可计算的基于信任的授权委托模型*)

雷建云[1,2] 崔国华[1] 章丽平[1] 邢光林[2]

(华中科技大学计算机科学与技术学院 武汉 430074)[1] (中南民族大学计算机科学学院 武汉 430074)[2]

摘 要 在开放式多域环境中,信任管理是最常用的访问控制方法。但是,目前的信任管理系统存在着以下不足:(1)没有给出实体之间信任的计算方式,使得模型难以实现;(2)信任的传递过程没有得到很好的控制。针对上述问题,提出了一种多域系统中可计算的基于信任的授权委托模型——CTBAD模型(Computable Trust-Based Authorization Delegation model),重点探讨了CTBAD模型的信任计算方法以及信任传递机制,并且进行了信任关系计算的数据仿真。

关键词 访问控制,信任管理,授权委托

Computable Trust-based Authorization Delegation Model

LEI Jian-yun[1,2] CUI Guo-hua[1] ZHANG Li-ping[1] XING Guang-ling[2]

(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]

(College of Computer Science, South-Central University for Nationalities, Wuhan 430074, China)[2]

Abstract Trust management is a common approach on access control in open multi-domain environment. However, the existing trust management systems have some faults as follows: the calculate method of trust between entities is not described in these systems and the delivery of the trust is not controlled effectively. To address the problems, this paper proposed a computable trust-based authorization delegation model in multi-domain systems, called CTBAD model, and discussed the calculate method of trust and the mechanism of trust delivery in CTBAD model. The emulation of the trust calculation is also done.

Keywords Access control, Trust management, Authorization delegation

1 引言

随着互联网技术的兴起和发展,一些开放分布式多域系统(如网格、多Agent系统等)迅速发展,计算系统正渐渐地从传统的封闭式系统向开放式分布式系统转变。尝试通过信任管理方法使开放式分布式计算系统更加高效和安全是当前研究的一个热点。信任管理技术[1-6]作为一种支持分布式访问控制的技术,可以较好地用于支持多域间的安全互操作,其实质是一种信任的传播技术。通过信任的传播,表达了权限的传递。其主要特点是能够支持系统不认知的主体访问系统,并采用可传递性授权的机制,支持分布式应用可伸缩的特点。但是,目前存在的信任管理系统存在两个方面的问题:(1)没有给出实体之间信任的计算方式,使得模型难以实现。文献[2]提出了信任应该基于经验、知识、推荐等等因素,但还是缺乏很好的可操作的算法;(2)信任的传递过程没有得到很好的控制。文献[3]给出了一种基于深度的信任传递控制方法,但存在一定的局限性。本文针对上述两个问题,提出了一种新的适合于多域环境的授权委托模型,对该模型的信任计算和信任传递过程进行了详细的讨论。

2 CTBAD模型

在此详细地介绍可计算的基于信任的授权委托模型——CTBAD模型(Computable Trust-Based Authorization Delegation model)的组成要素[8]及语义。

(1)实体

实体(Entity)是指用户、主机、服务等对象,所有实体能够惟一地标识每个主体,并且对该主体发布的委托进行数字签名。

(2)角色

角色(Role)是特定实体名字空间里的名字,表示一组权限的集合。

(3)主体

主体(Subject)是指被委托的对象,主体是一个实体或者角色。如果主体是一个角色,则该主体所对应的实体为定义该角色的实体。

(4)客体

客体(Object)是指委托的对象,是一个实体或角色。如果客体是一个角色,则该客体所对应的实体为定义该角色的实体。

(5)信任值

信任值(Trust Value)是指一个实体对另一个实体的信任程度,用一个实数表示,取值范围为0~100。如果信任值为0,表示一点也不信任;如果为100,表示完全信任。信任值越大,表示信任的程度越高。信任值的计算在第4节里有详细的阐述。

(6)授权源

*)本文得到国家自然科学基金(60403027)资助。**雷建云** 博士生,副教授,研究方向为分布式访问控制;**崔国华** 教授,博士生导师,研究方向为信息安全;**章丽平** 博士生,研究方向为信息安全;**邢光林** 博士,副教授,研究方向为访问控制与安全模型。

授权源(Authorization Root)是授权委托的起源点,是资源所有者发布的访问控制列表(Access Control List,ACL)。ACL存储在本地,且永远不会传送出去,因而ACL是安全可靠的。一个ACL条目由权限(Right)、主体(Subject)和信任阈值(Trust Threshold)三部分组成。此处的信任阈值是表示权限能够被授予的一个度量值,即只有当该权限的请求者所拥有的信任值达到该条目中的信任阈值时,才能把该权限授予给请求者。

(7)委托

委托(delegation)是指在不需要资源所有者干预的情况下把权限从一个主体传递给另一个主体,用证书表示,并且证书的发布者用自己的私钥对证书进行数字签名。

委托的形式化表示为[8]:[Object→Subject with Trustvalue,Expireddatetime] Issuer,其中Object和Subject是一个角色或者实体;Issuer是一个实体,表示证书的发布者,与Object对应的实体相同,Issuer用自己的私钥对证书进行数字签名;Trustvalue表示Issuer对Subject的信任值;Expireddatetime表示证书失效时间;→表示把Object所拥有的权限传递给Subject。

上述委托[Object→Subject with Trustvalue,Expireddatetime] Issuer的语义为:发布者Issuer发布证书,宣称把Object所拥有的权限委托给Subject,Issuer对Subject的信任值为Trustvalue,证书的有效期至expireddatetime,Issuer用自己的私钥对证书进行签名,以防止证书被伪造或篡改。

在CTBAD模型中,角色沿袭了Sandhu等在RBAC中的定义。委托是模型中最核心的概念,它将授权源、主体、客体和信任值等等概念紧密联系在一起。

3 一致性验证

在CTBAD模型中,请求的访问是否能够被接受是根据访问的请求者是否被授予所要求的权限来决定的,问题的关键是"访问的请求者所提供的证书集合C是否能够证明请求r与本地安全策略P一致",也就是一致性验证问题。在CTBAD模型中,一致性验证的关键问题是证书链的查找和信任的传递。文献[8]中对证书链的查找算法给出了前向搜索法、后向搜索法以及双向搜索法,并给出了证书链查找算法的复杂度的证明,在此不再复述,而把重点放在信任关系的计算和信任的传递算法上。

4 信任关系的计算

信任是一个实体对其它实体特定行为的可能性预测,具有如下特性[4-5,7]:

主观性:不同的实体对同一事物的信任值有所不同,因此有不同的信任程度。

传递性:我们认为信任在一定条件限制下是可以传递的。但在现实生活中,不是所有的信任关系都具备可传递性,如A信任B,B信任C,但A不一定信任C。

非对称性:A信任B,但B不一定信任A,或者两者互相信任的程度是不同的。

可量化性:信任像信息和知识一样能够量化。

多样性:信任的实体和目的具有多样性。

上下文相关性:信任是相对于某个上下文而言的,这是信任的系统属性。

实体属性相关性:即使同样的上下文,信任值也会不同,信任来自多方面的因素,这是信任的实体属性。

动态性:信任与时间有关,信任度会随着时间的推移上升或者下降。

从以上的分析可以看出,信任应该是基于内容的且与经验(历史)、知识和推荐相关的一个值。

定义1[2] 用$(A \xrightarrow{c} B)_t$表示A关于内容c的对B的信任关系,$(A \xrightarrow{c} B)_t=[{}_AE_B^c, {}_AK_B^c, {}_\Psi R_B^c]$是一个包含三个分量的向量,其中${}_AE_B^c$表示$A$关于内容$c$的对$B$的信任经验,${}_AK_B^c$表示$A$关于内容$c$的对$B$的信任知识,${}_\psi R_B^c$表示$A$得到的关于内容$c$的其他实体对$B$的信任推荐。

为了计算每个分量的值,在此假设每个分量的取值范围是一个实数,且$\in[-1,1]$,取-1表示一点也不信任,取1表示完全信任,0表示中立。

4.1 信任经验的计算

A根据就内容c和B的多个时段的交互历史,可以计算出历史上每个时段交互的经验值。假设在历史上的第j个时段,共有n_j次交互,其中第k次交互的经验值v_k^j有两个可能:如果第k次交互是成功的,则记为$+1$,反之记为-1。

定义2 第j个时段的经验值

$$I_j=\begin{cases}0, \text{if } n_j=0\\ \dfrac{\sum_{k=1}^{n_j} v_k^j}{\sum_{k=1}^{n_j}|v_k^j|}, \text{if } n_j\neq 0\end{cases},$$

定理1 $I_j\in[-1,1]$且I_j与该时段内的每次交互经验有关,若n_j次交互都是不成功的,则$I_j=-1$;若n_j次交互都是成功的,则$I_j=+1$。

证明:当$n_j=0$,定理显然成立;当$n_j\neq 0$时,由于$v_k^j=+1$或者-1,因此$|\sum_{k=1}^{n_j}V_k^j|\leqslant|\sum_{k=1}^{n_j}|V_k^j||$,所以$I_j\in[-1,1]$。若$n_j$次交互都是不成功的,则所有的$v_k^j=-1$,所以$\sum_{k=1}^{n_j}V_k^j=-|\sum_{k=1}^{n_j}|V_k^j||$,$I_j=-1$。同理可证,若$n_j$次交互都是成功的,则$I_j=+1$。

给历史上每个时段的交互设定一个重要系数(权重),假设第i个时段的权重为W_i,就可以计算出A关于内容c的对B的信任经验值。

定义3 A根据就内容c和B的信任经验

$${}_AE_B^c=\sum_{i=1}^{n} w_i I_i$$

其中$W_i\in[0,1]$且$\sum_{i=1}^{n} w_i=1$。一般说来,距离当前时段越近的时段的权重越大,而离当前时段已经很远的,即很久以前发生的事件,往往可以从轻考虑,甚至忽略不计。

4.2 信任知识的计算

A关于内容c的对B的信任知识来自两个方面,一个是直接的(direct),另一个是间接的(indirect)。间接的知识其实就是关于B的声誉。分别用d,i来表示直接知识和间接知识,然后A根据自己的应用背景确定两个系数W_d和W_i,分别表示直接知识和间接知识所占的权重。

定义4 A关于内容c的对B的信任知识

$${}_AK_B^c=W_d*d+W_i*i,$$

其中,$d,i\in[-1,1]$,$W_d,W_i\in[0,1]$且$W_d+W_i=1$。

4.3 信任推荐的计算

A 可能接收到关于内容 c 的对 B 的若干推荐。每个推荐人根据历史记录给出信任值，A 同时给出一个相应的重视程度值作为该次信任值的权重。

定义 5[2] A 关于内容 c 的对 B 的信任推荐

$$ {}_{\Psi}R_B^c=\frac{\sum_{i=1}^{n}((v(A\xrightarrow{rec}j)_t^N)\cdot V_j)}{\sum_{j=1}^{n}\left|v(A\xrightarrow{rec}j)_t^N\right|} $$

其中，ψ 表示 n 个推荐者的集合，$v(A\xrightarrow{rec}j)_t^N$ 表示第 j 个推荐者根据 N 次历史记录(record)提供给 A 的关于内容 c 的对 B 的信任值，V_j 表示 A 对第 j 个推荐者给出信任值的重视程度值。信任值的取值范围$\in[-1,1]$，而重视程度值的取值范围$\in[0,1]$。当重视程度值取 0 时，表示本次推荐无效；而当重视程度值取 1 时，表示非常重视此次推荐。A 根据自己对每个推荐者的认识和判断来确定相应的重视程度值。

定理 2 ${}_{\Psi}R_B^c\in[-1,1]$，且当所有的重视程度值为 1 时，若所有推荐者给出的信任值都是负数，则${}_{\Psi}R_B^c=-1$；所有推荐者给出的信任值都是正数，则${}_{\Psi}R_B^c=+1$。

证明：因为 $V_j\in[0,1]$，所以$|\sum_{j=1}^{n}((v(A\xrightarrow{rec}j)_t^N)\cdot V_j)|\leqslant|\sum_{j=1}^{n}||v(A\xrightarrow{rec}j)_t^N||$，因此${}_{\Psi}R_B^c\in[-1,1]$，当所有的 $V_j=1$ 时，若所有推荐者给出的信任值都是负数，则$\sum_{j=1}^{n}((v(A\xrightarrow{rec}j)_t^N)\cdot V_j)=-\sum_{j=1}^{n}|v(A\xrightarrow{rec}j)_t^N|$，所以${}_{\Psi}R_B^c=-1$。同理可证此条件下当所有推荐者给出的信任值都是正数时，${}_{\Psi}R_B^c=+1$。

4.4 信任值的计算

为了与现实中的思维习惯相符，需要将三个分量经过一定的换算才能得到真正的信任值。为了便于计算，首先将${}_AE_B^c$，${}_AK_B^c$，${}_{\Psi}R_B^c$ 在$[-1,1]$中的取值映射到$[0,1]$域中来。计算方式为，将${}_AE_B^c$，${}_AK_B^c$，${}_{\Psi}R_B^c$ 分别加 1，然后除以 2，得到新的${}_AE_B^{c'}$，${}_AK_B^{c'}$，${}_{\Psi}R_B^{c'}$。

根据应用背景定义一个 W 向量，称之为权值向量。它包含三个分量为 W_E，W_K，W_R，分别表示信任经验、信任知识和信任推荐在本应用系统中占据的权值份量，满足 W_E，W_K，$W_R\in[0,100]$且 $W_E+W_K+W_R=100$。

定义 6 A 关于内容 c 的对 B 的信任值

$${}_AT_B^c={}_AE_B^{c'}*W_E+{}_AK_B^{c'}*W_K+{}_{\Psi}R_B^{c'}*W_R$$

很容易得到验证，当${}_AT_B^c=0$ 时，表示 A 关于内容 c 对 B 一点也不信任；而当且仅当${}_AE_B^{c'}$，${}_AK_B^{c'}$，${}_{\Psi}R_B^{c'}$ 都为 1 时，A 关于内容 c 对 B 完全信任，此时${}_AT_B^c=100$。

4.5 信任计算的数据仿真

在实验室进行数据仿真计算时，信任经验计算的参数取 $W_i=\frac{1}{2^i}$，其中 i 表示距离当前时段的时段数。i 为 1 表示前一时段。i 为 2 表示前一时段的再前一时段，假设进行长久的交互，容易得到验证 $W_i\in[0,1]$且$\sum_{i=1}^{n}w_i\to1$，满足参数所需的要求。且距离当前时段越近的时段的权重越大，而离当前时段已经很远的，即很久以前发生的事件是从轻考虑。

信任知识的计算参数取 $W_d=0.5$ 和 $W_i=0.5$，即直接知识和间接知识所占的权重各占 50%。

信任推荐的计算参数取所有的 $V=1$，即 A 对每个推荐者给出信任值都非常重视。

权值向量的三个分量 W_E，W_K，W_R 分别取值 40，30，30，即信任经验、信任知识与信任推荐所占的份额分别为 40%，30%，30%。

假定计算出来的信任值在 20 以下，定义为不信任，80 以上定义为信任，介于两者之间为不明确。

随机取 100000 组有意义的交互经验值、直接知识和间接知识值以及信任推荐值，分成 100 次交互。在取值的过程中，根据实际的情况，交互经验值进行积累并且直接知识值、间接知识值和推荐值越来越接近是否信任的现实，得到数据仿真的信任计算准确率如图 1 所示。其中计算不准确的主要原因是计算出来的信任值介于 20～80 之间，导致信任关系不明确。

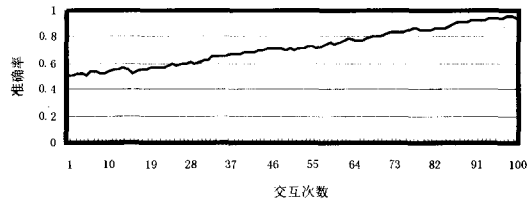

图 1 信任计算准确率

从结果可以看出，取上述参数时，当交互达到一定次数以上，且直接知识与间接知识的获得以及信任推荐的工作越来越成熟和完善时，信任计算准确率可达到一个很高的比例。

在一个实际的信任系统中，可以依照系统本身的应用特点与规律来确定上述参数，应该可以取得比实验结果更为理想的效果。

5 信任的传递

5.1 信任传递的计算

如果 A 对 B 的信任值为 t_1，B 对 C 的信任值为 t_2，那么 A 对 C 的信任值 t 应该是多少？信任的传递计算应该与具体的应用环境相关，应用背景不同，信任的传递计算也不相同。为了便于讨论，我们将信任传递计算用函数 $t=f(t_1,t_2)$ 来表示。在此先给出两条计算信任传递的准则[8]：

(1)信任传递计算函数 $f(t_1,t_2)$ 是单调递减函数，即函数 $f(t_1,t_2)$ 的值 $t\leqslant\min(t_1,t_2)$。这条准则保证了随着委托传递深度的增加，委托链起点的实体对委托链终点的实体的信任值将会越来越低，这同实际情况是相符的。

(2)信任传递计算函数 $f(t_1,t_2)$ 是有界函数。即函数 $f(t_1,t_2)$ 的计算结果 MIN$\leqslant t\leqslant$MAX。MIN 和 MAX 分别表示信任值域中的最小值和最大值。在 CTBAD 模型中，MIN=0，MAX=100。这条准则保证信任传递计算函数 $f(t_1,t_2)$ 的计算结果有意义。

5.2 委托的深度控制

目前的委托深度控制方案有一定的局限性，文献[3]给出了一种深度控制的方案，但与现实情况中的委托深度控制不是很符合，而且实现起来比较麻烦。CTBAD 使用信任阈值的形式达到对委托深度的有效控制。

例如，在形如 $R\xrightarrow{80}A\xrightarrow{90}B\xrightarrow{95}C\xrightarrow{80}D\xrightarrow{80}E$ 的授权委托链(其中 R 表示权限，A,B,C,D,E 表示主体或客体)中，如何进行委托的深度控制呢？

用 T_A,T_B,T_C,T_D,T_E 分别表示 A,B,C,D,E 拥有权限 R 的信任值，用 $f(t_1,t_2)$ 表示信任传递函数，不妨假设 $f(t_1,t_2)=t_1*t_2/100$，则 $T_A=100$，$T_B=f(100,90)=90$，$T_C=$

(下转第 85 页)

我们还采用 ROC[8](Receiver Operating Characteristic Analysis)曲线下的面积 AUC(Area Under the ROC)来衡量分类器的结果,ROC 克服了使用正确率忽略代价的不足,它使用正确分类的比率 TPR (True Positive rate)与错误分类的比率 FPR(False Positive rate)的比值衡量分类器的性能,AUC 是 ROC 曲线下的面积,AUC 越大分类器性能越好,我们对实验 4 使用 LibSVM 的 Plotroc 工具得到 AUC=0.9993,其他的实验结果见表 2。

表 2 实验结果

Test	C-SVM			LS-SVM		
	Test correct	AUC	Test time	Test correct	AUC	Test time
1	99.65%	1.0000	0.5s	84.45%	0.9998	0.2s
2	99.58%	0.9999	0.7s	85.567%	0.9899	0.4s
3	99.53%	0.9998	1.1s	85.652%	0.9890	0.6s
4	99.30%	0.9993	1.4s	86.213%	0.9989	1.0s

从表 2 可以看出,SVM 比 LS-SVM 的检测准确率高,AUC 大,说明 SVM 分类能力强,而 LS-SVM 的检测时间比 SVM 少,说明其检测速度更快。因此,在使用两种方法进行入侵检测时,应该根据实际检测要求选用不同的方法,对于实时性要求高的选用 LS-SVM,准确性要求高的选用 SVM。

结束语 SVM 和 LS-SVM 都是基于结构化风险,克服了传统学习方法的过拟合、局部最小点的缺点,本文将二者用于入侵检测之中,采用 KDDCUP'99 数据集对二者的性能进行了比较。比较发现,SVM 的 AUC 比 LS-SVM 大,但是 LS-SVM 的检测速度更快。这主要是 LS-SVM 采用等式约束条件,克服了 SVM 求解 QP 问题耗时多的缺点,但是另一方面它失去了 SVM 稀疏性的优点。如何克服 LS-SVM 的稀疏性,提高其准确率,以及对 SVM 进行改进,提高其检测效率,是我们下一步要研究的工作。

参 考 文 献

[1] Vapnik V. The nature of statistical learning theory [M]. New York: Springer-Verlag, 1995

[2] Burges C. A tutorial on support vector machines for pattern recognition[J]. Data Mining and Knowledge Discovery, 1998, 2(2): 121-167

[3] Suykens J A K, Vandewalle J. Least Squares Support Vector Machine Classifiers [J]. Neural Processing Letters (S1370-4621), 1999, 9(3): 293-300

[4] Suykens J A K. LS-SVMlab Toolbox User's Guide [EB/OL]. http://www.esat.kuleuven.ac.be/sista/lssvmlab/

[5] http://kdd.ics.uci.edu/databases/kddcup99/task.htm

[6] 边肇祺,张学工,阎平凡,等. 模式识别[M]. 北京:清华大学出版社,2000

[7] Lin Chihjen. LIBSVM: a library for SVMs (Version 2.6) [DB/OL]. http://www.csie.ntu.edu.tw/~cjlin/papers/libsvm.pdf

[8] Bradley A P. The use of the area under the ROC curve in the evaluation of machine learning algorithms. Pattern Recognition, 1997, 30 (7): 1145-1159

(上接第 75 页)

$f(90,95)=85.5$, $T_D=f(85.5,80)=68.4$。由于 $T_D<80$(拥有权限 R 的信任阈值),因此 D 不仅不能被授予权限 R,而且委托$(D,E,80)$是没有意义的,从而实现了委托的深度控制。

跟其他的深度控制方案相比,CTBAD 模型的深度控制既简单又灵活实用,很好地控制了委托传递的深度。

5.3 授权冲突问题

设想有这么一种情况:如果从某一权限到某一主体存在多条授权路径,即存在多条证书链,那么可能会存在授权冲突,即对某条路径而言,一致性验证得到通过,而对另外一条路径,一致性验证不通过,此时应该如何来解决。

可以有两种解决方法:一种是选择信任值传递计算结果为最大的那条授权路径进行一致性验证,即在多条授权路径的情形下,只要有一条授权路径通过了一致性验证,就可以通过一致性验证,这是基于对每条授权路径的合法性和合理性的认同而做出的决定。另一种方法是选择信任值传递计算结果为最小的那条授权路径进行一致性验证,即在多条授权路径的情形下,只要有一条授权路径没有通过一致性验证,就不能通过一致性验证,这是基于对高度敏感信息的保护需求而做出的决定。

在具体应用的过程中,可以对两种解决方法有选择地加以利用。如果是针对一般性的非敏感信息,可以采用前一种算法;而对于高度敏感的信息,基于安全原则,应该采用后一种算法。

结束语 在多域环境下,保护被访问资源的安全是一个很重要的问题,很多学者在这个领域进行了深入的研究,已经有了大量的研究成果。但信任的计算以及委托深度控制等问题还没有得到比较好的解决。本文对目前信任管理系统中存在的上述问题进行了一定的研究,提出了一种可计算的基于信任的授权委托模型——CTBAD 模型,重点探讨了 CTBAD 模型的信任计算方法以及信任传递机制。跟目前的信任管理系统相比,CTBAD 模型不仅具有很强的实用性和灵活性,而且实现比较简单。

参 考 文 献

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management // Proceedings of the 1996 IEEE Symposium on Security and Privacy. Washington, DC, USA, 1996: 164-173

[2] Chakraborty S, Ray I. TrustBAC - Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems // SACMAT'06. Lake Tahoe, California, USA, 2006: 49-58

[3] Hong Fan, Zhu Xian, Wang Shaobin. Delegation Depth Control in Trust-management System // Proceedings of the 19th International Conference on Advanced Information Networking and Applications. 2005: 1-4

[4] Chu Yang-Hua, Feigenbaum J, et al. REFEREE: Trust management for Web applications. World Wide Web Journal, 1997, 2 (3): 127-139

[5] Li Ning-Hui, Mitchell J C, Winsborough W H. Design of a role-based trust-management framework // Proceedings of the 2002 IEEE Symposium on Security and Privacy. Oakland, CA, USA, 2002: 114-130

[6] Bertino E, Ferrara E, Squicciarini A C. Trust-X: A Peer to Peer framework for trust negotiations. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 827-842

[7] Freudenthal E, Pesin T, Port L, et al. dRBAC: Distributed role-based access control for dynamic coalition environments // Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS' 02). Vienna, Austria, 2002: 411-434

[8] 廖俊国,洪帆,朱更明,等. 基于信任度的授权委托模型[J]. 计算机学报,2006,29(8):1265-1270