

一种加强 C2C 诚信交易的安全解决方案

张晓杰¹, 卫红春¹, 王义海², 雷卓琳²

(1 西安石油大学 计算机学院, 陕西 西安 710065; 2 陕西西部数通电信资讯有限公司, 陕西 西安 710068)

摘 要: 在对 C2C 交易中存在诚信问题深入分析的基础上, 提出了安全解决方案. 该方案可以很好的改善 C2C 交易中诚信度不高、容易出现欺诈行为等问题. 方案已在安捷支付系统中得到应用.

关键词: 电子商务; C2C 交易; 移动支付; 安全性

中图分类号: TP39

文献标识码: A

文章编号: 1000-7180(2010)05-0193-03

C2C Transactions Strengthen the Integrity of a Security Solution

ZHANG Xiao-jie¹, WEI Hong-chun¹, WANG Yi-hai², LEI Zhuo-lin²

(1 Department of Computer, Xi'an Shiyu University, Xi'an 710065, China;

2 Shanxi Cyberwest Telecom Co. LTD, Xi'an 710075, China)

Abstract: The security solution is proposed based on the credibility of in-depth analysis which existed in C2C transactions. The program can improve the low integrity, susceptible to fraud and other issues in C2C transactions, and it has been applied in Angel payment system.

Key words: e-commerce; C2C transactions; mobile payment; security

1 引言

在电子商务中, C2C 是指消费者与消费者之间通过电子商务平台进行交易的一种交易模式, 与 B2B(企业对企业)和 B2C(企业对个人)分属电子商务的三种模式^[1-2].

网络购物因其方便、快捷、低成本、送货上门、可即时同步互动的特性, 逐渐成为购物的重要形式. 然而, 由于网络的虚拟性、交易双方的匿名性、欠缺健全的身份认证及监管制度, 它的安全问题一直令人困扰. 诚信问题是目前制约 C2C 电子商务健康快速发展的瓶颈, 加强对 C2C 电子商务模式下的诚信交易的研究就成了一个重要问题^[3-4].

2 C2C 电子商务存在的主要诚信问题

2.1 实际商品与宣传不符

在网络上双方通过在线交易平台进行交易^[5],

买家只能通过商品的图片、视频以及文字介绍来了解商品的性能和质量. 这样就存在很大的不确定性, 给那些存在投机心理的卖家提供了夸大商品性能、以次充好的机会^[6].

2.2 信用炒作, 套取诚信

C2C 交易双方是交易个体, 大多不具有法人资格, 没有商业实体作为依托. 在交易过程中完全可以采用匿名方式进行交易, 或在交易平台上注册多个用户, 行骗后, 可以更换用户名. 也可借用他人身份进行虚假交易. 利益相关者之间可能相互进行满意度的评估, 以套取诚信. 会员之间协议互换好评, 买卖双方之间虚假交易但给予评价.

2.3 恶意竞拍情况屡屡发生

有些人在交易平台上竞拍买下商品后不支付, 消失不见, 但又通过另一个注册名进行网上购物, 电子商务系统对这些恶意竞拍没有有效的惩罚措施. 同样, 若某个交易者存在多个较强的竞争对手, 他可

收稿日期: 2009-06-13; 修回日期: 2009-08-20

基金项目: 陕西省自然科学基金项目(2007F33); 陕西省教育厅专项科研计划项目(09JK697)

以注册多个用户与竞争对手发生虚假交易,并对对手的诚信进行恶意评价,从而达到相对提升自己诚信的目的。

2.4 利用管理漏洞违背诚信

一些用户非法利用交易平台在电子支付工具管理方面存在的漏洞从事违背交易诚信和规则的交易行为:

(1) 用户可利用交易平台进行虚假交易,根据交易平台提供的支付工具实现异地不同账户之间的转账,从 A 银行账户转至 B 银行账户,从而避开银行汇划手续费等相关费用。

(2) 进行信用卡套现,利用信用卡免息还款期,进而套取银行信贷资金的失信行为。

(3) 通过提高商品价格进行虚假交易,从而进行“洗钱”等违法犯罪行为。

3 加强 C2C 诚信交易的解决方案

3.1 构建 C2C 诚信交易系统

完整的 C2C 诚信交易系统由商品交易平台,交易支付平台,金融系统,IVR 系统等部分构成,其体系结构见图 1。

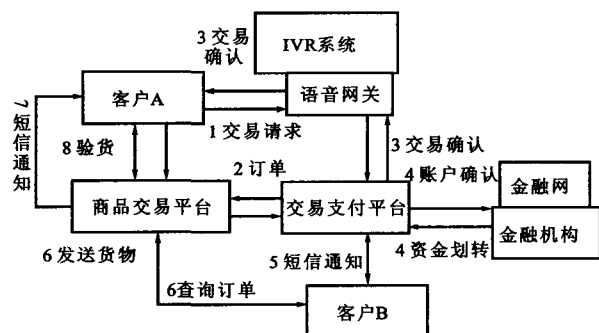


图1 C2C 诚信交易系统体系框架

本系统要求参与交易的客户必须在相关银行有自己的账户,并进行了实名注册。系统将对客户的注册名、手机号和银行账户进行绑定。

客户 A 和 B 是通过本系统进行 C2C 交易的双方, A 承担买家的角色, B 承担卖家的角色。

商品交易平台是本系统提供的用于卖家展示商品, 买家选购商品的一个平台。平台将通过直观的形式向客户展现卖家发布的商品信息。买家可以通过此平台查找自己所要购买的商品, 在了解商品的相关信息的同时, 也可以了解到卖家的信誉信息。

交易支付平台是与客户、商品交易平台、金融系统和 IVR 系统以及短信系统联系的用于进行交易业务支付的系统平台。本系统将与多个金融机构绑

定, 通过金融系统从买家的金融账户将资金划拨到卖家的金融账户。对每一笔交易, 交易支付平台要通过 IVR 语音播报系统拨通买家的绑定手机, 要求买家在手机上给出支付确认。只有通过了确认交易方能进行, 否则交易被终止。

3.2 采用动态身份验证机制

动态口令 $M = \text{Random} \{[(\text{RandomNumber} * \text{TimeNumber}) < -^6] + (\text{Random}^4[A-Z])\}$

产生的算法描述如下:

用户登录商品交易平台输入用户名后, 先点击“获取口令”。服务器产生 4 位随机数字记为 RandomNumber, 并记录下点击的时间 Time, 精确到秒, 如: 1998 年 10 月 10 日 21 时 9 分 2 秒, 记为 TimeNumber。将 TimeNumber 与 RandomNumber 相乘得到的结果从右向左取 6 位记为 N, 从 A-Z 这 26 个英文字母里随机取 4 个字母标记为 Z, 将 N 与 Z 的字符随机组合记为十位字符串 M, 保存在服务器中, 同时将 M 作为动态口令发送到用户注册时绑定的手机上。

用户查看手机上的动态口令, 输入此口令, 商品交易平台得到口令后与保存在服务器上的 M 作对比, 相同即可登录, 否则不允许登录。以此得到变化的、不会重复的动态口令, 这个口令是不需要记忆的, 且前后两次口令不能重复, 重复将被拒绝接受。流程图如图 2 所示。

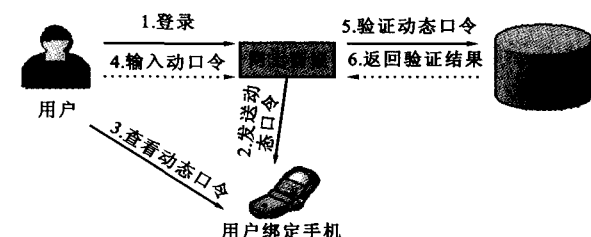


图2 C2C 诚信交易动态身份验证机制

3.3 设计安全的 C2C 诚信交易流程

交易支付平台 (MPP) 处在系统框架的中心位置, 它联系了客户 A (UserA)、客户 B (UserB)、商品交易平台 (WebSite)、金融系统 (FS) 等实体, 还需要 IVR 语音系统、移动系统 (MS) 中短信 (SMS) 系统的支持。交易支付流程如下^[4]:

(1) UserA → WebSite/Search (Goods) → Order

A 首先登录商品交易平台, 搜索自己要购买的商品。搜到后, 点击商品图片或介绍, 显示该商品的详细信息。此时输入要购买商品的数量、送货的地址、联系方式等一系列信息, 点击“立即购买”, 产生

一个购货订单。

(2) Order + Apply() → MPP

购货订单包含交易的所有信息,如:商品名称、价格、详细信息等和买家的一些信息,如买家购买的数量及送货地址、联系方式等信息。此时买家并没有付款,还可以撤消该订单。若买家决定付款,点击“立即付款”,将会产生一个支付订单,包含了购货订单信息及买家的一些身份信息。

(3) MPP → IVR/Call(Order) → UserA + Apply()

此时,移动支付平台会通过 IVR 语音系统给买家的绑定手机拨打电话,请求买家确认订单信息的合法性。

(4) MPP → Order → FS

买家确认后,移动支付平台通过金融机构接口将订单信息传送给金融机构,金融机构根据订单信息将货款从买家账户划转到移动支付系统的中间账户上,此时商品交易平台中订单状态已变为“买家已付款,等待卖家发货”。

(5) MPP → SMS → UserB

交易支付平台通过 SMS 系统向卖家发送短信信息,告知卖家有了购物订单信息,且货款已付,等待卖家发送货物。

(6) UserB → WebSite/Search (Order) → Send (Goods)

卖家登录商品交易平台,搜索求购订单信息,根据订单上的信息,查看库存,若库存充足,便依据订单信息发送货物,如果货存不足,就补充货存并发货。

(7) Mpp → UserA + SMS

交易支付平台通过 SMS 系统给买家发送短信信息,

告知卖家已发送货物,请注意查验。

(8) UserA + Goods → MPP + Apply() → FS → SMS → UserB

买家收到货物后,检验货物是否与购买的一致,若不一致,则向卖家提出异议,或退款或退货或者提交仲裁机构来裁决;如果与所要购买的一致,则做出一个收到货物的确认,交易支付平台收到这个确认信息便会通知金融机构,金融机构将交易支付平台中间账户里的货款转账给卖家,并通过 SMS 系统短信通知卖家,货款已汇到,至此,一个完整的交易完成。

其中的一些标识的说明:

X/Y :表示实体 X 将信息以 Y 这种方式进行操作。

$X/Y(Z)$:表示实体 X 关于 Z 的某种 Y 功能。

$X \rightarrow Y$:表示信息流从实体 X 传递到实体 Y 。

$X + Y$:表示实体 X 与实体 Y 是串联操作执行的。

Apply():表示确认操作。

Send(Goods):表示发送货物操作。

4 C2C 诚信交易解决方案的效果分析

(1) 用户注册时将身份证号码、手机号码及银行卡号绑定在一起,可以唯一的确定用户的身份。当出现商品与宣传不符时,买家可以与卖家联系,商议解决。对协商不能解决的,可通过第三方仲裁机构,或提交工商管理部门解决。买家下订单后会收到交易平台的 SMS 信息,确认支付时会收到交易平台的 IVR 确认电话,这些信息会记录在案,可作为双方有分歧时的证据。

(2) 针对信用炒作,套取诚信问题,用户注册时,系统会检验用户的身份信息,若发现身份证或银行卡号在系统中已存在,便不允许再次注册,这就避免了一个实体多个账户,也就避免了虚假交易及套取诚信和刷信用等现象的发生。对于信用系统来说,信用记录也是真实可查的。对于那些信用记录不良的买或卖家,系统会给出警示信息,提醒用户交易时要谨慎小心。

(3) 针对恶意竞拍的问题,因为用户的唯一可确认性,在恶意竞拍发生时,可通过相关信息找到其人,通过协商、第三方仲裁机构解决出现的问题,严重的也可通过司法机关解决处理。

(4) 针对利用管理漏洞的违背诚信问题,因为不允许自己和自己交易。一个手机号与一个身份证号码只能对应一个银行卡账号,交易支付时,发送 SMS 短信和回拨的 IVR 电话前会判断,若交易双方的手机号码与身份证号码及银行卡账号任何一个相同时,便拒绝进行交易。只有真实有效的两个实体之间才能进行交易,也就杜绝了信用卡套现和利用虚假交易洗钱等违法犯罪活动的发生。

5 结束语

在交易流程的各个环节中,都可通过一些方法来验证双方的身份信息,操作中还有 SMS 信息及 IVR 电话的实时确认,使交易的安全性得到有效保证。保证了交易双方身份信息的真实可信,达到实现诚信交易的目的。此方案已经在现实中得到了实施,并且取得了良好的效果。

(下转第 198 页)

从表 5 可以看出,采用三次参数样条函数方法优于列平均值方法,接近主成分方法,三次参数样条函数方法与其他方法相比,算法简单、容易实现,特别是在数据点呈曲线变化时三次参数样条函数的效果更佳,由于本例中,数据点基本上呈直线变化,故主成分分析方法与三次参数样条方法相似。

对于利用小波分析、傅立叶函数、神经网络等技术进行缺失数据修补的方法这里没有应用,因为他们都要进行大量的样本训练,而三次参数样条函数方法不进行样本训练,所以我们采用了主成份分析方法和列平均值方法进行了比较。

文中算法可用于修补缺失数据的中间点,但对于端点的缺失数据修补应进一步研究,若采用文献[8]的方法进一步去构建精确的三次参数样条函数并采用 5 个定位点,将取得更好的效果。

参考文献:

- [1] Grawa A I, R annila M H, Srikant R, et al. Fast discovery of association rules[C]// Advance in Knowledge Discovery and Data Mining. Menlo Park, CA: AAA I Press, 1995:307-328.
- [2] Ragel A, Crem illeux B. Treatment of missing values for

association[C]// Research and Development in Knowledge Discovery and Data Mining. New York: Springer - Verlag, 1998:258-269.

- [3] Kononenko I, Bratko I. Experiment in automatic learning of medical diagnostic rules[R]. Jozef Stefan Institute, 1984.
- [4] Quinlan J R. C4. 5: Programs for machine learning[M]. SanMateo, CA: Morgan Kaufmann Publishers, Inc., 1993.
- [5] Lakshminarayanan K, Harp S, Goldman R, et al. Imputation of missing data using machine learning techniques [C]// Proceedings of the 2nd International Conference on Knowledge Discovery and Data Mining. Menlo Park, CA: AAA I Press, 1996:140-145.
- [6] 刘峰,翟俊.基于聚类分析和神经网络的时间序列预测方法[J].微电子学与计算机,2006,23(9):85-87.
- [7] 王清毅,蔡智,邹翔.部分数据缺失环境下的发现方法[J].软件学报,2001,12(10):1516-1524.
- [8] 张彩明.高精度三次参数样条曲线的构造[J].计算机学报,2002,25(3):262-268.

作者简介:

张春生 男,(1965-),硕士,教授.研究方向为数据库技术、数据挖掘、应用软件开发.

(上接第 195 页)

参考文献:

- [1] Chen Lei-Da. A model of consumer acceptance of mobile payment [J]. International Journal of Mobile Communications, 2008, 6(1):32-52.
- [2] 许芸.在电子商务数据管理中分布式数据库的安全性策略[J].微电子学与计算机,2002,19(9):13-15.
- [3] 王潇雨.移动支付安全交易平台的研究与开发[J].计算机工程与设计,2006(11):213-216.
- [4] 施小华,王志坚.移动支付的安全方案研究[J].计算机技术与发展,2007(4):114-118.
- [5] 张慧,章丽玲.移动支付及其安全技术研究[J].湖北第二师范学院学报,2008(8):52-55.

- [6] 湛玉婕,张必春.C2C 电子商务诚信问题改良初探[J].经济师,2009(1):254-255.

作者简介:

张晓杰 男,(1982-),硕士研究生.研究方向为管理信息系统与计算机网络.

卫红春 男,(1956-),教授.研究方向为管理信息系统与软件工程.

王义海 男,(1958-),高工.研究方向为信息系统安全技术.

雷卓琳 女,(1975-),工程师.研究方向信息系统工程.