第 33 卷 第 6 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.6 Computer Engineering March 2007
·安全技术· 文章编号：1000—3428(2007)06—0132—02 文献标识码：A 中图分类号：TP309

自动信任协商在 P2P 系统中的应用

冯 真，张红旗，刘育楠
(信息工程大学电子技术学院，郑州 450004)

摘 要：由于 P2P 系统具有分布性、开放性等特点，传统的访问控制和认证的方法不能很好地在 P2P 系统中适用。一些专门解决 P2P 系统中的信任问题的声誉系统也存在着容易被虚伪的节点所攻击的缺陷。文章研究了自动信任协商机制如何通过互相出示证书的方法合理地解决了 P2P 系统中的访问控制和认证问题，针对自动信任协商中存在策略循环依赖的问题使用建立 LTTP 的方法加以解决，并通过模拟实验证明 LTTP 的确能够提高信任协商的成功率。

关键词：信任；声誉系统；自动信任协商；策略循环依赖；局部可信第三方

Application of Automated Trust Negotiation in P2P System

FENG Zhen, ZHANG Hongqi, LIU Yunan
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 As P2P system is inherently decentralized and open, some traditional access control and authentication approaches cannot be adapted in P2P system. Some reputation systems which aim to solve the trust problem in P2P system may be easily attacked by some hypocritical peers. This paper researches on automated trust negotiation mechanisms which use exchanging credentials to completely solve the access control and authentication problems in P2P systems, builds LTTP to solve the cyclic interdependent policies problem in ATN, experiments prove that LTTP can improve the success rate of ATN.

【Key words】 Trust; Reputation system; Automated trust negotiation; Cyclic interdependent policies; Local trusted third party

1 概述

P2P 系统的分布性和开放性等特点使得 P2P 系统中的认证和访问控制变得异常复杂。传统的一些授权方法面临着一些新的问题：(1)传统的一些方法如访问控制列表(Access Control List，ACL)等都是基于访问主体是已知的假设，而 P2P 系统中 Peer 的身份往往是未知的；(2)传统的 C/S 和 B/S 模式中，一般是服务器认证客户端，只有客户端通过认证和授权才能访问服务器的资源。而 P2P 系统中的节点同时拥有服务器和客户端的身份，而且一个节点可以选择从哪个资源提供者处访问资源，因此往往也需要资源请求者对资源提供者进行一定的认证。

一些学者提出使用信任管理的方法来解决分布式系统的访问控制等问题，他们大多是通过建立一个声誉系统来管理信任，这种系统通常是将本节点的经验与其它节点的推荐结合起来而得出对目标节点的一个信任度，依据这个信任度来进行授权。这种方法也存在一些问题：

(1)声誉系统中的节点要求必须使用真实的身份，如现实中的姓名。这样才能有效地将身份与信任度对应起来。而在一些 P2P 系统中，有些节点可能更愿意匿名地加入系统。

(2)有些节点由于是初次进入 P2P 系统中，会因信任度偏低而被拒绝服务或服务质量得不到保证。

(3)对于处理一些非常敏感的信息，如高额的电子贸易等时，存在一定的风险。有些节点可能会通过多次诚实的小数额交易来骗取高的信任度而进行一次大数额的诈骗。

本文对自动信任协商(Automated Trust Negotiation，ATN)作了深入的分析，认为自动信任协商可以很好地克服声誉系统中存在的一些问题。如果将自动信任协商与声誉系统很好地结合起来，必定可以建立一个更加完善的信任管理系统。

2 相关工作

最常见的声誉系统有 eBay、Yahoo Auction 等，这些系统通过收集与卖方交易过的一些买方的评价而为每个卖方形成一个综合的信任度来指导以后的交易。这些信任度的信息保存在 eBay 网的一些服务器上。

Aberer 和 Despotovic 在文献[1]中比较早地提出了以分布的方法来管理 P2P 系统中的信任。他们通过分析节点以前的一些交易来计算出一个声誉值。论文重点研究了 3 个问题：计算节点信任度的全局信任模型(global trust model)；分布式数据管理(decentralized data management)方法用于保存计算信任相关的数据；节点本地计算信任的一个算法。

Ye Song, William H, Yu Ting 等在文献[2～4]中都对自动信任协商进行了详细的介绍，自动信任协商的提出是为了解决分布式系统中的访问控制和认证的问题。它通过在不同节点之间互相出示证书来建立信任。

Li Ninghui 等提出了一个节点间相互签名认证的方法[5]，称为OEBS(Oblivious Envelope-Based System)来解决信任协商时策略循环依赖的问题，OEBS中要求证书必须是由同一个权威机构所颁发的。

3 自动信任协商

自动信任协商是一种解决开放的分布式环境下访问控制和认证问题的方法，自动信任协商为每个资源赋予若干条策

作者简介：冯 真(1982－)，男，硕士生，主研方向：计算机网络安全；张红旗，教授；刘育楠，硕士、副教授
收稿日期：2006-03-28 **E-mail：**fzhen@126.com

略，节点依据这些策略来对该资源进行访问[2]。每一条策略是一个由若干证书通过逻辑运算形成的表达式。如R←C_1∧C_2，表示只有当访问者出示证书C_1和C_2时，才允许其访问资源R。

3.1 证书的组成

证书是由权威机构数字签名了的断言组成，该断言包含若干条属性及对应的属性值。签名保证了这些属性的真实性、不可伪造性和可验证性。

签名采用非对称密钥算法，如 RSA。在非对称密钥算法中，密钥由一对公私钥组成，其中公钥公开，私钥保密。由公钥加密的数据必须由对应的私钥才能够解开，相反由私钥加密的数据必须使用对应的公钥解密。

在签名的时候由颁发者使用自己的私钥对所签名的数据加密，因为任何人都可以拥有颁发者的公钥，所以很容易对证书进行验证。而只有颁发者自己拥有私钥，从而保证了证书的不可伪造。只要信任颁发者的公正，那么就可以信任证书的内容。

3.2 策略的组成

策略有两种类型：资源访问策略和证书访问策略。

使用如文献[4]中的表达方式，资源访问策略为P_R←F_R(C_1, C_2, …, C_k)，证书访问策略为P_C←F_C(C_1, C_2, …, C_k)。其中F_R(C_1, C_2, …, C_k)和F_C(C_1, C_2, …, C_k)是由证书C_1, C_2, …C_k等通过∧和∨运算(必要时可以加括号)得到的布尔表示式，只有当对方出示C_i时C_i为真，当表达式为真时才出示箭头左边的资源或证书。

特别是在当箭头右边的表达式直接为 true 时，表示资源或证书公开，为 false 时为不公开。

3.3 信任协商的过程

假定P2P系统中有P_1, P_2, …, P_n等n个节点，每个节点P_i只拥有一个资源R_i，不存在恶意的节点，所有节点都信任全局可信第三方(global trusted third party，GTTP)所签发的 证书。下面以一个例子来说明信任协商的过程，其中$C_i^{P_i}$表示P_i的第i个证书。

P_1的策略为：

$R_1 \leftarrow C_1^{P_2} \wedge C_2^{P_2}$

$C_2^{P_1} \leftarrow C_1^{P_2}$

$C_1^{P_1} \leftarrow C_3^{P_2} \wedge C_4^{P_2}$

$C_3^{P_1} \leftarrow C_3^{P_2}$

$C_4^{P_1} \leftarrow true$

P_2的策略为：

$C_2^{P_2} \leftarrow C_1^{P_1} \wedge C_2^{P_1}$

$C_1^{P_2} \leftarrow C_1^{P_1}$

$C_3^{P_2} \leftarrow true$

$C_4^{P_2} \leftarrow true$

如果相互出示证书的序列为：$\{C_3^{P_2}, C_4^{P_2}\}, \{C_1^{P_1}\}, \{C_1^{P_2}\}, \{C_2^{P_1}\}, \{C_2^{P_2}\}, \{R_1\}$，则$P_2$可以成功地访问到$P_1$的资源$R_1$。

这个序列中大括号内的证书分别为P_2和P_1依次所出示的，首先P_2出示证书$C_3^{P_2}$和$C_4^{P_2}$后，满足了P_1的策略$C_1^{P_1} \leftarrow C_3^{P_2} \wedge C_4^{P_2}$，$P_1$会向$P_2$出示证书$C_1^{P_1}$，同理，$P_2$会出示证书$C_1^{P_2}$，直到$P_2$被允许访问资源$R_1$。可以发现这个序列中没有用到$P_1$的证书$C_3^{P_1}$，其实，上面提出的序列是$P_2$访问资源$R_1$时交换证书最少的序列。任何包含该序列的序列都能够协商成功。

可以看出，信任协商的方法与Blaze所提出的KeyNote信任管理系统[6]在访问控制方面相比有明显的优点：(1)提供了对证书的保护，只有当对方出示某些证书后使策略满足时才会出示自己的证书，这样证书就不会随便地出示给一些不相关节点；(2)加入了对资源提供者的认证，资源提供者需要提供一定的证书才能使得协商继续。

4 策略循环依赖问题及解决方法

4.1 策略循环依赖的产生

在这面的例子中，如果P_2的第 2 条策略改为$C_1^{P_2} \leftarrow C_2^{P_1}$，则$P_1$、$P_2$之间的信任协商不会成功，因为策略$C_1^{P_2} \leftarrow C_2^{P_1}$与$P_1$的策略$C_2^{P_1} \leftarrow C_1^{P_2}$导致了策略循环依赖(cyclic interdependent policies)问题。P_1要求P_2先出示证书$C_1^{P_2}$，而P_2要求P_1先出示证书$C_1^{P_2}$，这样谁都不肯先出示对方所需证书，形成了一种类似死锁的僵局，导致协商没法继续。

4.2 解决方法

文献[2]中提出，策略循环依赖问题可以通过建立一个局部可信第三方(local trusted third party，LTTP)来解决。这个局部可信第三方是一个P_1和P_2都信任的节点，如P_3。如果P_1和P_2的协商没法继续，那么P_1和P_2都将它们的策略和已经出示过的证书发送给P_3。P_3中会事先保存有P_1和P_2的一些证书，如果P_3发现有策略循环依赖问题，P_3会向P_1或P_2发送导致此问题的证书，如P_3向P_1发送P_2的证书$C_1^{P_2}$，这样信任协商就可以顺利完成。

在上面的解决方法中首先要解决的一个问题就是如何找到一个双方都信任的第三方，一种最简单的方法就是其中一个节点P_1把自己相信的所有LTTP的名称都发送给P_2，然后P_2从中找出自己也信任的LTTP。这种方法存在的一个缺陷是，P_1的可信第三方的信息完全向P_2公开了，这并不一定是P_1所期望的。

这个问题可以这样解决，P_1分别以它信任的每个LTTP的名称的哈希值为密钥对相应LTTP的名称加密，将密文发给P_2，P_2使用它信任的每个LTTP的名称的哈希值对每段密文解密，如能得到此LTTP的名称，说明此LTTP为P_1和 P_2所共同信任的，这样避免了暴露P_1的LTTP信息。

5 实验结果

我们使用 PeerSim 分别对未使用 LTTP 和使用 LTTP 的 P2P 系统进行模拟，模拟了 1 000 个节点的情况，每个节点仅有一个资源，每个节点的证书数为小于 10 的一个随机数，随机生成了几条策略，重复实验了 10 次，取平均值作图，结果如图 1，可以看出，使用 LTTP 后协商成功率会明显上升。

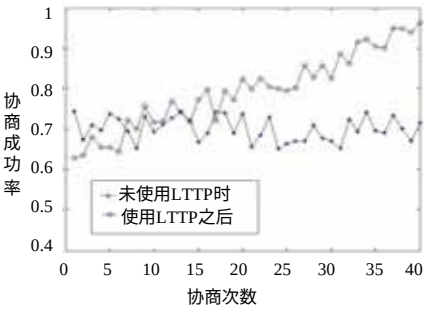

图 1 使用 LTTP 和未使用 LTTP 时协商成功率对比

(下转第 160 页)