

一个分布式系统下的多级授权管理模型

马国富¹, 王子贤², 董彦军³

(1 中央司法警官学院 信息管理系, 河北 保定 071000; 2 中央司法警官学院 现代教育技术中心, 河北 保定 071000;
3 保定学院 教育信息技术系, 河北 保定 071000)

摘 要: 针对目前有关授权中存在的一些问题, 如: 一次授权, 终身有效; 授权控制深度不够等特点. 文中给出了一种分布式系统下的多级授权管理模型. 该模型采用基于信任度的方式进行授权并且定期对各个实体的可信性进行验证, 对不符合条件的实体可以及时处理, 并且对各个实体的授权均要与授权源及一些相关实体通信, 加强了授权的控制.

关键词: 授权; 信任; 信任管理; 信任度

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)05-0136-03

A Multi-Level Authorization Management Model in Distributed System

MA Guo-fu¹, WANG Zi-xian², DONG Yan-jun³

(1 Department of Information Management, The Central Institute for Correctional Police, Baoding 071000, China;
2 Modern Education Technical Center, The Central Institute for Correctional Police, Baoding 071000, China;
3 Department of Education and Information Technology, Baoding University, Baoding 071000, China)

Abstract: Authorization is a part of trust management, the existing systems have some faults as follows: one is "one time authorization, effective for ever", the other is authorization depth is not controlled effectively. To address the problems, this paper proposes a multi-level authorization management model in distributed system. This model uses a way based on the trustworthiness to authorize and inspect every entity regularly. To the entities that does not conform the condition, they will be took out. Moreover, the correspondence among the entities is controlled by the authorization root, strengthen the depth control.

Key words: authorization; trust; trust management; trustworthiness

1 引言

随着 Internet 的广泛普及和网络技术的发展, 网络安全问题日益突出. 在网络时代, 安全的前提是信任, 因此对有关信任问题的研究, 吸引了众多学者. Blaze M. 等人在 1996 年第一次提出了信任管理 (Trust Management, TM) 的概念. 信任是安全的基石, 安全服务都是建立在信任的基础上的. 按照 Blaze M. 的定义, 信任管理是采用一种统一的方法描述和解释安全策略 (Security Policy)、安全凭证

(Security Credential), 以及用于直接授权关键性安全操作的信任关系^[1] (Trust Relationship).

在网络环境下, 分布式系统中用户和资源的可信性对于整个系统的安全性至关重要. 现有的信任系统中, PolicyMaker 没有考虑有效期问题, 一旦被授权, 将永远有效, 不能表示否定授权的证书^[2], 还有基于模糊理论的评估模型^[3]. 文中主要讨论信任管理中的授权方式, 改变了那种终身授权机制, 并参考经验的影响, 针对分布式系统给出了一个基于信任度的多级授权委托模型, 并作具体分析.

收稿日期: 2009-04-03; 修回日期: 2009-07-18

基金项目: 国家自然科学基金项目 (60873203); 河北省自然科学基金项目 (F2008000646)

2 授权模型

文中通过直接信任与间接信任建立基于信任度的多级授权委托模型进行授权.实体的直接信任即该实体的父实体计算出的该实体的信任度,间接信任通过该实体的父实体与授权源协商形成的该实体的信任度.授权中经常涉及到以下概念:

实体(Entity):是指用户、主机、服务等对象.所有实体都分别与一对公/私钥对相对应,以便能唯一地标识每个主体和对该主体发布的委托进行数字签名.每个实体能够定义包含角色的名字空间;

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;

客体(Object):被访问的对象,如文件、数据等;

主体(Subject):发出访问操作的主动方,可以将用户、用户组、计算机或服务都看成是一个安全主体;

信任度(Trustworthiness):是指一个实体对另一个实体的信任程度;

授权源(authorization root)是授权的起源点,是资源所有者发布的访问控制列表;

该授权委托模型形成一个可信授权树,其逻辑结构如图1所示.

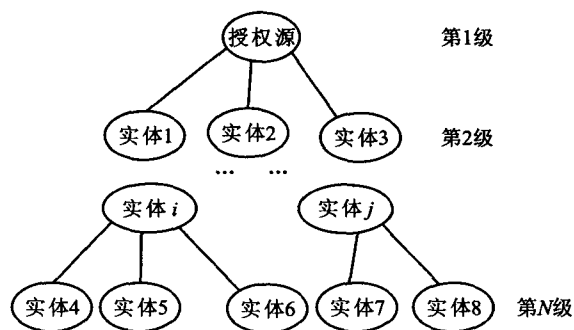


图1 多级授权委托模型逻辑结构图

该授权树的第一级(根节点)为授权源,被用户绝对信任;第二级为被授权源直接认证的实体;以下的实体被其父实体直接认证并通过与授权源的间接认证机制进行授权.

授权源由可信平台担当,是认证的发行者,其他实体的授权均要通过授权源来节制.模型中的其他节点既是认证发行者,又是信任请求者.

3 基本操作

3.1 初始化操作

对可信授权树的初始化主要是可信授权树的生成过程.

可信授权树中的每个父节点都必须与它的孩子节点有强可信关系,我们定量地定义可信度范围为 $[0,1]$,值越小说明越不信任.例如:一个节点1可以指定它的孩子的可信度为0.9,那么一个实体要想成为节点1的孩子,该实体对于节点1的可信度必须高于0.9.另外还要与授权源协商来确定这个实体的间接信任度,只有两个信任度均达到用户要求的阈值,实体才能被授权,而被同一父级实体授权的实体又被分为一组.

授权源为用户直接信任的节点,授权源通过检查它的历史记录,使每一个与它直接相关且信任度超过它设定的阈值的实体作为它的孩子(逻辑图中为实体1、实体2和实体3).其他节点直接信任度和间接信任度均要高于设定的阈值才能加入到授权树中.

授权树建立以后,除授权源及最下面的叶子节点外,每一节点都存有父、子、兄弟以及授权源对自己的信任协商认证信息.授权源系统中各种操作结果定期对授权树中的节点进行检查,对授权树进行更新.

3.2 更新操作

授权树建立起来之后,并不是一成不变的.有的节点随着时间和经验的变化信任度会改变:信任度可能会减少,也可能会增加.这时候就要对授权树进行更新.授权树的更新操作包括节点的切出、升级、降级.

如果一个节点因为信任度太低而必须从授权树切出,那么它的所有孩子节点也随着其一起切出.如图2所示,节点3被切出,则它的孩子节点4和5也一起被切出.

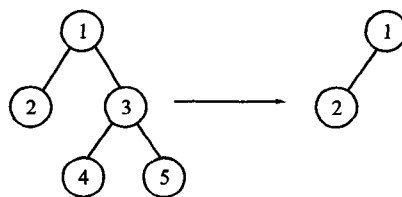


图2 节点的切出

如果某一个节点的隶属关系改变,而它的信任度仍在许可范围之内则可分为以下两种情况:

图3中的节点4由隶属于节点3变为隶属于节点1,则它在授权树中的等级上升一级,同时它的所有孩子也同它一起上升一级.

图4中的节点3由隶属于节点1变为隶属于节点2,则它在授权树中的等级下降一级,同时它的所

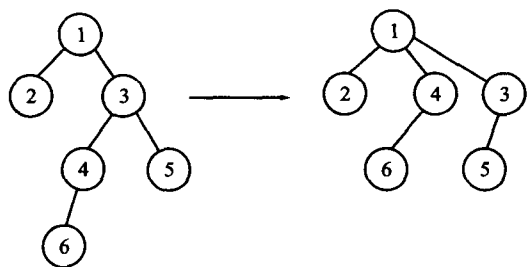


图3 节点的升级

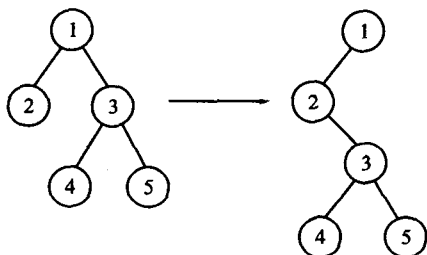


图4 节点的降级

有孩子也同它一起下降一级。

在节点的升级及降级操作的时候,仍然需要对节点进行验证,就像授权树初始化一样.因为在作出这些决定的时候只能判断节点的信任度不满足现在的状况并不能判断出是否满足下一个状态.而节点的切出操作则无须再次认证.

4 信任度计算

在 TCG 规范中,缺少一个对可信程度的评估,它的可信只有两种状态,即可信与不可信,不存在第三种状态.这无法符合人们日常使用的需要,对可信性要求不高的用户可能带来诸多不便^[4].信任可分为多个级别,文中将节点 i 对节点 j 的信任度定义为 $T(i, j)$.节点 j 的信任度可以通过直接信任和间接信任获得.直接信任可以通过两个节点直接交互的经验获得,即节点 j 的父节点.间接信任可以从授权源对节点 j 的反馈信息获得.用 T_j 表示节点 j 的最终信任度,则 T 可以使用以下式定义:

$$T_i = T(i, j) \times T(0, i) \quad (1)$$

其中, $0 \leq T(i, j) \leq 1$, $0 \leq T_j \leq 1$, i 节点为 j 节点的父节点, $T(0, i)$ 为授权源对节点 i 的信任度.从式中可以看出:无论是授权源对节点 i 不信任还是节点 i 对节点 j 不信任,节点 j 都无法被授权,也就无法加入到节点 i 的孩子中.信任度的初始值设置可参见相关文献^[4-5].

以上是节点第一次加入到授权树时的计算方法.为了使每个节点时刻保持可信还要定期检查节点的信任度,对节点重新进行管理.此时的计算方法

如下:

$$T_j = T(i, j) \times T(0, i) + \frac{\sum_{l=1}^n P_l}{n} - x \frac{\sum_{k=1}^m Q_k}{m} \quad (2)$$

在式(2)中除了式(1)中的计算结果,又引入了两项:成功操作的影响 $(\sum P)/n$ 和失败操作的影响 $x \times (\sum Q)/m$. P 、 Q 分别表示对节点提供服务的满意度: $0.5 \leq P \leq 1$, 表示对 j 节点提供的服务比较满意, $0 \leq Q \leq 0.5$ 表示对 j 节点提供的服务比较失望; m 和 n 分别为失望次数和满意次数.由于操作失败和成功对信任的影响是不一致的,即信任的增加或减少是不对称的,信任以不同的速度增加和减少^[6].可能经过多次成功的操作建立起来的信任在一、两次的操作失败后就会迅速降低至零.因此引入了影响系数 x 来准确体现这一影响.

5 结束语

文中针对分布式系统下的信任授权问题,给出了一个采用直接信任与间接信任相结合的多级分组授权委托模型.该模型提高了委托深度控制,每一个受委托实体的加入均受到授权源的控制,这样使整个系统更加紧密.另外,在信任度的计算上充分考虑了实体的行为对信任度的影响,引入了影响系数,使得节点的信任度能够更准确地反映系统的变化,提高了信任评价的准确性.下一步将研究如何确定影响系数 x 使之更合理的反映失败和成功对信任度的影响.

参考文献:

- [1] Blaze M, Feigenbaum J, Ioannidis J, et al. The role of trust management in distributed systems security[C]// Secure Internet Programming: Issues for Mobile and Distributed Objects. Berlin, 1999:185-210.
- [2] Clarke D, Eilen J E, Ellison C M, et al. Certificate chain discovery in SPKI/SDSI[J]. Journal of Computer Security, 2001, 9(4):285-322.
- [3] 张亚红,王勇,陈辉. 网格中基于模糊理论的信任评估模型[J]. 微电子学与计算机, 2008, 25(6):74-77.
- [4] Manchala D W. E-commerce trust metrics and models[J]. Internet computing, 2000, 4(2):36-44.
- [5] 付争方,王小明,窦文阳,等. 基于信任授权的模糊访问控制模型[J]. 微电子学与计算机, 2007, 24(9):29-32.

(下转第 142 页)

受同样的攻击后,图像主观质量明显退化,退化质量与文献[2]和文献[3]类似,但文中算法有更高的 NC 和 PSNR 值.尤其对常见的几何操作,文中算法效果更加优于文献[2]和文献[3].

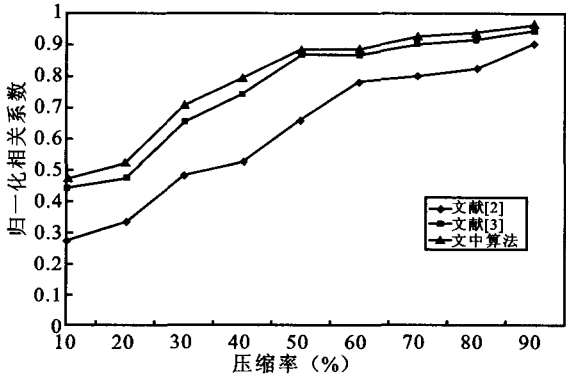


图3 JPEG 压缩性能比较

表2 对水印各种攻击的性能比较

攻击类型	文献[2]算法		文献[3]算法		文中算法	
	PSNR	NC	PSNR	NC	PSNR	NC
JPEG 压缩 10%	30.030	0.2735	30.036	0.4459	31.052	0.4721
中值滤波 3×3	35.002	0.6668	35.031	0.8185	36.041	0.8253
中值滤波 5×5	30.871	0.2231	30.875	0.3858	31.860	0.4523
维纳滤波 3×3	37.127	0.7435	37.182	0.8823	32.282	0.8965
维纳滤波 5×5	34.221	0.3703	34.245	0.5378	35.678	0.6128
高斯加噪(0.01)	19.686	0.2442	19.689	0.2903	22.689	0.4329
高斯加噪(0.02)	22.121	0.2801	22.063	0.3199	25.063	0.4498
比例缩放(25%)	32.372	0.5098	32.387	0.7179	35.387	0.7229
旋转 10°	17.065	0.1938	17.063	0.2375	32.128	0.4928

4 结束语

文中基于对 HVS 特征和块能量特征 FCM 模

糊聚类基础上,提出了一种改进的小波域水印方法.算法充分考虑了各细节子图的分块能量特征,采用模糊聚类 FCM 的方式进行可嵌入块的选取,改变了采用硬性划分方式区分嵌入块和非嵌入块的方法.FCM 划分方式不仅保证了视觉质量,而且满足了水印的不可见性和鲁棒性的统一.能够有效地经受噪声,压缩和剪切等的攻击.

参考文献:

[1] Cox IJ, Killian J, Leighton T, et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Trans. on Image Process, 1997, 6(12): 1673-1687.

[2] 练秋生, 卢耀斌, 王成儒, 等. 基于小波分析的自适应数字水印算法[J]. 仪器仪表学报, 2002, 23(6): 617-619.

[3] 宋兴利, 张家树. 基于小波系数块能量分析的自适应数字水印算法[J]. 计算机应用, 2006, 26(4): 830-832.

[4] 刘铁柱, 张建伟, 刘红岩. 数字水印的鲁棒性和易脆性相结合的研究[J]. 微电子学与计算机, 2009, 26(1): 155-158.

[5] 张敏, 于剑. 基于划分的模糊聚类算法[J]. 软件学报, 2004, 15(6): 858-868.

[6] Podilbuk C I, Delp E J. Digital watermarking algorithms and application [J]. IEEE Signal Processing Magazine, 2001, 18(4): 33-46.

[7] 赵华, 王志坚, 袁盾韬. 基于小波系数关系的半脆弱水印方案[J]. 微电子学与计算机, 2007, 24(7): 53-55.

作者简介:

张 民 女, (1972-), 硕士, 讲师. 研究方向为信息安全、图像处理.

郭玉彬 女, (1973-), 博士. 研究方向为网络安全、计算机应用技术.

(上接第 138 页)

[6] Josang A, Pope S. Semantic constraints for trust transitivity [C]// Proceedings of the 2nd Asia-Pacific Conference on Conceptual Modelling (APCCM2005). Newcastle, NSW, Australia, Australian Computer Society, 2005: 59-68.

作者简介:

马国富 男, (1974-), 硕士, 讲师. 研究方向为信息安全.

王子贤 男, (1980-), 硕士, 讲师. 研究方向为网络安全.

董彦军 男, (1974-), 硕士, 讲师. 研究方向为网络安全.