一个基于信任的 P2P 访问控制模型

刘义春
LIU Yi-chun

广东商学院 广东省电子商务重点实验室,广州 510320
Guangdong Key Lab of Electronic Commerce,Guangdong University of Business Studies,Guangzhou 510320,China
E-mail:liuyichun@126.com

LIU Yi-chun.Trust-based P2P access control model.Computer Engineering and Applications,2008,44(1):145-147.

Abstract: Most of existing access control models have been studied in centralized and static environment,and they don't meet the requirements of some collaborative environments in which the subjects and objects vary dynamically.In this paper,the trust mechanism of P2P network is analyzed,a scheme is introduced for calculating the peer's trust value by considering the transaction context factors,and a dynamic trust-based access control model is developed to address to the access security in P2P environments.This scheme constructs access control system based on trust degree of P2P members,and dynamically manages the access permission according to the trust values of subjects and objects.The concrete strategies are given for access control of different access services in P2P applications.

Key words: access control;P2P system;trust;access permission

摘 要:多数访问控制模型都针对集中式的和相对静态的系统,不适宜主客体动态变化的协同环境。文章分析了 P2P 系统的信任机制,介绍了考虑事务上下文因素的信任度计算方法,提出一种基于信任的动态访问控制模型 dTBAC,以解决 P2P 环境的安全问题。该模型从网络个体信任的角度建立访问控制体制,根据主客体的信任值对访问权限进行动态管理。文章还就 P2P 应用中不同的访问服务类型给出了具体的访问授权策略。

关键词:访问控制;P2P 系统;信任;访问权限
文章编号:1002-8331(2008)01-0145-03 **文献标识码**:A **中图分类号**:TP309

访问控制是 ISO 网络安全体系标准(ISO7498-2)定义的五大安全服务之一。目前被广泛研究和应用的访问控制模型主要有自主型的访问控制 DAC[1]、强制型的访问控制 MAC[1]和基于角色的访问控制 RBAC[2,3]。这些访问控制模型主要针对集中式的和相对静态的系统环境。访问主体、客体和资源相对静态,授予某主体对一客体的访问权限在一定时期内相对固定。主体一般为客户端进程或用户,客体一般为服务器端资源。这类访问模式显然不适宜于主客体动态变化的协同系统[4],如 P2P 系统。

在 P2P 系统中,所有的个体是对等的,具有相同的责任与能力并协同完成任务,对等点之间通过直接互连共享信息和资源,无需依赖中央服务器或资源就可完成。P2P 系统中,成员个体及其提供资源均为动态,随时可能有成员加入系统、退出系统。个体既可能在线,也可能处于离线状态。P2P 系统缺乏中央控制,不宜存在进行角色或权限分配的超级用户和中央控制节点。因此不适宜用分配角色或直接分配权限等方式进行系统资源的访问控制,应针对 P2P 系统的具体特点,确定其访问控制机制。

本文通过对 P2P 系统中安全访问问题的具体分析,针对 P2P 系统的特点,提出一种新的访问控制机制——基于信任的动态访问控制模型(dTBAC),以解决 P2P 网络的安全访问控制问题。

1 P2P 系统的信任机制

1.1 P2P 系统的信任

P2P 系统中的信任指 P2P 个体在访问或服务活动中所表现的可靠性、诚信度、满意度。确定某个体信任状态的途径有两种:通过多次直接进行事务性接触,总结出该个体的信任度;或请 P2P 团队其他成员推荐该个体的信任度[5,6]。基于推荐的信任学习能更加全面了解个体的信任状况,但须考虑推荐者的信任,因为恶意个体的合伙人可能进行不真实的推荐。

恶意的个体可能在若干普通事务中表现良好以抬高其信任度,而在一次重要事务中表现不诚实。因此分析个体以前参与事务所表现的信任状况以确定个体信任值时,需要考虑所参与事务的重要程度,而不能进行简单平均计算。

为了标识某事务对个体信任的影响程度,引入事务影响因子(Transaction Context Factor)的概念。事务影响因子越大,表明该事务对个体信任值的影响越大;反之,该事务对个体信任值的影响越小。如大额交易的事务影响因子大于小额交易,重

基金项目:浙江省自然科学基金(the Natural Science Foundation of Zhejiang Province of China under Grant No.Y106802);浙江省教育厅资助科研课题(the Research Project of Department of Education of Zhejiang Province,China under Grant No.20060239)。

作者简介:刘义春(1965-),男,博士,副教授,主研方向:信息安全。

要文件服务的事务影响因子大于普通文件服务。

不同的访问或服务对个体的信任状况要求不同,例如写访问对个体信任要求高于读访问;机要数据访问则高于一般数据访问。为了应对不同访问服务的不同信任要求,个体的信任度值应分布在某一区间内。如信任度取值于区间[0,1],0 表示绝对不可信,1 表示完全可信。信任值越高,个体被视为越可信。

1.2 P2P 系统的信任度评估

如果与个体 u 直接发生 m 次事件接触,第 i 次接触的满意度为 $S(u,i)$,$S(u,i)\in[0,1]$。$S(u,i)$越大,满意度越高。第 i 次事件的事务影响因子为 $TF(u,i)$,那么通过直接经验得到的个体 u 的信任值可计算如下:

$$T(u)=\frac{\sum_{i=1}^{m}S(u,i)*TF(u,i)}{\sum_{i=1}^{m}TF(u,i)}$$

如果在所有事件中个体均表现令人绝对满意,即对所有 i 均有 $S(u,i)=1$,则 $T(u)=1$,认为 u 绝对可信。

如果从 P2P 团体中其他成员处获得个体 u 的信任推荐,n 为总的事件次数,$p(u,j)$为参与第 j 次事件的推荐者,$S(u,j)$为第 j 次事件中 $p(u,j)$对 u 的满意度,$T(p(u,j))$为推荐者信任值,第 j 次事件的事务影响因子为 $TF(u,j)$,那么基于推荐的信任计算如下:

$$T(u)=\frac{\sum_{j=1}^{n}S(u,j)*T(p(u,j))*TF(u,j)}{\sum_{j=1}^{n}T(p(u,j))*TF(u,j)}$$

如果所有推荐者都对个体绝对满意,即对所有 j 均有 $S(u,j)=1$ 时,则 $T(u)=1$,认为个体 u 绝对可信。

如果既考虑与个体 u 直接接触所总结的信任度,又综合其他个体的推荐信任,则对直接接触所得的信任值和基于推荐所得信任值进行加权平均,即选定一权值 $\alpha\in(0,1)$,计算:

$$T(u)=\alpha*\frac{\sum_{i=1}^{m}S(u,i)*TF(u,i)}{\sum_{i=1}^{m}TF(u,i)}+(1-\alpha)*\frac{\sum_{j=1}^{n}S(u,j)*T(p(u,j))*TF(u,j)}{\sum_{j=1}^{n}T(p(u,j))*TF(u,j)}$$

按照上述方法计算 P2P 网络中个体的信任度,既分析与个体直接接触所获得的信任信息,又综合其他个体的推荐信任,还考虑了事件重要程度对信任的影响,可以较客观、准确地获得目标个体的信任值。

2 基于信任的访问控制模型

在传统的集中式系统或 C/S 系统中,要求对访问者身份进行认证及根据其身份或角色进行权限授予,访问控制体现针对访问主体的控制。而在 P2P 环境中,访问控制同时针对访问主体和客体,特定的访问操作要求主体或客体具有特定的信任等级,或主体客体双方都具有一定的信任等级。

2.1 dTBAC 术语定义

实体(Entity):P2P 系统中的成员及其进程、程序、作业或资源。

主体(Subject):可对其他实体实施操作的主动实体。主体可以是 P2P 成员、进程、程序或作业等。

客体(Object):接受其他实体访问的被动实体,可以是 P2P 成员或 P2P 成员拥有的某特定资源。一粗粒度客体(P2P 个体或多播组)可包含多个较细粒度客体(目录、文件、页面、元组、视图等)。

操作(Operation):主体对客体进行的原子动作(如读、写、浏览、执行、选择等)的序列。

权限(Permission):对客体进行特定访问的许可。

信任值(Trust Value):在 P2P、网格等协同计算环境中,对个体在访问或服务活动中所表现的可靠性、诚信度、满意度的综合评价。

信任阈值(Trust Threshold):个体获得特定操作权限所需的最小信任值。当个体信任值低于进行某种操作所需阈值时,将被视为信任不够而被拒绝进行该操作。

上下文环境(Context):影响信任值和访问控制的环境因素,如被访问客体的重要性、推荐信任的实体的信任值、通信信道带宽、信任刷新周期等。

2.2 dTBAC 模型的描述

定义 1 dTBAC 模型是如下元素组成的多元组:

E 是 P2P 实体集合;

$S\subseteq E$ 是 P2P 主体集合;

$O\subseteq E$ 是 P2P 客体集合;

OP 是对客体资源的操作集合;

$TV:E\rightarrow[0,1]$(实体信任值计算);

$TT\_S:O\times OP\rightarrow[0,1]$ (对客体进行某操作所需主体的信任阈值);

$TT\_O:S\times OP\rightarrow[0,1]$ (主体进行某操作所需客体的信任阈值);

$F:S\times O\times OP\rightarrow\{0,1\}$(访问授权规则)。

在 dTBAC 模型中,映射 $F:S\times O\times OP\rightarrow\{0,1\}$表示将主体对客体进行某操作的权限映射到{0,1}集合。其中 1 表示该访问获许进行,0 则意味着未获许可。

定义 2 基于信任的访问控制策略如下:

$\forall s\in S,o\in O,op\in OP$,

$F(s,o,op)=TV(s)\geqslant TT\_S(o,op)\wedge TV(o)\geqslant TT\_O(s,op)$

当主体信任值不小于对客体进行操作所需信任阈值,并且客体信任值不小于主体进行操作所需信任阈值时,访问权限映射为 1,准许主体访问客体;否则访问权限映射为 0,禁止主体对客体进行访问。

文中约定逻辑运算的结果为 1(真)或 0(假)。

基于信任的访问控制机制从应用和网络全局的角度解决安全问题。由于成员间的信任并非静止不变的,随着上下文环境变化而变化,需要定期刷新,因而来自同一用户的访问权限会发生相应变化。

3 dTBAC 在 P2P 访问中的应用

在 P2P 系统中,实体间具有多种访问方式,如读、写、存储、浏览、发布、下载、执行、视图、链接等,每种访问方式所对应的访问控制各不相同[7,8]。下面根据对实体信任需求的不同,以几种常见的访问为例,说明 dTBAC 的具体应用。

3.1 基于主体信任值的访问控制

在 P2P 网络中,主体从客体处读数据时,客体需要评估访问主体的信任,只有当主体的信任值不低于从客体获取文件所需信任阈值时,主体才被获准进行读访问。在读操作中,对客体的信任等级无特别要求,所需客体信任阈值 $TT\_O(s,\text{“}read\text{”})=0$。在读访问情形下,访问控制策略为:

$$\forall s\in S,o\in O$$

$$F(s,o,\text{“}read\text{”})=TV(s)\geqslant TT\_S(o,\text{“}read\text{”})$$

对文件编辑、删除时与读访问情形相同,只要求主体具有必要的信任等级。

3.2 基于客体信任值的访问控制

在 P2P 系统中,主体将其文件存于客体处时,主体需要评估客体的信任值。主体希望能将文件存放在一个非恶意、健壮的、值得信任的客体节点,以确保存放的文件不会被恶意修改、删除或发生系统崩溃。主体将会评估客体的信任等级,只有当客体的信任值高于存放文件所需信任阈值时,主体才会在客体存放文件。存放一个重要文件所要求的客体信任等级较存放一个普通文件要高。

$$\forall s\in S,o\in O$$

$$F(s,o,\text{“}store\text{”})=TV(o)\geqslant TT\_O(s,\text{“}store\text{”})$$

3.3 基于主体和客体信任值的访问控制

在 P2P 系统中,主体将其文件在共享服务器处发布时,主体和客体都需要评估对方的信任值。主体希望能将文件在一个非恶意、健壮的、值得信任的服务器节点发布,以确保信息不会被恶意修改、删除或发生系统崩溃,而能安全地发布信息;客体则希望主体是可信任的,不会发布不法宣传品、色情内容或病毒、木马等恶意信息。主体会评估客体的信任等级,只有当客体服务器的信任值高于发布信息所需信任阈值时,主体才会在该服务器信息发布;同样,客体也会评估主体的信任等级,只有当主体的信任值高于客体服务器发布信息所需信任阈值时,主体才被获准在客体发布信息。

此类操作情形下,访问控制策略为:

$$\forall s\in S,o\in O$$

$$F(s,o,\text{“}publish\text{”})=TV(s)\geqslant TT\_S(o,\text{“}publish\text{”})\wedge TV(o)\geqslant TT\_O(s,\text{“}publish\text{”})$$

文件的执行操作类似,需要主客双方分别具有一定的信任等级,既防止未授权主体对客体的非法执行,又防止恶意客体用恶意程序假冒合法执行资源。

4 结论

由于 P2P 系统具有无中央机构、全分布、动态、异构等特点,传统的访问控制机制不能很好地解决 P2P 系统中的访问控制问题。本文提出一种新的访问控制模型——基于信任的动态访问控制 dTBAC, 用以解决 P2P 网络等新一代分布式系统的访问控制问题。在进一步的研究中,可以利用 dTBAC 并结合基于角色的访问控制模型、访问认证等安全机制,解决复杂系统的访问控制问题。(收稿日期:2007 年 7 月)

参考文献:

[1] Snyder L.Formal models of capability-based protection systems[J]. IEEE Transactions on Computers,30(3):172-181.

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

[3] Ferraiolo D F,Sandhu R,Gavrila S.Proposed NIST standard for role-based access control[J].ACM Transactions on Information and System Security,2001,4(3):224-274.

[4] Shen H,Dewan P.Access control for collaborative environments[C]// Proceedings of ACM Conference on Computer-Supported Cooperative Work(CSCW'92).ACM Press,1992:51-58.

[5] Xiong L,Liu L.A reputation-based trust model for peer-to-peer e-commerce communities[C]//Proceedings of IEEE International Conference on E-Commerce 2003.IEEE Press,2003:275-285.

[6] Wang Y,Vassileva J.Trust and reputation model in peer-to-peer networks[C]//Proceedings 3rd International Conference on Peer-to-Peer Computing.IEEE Press,2003:150-157.

[7] Kagal L,Finin T,Joshi A.Trust-based security in pervasive computing environments[J].IEEE Computer,2001,34(12):154-157.

[8] Li N,Mitchell J C,Winsborough W.Design of a role-based trust management framework[C]//Proceedings of the 2002 IEEE Symposium on Security and Privacy.IEEE Press,2002:114-131.

(上接 102 页)

力、缓解网络攻击所造成的危害、发现潜在恶意的入侵行为、提高系统的反击能力等具有十分重要的意义,对于未来的军事信息战意义更重大。国内目前对态势感知系统的研究才刚刚起步,相关理论和技术还很不成熟。本文在深入分析国内外相关研究后,建立了网络安全态势感知概念模型和体系结构,分析研究构成网络安全态势感知系统的数据的特征提取、网络安全评估、网络应急响应、网络安全预警等重要组成部分。网络态势感知中诸如海量网络数据的实时处理、数据融合、态势评估、威胁评估、态势可视化等方面均有许多问题需要研究。

(收稿日期:2007 年 9 月)

参考文献:

[1] Bass T,Gruber D.A glimpse into the future of id[EB/OL].(1999). http://www.usenix.org/publications/login/199929/features/future.html.

[2] Carnegie Mellon's SEI.System for Internet Level Knowledge(SILK)[EB/OL](2005).http://silktools.source forge.net.

[3] Office of The Secretary of Defense(OSD) deputy director of Defense Research & Engineering Deputy Under Secretary of Defense (Science & Technology).Small Business Innovation Research(SBIR) FY 2005.3 Program Description,USA.

[4] LIU Huan,Setiono R.A probabilistic approach to feature selection[C]// Proceedings of Internatinoal Conference on Machine Learning.Morgan Kaufmann Publishers,1996:319-327.

[5] Liu Huan,Setiono R.Scalable feature selection for large size database[C]//Proceedings of the Fourth World Congress on Expert Systems.Morgan Kaufmann Publishers,1998.

[6] 毛捍东,陈锋.信息安全风险评估方法研究[C]//中国信息协会信息安全委员会年会集,2004.

[7] Lee C P,Trost J,Gibbs N,et al.Visual firewall:real-time network security monitor[C]//Visualization for Computer Security VizSEC 2005.IEEE,2005.

[8] Rabiner L R.A tutorial on hidden Markov models and selected applications in speech recognition[J].Proceedings of the IEEE,1989, 77(2):257-289.