of the ABAC model is the time complexity for inquiring the rules of the access control. As the rule inquiry can be optimized through multiple methods in the practice, the exact time complexity of the model cannot be obtained.

Security. The security of the access control models is the comprehensive evaluation for the access control granularity, the authorization in the access control, and the reliability of the decision

process.

The security of the TCBEAC model:

1. The granularity of the model is at attribute level, which is a fine granularity.
2. As the thought similar to that of the RBAC model is employed and modified, the authorization and the decision policy of the model are equal or more reasonable than those of the RBAC model.

The security of the RBAC model:

1. The minimum unit controlled by the model is the role; therefore, the model shows relatively fine granularity.
2. The theoretical and practical verification indicates that the authorization and the decision policy of the model are reliable.

The security of the ABAC model:

1. The model presents fine granularity as the minimum unit controlled is the attribute.
2. The authorization and the decision policy of the model have been proved theoretically. However, the verification is difficult to be conducted in the practice with the frequent occurrence of the incorrect configuration.

In summary, the security of the ABAC model is superior to that of the TCBEAC model, and the RBAC model presents lowest security.

Table 1. Security of TCBEAC, RBAC and ABAC

Model	Complexity of permission assignment	Time complexity of access decision	Security
TCBEAC	$O(\|tsae\|\cdot\|toae\|\cdot\|op\|)$	$O(nlog(n))$, where n represents the number of the elements satisfying the accessible meta-permission set.	High, at the granularity of the attribute
RBAC	$O(\|role\|\cdot\|obj\|\cdot\|op\|)$	$O(n)$, where n is the number of the transactions of the subjects	Relatively low, at the granularity of the role
ABAC	$O(2^{\|sae\|}\cdot 2^{\|oae\|}\cdot\|op\|)$.	Uncertain	High, at the granularity of the attribute

Table 1 shows that the TCBEAC model integrates the security of the ABAC model and the advantages of the RBAC model in the permission assignment. Therefore, its complexity of permission assignment is superior to that of the ABAC model and the security is higher than the RBAC model. The results suggest that the overall performance of the TCBEAC model is superior to that of the ABAC and the RBAC models

The framework of the TCBEAC system

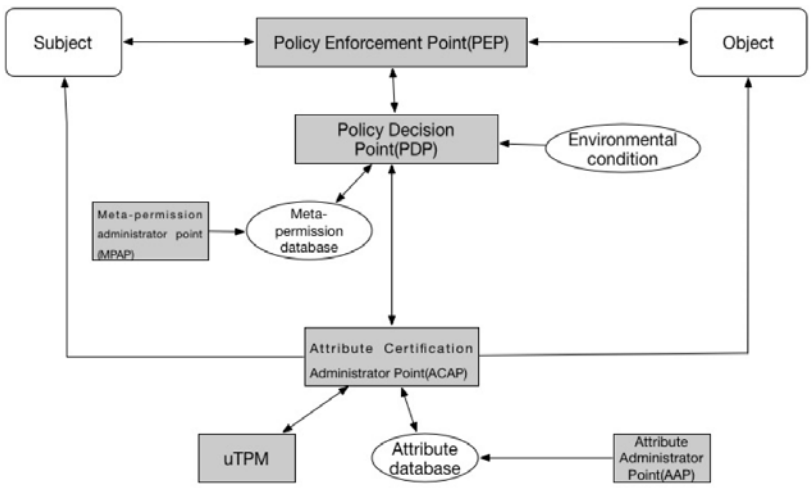


Fig.4 The framework of the TCBEAC system

According to the definition of the TCBEAC model, the framework of the TCBEAC system is shown in Fig.4. Following components are incorporated in the access control module of the model.

1. The attribute administrator point (AAP). It is designed to maintain the attribute database by the security administrator, which adds, deletes, modifies, and inquires the attributes.
2. The attribute certification administrator point (ACAP). The component issues and manages the trusted attribute certificates to the subjects and the objects, and handles the request for validating the certificates.
3. The Meta-permission administrator point (MPAP). Based on the MPAP, the users can maintain the meta-permission database and therefore realize the addition, deletion, modification, and inquiry of the meta-permissions corresponding to the attribute expressions. By extending the function of the MPAP, the functions of permission constraints and privileges can be added.
4. The policy decision point (PDP). It decides whether an access is permitted or not by analyzing the credibility of the subjects and the objects and the validity of the access.
5. The policy enforcement point (PEP). The PEP is mainly responsible for the interception of the access requests sending from the subjects to the objects and executes the decision of the PDP.

Future Work

The TCBEAC, as the first model that integrates the trusted computing, as well as the advantages of the RBAC model and the ABAC model, provides a more secure and efficient scheme for the access control on stand-alone computers. Considering that the access control models have to adapt to more changeable environment, the universality of the model needs to be improved. The following aspects are expected to be investigated in the future:

1. Analyzing the applicability of the classification schemes of the users' grade and the attribute administrating level in different environment.
2. More concretely defining the rules for assigning and administrating the attributes and the meta-permissions.
3. Recording and analyzing the history behavior of the entities to evaluate the risk degree of the entities.
4. Analyzing the environmental factors in the access control.

Conclusions

TCBEAC model is developed by combining the authorization policy of RBAC and the attribute concept of ABAC. The model is less difficult than ABAC in the configuration and more secure than RBAC. By grading the users and the attributes, as well as introducing the permission constraints and the privileges, the model optimizes the permission administration process in the access control model. Moreover, the uTPM based attribute certificate is proposed to solve the credibility validation of the identity of the entities which is absent in the access control. The construction of the TCBEAC model contributes to the extensive application of the access control model on stand-alone computers with the granularity of attributes.

References

[1] R. Shirey. RFC 4949: Internet Security Glossary, Version 2[J]. ITEF, August, 2007

[2] Sandhu R S, Samarati P. Access control: principle and practice[J]. Communications Magazine, IEEE, 1994, 32(9): 40-48.

[3] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.

[4] Wang L, Wijesekera D, Jajodia S. A logic-based framework for attribute based access control[C].

Proceedings of the 2004 ACM workshop on Formal methods in security engineering. ACM, 2004: 45-55.

[5] Jin X, Sandhu R, Krishnan R. RABAC: role-centric attribute-based access control[M]. Computer Network Security. Springer Berlin Heidelberg, 2012: 84-96.

[6] Bijon K Z, Krishman R, Sandhu R. Constraints Specification in Attribute Based Access Control[J]. Science, 2013, 2(3): pp. 131-144.

[7] Kuhn D R, Coyne E J, Weil T R. Adding attributes to role-based access control[J]. IEEE Computer, 2010, 43(6): 79-81.

[8] Trusted Computing Group. TCG Design, Implementation, and Usage Principles (Best Practices), Version 3.0[M]. TCG published. 2009.

[9] Trusted Computing Group. TCG Architecture Overview Version 1.4 [M]. TCG Published. 2009.

[10] Challener D, Yoder K, Catherman R, et al. A practical guide to trusted computing[M]. Pearson Education, 2007.

[11] Trusted Computing Group. TPM Main Specification Part 1 - Design Principles, version 1.2, revision 116 [M]. TCG Published. March, 2011.

[12] Ahn G J, Sandhu R. Role-based authorization constraints specification[J]. ACM Transactions on Information and System Security (TISSEC), 2000, 3(4): 207-226.