



(12) 发明专利

(10) 授权公告号 CN 101751629 B

(45) 授权公告日 2015.05.27

(21) 申请号 200910208379.4

US 2006236103 A1, 2006.10.19, 全文.

(22) 申请日 2009.11.12

US 6041411 A, 2000.03.21, 全文.

(30) 优先权数据

审查员 邢鹏

12/336, 189 2008.12.16 US

(73) 专利权人 国际商业机器公司

地址 美国纽约阿芒克

(72) 发明人 E·E·凯利 F·莫蒂卡

W·M·德利亚

(74) 专利代理机构 北京市金杜律师事务所

11256

代理人 吴立明 唐文静

(51) Int. Cl.

G06F 17/30(2006.01)

(56) 对比文件

CN 1956002 A, 2007.05.02, 全文.

CN 1758276 A, 2006.04.12, 全文.

CN 1845185 A, 2006.10.11, 全文.

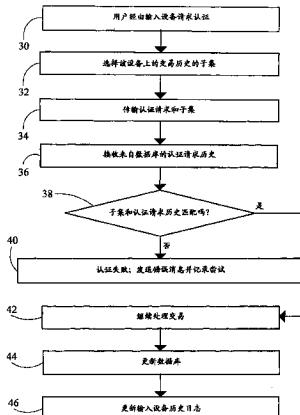
权利要求书1页 说明书7页 附图2页

(54) 发明名称

使用变化唯一值的多因素认证的方法和系统

(57) 摘要

本发明涉及使用变化唯一值的多因素认证的方法和系统。本发明的认证方法包括步骤：提供具有安全服务器的交易服务提供商；提供用户；由用户向服务提供商的服务器请求访问授权，该服务器存储从该授权访问请求中获得的一组使用参数，在用户的后续的访问服务器的请求中，该使用参数至少包括供交易服务提供商在认证期间使用的若干先前位置坐标、访问方法、交易信息和所用的访问硬件，在认证中使用的使用参数将利用最新的数据进行持续更新。



1. 一种用于具有变化的唯一值的多因素认证的方法,包括步骤：
维护用户所做的交易的访问历史数据库；
维护输入设备上的客户端设备历史日志；
接收来自所述输入设备的交易请求；
使所述输入设备从所述客户端设备历史日志中选择子集；
将所述子集与所述请求一起发送给认证服务器；
将所述子集与所述访问历史数据库进行比较；
当在所述子集与所述访问历史数据库之间找到匹配时,继续处理所述交易;以及
当在所述子集与所述访问历史数据库之间没有找到任何匹配时,终止所述交易。

2. 根据权利要求 1 所述的方法,其中所述继续处理步骤包括步骤：

用交易记录来更新所述客户端设备中的所述客户端设备历史日志;以及
用所述交易的记录来更新所述访问历史数据库。

3. 根据权利要求 2 所述的方法,其中对于每个交易,所述访问历史数据库包括设备 ID、账号、与所述账号相关联的口令、交易的日期、交易的时间、交易的位置、服务位置、服务类型和用户的生物统计学 ID。

4. 一种利用变化的唯一值来执行多因素认证的系统,包括：

用户所做的交易的访问历史数据库；

输入设备上的客户端设备历史日志；

用于接收来自所述输入设备的交易请求的装置；

用于使所述输入设备从所述客户端设备历史日志中选择子集的装置；

用于将所述子集与所述请求一起发送给认证服务器的装置,其中,所述认证服务器将所述子集与所述访问历史数据库进行比较；

用于当在所述子集与所述访问历史数据库之间找到匹配时继续处理所述交易的装置；
以及

用于当在所述子集与所述访问历史数据库之间没有找到任何匹配时终止所述交易的装置。

5. 根据权利要求 4 所述的系统,进一步包括：

用于用交易记录来更新所述客户端设备中的所述客户端设备历史日志的装置;以及

用于用所述交易记录来更新所述访问历史数据库的装置。

6. 根据权利要求 5 所述的系统,其中针对每个交易,所述访问历史数据库包括设备 ID、账号、与所述账号相关联的口令、交易的日期、交易的时间、交易的位置、服务位置、服务类型和用户的生物统计学 ID。

使用变化唯一值的多因素认证的方法和系统

技术领域

[0001] 本发明一般涉及针对系统访问的用户认证的领域，并且更具体地涉及具有变化的唯一 (unique) 值的多因素认证。

背景技术

[0002] 像其他电子数据处理系统一样，支付交易 (transaction) 处理系统容易遇到欺骗 (fraud)。这种欺骗可给这种系统的用户带来很多麻烦，其中常包括危及这种系统的敏感信息 (sensitive information) 的安全以及增加对这种系统的不信任。这种欺骗还给依赖于这种系统的实体 (诸如银行、信用卡公司、在线零售商店，等等，) 强加额外的成本，这些实体将承担欺骗带来的冲击。虽然存在欺骗检测和阻止机制，但是对这种系统的安全性的改善通过防止另外的欺骗实践来赔偿它们自身。

[0003] 如果用户通常在特定区域购买东西，则一个几千英里之外的购买可以向 (flag) 系统标记这可能是一个欺骗性的交易。类似地，如果用户通常仅使用信用卡购买汽油，则如果该卡被用于购买昂贵的等离子体屏幕 TV，则该交易可能再次向系统标记。通常，现在的系统使用各种数据点来开发交易的可信分值。

[0004] 专利号为 5,629,981 (Nerlikar) 的美国专利公开了一种将交易的位置信息附着到安全交易的系统和方法，但是这种信息没有被用在认证用户是否有权访问系统以进入安全交易。Nerlikar 专门依赖 RFID 标签来确定位置。虽然 Nerlikar 教导基于位置来传输具有经认证的收条的交易，但是没有基于以前交易的位置的相关性来对用户进行认证。

[0005] 公开的序列号为 2006/0253894 (Bookman 等人) 的美国专利申请公开了一种安全移动计算平台，其将认证建立在所选的信任模型基础上，但是没有基于与以前的交易时间和位置的相关性来对用户进行认证。

[0006] 公开的序列号为 2007/0174082 (Singh) 的美国专利申请公开了一种认证系统和方法，其使用位置数据来生成提供认证置信度值 (confidence value) 的位置分值。没有提及与应用服务器和交易客户端上所存储的历史关联的时间和位置数据的组合。

发明内容

[0007] 简言之，一种认证方法包括步骤：提供具有安全服务器的交易服务提供商；提供用户；由用户向服务提供商的服务器请求访问授权，该服务器存储从该授权访问请求中获得的一组使用参数，在用户的后续的访问服务器的请求中，该使用参数至少包括供交易服务提供商在认证期间使用的若干先前位置坐标、访问方法、交易信息和所用的访问硬件，在认证中使用的使用参数将利用最新的数据持续进行更新。

[0008] 根据本发明的一个实施例，一种用于具有变化的唯一值的多因素认证的方法包括步骤：(a) 维护由用户所做的交易的访问历史数据库；(b) 维护输入设备上的客户端设备历史日志；(c) 接收来自所述输入设备的交易请求；(d) 使所述输入设备从所述客户端设备历史日志中选择子集；(e) 将所述子集与所述请求一起发送给认证服务器；(f) 将所述子集

与所述访问历史数据库进行比较；(g) 当在所述子集与所述访问历史数据库之间找到匹配时，继续处理所述交易；以及 (h) 当在所述子集与所述访问历史数据库之间没有找到任何匹配时，终止所述交易。

[0009] 根据本发明的一个实施例，一种用于具有变化的唯一值的多因素认证的计算机程序产品包括：计算机可读介质；用以维护由用户所做的交易的访问历史数据库的第一程序指令；用以维护输入设备上的客户端设备历史日志的第二程序指令；用以接收来自所述输入设备的交易请求的第三程序指令；用以使所述输入设备从所述客户端设备历史日志中选择子集的第四程序指令；用以将所述子集与所述请求一起发送给认证服务器的第五程序指令；用以将所述子集与所述访问历史数据库进行比较的第六程序指令；用以当在所述子集与所述访问历史数据库之间找到匹配时继续处理所述交易的第七程序指令；用以当在所述子集与所述访问历史数据库之间没有找到任何匹配时终止所述交易的第八程序指令；其中所述第一、第二、第三、第四、第五、第六、第七、第八程序指令被存储在所述计算机可读介质上。

[0010] 根据本发明的一个实施例，一种系统用变化的唯一值来执行多因素认证，该系统包括：由用户所做的交易的访问历史数据库；输入设备上的客户端设备历史日志；用于从所述输入设备接收交易请求的装置；用于使所述输入设备从所述客户端设备历史日志中选择子集的装置；用于将所述子集与所述请求一起发送给认证服务器的装置；用于将所述子集与所述访问历史数据库进行比较的装置；用于当在所述子集与所述访问历史数据库之间找到匹配时继续处理所述交易的装置；以及用于当在所述子集与所述访问历史数据库之间没有找到任何匹配时终止所述交易的装置。

[0011] 本发明一般地涉及针对安全交易的系统访问进行的用户认证。本发明特别涉及包括对于用户的先前交易历史是唯一的静态标识数据（账号、口令、输入设备序列号、生物统计学标识）以及动态数据（GPS 位置、日期、时间）的组合的认证标准。

附图说明

[0012] 图 1 示出根据本发明的一个实施例的、用于对交易进行认证的系统的概略图。

[0013] 图 2 是根据本发明的一个实施例的认证过程的流程图。

具体实施方式

[0014] 总体上，本发明是一种基于先前交易的参数（时间、方法和位置坐标）的历史来对安全交易的可能用户进行认证的系统。当新账号建立时，用户的设备可以被注册到系统，并且可以种植有（seed）在客户端设备和安全服务器都知道的伪交易历史的随机化列表。安全交易服务提供商接着维护账号 ID 号、访问日期、访问时间、访问方法（也即，标识用户的蜂窝电话、PDA 或来自具体计算机的网络访问的信息）、交易时间以及经由 GPS 信号的交易位置的数据库。

[0015] 合法用户能够从一个特定设备指明他的账号 ID 以及或许指明口令（password），从而可以通过比较已经从该特定设备做出的先前交易的历史（日期 / 时间和位置）来对用户进行认证。因此，来自没有保留任何交易参数数据的历史的其他设备的非授权访问是不可能的。

[0016] 例如,黑客可以通过键盘记录(keylogging)、窃听或屏幕截图技术来获得传统的账号证书(credential)。这些泄密的账号证书对于从其他设备来访问该账号是无用的,推测这些其他设备不包含任何先前交易的历史。

[0017] 如本领域的普通技术人员将意识到的那样,本发明可以具体实现成一种系统、方法或计算机程序产品。因此,本发明可以采用完全硬件实施例、完全软件实施例(包括固件、驻留软件、微码,等等)的形式、或者组合了软件和硬件方面的实施例的形式,它们在此可以总称为“电路”、“模块”或“系统”。此外,本发明可以采用在表达有计算机可用的程序代码的任何有形的介质中具体实现的计算机程序产品的形式。

[0018] 一个或多个计算机可用或计算机可读介质的任何组合都可以被使用。计算机可用或计算机可读介质可以是(但不限于)例如电子的、磁的、光的、电磁的、红外的或半导体的系统、装置、设备或传播介质。计算机可读介质的更为具体的例子(非穷举列表)将包括以下:具有一个或多个导线的电气连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦写可编程只读存储器(EPROM或闪存)、光纤、便携式致密盘只读存储器(CD-ROM)、光存储设备、诸如支持因特网或内部网的那些传输介质,或者磁存储设备。注意,计算机可用或计算机可读介质甚至可以是纸或可以打印程序的另外的合适的介质,因为程序可以经由例如对纸或其他介质的光学扫描而被电气捕获、接着被编辑、被翻译或者以合适的方式来进行其他处理,如果必要,并且接着被存储在计算机存储器中。在本文档的上下文中,计算机可用的或计算机可读的介质可以是可以包含、存储、通信、传播或传送程序以供由指令执行系统、装置或设备或结合其来使用的任意介质。计算机可用介质可以包括其中包含计算机可用程序代码的传播的数据信号,其可以是在基带中或者可以作为载波的一部分。计算机可用程序代码可以通过使用任何合适的介质来传输,这些介质包括但不限于无线、有线、光缆、RF等等。

[0019] 用于执行本发明的操作的计算机程序代码可以用一种或多种编程语言的任何组合来编写,这些语言包括诸如Java、Smalltalk、C++等等之类的面向对象的编程语言和诸如“C”编程语言或类似的编程语言之类的传统过程语言。程序代码可全部在用户的计算机上、部分地在用户的计算机上作为单机软件包执行、部分地在用户计算机上且部分地在远程计算机上执行、或者全部在远程计算机或服务器上执行。在后面这种情况下,远程计算机可以经由任何类型的网络连接到用户计算机,这些网络包括局域网(LAN)或广域网(WAN)或者可以连接到外面计算机的连接(例如,通过使用因特网服务提供商的因特网)。

[0020] 下面,参考根据本发明的实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图来描述本发明。应当理解,流程图和/或框图中的每个框、以及流程图和/或框图中的框的组合,可以用计算机程序指令来实现。这些计算机程序指令可以提供给通用计算机、专用计算机或者产生机器的其他可编程数据处理装置中的处理器,从而经由计算机或其他可编程的数据处理装置的处理器来执行指令时,创建用于实现在流程图和/或框图的一个或多个框中所指明的功能/行为。

[0021] 这些计算机程序指令还被存储在计算机可读介质中,其可以命令计算机或其他可编程数据处理装置以特定方式来工作,从而在计算机可读介质中所存储的这些指令产生一个制造品,其包括实现流程图和/或框图的一个或多个框中所指明的功能/行为的指令装置。

[0022] 该计算机程序指令还可被装载到计算机或其他可编程数据处理装置上,以使得一系列操作步骤在该计算机或其他可编程装置上执行以产生计算机实现的处理,从而在计算机或其他可编程装置上执行的指令提供用于实现在流程图和 / 或框图的一个或多个框中所指明的功能 / 行为的处理。

[0023] 参考图 1,用户 10 经由输入设备 12 输入安全交易请求,该输入设备 12 可以是 PDA、蜂窝电话、专用机器,等等。输入设备 12 将访问服务的认证请求与来自输入设备 12 中所保存的(或者保存在存储器中的或者保存在直接访问存储设备中的)客户端设备历史日志的交易历史的子集(也即部分或全部)一起发送给管理服务器 14。在代表用户处理该交易之前,对该访问尝试进行认证。该认证请求通常包含常用的安全数据(诸如口令和账号标识),并且可包括诸如指纹之类的生物统计学标识的形式的附加安全数据。

[0024] 管理服务器 14 将认证请求传递给认证服务器 24,认证服务器 24 处理对该请求的认证。认证服务器 24 接收认证请求和输入设备 12 上的交易历史的子集。认证服务器 24 将该子集与来自管理服务器 14 所维护的访问历史数据库 16 的用户的访问历史进行比较。如果输入设备 12 子集与管理服务器 14 中的访问历史数据库 16 相匹配,则该请求得到认证,并且管理服务器 14 命令交易服务器 18 继续处理交易,如框 22 中所示。交易服务器 18 还确保交易历史(例如记录日期、时间、位置、设备 ID 和交易 ID)被记录在交易历史数据库 20 和输入设备 12 中的客户端设备历史日志二者中。

[0025] 交易服务器 18 可以在与认证服务器 24 相同的计算机上,或者可以是在不同位置处的一个完全不同的计算机。也即,两个应用(认证和交易处理)可以运行在相同的计算机上,或者两个应用均可以运行在它们自己的计算机上,在后一种情况下交易从认证服务器 24 经由管理服务器 14 传输到交易服务器 18。

[0026] 管理服务器 14 的作用是执行确定交易请求是否被授权的应用。一个常见的例子可以是银行余额查询交易请求,其首先需要通过由认证服务器上的应用所执行的验证操作。该交易请求被附着到由请求交易的用户所输入的账号和 PIN。在处理该交易之前,认证服务器必须验证所提供的身份证件是否足够来进行该交易。

[0027] 参考图 2,示出了根据本发明的一个实施例的方法。在步骤 30 中,用户通过使用输入设备 12 向管理服务器 14 请求认证,该输入设备 12 在存储器或直接访问存储设备中具有交易历史。在步骤 32 中,选择该设备上的交易历史的子集(部分或全部)。在步骤 34 中,该认证请求和交易历史被传输到管理服务器 14。在步骤 36 中,认证服务器 24 从管理服务器 14 接收访问历史数据库 16。在步骤 38 中,认证服务器 24 确定输入设备交易历史是否与管理服务器历史相匹配,如果不匹配,则在步骤 40 中,该认证失败,发送错误消息并且记录该尝试。如果在步骤 38 中该请求得到认证,则在步骤 42 中,该交易继续前进,在此之后,在步骤 44 中更新数据库 16 并且更新输入设备 12 中的输入设备历史日志。

[0028] 同样,下面参考表 1 和表 2,示出本发明的实施例的一个例子。从具有序列号 7003021、账号 waynedelia、口令 <passwd>、生物统计学标识 <thumbprint(拇指指纹)> 的设备做出对访问 www.chase.com 上的服务的认证请求。从客户端设备历史日志文件(表 1)中抽取针对 Chase Bank 公司的先前访问交易的子集,并将其传输给 Chase 认证服务器。来自客户端设备历史日志的记录与认证服务器主数据库(访问历史数据库 16)的比较将确定认证。表 2 示出访问历史数据库 16 中的记录的例子。

[0029] 本发明的方法如下防止非授权的使用：由黑客、窃听器等等经由其他设备输入的泄密的主要认证访问参数（也即，账号 / 口令或生物统计学信息）被限制，因为该非法输入设备与在认证服务器上所存储的具有先前的交易日期、时间和位置的预期的交易历史子集不匹配。

[0030]

账号	口令	生物统计学 ID	日期	时间	位置	服务类型	服务位置
waynedelia	<passwd>	<thumb print>	2008.10.01	15:32	<loc>	转账	www.chase.com
waynedelia	<passwd>	<thumb print>	2008.10.05	08:17	<loc>	取款	www.chase.com
Deliaw	<passwd>	<thumb print>	2008.10.07	12:25	<loc>	查询	www.hvfcu.org
waynedelia	<passwd>	<thumb print>	2008.10.12	14:05	<loc>	存款	www.chase.com

[0031] 表 1 :客户端输入设备上的设备交易历史日志文件 (加密的)

[0032]

设备 ID	账号	口令	生物统计学 ID	日期	时间	位置	服务类型	服务位置

7003021	waynedelia	<passwd>	<thumb print>	2008. 10. 01	15:32	<loc>	转账	<u>www.chase.com</u>
7003021	waynedelia	<passwd>	<thumb print>	2008. 10. 05	08:17	<loc>	取款	<u>www.chase.com</u>
6453827	edkelley	<passwd>	<thumb print>	2008. 10. 08	07:13	<loc>	取款	<u>www.chase.com</u>
7003021	waynedelia	<passwd>	<thumb print>	2008. 10. 12	14:05	<loc>	存款	<u>www.chase.com</u>

[0033] 表 2 :服务提供商 Chase 银行公司的服务提供商的管理服务器数据库上的认证历史日志表 (加密的)

[0034] 尽管已经参考优选实施例和附图描述了本发明,但是本领域的普通技术人员应该理解,本发明不局限于优选的实施例,并且在不偏离在所附权利要求书中所定义的本发明的范围的条件下可以做出各种修改等等。

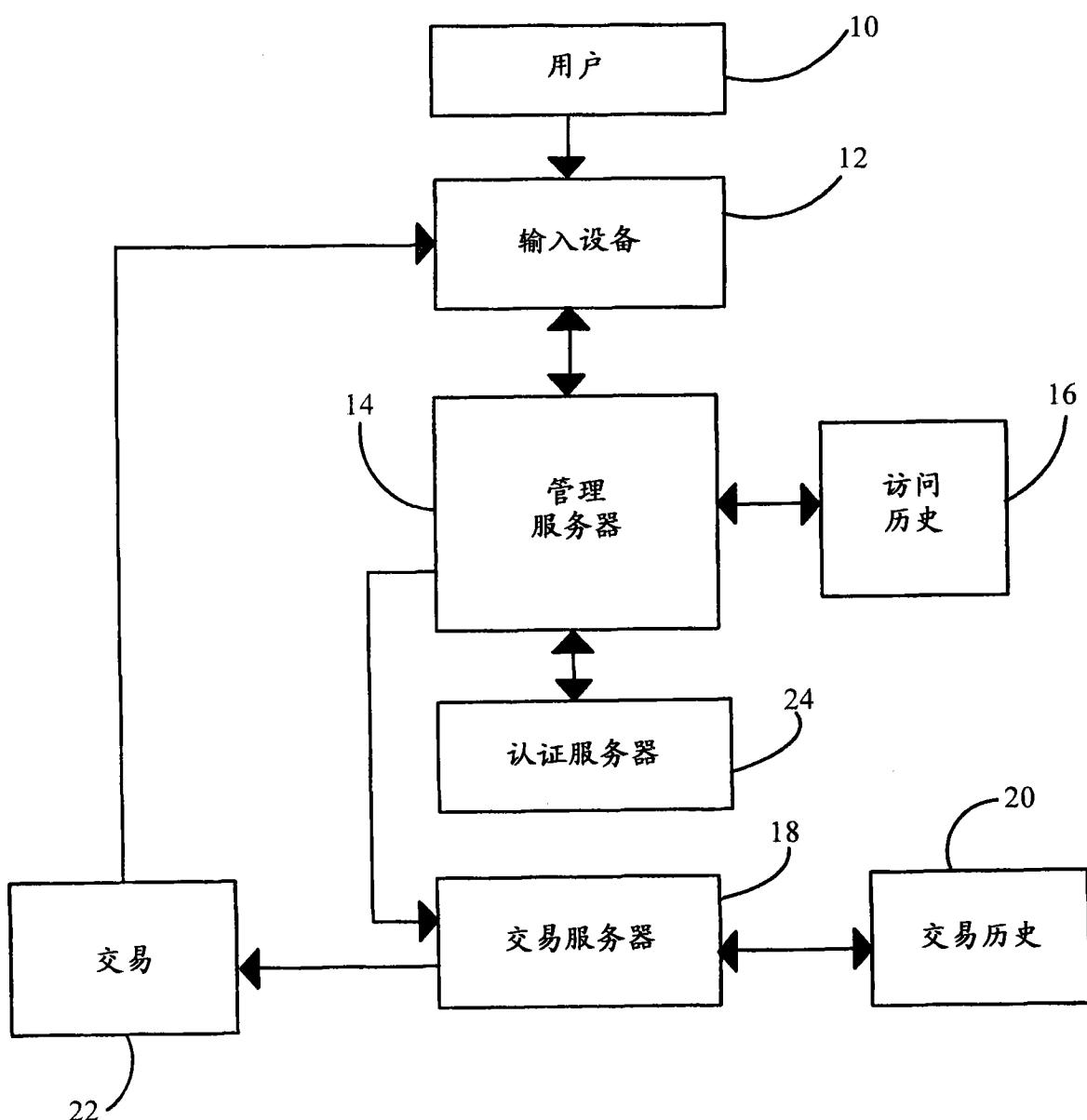


图 1

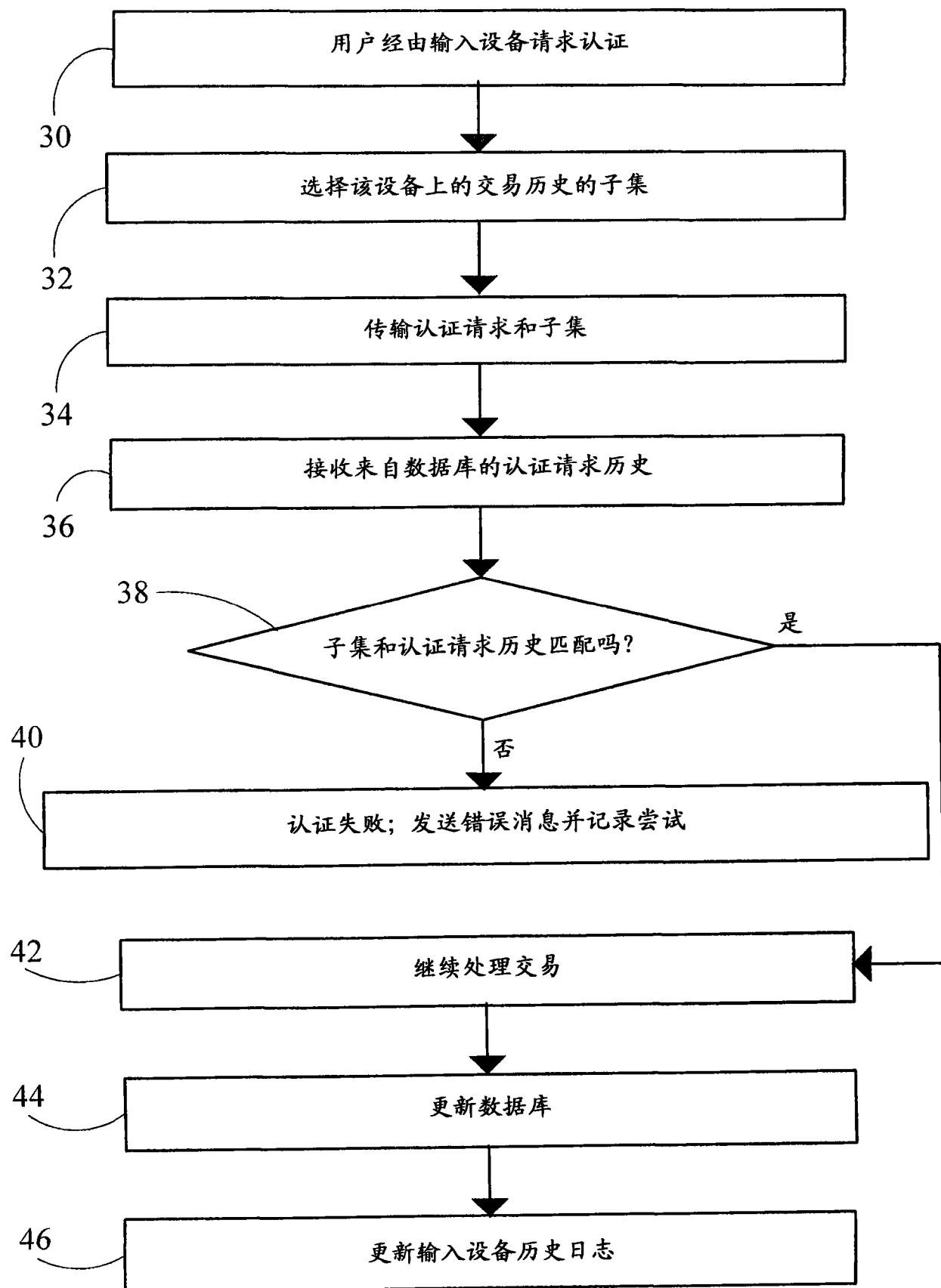


图 2