

文章编号:1001-9081(2007)06-1349-04

## 面向 C2C 的基于声誉的信任模型设计与分析

荆博贤<sup>1,2</sup>,徐 锋<sup>1,2</sup>,王 远<sup>1,2</sup>,吕 建<sup>1,2</sup>

(1. 南京大学 计算机软件新技术国家重点实验室, 江苏南京 210093;

2. 南京大学 计算机软件研究所, 江苏南京 210093)

(jbx@ics.nju.edu.cn)

**摘要:**现有的信任模型或基于信任链,不能充分利用门户网站上丰富的推荐信息;或缺乏对推荐信息有效性的分析,不能很好地应对信任炒作和诽谤。将以往模型进行改进,对推荐信息采用长期分析和短期分析结合的方法,充分利用了推荐信息,并能有效应对信任炒作和诽谤,可以更好地辅助 C2C 电子交易系统的用户进行决策。

**关键词:**C2C; 电子商务; 声誉; 信任; 防炒作; 模型

**中图分类号:** TP393.08      **文献标识码:**A

### Design and analysis of C2C-oriented and reputation-based trust model

JING Bo-xian<sup>1,2</sup>, XU Feng<sup>1,2</sup>, WANG Yuan<sup>1,2</sup>, Lü Jian<sup>1,2</sup>

((1. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing Jiangsu 210093, China;

Institute of Computer Software, Nanjing University, Nanjing Jiangsu 210093, China)

**Abstract:** Current trust models either use trust chain which cannot make the best of the recommendation information on the Web, or lack of analysis on the credibility of the recommendation information which can not deal with the hype and gossip in trust. Based on the models in existence we developed a new trust model that takes recommendation information by both long-term analysis and short-term analysis. It takes full advantage of the recommendation information and can effectively stand against the hype and gossip in trust. This model can help the users of C2C e-business system make better decision.

**Key words:** C2C; e-business; reputation; trust; anti-hype; model

### 0 引言

随着 Internet 的广泛普及,基于网络的 C2C 结构的电子商务系统正受到越来越广泛的关注,用户在享受网上交易带来的方便同时,还需要应对开放网络所带来的各种安全风险。如何在开放环境下进行安全的交易是当前研究的热点问题。一些典型的电子商务系统,如 eBay, Amazon, Taobao 等,其交易方式大体如图 1 所示:电子商务系统运行在一个集中的服务器上,用户通过注册和登陆过程,可在上面发布商品信息,寻找需要购买的商品,并可对商品和交易对方进行评价,评价信息的完整性受到系统保证,其内容的真实性通常也可以通过附加的投诉机制受到系统的有限担保,同时,用户也可方便地获得他人的评价信息。系统通过简单的计算向用户提供交易伙伴的声誉,如总交易成功数量等,使用户对当前交易的风险有初步判断。

但在应用中此类系统存在以下缺点:1)声誉计算过程过于简单,缺乏对时间等因素的关注,不能反映对方的真实声誉。2)多数模型假定评价者是诚实的<sup>[1]</sup>,无法应对信任炒作和诽谤行为的出现。3)评价信息数量多,信息量大,用户不可能完全参照。因此有必要引入合理的易于实现的信任模型辅助用户分析大量的第三方提供的评价信息,并给出合理的

结论帮助用户进行交易决策。而现有的信任模型在声誉计算、结构等方面都不适合在 C2C 电子交易环境下解决上述问题,如文献[2]、PET 模型<sup>[3]</sup>和文献[4]计算声誉值时对推荐信息可信度的处理相对简单,不能有效防止信任炒作;文献[5]、[6]假定推荐者不会炒作或诽谤,使得模型在实际应用中比较脆弱;文献[7]~文献[10]的结构难以应用于有中心机构的网上交易门户系统。并且以上大部分模型在应用中难以应对负面评价带来的“饥饿效应”,违背了 C2C 环境下鼓励交易的原则。

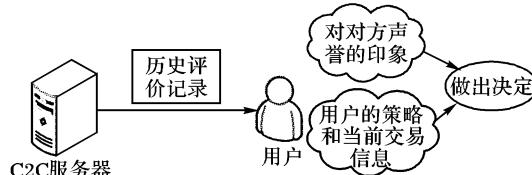


图 1 C2C 电子商务交易方式

本文针对 C2C 电子商务系统的特点,提出了一个新的基于声誉的信任模型。数据处理上,对交易对象历史评价数据进行长期和短期分析,使实体的行为及时反映在声誉值上,并有效防止了“饥饿效应”的发生。在声誉形成过程中依据代价、评价者的交易经验、时间等因素采信交互记录,使声誉值更加合理,可以有效应对信任炒作和诽谤的问题。

收稿日期:2006-12-30

基金项目:国家 973 规划项目(2002CB312002);国家 863 计划项目(2006AA01Z159);国家自然科学基金资助项目(60603034);江苏省自然科学基金资助项目(BK2006712)

作者简介:荆博贤(1983-),男,山东蓬莱人,硕士研究生,主要研究方向:网络安全、信任计算; 徐锋(1975-),男,江苏张家港人,副教授,博士,主要研究方向:可信计算; 王远(1980-),男,山东青岛人,博士研究生,主要研究方向:分布对象技术、可信计算、Web 服务技术; 吕建(1960-),男,江苏人,教授,博士,博士生导师,主要研究方向:软件自动化、面向对象语言与环境和并行程序的形式化方法。

## 1 面向 C2C 的基于声誉的信任模型

电子商务系统中最重要的问题就是如何保证用户交易的安全。尤其在 C2C 模式的电子交易过程中,对方往往是完全陌生的实体,安全问题变得更加突出。目前的研究表明信任是解决开放环境下安全问题的有效途径。关于信任有许多不同的定义,目前被许多人认可的是 Gambetta<sup>[11]</sup> 的定义:信任是在无法监控对方行为的情况下一个实体对另一实体将要进行在某方面影响自己的行为的可能性之主观预测。可以看出信任是主观的,即不同的实体对同一实体的信任不同。其他研究得出信任有两个属性,信任度和确定度。信任度越大表示越信任。确定度表示作出这一预测的准确程度。

与信任相关的概念是声誉。文献[12]中对声誉的定义为由某一实体的行为历史信息或对其行为的观察得出的对这个实体未来行为的期望。由于开放环境下能够得到的关于一个实体的信息十分有限而不能得出信任,其声誉往往用来形成信任。声誉可以来源于其他实体的推荐,或者是与这个实体的直接交互结果,也可以是两者的结合。信任是对实体未来某种行为的预测,因而它和未来行为的信息是相关的。把信任的形成看成两个过程:声誉形成——通过其他实体的推荐信息和自身交互信息得出声誉值;信任形成——结合声誉值与未来行为信息得出信任值。

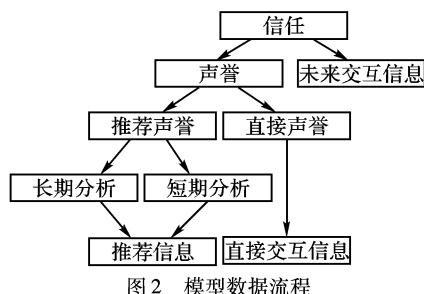


图 2 模型数据流程

本文提出的信任模型的数据处理流程如图 2。由于在开放环境下遇到的交互实体往往是陌生的,所以本模型主要利用推荐信息得出声誉,这也是模型的主要部分。在推荐声誉的形成过程中我们提出长期分析和短期分析结合的方法,既保留了以往模型的历史积累信息的影响,又做出短期趋势的预测,使得模型在应用中更加灵敏。在取信推荐信息时,我们考虑了交易时间、交易额、推荐实体交易次数、推荐实体角色(卖家或买家)等因素,使模型能较好的应对信任炒作和诽谤。



图 3 模型的演化

模型的结构随时间进行变化,当和一个陌生实体开始交互时,模型处于初始阶段,对陌生实体声誉值的判断完全或大部分来源于其他实体的推荐。当和这个实体交易若干次后,声誉值就依赖于其他实体的推荐和自己的直接交互。当交易次数继续增加到一定数量,对方已成为熟悉的交互伙伴,声誉值可以完全或大部分依赖于直接交互信息。下面给出模型中的相关概念。

**定义 1 实体:**在开放环境中进行交互的个体。可以是一个 Agent 或一段程序,也可以是一个电子交易的用户。本文用大写字母表示实体,如 A,B。

**定义 2 可信记录:**是被可信第三方保证的事实记录。

根据需要,本文采用多元组的方式描述证据。例如在电子商务中可以采用元组 ( subject, object, time, action, price, goods, results) 描述一次交互的证据,其中 subject 表示动作主体, object 表示动作客体, time 表示动作时间, action 表示动作(买或卖), price 表示价格, goods 表示商品名, results 表示这次交互的结果(成功或失败)。交互记录必须要有可信第三方保证从创建开始的不可篡改性,如淘宝网页上的某用户的交易记录就是可信记录。

**定义 3 推荐:**对于信任主体来说,第三方对信任客体的评价叫做推荐。如淘宝系统中的用户评价(包括各种评价)就是推荐。本文用 -1 ~ 1 之间的浮点数表示推荐,大于 0 时表示评价者对此次交互满意,小于 0 表示不满意,等于 0 表示不确定。推荐是评价实体对被评价实体在某方面的预测。本文讨论的推荐是基于可信记录的,表示在一条可信记录代表的交易后,评价实体对被评价实体关于这次交互的评价,而不是传统意义上的对被评价实体的综合评价。因而在本文中,一个实体对另一实体可以有多个推荐,分别来源于不同的可信记录。

**定义 4 声誉:**由实体历史交互信息得出的对其未来行为的期望。这个预测是对未来行为的概括预测,不包含未来行为信息。本文用 [ -1, 1 ] 的实数表示声誉,这个数越大,表示实体的声誉越好。

**定义 5 信任:**一个实体对另一实体按当前交互行为期望而行动的可能性的预测。本模型用 [ 0, 1 ] 的实数表示信任值,数越大,表示实体越可能按照我们的期望行动。

**定义 6 直接声誉:**由实体直接交互得出的声誉。

**定义 7 推荐声誉:**由推荐信息得出的声誉。

### 1.1 推荐声誉

声誉计算的关键是确定每个推荐的影响程度。基于信任链的模型<sup>[13]</sup>中,推荐信息的影响力是由以这个推荐作为结尾的信任链上的所有信任值决定的。这类模型应用于 C2C 环境下有以下不足:首先在陌生实体较多的情况下,信任链很难形成;其次在网上交易系统里,交易信息在一定程度上是可靠的,可以不用构建信任链而直接采用,构建信任链本身会导致较大的开销。本模型的是声誉计算基于 C2C 交易网站提供的所有推荐信息(包括陌生实体的推荐),计算过程包括长期分析和短期分析两个部分。

#### 1.1.1 长期分析

长期分析是对所有记录的分析,得到被评价实体的累积声誉。输入的数据是历史交互记录和评价,其结构如下:

(EID, duty, amount, Time, rec, c\_rep)

EID 是评价者的 ID, duty 是评价者在这次交易中的角色(卖家或买家), amount 是交易额, time 是交易时间, rec 是评价者对被评价者的评价(推荐), c\_rep 是评价者作为相同角色的声誉(用得到好评的次数表示)。

淘宝中有三种评价  $rec \in \{“好评”, “中评”, “差评”\}$ 。“好评”表示对交互结果很满意,“中评”表示交互成功完成,但是产品质量或服务质量有部分缺陷,“差评”表示欺诈行为或产品质量与描述严重不符。为了便于计算,引入映射函数:

$$f(rec) = \begin{cases} 1.0 & (rec = “好评”) \\ 0.3 & (rec = “中评”) \\ -1.0 & (rec = “差评”) \end{cases}$$

评”,“差评”|

$c\_rep \in N$ ,  $c\_rep$  越大其评价的可信度越高。 $c\_rep$  是评价

者得到的好评数,  $c\_rep$  越大, 说明评价者在以往的成功交易越多, 从而它是非恶意实体的可能性越大, 因此它给出客观评价的可能性越大。同样定义一个  $N \rightarrow [0, 1]$  的函数:

$$g(c\_rep) = \begin{cases} \sqrt{c\_rep}/13 & (c\_rep \leq 169) \\ 1.0 & (c\_rep > 169) \end{cases}$$

$duty$  的作用在于确定历史记录和当前交互的相似程度。当前交互中使用模型的实体的角色用  $my\_duty$  表示。 $my\_duty, my\_duty \in \{\text{买家}, \text{卖家}\}$ , 定义  $\{\text{买家}, \text{卖家}\}^2 \rightarrow [0, 1]$  的函数  $likeness$  用以区别不同角色的评价记录对当前声誉影响的差异:

$$likeness(duty, my\_duty) = \begin{cases} 0.3 & (duty \neq my\_duty) \\ 1.0 & (duty = my\_duty) \end{cases}$$

当评价记录中的评价者是买家并且用户当前角色也是买家时, 这条记录的影响应较大,  $likeness$  为 1.0。反之角色不同时, 评价记录的影响应减小,  $likeness$  为 0.3。

时间  $time$  表示记录中交互的时间, 由于实体行为在时间上的集中性, 很久以前发生的交易对当前交易的影响应被淡化。 $cur\_time$  表示当前时间。 $cur\_time, Time \in N$ , 定义  $N^2 \rightarrow [0, 1]$  的函数  $t$ :

$$t(time, cur\_time) = \begin{cases} 1 - \frac{cur\_time - time}{365} & (cur\_time - time < 365) \\ 0(o.w) & \end{cases}$$

$amount$  是交易额。 $amount$  越大的交互记录应该更可信, 因为炒作行为一般是用小额度的成功交易换取好评, 所以大额交易更可能是真实交易, 应具有更大的影响力。 $amount \in [0, +\infty)$ , 定义  $[0, +\infty) \rightarrow [0, 1]$  的交易代价函数  $dc$  如下:

$$dc(amount) = \begin{cases} 1 & (amount \geq 300) \\ \frac{amount}{300} & (amount < 300) \end{cases}$$

整条记录的采信因子  $aff$  是综合以上各函数得出的  $[0, 1]$  上的值。

$$aff = f \times g \times likeness \times t \times dc$$

某实体共有  $n$  条历史记录, 其长期声誉值  $long\_rep \in [-1, 1]$  由下式给出:

$$long\_rep = \frac{\sum_{i=1}^n dff_i \times rec_i}{\sum_{i=1}^n dff_i}$$

### 1.1.2 短期分析

实体的行为在短期内有较大的相关性, 所以通过对实体短期行为的分析, 可以得出未来短时间内实体行为的趋势。模型的做法是通过对两周的最近五条记录的拟和得出实体评价值的趋势, 算出当前时间对应的预测值。具体做法如下: 以  $x = time - (cur\_time - 14)$  作为横坐标,  $y = rec$  作为纵坐标, 对  $x > 0$  (两周内) 的近五条记录作线性回归, 如果两周内不足五条记录, 就将短期声誉取一个默认值, 如 0.5。设五个采样点分别为  $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5)$ 。考虑到计算效率, 我们用简单的方法进行拟合。首先由五个采样点得到三个加权后的平均采样点:

$$\bar{x}_i = \frac{1}{3}(x_i + x_{i+1} + x_{i+2}), i = 1, 2, 3$$

$$\bar{y}_i = \frac{aff_i \times y_i + aff_{i+1} \times y_{i+1} + aff_{i+2} \times y_{i+2}}{aff_i + aff_{i+1} + aff_{i+2}}, i = 1, 2, 3$$

对三个平均采样点作简单拟合, 得到直线  $y = ax + b$ ,

$$a = \frac{1}{2} \left( \frac{\bar{y}_3 - \bar{y}_2}{\bar{x}_3 - \bar{x}_2} + \frac{\bar{y}_2 - \bar{y}_1}{\bar{x}_2 - \bar{x}_1} \right), b = \bar{y} - a \times \bar{x}$$

$$\text{其中 } \bar{x} = \frac{1}{3} \sum_{i=1}^3 \bar{x}_i, \bar{y} = \frac{1}{3} \sum_{i=1}^3 \bar{y}_i$$

这条直线基本反映了实体近期声誉值的变化趋势。如果最近的一条记录的时间和当前时间差距较小时就可以用这条直线来预测当前的短期声誉值, 但是如果这个时间差比较大时, 这种预测过于机械。我们设计了一个随时间增长的有衰减功能的预测方法, 使预测线随时间增长越来越平缓, 也就是使斜率的绝对值随时间的增长逐渐减小。可以写出方程:

$$\begin{cases} y(\bar{x}) = \bar{y} \\ \frac{dy(\bar{x})}{dx} = a, \text{ 解为 } y = -\frac{ax^2}{x} + ax + \bar{y} \\ y = \frac{c}{x} + d \end{cases}$$

$$\text{其中 } \bar{x} = \frac{1}{3} \sum_{i=1}^3 \bar{x}_i, \bar{y} = \frac{1}{3} \sum_{i=1}^3 \bar{y}_i$$

$$\text{代入当前时间 } x = 14, \text{ 得到 } cur\_rec = -\frac{ax^2}{14} + ax + \bar{y}, \text{ 短期声誉值由下式给出:}$$

$$short\_rep = \begin{cases} 1 & (cur\_rec > 1) \\ -1 & (cur\_rec < -1) \\ cur\_rec(o.w) & \end{cases}$$

### 1.1.3 推荐声誉

推荐声誉是累计声誉和短期声誉的综合。

$$rec\_rep = \alpha \times long\_rep + (1 - \alpha) \times short\_rep$$

$\alpha$  是  $[0, 1]$  的实数, 用来控制累积声誉的权重。 $\alpha$  的选取依赖于用户的策略。如果更看重历史积累信息, 可以将  $\alpha$  选大一些。如果在高度动态的环境, 可以更相信近期记录, 应该将  $\alpha$  选小一些。本文选取  $\alpha = 0.5$ 。

## 1.2 声誉

如果用户已经和对方实体多次交互过, 模型演化到了中间阶段, 会对已有的直接交互做出分析, 得到直接声誉值。做法是从对方历史交互记录中查询历史记录, 如果发现自己的交互记录, 就将其标记, 然后对这些记录做与长期分析类似的处理, 得出直接声誉值  $dir\_rep$ 。如果没有找到与自己的交互记录, 可将直接声誉值为一个  $[-1, 1]$  的常数或推荐声誉值。

综合的声誉值由下式给出:

$$rep = \beta \times rec\_rep + (1 - \beta) \times dir\_rep$$

$\beta$  是  $[0, 1]$  的实数, 用于控制在综合声誉中推荐声誉和直接声誉所占的比重。 $\beta$  的选择取决于用户更看重推荐信息还是直接交互信息。由于 C2C 网上交易的实体为数众多, 遇到陌生实体的可能性较大, 因此利用直接声誉的几率较小, 所以本文选取  $\beta = 0.7$ , 更看重推荐信息得出的声誉值。

### 1.3 信任

已有的许多模型都用声誉值来代表信任值, 这种做法应用于 C2C 环境中不够灵活。比如某个声誉值不高的卖家在小额交易上往往不会欺诈, 因为那会损害他的声誉而又得不到多少好处, 所以如果当前交易额较小时, 应使信任值相对较大。这体现了声誉和信任的区别: 声誉值代表对对方未来某类行为的预测, 而信任将这一预测和当前的行为信息结合, 得出对当前行为的预测。

本模型用  $[0, 1]$  的实数表示信任值。 $Rep$  表示信任值集合,  $Amount$  表示当前交易额值集合, 信任形成过程是  $Rep \times$

*Amount -> [0,1] 的函数:*

$$trust = \frac{1 + rep}{2} \times e^{-\frac{amount}{\eta}}$$

上式表示在声誉值为 1 时,如果在当前交易额为  $\eta$  元,得出的信任值约为 0.37,即对当前交易会成功进行的可能性的预测值是 0.37。如果用户更能承受风险,可以将  $\eta$  大些。若用户更谨慎,可设小些。本文讨论的信任值是对实体会发生预期行为的概率的预测,而不是概率。由于实体行为的不规则性和环境的复杂性,无法对概率进行准确建模,只能采取满足概率性质的预测值。

最终决策是将算出的信任值与策略中的信任阈值比较,如果大于阈值,就建议交易,小于阈值就建议不交易。信任阈值的选取很重要,如果选得过小会使恶意实体有机可乘,如果选得过大则会使交易对象的选择范围变小,实际应用中应当基于交互经验进行调整。

## 2 实验结果及分析

我们把模型应用于淘宝电子商务系统。模型从淘宝服务器取得用户指定的交易对象的所有历史交互记录,分析后得出建议结果。为了简单只讨论推荐声誉的演化。图 4(a)显示了某卖家从 2006 年 6 月 18 日到 12 月 10 日的推荐声誉值随时间的变化。横坐标以 6 月 18 日作为 0 点,以一天为单位。

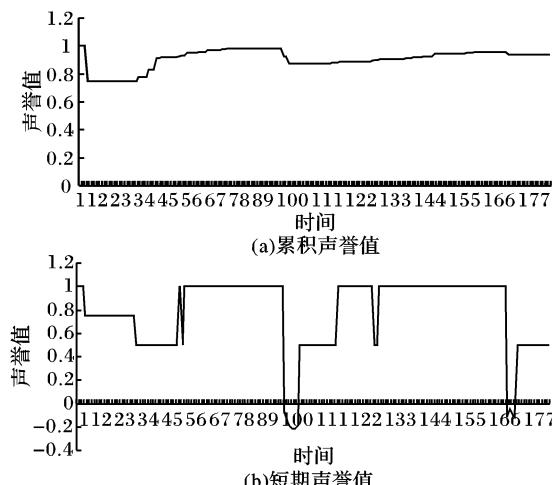


图 4 累积声誉和短期声誉

这个卖家在第三天(21 日)有一条记录是差评,导致历史累积声誉值的下降,但随后的好评记录渐渐将累积声誉值提升,第 82 天和第 83 天的两条记录都是差评,说明短时间内的实体行为有一定程度的集中性,但历史累积声誉值只有有限的下调,对短期内的实体行为的变化不够敏感。单纯依靠历史累积声誉值的模型应对这种情况时,只能对差评记录设定较大的惩罚值,但这种做法将导致如下情况:差评实体声誉值被降低后,其他实体由于对它的不信任而停止和它交互,从而得到差评的实体将一直维持这个声誉值,出现“饥饿”现象,这在 C2C 环境中是不允许的。如果这个差评是其他实体对它的诽谤,这将表现为整个系统的抗诽谤能力很差。我们的模型采用长期分析结合短期分析,在保证恶意行为的发生能被及时反映的前提下,让得到差评的实体经过一段时间或进行一定数量的成功交易后恢复声誉值,更适应 C2C 环境鼓励交易的原则,并且下面的讨论可以看出这种做法基本不会损害交易的安全性。

图 4(b)是短期分析的结果,可以看出短期声誉对差评非常敏感,一次差评就可以使声誉值有相当程度的下调,连续的差评将会更大的拉动声誉值。图中第 82 天附近的两条差评记录使短期声誉值大幅度下调,4 天后当近两周交互记录小于 5 条时,短期声誉被置为一个默认值,使卖家的声誉得到一定程度的恢复,某些实体可能愿意和它继续交互。当几次成功交互后,卖家的推荐声誉完全恢复。对于恶意实体,每进行一次欺骗交易,要平均等待约 4 天或有实体愿意冒险和它交易并成功才能恢复声誉值。这样可以有效地减少恶意实体的“工作效率”,使其得到的利益很少而放弃欺骗行为。对于受到诽谤的实体,只需通过等待一段时间就可以恢复一部分声誉,有效地防止了诽谤带来的“饥饿”现象。系统在应用中要权衡这个等待时间(本例中为 4 天),既不能过长而损害了受到诽谤的实体的利益,也不能过短使恶意实体得不到应有的惩罚。综上,长期与短期分析结合的方法在保证实体安全交易的情况下,鼓励了交易进行,比以往模型更适合于 C2C 的电子交易环境。

信任形成的例子如某用户在第 85 天要向此卖家购买价值 50 元的物品,信任形成公式中的  $\eta$  被用户设为 50, 用户策略中的信任阈值是 0.23, 这时算出的卖家声誉值为 0.32, 由此计算出的信任值为 0.12, 未能到达阈值, 系统建议不交互。如果这个用户在一周后再做同一交易, 卖家声誉值恢复为 0.69, 计算出的信任值是 0.26, 超过阈值, 系统建议交互。

综上,本模型充分利用了交互网站上提供的推荐信息,可以有效地应对信任炒作和诽谤,在保证安全的前提下鼓励了交易,在配置上也比较灵活,更好地适应 C2C 环境下电子交易的特点。

## 3 结语

本文分析了已有的部分信任模型,讨论了它们在应用于 C2C 电子交易系统时的缺陷,提出了一个基于推荐的长期与短期分析相结合的声誉模型和信任模型,使其更适应 C2C 环境的特点和需求。在处理推荐信息的可信度时综合了时间、相似度等多方面因素,可以有效地应对信任炒作和诽谤。目前的模拟实验仅初步验证模型的合理性,需要进一步的应用来证实其有效性。

### 参考文献:

- [1] MALAGA RA. Web-based reputation management systems: Problems and suggested solutions[ EB/OL]. <http://www.springerlink.com/index/M8582910783X5368.pdf>, 2001.
- [2] ABDUL-RAHMAN A, HAILES S. A Distributed Trust Model[ EB/OL]. <http://bikmrdc.im.fju.edu.tw/files/ADistributedTrustModel.pdf>, 1998.
- [3] LIANG ZQ, SHI WS. PET: A Personalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing[ EB/OL]. <http://141.217.17.111/papers/liang05-pet.pdf>, 2005.
- [4] WANG Y, LIN F - R. Trust and Risk Evaluation of Transactions with Different Amounts in Peer-to-Peer E-commerce Environments [ EB/OL]. [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=4031639](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4031639), 2005.
- [5] ZACHARIA G, MAES P. Trust management through reputation mechanisms[ EB/OL]. <http://taylorandfrancis.metapress.com/index/DNR78BMG0DMY6CC4.pdf>, 2000. (下转第 1359 页)

查询,检查是否能进行保护域的转换。检查通过之后内核先保存好原保护域的相关信息,更新进程的有效保护域标记符为要切换到的保护域标记符,然后更改进程描述符的页全局目录表地址和强制访问控制信息为有效保护域所对应的页全局目录表地址和强制访问控制信息。在完成保护域的切换后,内核回调新保护域的用户态入口函数。由于x86体系结构不支持高特权级的代码直接调用低特权级的代码,此处采用的方法是在内核堆栈中人为构建一个返回用户态的上下文<sup>[7,8]</sup>,先将用户态入口函数的参数拷贝到新保护域的堆栈中,将新保护域的堆栈指针和用户态入口函数地址值分别压入到内核堆栈中,然后执行lret指令,即可返回到用户态新保护域的入口函数处执行。此时进程进入新保护域,将以新保护域的访问方式对系统资源和程序地址空间进行访问。当进程在新保护域中完成相应的任务后调用ReturnProtD返回。返回时内核执行与前述相反的动作,重新切换到原保护域。

### 3.3 性能分析

在完成对内核的修改之后,编译生成新的内核,并用其重新启动系统,在新内核下测试该模型给应用程序带来的性能影响。测试基于P4 CPU 3.00GHz,512M内存的硬件环境,采用的操作系统是Linux的Fedora Core 4发行版本。

实验测试了内核新增的系统调用需要的执行时间,并与原内核中一些典型的系统调用所需要消耗的执行时间进行了比较,结果如表1(表中的结果是测量1000次取平均值所得,时间单位为μs)。

从表1可以看出,新增加的系统调用的执行时间大致是一些快速系统调用(如close)的5~8倍,与一些中速系统调用(如read, 20K bytes)的执行时间相当。在使用本模型的应用程序中,在程序的初始化时,调用CreatProtD和RegisterEntry来注册保护域以及域之间的转换入口地址,此后在程序的执行过程中,本模型所带来的性能开销就只存在于各个保护域之间的切换。同时,考虑到一般的程序划分成的保护域数目不会太多,应用程序在各个保护域之间的切换不会过于频繁,因此本模型不会

表1 各种系统调用消耗时间比较

系统调用	消耗时间
open	3.322
close	1.462
read(1 byte)	2.046
read(20K bytes)	6.190
read(1M bytes)	1057.896
CreatProtD	11.262
RegisterEntry	10.256
ChangeProtD	7.632

给应用程序带来很大的性能降低。

## 4 结语

本文讨论了在进程内部划分多个保护域的方法和模型。针对进程的不同执行阶段权限的改变,将进程相应的划分为保护域,并引入一个有效保护域的概念,使得进程执行时所具有的权限与有效保护域关联起来,细化了对进程执行操作的控制。在该细粒度保护域模型中,将保护域与进程地址空间的访问控制关联起来,做到进程的不同执行阶段对地址空间有不同的访问方式,避免了应用态代码注入攻击。同时,将强制访问控制机制引入到此模型中,进程对系统资源的访问通过强制访问控制框架来实施,保证了系统的安全性满足安全策略的需要。

### 参考文献:

- [1] WALKER KM, STERNE DF, BADGER ML, et al. Confining Root Programs with Domain and Type Enforcement[ A]. In Proceedings of the Sixth USENIX UNIX Security Symposium[ C]. August 1996.
- [2] SPENCER R, SMALLEY S, LOSCOCCO P, et al. The Flask Security Architecture: System Support for Diverse Security Policies[ A]. In Proceedings of the Eighth USENIX Security Symposium[ C]. August 1999.
- [3] LOSCOCCO P, SMALLEY S. Integrating Flexible Support for Security Policies into the Linux Operating System[ A]. In Proceedings of the FREENIX Track: 2001 USENIX Annual Technical Conference [ C]. 2001.29 ~ 42.
- [4] SELinuxhomepage[ EB/OL]. <http://www.nsa.gov/selinux/>, 2006.
- [5] SWIFT M, BERSHAD B, LEVY H. Improving the Reliability of Commodity Operating Systems[ A]. In Proceedings of the 19th ACM Symposium on Operating Systems Principles[ C]. 2003.
- [6] TAKAHASHI M, KONO K, MASUDA T. Efficient Kernel Support of Fine-Grained Protection Domains for Mobile Code[ A]. In Proceedings of the 19th IEEE International Conference on Distributed Computing Systems[ C]. 1999.
- [7] 谢钧,黄皓,张佳.多保护域进程模型及其实现[J].电子学报,2005,33(1):38 ~ 42.
- [8] CHIUEH T-C, VENKITACHALAM G, PRADHAN P. Integrating segmentation and paging protection for safe, efficient and transparent software extensions[ A]. In Proceedings of 17th ACM Symposium on Operating System Principles[ C]. December 1999. 140 ~ 153.

(上接第1352页)

- [6] YU B, SINGH MP. A social mechanism of reputation management in electronic communities [ EB/OL]. <http://www.springerlink.com/index/J3HW7TYMMW067WGM.pdf>, 2000.
- [7] TRAN T, COHEN R. Improving User Satisfaction in Agent-based e-lectronic Marketplaces by reputation modelling and adjustable product quality[ EB/OL]. <http://www.site.uottawa.ca/~ttran/teaching/csi5389/Improving%20User%20Satisfaction.pdf>, 2004.
- [8] BAMASAK O, ZHANG N. A Distributed Reputation Management Scheme for Mobile Agentbased E-commerce Applications[ EB/OL]. [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=1402307](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1402307), 2004.
- [9] LIN KWEI-JAY, LU HY, YU T, et al. A Reputation and Trust Management Broker Framework for Web Applications[ EB/OL]. [http://linux.ece.uci.edu/DIRECT/docs/EEE2005\\_Lin\\_KweiJay.pdf](http://linux.ece.uci.edu/DIRECT/docs/EEE2005_Lin_KweiJay.pdf), 2004.
- [10] REBAHI Y, MUJICA-V VE, SISALERN D. A Reputation-Based Trust Mechanism for Ad hoc Networks [ EB/OL]. [http://www.fokus.gmd.de/bereichsseiten/kompetenzzentrum/mobis/Publikationen/2005/rebahiy\\_reputation.pdf](http://www.fokus.gmd.de/bereichsseiten/kompetenzzentrum/mobis/Publikationen/2005/rebahiy_reputation.pdf), 2005.
- [11] GAMBETTA D. Trust[ M]. Oxford, Blackwell, 1990.
- [12] ABDUL-RAHMAN A, HAILES S. Supporting trust in virtual communities[ EB/OL]. <http://csdl.computer.org/comp/proceedings/hicss/2000/0493/06/04936007.pdf>, 2000.
- [13] 徐锋,吕建,郑玮,等.一个软件服务协同中信任评估模型的设计[J].软件学报,2003,14(6):1043 ~ 1051.