第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)17—0139—02 文献标识码：A 中图分类号：TP391

基于改进策略库的资源敏感保护机制

孔华锋[1,2]，鲁宏伟[1]，刘百灵[1]
(1. 华中科技大学计算机科学与技术学院，武汉 430074；2. 华中科技大学图像识别与人工智能研究所，武汉 430074)

摘 要：自动信任协商是陌生实体之间通过请求和披露信任进而逐步建立信任关系的重复过程，其中资源的拥有敏感保护已经引起了广泛的关注。该文给出关联属性的形式化定义，提出关联属性保护策略的层次契约模型，基于以上理论，通过在策略库系统中设置一个契约中间件达到信息拥有敏感保护的目的。

关键词：策略库；关联属性；层次模型

Protection Mechanism of Possession Sensitive Attributes Based on Improved Policy Database

KONG Hua-feng[1,2], LU Hong-wei[1], LIU Bai-ling[1]
(1. School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074;
2. Institute of Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan 430074)

【Abstract】 Automated trust negotiation is an iterative process that establishes trust gradually between strangers by requesting and disclosing digital credentials. Protection of sensitive information in automated trust negotiation has been drawn much attention. In order to solve this problem, formal definition of relevant attributes is given. Relation model of relevant attributes is designed. A desideratum of policy for relevant attributes based on the relation model is presented. And the desideratum is enforced in a relevance contractor, which is an addition to the policy database system as improvement. The relevance contractor is used to check whether the policies satisfy the desideratum.

【Key words】 policy database; relative attribute; hierarchy model

1 概述

近年来随着Internet的发展，基于单个管理域和集中式管理的传统访问控制已经不再适用。文献[1]提出了自动信任协商(Automated Trust Negotiation, ATN)的概念。在ATN的研究中，敏感信息的保护至关重要。目前所涉及到的敏感信息不外乎两大类：资源的内容敏感和资源的拥有敏感[2]。在理想的情况下，只有当服务请求方满足服务提供方的访问控制策略，才能获得该访问控制策略所保护的信息。但是在实际应用中，仅靠访问控制策略来控制信息的披露还无法保证对敏感信息的严格保护。服务请求方可能还未满足服务提供方对于某一敏感信息的访问控制策略，就非授权获得该敏感 信息[3]。

为了解决资源的拥有敏感问题，文献[4]提出了一种非响应的方法，将属性策略的披露与该属性的拥有关系独立起来。文献[5]基于合适的对象讨论敏感话题的原则，提出了 ACK 策略，只有当敏感属性对应的 ACK 策略被对方满足，另一方才会承认自己是否拥有该属性。该方法保护了属性的拥有敏感，但是它要求所有用户对于某一特定属性都使用相同的 ACK 策略，这无疑破坏了自动信任协商的自治性。

为了既保护属性的拥有敏感，又不破坏自动信任协商的自治性，文献[6]提出了策略库(policy database)，拥有敏感属性的人将自己的策略匿名提交给策略库，而不拥有该敏感属性的用户从库中随机抽取相应的保护策略。但是，策略库依旧存在因概率推理而导致资源拥有敏感信息泄露的情况。

本文提出一种基于改进策略库的资源拥有敏感保护机制来解决以上问题，通过对改进的策略库进行安全性和可行性分析，证明改进后的策略库安全性更好，并且是可行的。

2 策略库

ATN 中的策略库是一个由可信任的第三方运行的策略库，该策略库收集策略库系统中用户保护敏感信息的策略。采用策略库的目的在于确保敏感信息的策略存在于不同的推理组件，从而达到系统对拥有敏感属性的保护。但是策略库存在着因概率推论而导致资源的拥有敏感信息泄露的情况。

3 改进策略库

3.1 关联属性

定义 1 对于任意属性 a 和 b，如果它们之间存在以下4种关系中的任何一种，就称属性 a 和属性 b 互为关联属性，其中属性 a 为主动关联属性，属性 b 为被动关联属性。

(1)$b \leftarrow a$。若资源请求方知道资源提供方拥有属性 a，那么资源请求方可以以很大的概率推理出资源提供方同时也拥有属性 b。

(2) $\neg b \leftarrow a$。若资源请求方知道资源提供方拥有属性 a，那么资源请求方可以以很大的概率推理出资源提供方不拥有属性 b。

(3)$b \leftarrow \neg a$。若资源请求方知道资源提供方不拥有属性 a，那么资源请求方可以以很大的概率推理出资源提供方拥有属性 b。

(4) $\neg b \leftarrow \neg a$。若资源请求方知道资源提供方不拥有属性

作者简介：孔华锋(1974－)，男，讲师、博士后，主研方向：计算机网络，多媒体技术，信息安全；鲁宏伟，教授、博士；刘百灵，硕士研究生

收稿日期：2007-09-15 **E-mail：**robin_kong@126.com

a，那么资源请求方可以以很大的概率推理出资源提供方不拥有属性 b。

3.2 关联属性保护策略的层次契约模型

定义 2 设关联属性的保护策略为集合 $Pi(i>0)$, $\forall a>0, b>0$，若 $\exists Pa \supset Pb$，则称策略 Pa 比策略 Pb 严格。

定理 1 $\forall Pa, Pb$，若 Pa 和 Pb 同样严格，那么策略 Pa 和策略 Pb 相等。

证明 因为 Pa 和 Pb 同样严格，所以 $Pa \supseteq Pb, Pb \supseteq Pa$，又由集合之间的关系可得，策略 Pa 和策略 Pb 相等。

定义 3 对任意策略 Pa 和 Pb，若 Pa 比 Pb 严格，就将其关系表示为 $Pa>Pb$；若两策略同样严格，则表示为 $Pa=Pb$；否则表示为 $Pa<Pb$，在本文中<、=、>、≤、≥叫做层次关系符。

定理 2 对于属性 a 和属性 b，如果它们之间互为关联属性，且 a 为主动关联属性，b 为被动关联属性，那么保护 a 的拥有敏感信息的策略 Pa 至少和保护 b 的拥有敏感信息的策略 Pb 同样严格，即 $Pa \geq Pb$。

证明 假设 Pb 比 Pa 严格，即 $Pa < Pb$，由定义 1 可知，若已知主动关联属性 a 的拥有情况，那么就可以以很大的概率推理出被动关联属性 b 的拥有情况。根据假设 Pb 比 Pa 严格，即满足 Pb 一定可以满足 Pa，而满足 Pa 未必能够满足 Pb，换言之，如果知道了被动关联属性 b 的拥有情况，就可以知道主动关联属性 a 的拥有情况，这与定义 1 相矛盾，因此，假设不成立。

定义 4 对于任意属性，若它们互为关联属性，那么它们的保护策略之间存在着定理 2 所叙述的关系，这种关系叫做层次关系。将互为关联属性的保护策略用层次关系联系起来，并且严格的策略在次严格策略的上层，即上层保护策略>下层保护策略，那么称其为层次契约模型。

例如：$Pa>Pb, Pa>Pc, Pb>Pd$，那么对应的层次契约模型如图 1 所示。

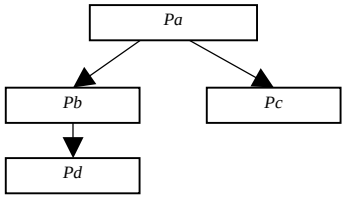

图 1 层次契约模型

根据定理 1 可知，在层次契约模型中，上层保护策略包含下层保护策略，下层策略包含于上层策略，互为关联属性的策略之间都存在着包含与被包含关系。

3.3 契约中间件

基于以上理论，笔者在策略库中设置契约中间件，主要通过比较策略之间的包含与被包含的契约关系来实现层次关系的检测与比较。例如若用户提交的策略经过契约中间件，它就用来检测所提交的策略之间是否存在层次关系，即检测是否存在包含与被包含的契约关系；若是在随机提取策略的时候用到，它就用来比较策略的层次契约关系，并根据检测或比较的结果采取相应的措施。

3.4 改进的策略库系统

策略库系统的工作分为 2 个阶段。

(1)用户制定提交策略阶段包括 2 种情况：

1)若用户拥有的属性不是互为关联属性，那么改进的策略库系统仍然保持原系统的处理方式不变。

2)当用户拥有的某些敏感属性互为关联属性时，需要对原策略库系统做如下改进：为了更好地保护属性的拥有敏感，要求用户在制定其保护策略的时候，参照关联属性保护策略的层次契约模型，并将制定好的策略一并匿名提交给策略库，策略库通过验证后，用契约中间件检测这些策略相互之间是否存在包含与被包含的关系，如果存在，系统将给这同时提交的策略附加一个相同的 ID 号，并存入策略库中，若检测到相同的策略，就只将其中一个策略存入策略库中，这有利于系统的安全性，其原因将在第 4 节中具体分析。若契约中间件检测出它们之间没有包含关系，就不做任何处理，系统还是把它们存入策略库中。

其中，系统根据用户一次提交的策略数目判断是否需要通过契约中间件，若一次提交一个策略，不用契约中间件，否则，要通过契约中间件的检测。

(2)用户提取策略阶段可能出现 3 种情况：

1)当用户要提取的属性策略之间没有层次关系时，还是采用原策略库的处理方式。

2)用户从策略库中随机提取一个特定属性的策略来保护自己资源的拥有敏感后，又需要提取和它互为关联属性的保护策略时，如果用户先前取出的策略存在一个 ID 号，那么用户就会将 ID 和这 2 个属性策略的层次关系(> 或 <)告诉策略库系统，那么策略库系统会先找与该 ID 号相同的给定属性的策略，并提取给用户；若没有，系统将会像原策略库那样随机地提取指定属性的策略，并在契约中间件里按用户给出的层次关系进行比较，若满足，提交给用户，否则，重新提取。若重新提取的次数为 2 次，系统将会提示用户使用先前提取的与该属性互为关联属性的策略保护该属性。当用户已有某一个敏感属性，但需要一个与它互为关联属性的策略时，也按上述的不存在 ID 号的情况处理。

3)当用户同时需要多个属性的保护策略，并且这些属性互为关联属性时，系统就在策略库中搜索具有相同 ID 号的特定属性的策略。如果没有，就先后从策略库中随机提取，利用契约中间件控制它们的层次关系，具体的操作与上面类似。

4 安全性分析

4.1 安全性定义

定义 5 如果服务请求方在满足服务提供方的保护策略之前无法通过关联属性、策略之间的关系和所披露的策略推理出任何拥有敏感信息，那么就称该系统是安全的。

4.2 改进策略库的安全分析

根据定义 5 来分析改进策略库的安全性。从服务提供方和服务请求方来看，由于改进只是针对互为关联属性的情况，因此非关联属性的情况不需要进行分析。

在服务提供方：

(1)在策略提交时，层次契约模型的引入保证了策略的层次关系。

(2)在存储时，契约中间件的引入保证了存储的关联属性的保护策略都具有层次关系。

(3)在提取时，ID 号和契约中间件的引入保证提取的策略之间满足层次契约模型，从而不会产生因关联属性和策略之间的关系的推理而造成的敏感信息的泄露。

在服务请求方(敌手)：

(1)由于对方披露的属性满足层次契约模型，因此不能通过关联属性和策略之间的关系推出对方对敏感属性的拥有情况。 （下转第 143 页）