Integrating Trust and Role for Secure Interoperation in Multi-Domain Environment

Jianfeng Lu [1], Ruixuan Li [1], Zhengding Lu [1], Bing Li [2]
[1] *Intelligent and Distributed Computing Lab, College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, P. R. China*
[2] *State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072, China*
E-mail: lujianfeng@smail.hust.edu.cn, {rxli, zdlu}@hust.edu.cn, libing@sklse-dns.sklse.org

Abstract

Traditional access control disciplines such as RBAC has difficulty in covering open and decentralized multi-centric systems because it has focused on a closed system where all users are known and primarily utilizes a server-side reference monitor within the system. Trust management has relaxed this known user restriction and allowed authorize for strangers based on their credentials. However, trust management has also been found to be lacking because of certain inherent drawbacks with the notion of credential. In this work, a new access control model T&RBAC is presented in this paper. It integrates RBAC and TM. User can be assigned to local roles, also can be assigned to foreign roles based on his credential and local roles. We proof that there is no security constraints in T&RBAC. To some extends, T&RBAC is only a core model and can be extended for specific requirement.

Keywords: Interoperation, Trust Management, RBAC, Multi-Domain

1. Introduction

Many studies have been done on secure operating system using secure kernel that has various access control policies for system security based on traditional access control disciplines. However, traditional access control disciplines have difficulty in covering open and decentralized multi-centric systems, because traditional access control has focused on controlling access to digital resources within closed system environments and it only deals with previously known user's access which is not adequate in today's open system environments. Trust management has relaxed this known user restriction and allowed controls on strangers' access to digital objects based on their credentials. However, trust management has also been found to be lacking because of certain inherent drawbacks with the notion of credentials. For instance, computing the trust value will exhaust huger computing resource. Additionally, in multi-domain environment, the identities of users are not known in advance. It is very difficult to be familiar with a stranger based on his trust degree because it may be uncertainty, half-baked and incapable for accuracy.

The above observations motivate us to consider how to absorb the advantages of the traditional access controls (e.g. RBAC) and credential based models, and decreasing their shortcomings. Traditional access control has the predominance of focusing on controlling access to digital resources within closed system environments, and credential based models solve the problem of access control in open systems to a great extent. In this way, a novel enhanced RBAC model named T&RBAC is proposed for secure interoperation which integrates the conventional role based access control models with the credential based models. In T&RBAC, a user is mapped to a trust rank based on its credential. For simplicity reasons we assume that the user's attributes are synonymous with local roles and trust rank in the T&RBAC model. In this case, the users will be able to be assigned to foreign roles based on theirs attributes (e.g. trust rank, local role) and can access to digital objects in foreign domains. And we employ two different access control policies for different environments respectively. This policy allows interoperation among multiple domains without any violation of collaborating domain's autonomy.

The rest of the paper is organized as follows. Section 2 gives an overview of related works. Section 3 defines the elements and their relationships. Section 4 discusses how T&RBAC performs access control on different intra-domain and inter-domain environments. The security issues are discussed in Section 5. Finally Section 6 concludes the paper.

2. Related Work

978-0-7695-3126-7/08 $25.00 © 2008 IEEE
DOI 10.1109/ISA.2008.30

Numerous studies have shown that unauthorized access, in particular by insiders, constitutes a major security problem for enterprise application environments [01], highlighting the need for robust access control management systems. This problem can get magnified in a collaborative environment where distributed, heterogeneous, and autonomous organizations interoperate with each other [2].

Nowadays, role based access control (RBAC) has become the predominant approach for advanced access control in large, distributed systems [3]. It offers many attractive features, such as policy neutrality, support for least privilege and efficient access control management [4]. With RBAC, security is managed at a level corresponding to an organization's human resource structure.A series of researches have been taken on the extended RBAC models to solve the secure interoperation issues in the distributed environment. Kapadia et al proposed a secure interoperability using dynamic role translation (IRBAC) implementing access control across domains in the form of role mappings among individual domains [5]. Basit Shafiq et.al [6] extended the IRBAC model by proposing a policy integration framework for merging heterogeneous Role-Based Access Control (RBAC) policies of multiple domains into a global access control policy.

Though these researches included description about the RBAC based interoperation in the multi-domain environments, they focused on controlling access to digital resources with previously known user's access which is not adequate in today's Internet world. In order to overcome the shortcomings of RBAC for open and decentralized multi-centric systems, some literatures have been proposed to use the concept of trust in access control because trust management has relaxed this known user restriction and allowed controls on strangers' access to digital objects based on their credentials. Sandhu et.al presented an architecture with trusted computing technology to enforce access control policies in peer-to-peer environment [7]. N. Li et.al had also integrated RBAC with trust computing only to facilitate security administration [8], [9], [10].

Ours work emphasizes on integrating role based access control model with trust management for secure interoperation in multi-domain environments. T&RBAC absorbs the merits of both the role based access control model and trust management so as to suit for open systems like the multi-domain environment.

3. T&RBAC Model

The T&RBAC model is defined in terms of a set of elements and relations among those elements, and illustrated in Figure 1. We use one-directional arrows with single-headed to denote one-to-many relationships and one-directional arrows with double-headed from the session to LR in Figure1 indicates that multiple roles are simultaneously activated. Two directional arrows with single-headed to denotes many-to-many relationships and two directional arrows with double-headed from the *U* to *LR* in Figure 1 indicates that multiple roles are simultaneously activated. We use plain lines to denote one-to-one relationships.

Definition 1: The T&RBAC model has the following components:

- *U, LR, FR, P, S, T, A, C.* (users, local roles, foreign roles, permissions, sessions, trust rank, attributes and constrains respectively)
- $UA \subseteq U \times R$, a many-to-many role to user assignment relation.
- $PA \subseteq P \times R$, a many-to-many permission to role assignment relation.
- $UTA \subseteq T \times U$, a one-to-many trust rank to user assignment relation.
- $TA \subseteq T \times A$, a many-to-many trust rank to attribute assignment relation.
- $RA \subseteq LR \times A$, a many-to-many local role to attribute assignment relation.
- $AA \subseteq FR \times A$, a many-to-many foreign role to attribute assignment relation.
- $RH \subseteq R \times R$ is a partial order on R called the role hierarchy or role dominance relation, also written as $\geq$.
- user : $S \rightarrow U$, a function mapping each session s_i to the single user user(s_i) (constant for the session's lifetime), and
- roles : $S \rightarrow 2^R$, a function mapping each session s_i to a set of roles
  $roles(s_i) \subseteq \{r | (\exists r' \geq r)[(user(s_i), r') \in UA]\}$
  (which can change with time) and session s_i has the permissions $\bigcup_{r \in roles(s_i)} \{p | \exists r'' \leq r[(p, r'') \in PA]\}$

The following discussion illustrated the above formalizes definition. *U*, *R*, *P*, *S*, *PA*, *UA* and *RH* are almost unchanged from the NIST RBAC. We do not want to discuss these components in detail in that this isn't our emphases. And we will discuss the rest components of T&RBAC in more details. Figure1 shows the set of elements and relations among those elements belongs to T&RBAC model. There are many differences that compare with RBAC model. We define these new elements in T&RBAC model as follows.

Local roles and foreign roles: The concept of role in the RBAC model is that a role is a job function or job

title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role. There is little difference with RBAC, there are two types of roles in T&RBAC: one is local role, another is foreign role .

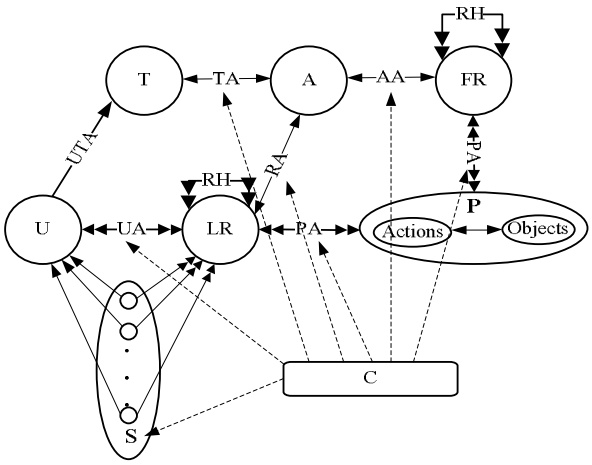

Figure 1. T&RBAC model

Trust rank: A trust rank is a set of real number between 0 and 1. 0 represents no trust, and 1 represents most trust.

Attributes: Attributes are properties of the users that can be used for the authorization process. For simplicity reasons we assume that the user's attributes are synonymous with local roles and trust rank in the T&RBAC model.

Associations between any two of above elements are specified by mathematical relations. Besides the *PA* and *UA* associations, the model has the following relations.

UTA (trust to user assignment): UTA $\subseteq$ T×U, it is a one-to-many relation where a user can have only one trust rank based his previous behavior. But a trust rank can be assigned to many users.

TA (trust to attribute assignment): TA $\subseteq$ T×A, it is a many-to-many trust rank to attribute assignment relation where a trust rank can be assigned to many attributes and a attribute can also be assigned to many trust rank.

RA (local role to attribute assignment): RA $\subseteq$ LR×A, it is a many-to-many local role to attribute assignment relation where a local role can be assigned to many attributes and a attributes can also be assigned to many local roles.

AA (foreign role to attribute assignment): AA $\subseteq$ FR×A, a many-to-many foreign role to attribute assignment relation where a foreign role can be assigned to many attributes and an attributes can also be assigned to many foreign roles.

4. Accessing Control using T&RBAC in Multi-Domain Environmental

The T&RBAC model is based on the trust management by employing the authentication and authorization center (AAC). We assume that all the domains operate under the RBAC model. Consider the scenario that the users in local domain are previous known, which is very suit for employing role-based access control because RBAC has focused on controlling access to digital resources within closed system environments and it deals with previously known user's access. But in foreign domain, the identities of users are not known in advance. In this scenario, we integrate RBAC with trust management by assigning a foreign role to local user by his role information and trust value. Local user will be assigned foreign roles based his local role and credential. We don't want to propose the arithmetic of computing users' credential since there are too many excellent works had been done [11] and that beyond this paper. We will pay our attention on the access control policy in intra-domain and inter-domain respectively.

4.1 Access control framework for intra-domain.

The structure of the access control framework in local domain is illustrated in Figure 2. It depicts the operational procedures for intra-domain access control framework. We use dotted lines to denote one-to-one communication relationships, one-directional arrows with plain line to represent message forwarding, two-directional arrows with plain line to represent communicate with each other. And the steps of the access control for intra-domain are described in Figure 2.

4.2 Access control framework for inter-domain.

The structure of the access control framework for two domains is illustrated in Figure 3. It depicts the operational procedures for inter-domain access control framework. The different kinds of lines denote the same meaning as in Figure 2. And the steps of the access control for intra-domain are described in Figure3. Multi-domain environment is similar to two domains scenario.

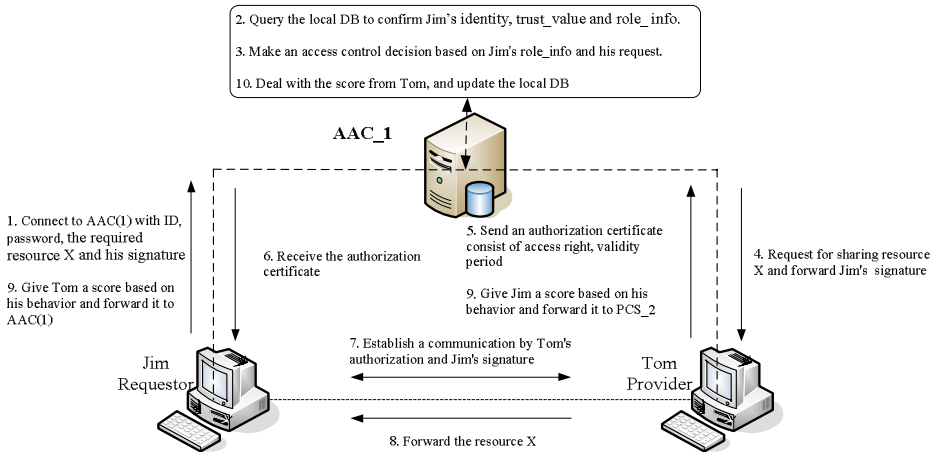

Figure 2. The framework of intra-domain access control

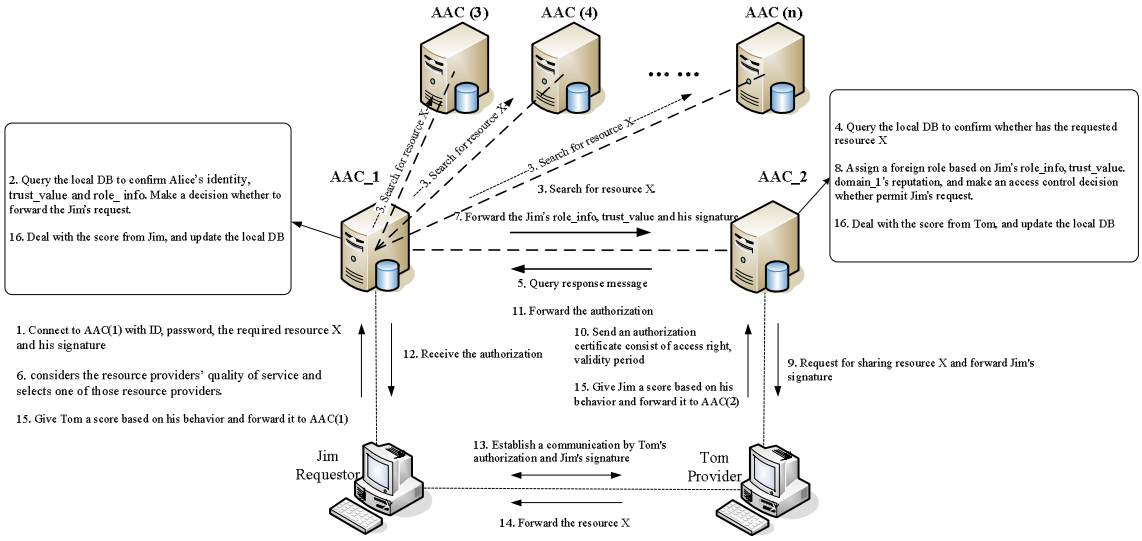

Figure 3. The framework of inter-domain access control

5. Security Issues

With the increasing in information and data accessibility, there is a growing concern for security and privacy of data. Especially in a collaborative environment where distributed, heterogeneous, and autonomous organizations interoperate with each other. Li Gong et al listed two principles of secure interoperation: autonomy principle and security principle [2].

5.1 Autonomy Principle

In the RBAC policy integration framework, violation of a domain's autonomy occurs because of the following two reasons [2]: Induced SoD constraint and asymmetric cardinality of mapped roles. In the following, we describe how this autonomy relaxation condition can be preserved in T&RBAC model.

Figure 4 illustrates an induced SoD constraint between domain A and domain B. There is a SoD constraint between R4 and R5. R2 and R3 will be caused by conflicting cross domain roles R4 and R5 by employing role mapping policy. In T&RBAC model, we don't employ direct role mapping policy. E.g. R2 mapping to R5 and R3 mapping to R4 isn't exit in T&RBAC model. We assume that there is no SoD constraint in local domain, but may has SoD constraint roles(e.g. R4 and R5 in domain B). So there is no induced SoD constraint since it doesn't exit a role which maps to the constraint roles. Similarly, although

there are various types of cardinalities associated with a given role, for T&RBAC policy, the cardinality of a senior role (e.g. R2) should not be greater than the cardinality of any of the junior roles(e.g. R4) that are related to the senior role in the I-hierarchy semantics.

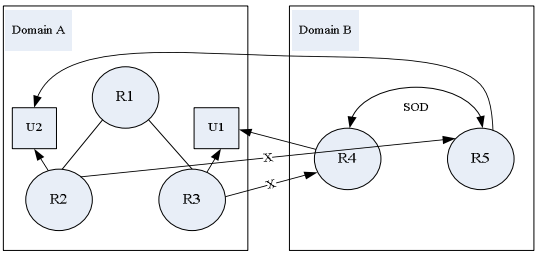

Figure 4. Integrated RBAC policy defining interoperation between domains A and B.

5.2 Security Principle

There are three security vulnerabilities that may lead to unauthorized accesses[12]: role-assignment violation, role-specific SoD violation, and user-specific SoD violation. Any access control state derived from the multi-domain RBAC policy is secure if it does not violate these three security constraints of collaborating domains' RBAC policies. In this section, we will prove that there is no security vulnerability due to these three constraints can occur in T&RBAC. This is formally stated in the following definition:

Theorem 2:

$access(u,r) \Rightarrow assign(u,r)$

It captures the role assignment constraint, Where

$$assign(u,r) = \begin{cases} 1 & user\ u\ is\ assigned\ to\ role\ r \\ 0 & otherwise \end{cases}$$

$$access(u,r) = \begin{cases} 1 & user\ u\ access\ role\ r \\ 0 & otherwise \end{cases}$$

Proof: if the user u can access the role r, there are only four conditions that permit $access(u,r)$:

If $\mathrm{Domain(u)=domain(r)}$:

(1) $assign(u,r)$

(2) $\exists r'(r' > r \wedge assign(u,r')) \Rightarrow assign(u,r)$

else if $\mathrm{Domain(u) \neq domain(r)}$:

(3) $\exists \mathrm{r}'(domain(r') = domain(u) \wedge map(r',r) \wedge assign(u,r')$

In T&RBAC model, we employ

$assign(u,r') \Rightarrow assign(u,r) \wedge credential(u)$

instead of employ direct role mapping police.

(4) $\exists \mathrm{r}'(domain(r') = domain(u) \wedge assign(u,r') \wedge \exists r''(domain(r'') = domain(r) \wedge r'' > r) \wedge map(r'',r)$

Similarly, it equals to $assign(u,r'') \Rightarrow assign(u,r)$

Having defined the four conditions and proof that all of them equal to assign(u, r), so the theorem 2 is proved to be true that means there is no security vulnerability due to role assignment constraint in T&RBAC

Theorem 3:

$\forall u \in U \wedge \forall r \in Conflict-Roles$

$\Rightarrow \sum_{r_i} access(u,r_i) \leq n-1$

It specifies that conflicting roles cannot be accessed by same user in any time, where U is the set of users, and $Conflict-Roles = \{(r_i,m,n) \mid r \in R, 1 \leq i \leq m, 1 \leq n \leq m\}$ denotes the conflicting set of roles, the total number conflict roles is m, and no more than n roles in Conflict-Roles can be assigned to the same user simultaneity.

Proof: let $R_{set}(u)$ denote role set of user u be assigned in local domain, and $R^{+}_{set}(u)$ denotes role set of user u be assigned in foreign domain.

Suppose $\exists r_{local} \in R_{set}(u)$ and $\exists r_{foreign} \in R^{+}_{set}(u)$

It can't educe that:

$\forall r'_{local}(r'_{local} > r) \Rightarrow r'_{local} > r_{foreign}$, similarly

$\forall r'_{foreign}(r_{foreign} > r'_{foreign}) \Rightarrow r_{local} > r'_{foreign}$

Because role mapping policy in T&RBAC has no I-hierarchy, which means it has no role in foreign domain can inherit the conflicting set of roles in local domain simultaneity.

Theorem 4:

$\exists r \in R(\forall u \in Conflict-Users)$

$\Rightarrow \sum_{u_i \in Conflict-Users} access(u_i,r) \leq n-1$

It defines the user-specific SoD constraint implying that conflicting users of a role cannot access that role concurrently in any secure state. Where R is the set of roles, and

$Conflict-Users =$

$\{(u_i,m,n,r) \mid u \in U, 1 \leq i \leq m, 1 \leq n \leq m, r \in R\}$

denotes the conflicting set of users for role r, the total number conflict users is m, and no more than n users in Conflict-users can be assigned to the same role simultaneity.

Proof: we suppose that domain(u_a)=domain(u_b) =domain(r) and access(u_a,r), access(u_b,r) can't occur simultaneity in local domain. If the conflicting users of u_a and u_b can access r concurrently, it must be the following four conditions:

(1) $\left.\begin{array}{l} \exists r'\left(domain(r') \neq domain(r) \wedge r' > r\right) \\ \wedge \left(assign(u_a,r') \wedge assign(u_b,r')\right. \\ \left.\vee (assign(u_b,r') \wedge assign(u_a,r'))\right) \end{array}\right\} \Rightarrow assign(u_a,r) \wedge assign(u_b,r)$

(2) $\left.\begin{array}{l} \exists r'\left(\begin{array}{l} domain(r') = domain(r) \\ \wedge r' > r \wedge assign(u_a,r') \end{array}\right) \\ \wedge \exists r''\left(\begin{array}{l} domain(r'') = domain(r) \\ \wedge r'' > r \wedge assign(u_b,r') \end{array}\right) \end{array}\right\} \Rightarrow assign(u_a,r) \wedge assign(u_b,r)$

(3) $$\left.\begin{array}{l}\exists r'\left(domain(r')\neq domain(r)\wedge map(r',r)\right)\\ \wedge\left(\left(assign(u_a,r')\wedge assign(u_b,r')\right)\right.\\ \left.\vee\left(assign(u_b,r')\wedge assign(u_a,r')\right)\right)\end{array}\right\}$$
$$\Rightarrow assign(u_a,r)\wedge assign(u_b,r)$$

(4) $$\left.\begin{array}{l}\exists r'\left(\begin{array}{l}domain(r')\neq domain(r)\wedge\\ map(r',r)\wedge assign(u_a,r')\end{array}\right)\\ \wedge\exists r''\left(\begin{array}{l}domain(r'')\neq domain(r)\wedge\\ map(r''>r)\wedge assign(u_b,r')\end{array}\right)\end{array}\right\}$$
$$\Rightarrow assign(u_a,r)\wedge assign(u_b,r)$$

The first and second conditions are about local administration which is beyond this paper and we assume that access(u_a,r) access(u_b,r) can't occur simultaneity in local domain. The precondition of the third and fourth conditions is that there must be role mapping. But in T&RBAC model, when the local user wants to access foreign resource, it will be assigned foreign role rather than mapping local roles to foreign role. It means that map(r',r) isn't exit, so the third and fourth conditions can't occur. In this case, there is no security vulnerability due to user specific SoD constraint in T&RBAC.

The above discussion illuminates that T&RBAC is secure without security vulnerability due to role-assignment violation, role-specific SoD violation, or user-specific SoD violation.

6 Conclusion

In this paper, a novel enhanced RBAC model is proposed for secure interoperation in multi-domain environments. This model is an extension of the RBAC with the notion of credential. It employs different access policies in intra-domain and inter-domain domain respectively. We proof that there is no security constraints in T&RBAC. To some extends, the T&RBAC is only a core model. We can extend this model for specific requirement.

Acknowledgment

This research is partially supported by National Natural Science Foundation of China under Grant 60403027, 70672041 and 60773191, National High Technology Research and Development Program of China under Grant 2007AA01Z403, Natural Science Foundation of Hubei Province under Grant 2005ABA258, Open Foundation of State Key Laboratory of Software Engineering under Grant SKLSE05-07.

References

[1] R. Power, Tangled Web': Tales of Digital Crime from the Shadows of Cyberspace, Que/Macmillan Publishing, Aug, 2000

[2] L. Gong and X. Qian, "Computational Issues in Secure Interoperation," IEEE Transactions on Software Engineering, 1996, 22(1): 43-52

[3] David Ferraiolo and Richard Kuhn: Role-based access controls, In 15th NIST-NCSC National Computer Security Conference, Baltimore, MD, October, 1992, pp. 554-563

[4] Osborn, S., Sandhu, R., Munawer, Q: Configuring Role based Access Control to Enforce Mandatory and Discretionary Access Control Policies, ACM Transactions on Information and System Security, 2000, 3(2): 85-106

[5] Apu Kapadia, Jalal Al2Muhtadi, R1 Campbell: IRBAC 2000: Secure interoperability using dynamic role translation. University of Illinois, Technical Report: UIUCDCS-R-2000-2162, 2000

[6] Basit Shafiq, James B.D. Joshi, Elisa Bertino, Fellow, Arif Ghafoor, Fellow: Secure Interoperation in a Multidomain Environment Employing RBAC Policies, IEEE Transactions on Knowledge and Data Engineering, 2005, 17(11): 1557-1577

[7] R. Sandhu and X. Zhang: Peer-to-Peer Access Control Architecture Using Trusted Computing Technology. In Proceedings of the 10th ACM Symposium on Access Control Models and Technologies (SACMAT'05), Stockholm, Sweeden, 2005, pp. 147-158

[8] N. Li and J. Mitchell. RT: A Role-based Trust Management Framework, In Proceedings of the 3rd DARPA Information Survivability Conference and Exposition, Washington D.C., April, 2003

[9] N. Li, J. Mitchell, and W. Winsborough: Design of a Role-Based Trust-Management Framework, Proceedings of the 2002 IEEE Symposium on Security and Privacy, Oakland, California, 2002, pp. 114-130

[10] N. Li, W. Winsborough, and J. Mitchell. Beyond Proof-of-Compliance: Safety and Availability Analysis in Trust Management. Proceedings of the 2003 IEEE Symposium on Security and Privacy, Oakland, California, 2003

[11] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 179-194

[12] S.I. Gavrila and J.F. Barkley, "Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management," Proc. Third ACM Workshop Role-Based Access Control, Oct. 1998