



(12) 发明专利申请

(10) 申请公布号 CN 104125064 A

(43) 申请公布日 2014. 10. 29

(21) 申请号 201310156443. 5

(22) 申请日 2013. 04. 28

(71) 申请人 阿里巴巴集团控股有限公司

地址 英国英属开曼群岛大开曼资本大厦一
座四层 847 号邮箱

(72) 发明人 任宏伟

(74) 专利代理机构 北京安信方达知识产权代理
有限公司 11262

代理人 吴艳 栗若木

(51) Int. Cl.

H04L 9/32(2006. 01)

H04L 29/08(2006. 01)

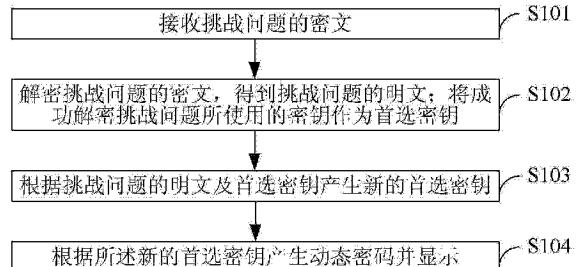
权利要求书3页 说明书15页 附图2页

(54) 发明名称

一种动态密码认证方法、客户端及认证系统

(57) 摘要

本申请公开了一种动态密码认证方法、客户端及认证系统；所述方法包括：接收挑战问题的密文；解密挑战问题的密文，得到挑战问题的明文；将成功解密挑战问题所使用的密钥作为首选密钥；根据所述挑战问题的明文及首选密钥产生新的首选密钥；根据所述新的首选密钥产生动态密码并显示。本申请能够更好地进行互联网应用中的身份认证。



1. 一种动态密码认证方法,包括:

接收挑战问题的密文;

解密挑战问题的密文,得到挑战问题的明文;将成功解密挑战问题所使用的密钥作为首选密钥;

根据所述挑战问题的明文及首选密钥产生新的首选密钥;

根据所述新的首选密钥产生动态密码并显示。

2. 如权利要求1所述的方法,其特征在于,所述从网络侧接收挑战问题的密文的步骤包括:

扫描网络侧生成的二维码图片,该二维码图片通过对挑战问题的密文编码产生;

对所述二维码图片解码得到挑战问题的密文。

3. 如权利要求1所述的方法,其特征在于:

所述挑战问题中至少包括交易数据;

所述根据挑战问题的明文及首选密钥产生新的首选密钥的步骤前还包括:

从所述挑战问题的明文中提取交易数据;

显示所述交易数据;

收到用户输入的确认信息后,进行所述根据挑战问题的明文及产生新的首选密钥的步骤。

4. 如权利要求3所述的方法,其特征在于:

所述挑战问题中至少包括起始时间;所述起始时间为所述挑战问题的产生时间;

所述显示所述交易数据的步骤前还包括:

从所述挑战问题的明文中提取起始时间;

判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值;

如果大于,则提示用户是否继续;

如果不小于,或接收到用户要求继续的指令则进行所述显示交易数据的步骤。

5. 如权利要求1到4中任一项所述的方法,其特征在于,所述解密挑战问题的密文,得到挑战问题的明文,将成功解密挑战问题所使用的密钥作为首选密钥的步骤包括:

采用首选密钥解密挑战问题的密文,如果解密成功则得到挑战问题的明文;如果失败,则采用次选密钥解密所述挑战问题的密文,如果解密成功则得到挑战问题的明文,将次选密钥作为首选密钥;如果解密失败则结束认证;

当采用首选密钥解密成功时,所述根据所述挑战问题的明文及首选密钥产生新的首选密钥的步骤前还包括:

将原先的首选密钥作为新的次选密钥。

6. 一种动态密码认证方法,包括:

当需要对用户进行认证时,产生对应于待认证用户的挑战问题,并根据该待认证用户对应的首选密钥加密所述挑战问题;

发送挑战问题的密文;

当接收到所述待认证用户输入的动态密码后,根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥;根据该新的首选密钥生成动态密码,并与接收的动态密码比对;如果一致,则完成认证。

7. 如权利要求 6 所述的方法,其特征在于,所述发送挑战问题的密文的步骤包括 :

根据挑战问题的密文进行编码,生成二维码图片数据 ;

发送所生成的二维码图片数据。

8. 如权利要求 6 或 7 所述的方法,其特征在于 :

所述挑战问题中至少包括起始时间 ;所述起始时间为所述挑战问题的产生时间 ;

所述根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥的步骤前还包括 :

从所述挑战问题的明文中提取起始时间 ;

判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值 ;如果大于,则结束认证 ;如果不小于,则进行根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥的步骤。

9. 一种客户端,其特征在于,包括 :

接收单元,用于接收挑战问题的密文 ;

解密单元,用于解密挑战问题的密文,得到挑战问题的明文 ;将成功解密挑战问题所使用的密钥作为首选密钥 ;

更新单元,用于根据所述挑战问题的明文及首选密钥产生新的首选密钥 ;

动态密码生成单元,用于根据所述新的首选密钥产生动态密码并显示。

10. 如权利要求 9 所述的客户端,其特征在于,所述接收单元从网络侧接收挑战问题的密文是指 :

所述接收单元扫描网络侧生成的二维码图片,该二维码图片通过对挑战问题的密文编码产生 ;对所述二维码图片解码得到挑战问题的密文。

11. 如权利要求 9 所述的客户端,其特征在于 :

所述挑战问题中至少包括交易数据 ;

所述客户端还包括 :

验证单元,用于在所述更新单元根据挑战问题的明文及首选密钥产生新的首选密钥前,从所述挑战问题的明文中提取交易数据,显示所述交易数据 ;收到用户输入的确认信息后,指示所述更新单元根据挑战问题的明文及产生新的首选密钥。

12. 如权利要求 11 所述的客户端,其特征在于 :

所述挑战问题中至少包括起始时间 ;所述起始时间为所述挑战问题的产生时间 ;

所述验证单元还用于在显示所述交易数据前,从所述挑战问题的明文中提取起始时间 ;判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值 ;如果大于,则提示用户是否继续 ;如果不小于,或接收到用户要求继续的指令则显示交易数据。

13. 如权利要求 9 到 12 中任一项所述的客户端,其特征在于,所述解密单元解密挑战问题的密文,得到挑战问题的明文,将成功解密挑战问题所使用的密钥作为首选密钥是指 :

所述解密单元采用首选密钥解密挑战问题的密文,如果解密成功则得到挑战问题的明文 ;如果失败,则采用次选密钥解密所述挑战问题的密文,如果解密成功则得到挑战问题的明文,将次选密钥作为首选密钥 ;如果解密失败则结束认证 ;

所述更新单元还用于当所述解密单元采用首选密钥解密成功时,在根据所述挑战问题的明文及首选密钥产生新的首选密钥前,将原先的首选密钥作为新的次选密钥。

14. 一种认证系统,其特征在于,包括 :

生成单元,用于当需要对用户进行认证时,产生对应于待认证用户的挑战问题;

加密单元,用于根据该待认证用户对应的首选密钥加密所述挑战问题;

通信单元,用于发送挑战问题的密文,接收所述待认证用户输入的动态密码;

认证单元,用于当所述通信单元接收到动态密码后,根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥;根据该新的首选密钥生成动态密码,并与接收的动态密码比对;如果一致,则完成认证。

15. 如权利要求 14 所述的认证系统,其特征在于,所述通信单元发送挑战问题的密文是指 :

所述通信单元根据挑战问题的密文进行编码,生成二维码图片数据;发送所生成的二维码图片数据。

16. 如权利要求 14 或 15 所述的认证系统,其特征在于 :

所述挑战问题中至少包括起始时间;所述起始时间为所述挑战问题的产生时间;

所述认证系统还包括 :

判断单元,用于在所述认证单元根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥前,从所述挑战问题的明文中提取起始时间,判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值;如果大于,则结束认证;如果不大于,则指示所述认证单元根据待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥。

一种动态密码认证方法、客户端及认证系统

技术领域

[0001] 本发明涉及网络安全领域，尤其涉及一种动态密码认证方法、客户端及认证系统。

背景技术

[0002] 随着互联网对社会的影响日益深入，越来越多的交易转移到网络上进行，然而网络环境安全性则不容乐观，病毒、木马横行，身份、账户被盗的情况屡见不鲜。虽然现有方案中有些会根据不同场景采用不同密码（比如登录或查询时用一个密码，支付时用另一个密码），但支付时采用的密码本质上还是静态密码，并且该密码也用于任何一笔交易，被盗后对用户的资金安全将造成重大威胁。

[0003] 互联网上目前的身份认证系统大致有下列几种：

[0004] 静态口令认证，缺陷在于一个密码多次使用，若密码被窃取，则很容易被假冒身份。

[0005] 基于硬件动态口令认证（事件、时间同步型），如 RSA SecurID；缺陷在于需要购买硬件设备，成本较高，存在同步问题，且产生的密码与业务无关，存在中间人窃取密码或篡改交易信息的可能。

[0006] 基于硬件动态口令认证（挑战应答型），带数字键盘，用户将挑战问题在令牌中输入，将得到的动态密码提交给后台系统认证身份，优点是密码与交易内容绑定；缺陷在于需要购买硬件设备，需要用户手工输入交易信息，不太方便，硬件的使用寿命一般是3-5年，成本较高。

[0007] 数字证书硬件（第一代 USBKey），借助 USBKey 来保存密钥，安全性较高；缺陷在于需要购买 USBKey，成本较高；而且对客户端系统有要求，下载安全补丁、安装证书对用户电脑操作水平要求较高；另外通过 USB 接口与电脑连接，存在被木马控制的风险。

[0008] 数字证书硬件（第二代 USBKey），安全性较高，带液晶屏，可显示交易内容，并且有用户确认键，需用户手工操作才可生成数字签名，可防范木马控制。缺陷在于需要购买 USBKey，成本较高，还需要安装相关软件、驱动程序，下载证书等，对用户电脑操作水平要求较高。

[0009] 基于手机短信的动态密码认证，服务端向用户手机发一条短信，包含用于认证身份的动态密码。此方案缺陷在于运营成本较高，发送短信需要向移动运营商支付费用，并且受移动通信网络影响，短信接收存在延迟，甚至接收不到短信；而且同样存在被中途被截获后假冒用户身份问题。

发明内容

[0010] 本申请要解决的技术问题是如何更好地进行互联网应用中的身份认证。

[0011] 为了解决上述问题，本申请提供了一种动态密码认证方法，包括：

[0012] 接收挑战问题的密文；

[0013] 解密挑战问题的密文，得到挑战问题的明文；将成功解密挑战问题所使用的密钥

作为首选密钥；

- [0014] 根据所述挑战问题的明文及首选密钥产生新的首选密钥；
- [0015] 根据所述新的首选密钥产生动态密码并显示。
- [0016] 进一步地，所述从网络侧接收挑战问题的密文的步骤包括：
- [0017] 扫描网络侧生成的二维码图片，该二维码图片通过对挑战问题的密文编码产生；
- [0018] 对所述二维码图片解码得到挑战问题的密文。
- [0019] 进一步地，所述挑战问题中至少包括交易数据；
- [0020] 所述根据挑战问题的明文及首选密钥产生新的首选密钥的步骤前还包括：
 - [0021] 从所述挑战问题的明文中提取交易数据；
 - [0022] 显示所述交易数据；
- [0023] 收到用户输入的确认信息后，进行所述根据挑战问题的明文及产生新的首选密钥的步骤。
- [0024] 进一步地，所述挑战问题中至少包括起始时间；所述起始时间为所述挑战问题的产生时间；
 - [0025] 所述显示所述交易数据的步骤前还包括：
 - [0026] 从所述挑战问题的明文中提取起始时间；
 - [0027] 判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值；
 - [0028] 如果大于，则提示用户是否继续；
 - [0029] 如果不大于，或接收到用户要求继续的指令则进行所述显示交易数据的步骤。
- [0030] 进一步地，所述解密挑战问题的密文，得到挑战问题的明文，将成功解密挑战问题所使用的密钥作为首选密钥的步骤包括：
 - [0031] 采用首选密钥解密挑战问题的密文，如果解密成功则得到挑战问题的明文；如果失败，则采用次选密钥解密所述挑战问题的密文，如果解密成功则得到挑战问题的明文，将次选密钥作为首选密钥；如果解密失败则结束认证；
 - [0032] 当采用首选密钥解密成功时，所述根据所述挑战问题的明文及首选密钥产生新的首选密钥的步骤前还包括：
 - [0033] 将原先的首选密钥作为新的次选密钥。
 - [0034] 本申请还提供了一种动态密码认证方法，包括：
 - [0035] 当需要对用户进行认证时，产生对应于待认证用户的挑战问题，并根据该待认证用户对应的首选密钥加密所述挑战问题；
 - [0036] 发送挑战问题的密文；
 - [0037] 当接收到所述待认证用户输入的动态密码后，根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥；根据该新的首选密钥生成动态密码，并与接收的动态密码比对；如果一致，则完成认证。
 - [0038] 进一步地，所述发送挑战问题的密文的步骤包括：
 - [0039] 根据挑战问题的密文进行编码，生成二维码图片数据；
 - [0040] 发送所生成的二维码图片数据。
 - [0041] 进一步地，所述挑战问题中至少包括起始时间；所述起始时间为所述挑战问题的产生时间；

[0042] 所述根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥的步骤前还包括：

[0043] 从所述挑战问题的明文中提取起始时间；

[0044] 判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值；如果大于，则结束认证；如果不大于，则进行根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥的步骤。

[0045] 本申请还提供了一种客户端，包括：

[0046] 接收单元，用于接收挑战问题的密文；

[0047] 解密单元，用于解密挑战问题的密文，得到挑战问题的明文；将成功解密挑战问题所使用的密钥作为首选密钥；

[0048] 更新单元，用于根据所述挑战问题的明文及首选密钥产生新的首选密钥；

[0049] 动态密码生成单元，用于根据所述新的首选密钥产生动态密码并显示。

[0050] 进一步地，所述接收单元从网络侧接收挑战问题的密文是指：

[0051] 所述接收单元扫描网络侧生成的二维码图片，该二维码图片通过对挑战问题的密文编码产生；对所述二维码图片解码得到挑战问题的密文。

[0052] 进一步地，所述挑战问题中至少包括交易数据；

[0053] 所述客户端还包括：

[0054] 验证单元，用于在所述更新单元根据挑战问题的明文及首选密钥产生新的首选密钥前，从所述挑战问题的明文中提取交易数据，显示所述交易数据；收到用户输入的确认信息后，指示所述更新单元根据挑战问题的明文及产生新的首选密钥。

[0055] 进一步地，所述挑战问题中至少包括起始时间；所述起始时间为所述挑战问题的产生时间；

[0056] 所述验证单元还用于在显示所述交易数据前，从所述挑战问题的明文中提取起始时间；判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值；如果大于，则提示用户是否继续；如果不大于，或接收到用户要求继续的指令则显示交易数据。

[0057] 进一步地，所述解密单元解密挑战问题的密文，得到挑战问题的明文，将成功解密挑战问题所使用的密钥作为首选密钥是指：

[0058] 所述解密单元采用首选密钥解密挑战问题的密文，如果解密成功则得到挑战问题的明文；如果失败，则采用次选密钥解密所述挑战问题的密文，如果解密成功则得到挑战问题的明文，将次选密钥作为首选密钥；如果解密失败则结束认证；

[0059] 所述更新单元还用于当所述解密单元采用首选密钥解密成功时，在根据所述挑战问题的明文及首选密钥产生新的首选密钥前，将原先的首选密钥作为新的次选密钥。

[0060] 本申请还提供了一种认证系统，包括：

[0061] 生成单元，用于当需要对用户进行认证时，产生对应于待认证用户的挑战问题；

[0062] 加密单元，用于根据该待认证用户对应的首选密钥加密所述挑战问题；

[0063] 通信单元，用于发送挑战问题的密文，接收所述待认证用户输入的动态密码；

[0064] 认证单元，用于当所述通信单元接收到动态密码后，根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥；根据该新的首选密钥生成动态密码，并与接收的动态密码比对；如果一致，则完成认证。

[0065] 进一步地,所述通信单元发送挑战问题的密文是指:

[0066] 所述通信单元根据挑战问题的密文进行编码,生成二维码图片数据;发送所生成的二维码图片数据。

[0067] 进一步地,所述挑战问题中至少包括起始时间;所述起始时间为所述挑战问题的产生时间;

[0068] 所述认证系统还包括:

[0069] 判断单元,用于在所述认证单元根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥前,从所述挑战问题的明文中提取起始时间,判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值;如果大于,则结束认证;如果不小于,则指示所述认证单元根据待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥。

[0070] 本申请的至少一个备选方案在每次正确的认证后,双方同步更换密码,因此用户密钥被盗用后,用户下次使用时能够发现,可避免更大损失,防范密钥被盗。本申请的一个优选方案可利用用户现有智能手机,在手机中安装客户端软件,扫描二维码图片即可产生动态密码,对交易客户端无其他要求,如浏览器、补丁、控件等;无需联网,无需购买其他认证终端,无额外运营成本,成本低廉,使用方便。本申请的又一个优选方案使用客户独有密钥加密挑战问题,其他网站不可能产生有效的二维码图片,防范钓鱼网站。本申请的又一个优选方案在二维码图片中含有交易信息,用户可再次确认;含有交易时间,可用于提醒用户,并且由于动态密码与用户进行的交易绑定,即使密码被盗,对攻击者也毫无用处,防范中间人攻击。当然,实施本申请的任一产品必不一定需要同时达到以上所述的所有优点。

附图说明

[0071] 图1是实施例一的动态密码认证方法的流程示意图;

[0072] 图2是实施例三的动态密码认证方法的流程示意图;

[0073] 图3是实施例四的例子的流程示意图。

具体实施方式

[0074] 下面将结合附图及实施例对本申请的技术方案进行更详细的说明。

[0075] 需要说明的是,如果不冲突,本申请实施例以及实施例中的各个特征可以相互结合,均在本申请的保护范围之内。另外,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0076] 在一个典型的配置中,客户端或认证系统的计算设备可包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0077] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0078] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、

动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[0079] 实施例一、一种动态密码认证方法，如图 1 所示，包括：

[0080] S101、接收挑战问题的密文；

[0081] S102、解密挑战问题的密文，得到挑战问题的明文；将成功解密挑战问题所使用的密钥作为首选密钥；

[0082] S103、根据所述挑战问题的明文及首选密钥产生新的首选密钥；

[0083] S104、根据所述新的首选密钥产生动态密码并显示。

[0084] 本实施例中，产生的动态密码只能使用一次，用后将被废弃，因为下次认证时将会产生新的动态密码；因此能够有效防范密码被盗的问题。

[0085] 本实施例的一种备选方案中，所述步骤 S101 具体可以包括：

[0086] 扫描网络侧生成的二维码图片，该二维码图片通过对挑战问题的密文编码产生；

[0087] 对所述二维码图片解码得到挑战问题的密文。

[0088] 该备选方案中，挑战问题不需要输入，而是可以在连接网络侧的电脑（比如但不限于台式机或笔记本电脑）上采用二维码形式展现出来，含有二维码解码软件的智能手机或其它终端通过自带的摄像头扫描，即可获得挑战问题，相对于只能输入有限几位数字的现有方案，该备选方案中挑战问题的信息量可以更大，因此可以包含更多交易信息，以便用户对交易内容进行确认。

[0089] 该备选方案中的方法可以由一个客户端实现，用户只需要拿安装了该客户端的手机等终端对屏幕上的二维码拍照，即可得到动态密码，甚至不需要该客户端联网，对于手机等终端而言，运营成本几乎为零，用户成本也几乎为零，且没有延时情况。另外，该备选方案对用于展现二维码的电脑系统也没有特别的要求，操作相当简单；并且不需要客户端与电脑连接，不存在被电脑中的木马控制的问题。

[0090] 本实施例的一种备选方案中，所述挑战问题中包括：已认证次数 S、起始时间 T、交易数据 D、校验数据 C；还可增加其他信息。所述起始时间为所述挑战问题的产生时间；所述校验数据 C 可以但不限于为对挑战问题中的其它信息连接而成的数据进行杂凑运算后所得到结果中部分指定位置的数据。所述挑战问题可以但不限于由上述信息连接而成；其它备选方案中，也可以设置只在挑战问题中包括上述信息中任一种或其任意组合。

[0091] 该备选方案的一种实施方式中，所述步骤 S103 前还可以包括：

[0092] 从所述挑战问题的明文中提取交易数据；

[0093] 显示所述交易数据；

[0094] 收到用户输入的确认信息后进行所述步骤 S103。

[0095] 本实施方式中，动态密码可与交易数据绑定，用户确认后才产生动态密码，因此该动态密码只对用户确认的交易有效，即使被中间人攻击，拿到这个动态密码对攻击者来说也没有用，不会给用户造成损失。

- [0096] 该实施方式中,所述显示所述交易数据的步骤前还可以包括:
- [0097] 从所述挑战问题的明文中提取起始时间;所述起始时间为所述挑战问题的产生时间;
- [0098] 判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值;
- [0099] 如果大于,则提示用户是否继续;
- [0100] 如果不大于,或接收到用户要求继续的指令则进行所述显示交易数据的步骤。
- [0101] 当时间间隔是否大于预定时间阈值时,说明该挑战问题可能失效,提醒用户是否继续产生动态密码;如果用户要求继续则显示交易数据供用户确认;如果不要求继续则可以结束认证。
- [0102] 该备选方案中,在得到挑战问题的明文后还可以利用所述校验数据 C 验证所得到的挑战问题的明文是否有效;如果有效则进行步骤 S103;如果无效且采用的是首选密钥解密,则使用次选密钥尝试解密后再验证所得到的挑战问题的明文是否有效;如果无效且采用的是次选密钥解密,则说明首选密钥和次选密钥都不正确,结束认证。
- [0103] 本实施例的一种备选方案中,所述步骤 S102 具体可以包括:
- [0104] 采用首选密钥解密挑战问题的密文,如果解密成功则得到挑战问题的明文;如果失败,则采用次选密钥解密所述挑战问题的密文,如果解密成功则得到挑战问题的明文,将次选密钥作为首选密钥;如果解密失败则结束认证;
- [0105] 当采用首选密钥解密成功时,步骤 S103 前还可以包括:
- [0106] 将原先的首选密钥作为新的次选密钥。
- [0107] 这里“原先的首选密钥”就是指解密挑战问题的密文成功时用的密钥;比如最初的首选密钥为密钥 A,次选密钥为密钥 B;如果步骤 S102 中采用密钥 A 时解密成功,则在进行步骤 S103 前,将次选密钥也替换为密钥 A,步骤 S103 中是根据密钥 A 和挑战问题的明文产生新的首选密钥。如果步骤 S102 中采用密钥 A 解密不成功,采用密钥 B 解密成功,则以密钥 B 作为首选密钥,由于此时的次选密钥就是密钥 B,因此不用再更新次选密钥;步骤 S103 中是根据密钥 B 和所述挑战问题的明文生成新的首选密钥。
- [0108] 在其它备选方案中,也可以保存解密成功时所使用的密钥,在生成动态密码后将解密成功时所使用的密钥作为次选密钥。
- [0109] 当采用首选密钥和次选密钥都无法解密挑战问题的密文时,说明密钥与网络侧不同步,密钥有可能被盗;可以进一步提示用户联系厂家更新密钥。
- [0110] 本实施例的一种备选方案中,所述步骤 S103 具体可以包括:
- [0111] 采用基于杂凑算法的 MAC 生成算法对所述挑战问题的明文及首选密钥进行计算,将计算结果作为新的首选密钥。
- [0112] 其它备选方案中,也可以采用其它算法或处理过程来得到新的首选密钥。
- [0113] 本实施例的一种备选方案中,所述步骤 S104 具体可以包括:
- [0114] 采用杂凑算法对所述新的首选密钥进行计算;
- [0115] 截取计算结果中的部分数据;
- [0116] 将截取的数据对 10 的 N 次方取模;其中 N 为动态密码的位数。
- [0117] 其它备选方案中,也可以采用其它算法或处理过程来得到动态密码。
- [0118] 实施例二、一种动态密码认证方法,包括:

[0119] 当需要对用户进行认证时,产生对应于待认证用户的挑战问题,并根据该待认证用户对应的首选密钥加密所述挑战问题;

[0120] 发送挑战问题的密文;

[0121] 当接收到所述待认证用户输入的动态密码后,根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥;根据该新的首选密钥生成动态密码,并与接收的动态密码比对;如果一致,则完成认证。

[0122] 本实施例的一种备选方案中,所述发送挑战问题的密文的步骤可以包括:

[0123] 根据挑战问题的密文进行编码,生成二维码图片数据;

[0124] 发送所生成的二维码图片数据。

[0125] 该备选方案中,可以但不限于由待认证用户所登录的电脑显示二维码图片;在其它备选方案中不限于此,比如也可以是待认证用户事先设定的一个终端设备来显示二维码图片。

[0126] 本实施例的一种备选方案中,所述挑战问题中包括:已认证次数 S、起始时间 T、交易数据 D、校验数据 C;还可增加其他信息。所述起始时间为所述挑战问题的产生时间;所述校验数据 C 可以但不限于为对挑战问题中的其它信息连接而成的数据进行杂凑运算后所得到结果中部分指定位置的数据。所述挑战问题可以但不限于由上述信息连接而成;其它备选方案中,也可以设置只在挑战问题中包括上述信息中任一种或其任意组合。

[0127] 该备选方案的一种实施方式中,所述根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥的步骤前还可以包括:

[0128] 从所述挑战问题的明文中提取起始时间;

[0129] 判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值;如果大于,则结束认证;如果不大于,则进行根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥的步骤。

[0130] 本实施例的一种备选方案中,所述根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥的步骤中,是采用基于杂凑算法的 MAC 生成算法对所述挑战问题的明文及首选密钥进行计算,将计算结果作为新的首选密钥。其它备选方案中,也可以采用其它算法或处理过程来得到新的首选密钥,客户端和网络侧采用的算法或处理过程需相同。

[0131] 本实施例的一种备选方案中,所述根据新的首选密钥产生动态密码的步骤具体可以包括:

[0132] 采用杂凑算法对所述新的首选密钥进行计算;

[0133] 截取计算结果中的部分数据;

[0134] 将截取的数据对 10 的 N 次方取模;其中 N 为动态密码的位数。

[0135] 其它备选方案中,也可以采用其它算法或处理过程来得到动态密码,客户端和网络侧采用的算法或处理过程需相同。

[0136] 实施例三、一种动态密码认证方法,如图 2 所示,包括:

[0137] S201、当需要对用户进行认证时,网络侧产生对应于待认证用户的挑战问题,并根据该待认证用户对应的首选密钥加密所述挑战问题;

[0138] S202、发送挑战问题的密文;

- [0139] S203、所述待认证用户的客户端接收所述挑战问题的密文；
- [0140] S204、所述客户端解密挑战问题的密文，得到挑战问题的明文；将成功解密挑战问题所使用的密钥作为首选密钥；
- [0141] S205、所述客户端根据所述挑战问题的明文及所述首选密钥产生新的首选密钥；
- [0142] S206、所述客户端根据所述新的首选密钥产生动态密码并显示；
- [0143] S207、所述网络侧接收所述待认证用户输入的动态密码；
- [0144] S208、所述网络侧根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥；根据该新的首选密钥生成动态密码，并与接收的动态密码比对；如果一致，则所述网络侧完成认证。
- [0145] 本实施例在每次正确的认证后，网络侧和客户端同步更换密钥，因此用户的密钥被盗用后，在下次使用时能够发现，可避免更大损失。网络侧当生成的动态密码和接收的不一致时可结束认证。
- [0146] 本实施例的一种备选方案中，所述步骤 S202 具体可以包括：
- [0147] 根据挑战问题的密文进行编码，生成二维码图片数据；
- [0148] 根据所述二维码图片数据显示所生成的二维码图片；
- [0149] 相应地，所述步骤 203 具体可以包括：
- [0150] 所述待认证用户的客户端扫描所述二维码图片；
- [0151] 所述客户端对所述二维码图片解码得到挑战问题的密文。
- [0152] 该备选方案中，可以但不限于由待认证用户所登录的电脑显示二维码图片；在其它备选方案中不限于此，比如也可以是待认证用户事先设定的一个终端设备来显示二维码图片。
- [0153] 本实施例的一种备选方案中，所述挑战问题中包括：已认证次数 S、起始时间 T、交易数据 D、校验数据 C；还可增加其他信息。所述起始时间为所述挑战问题的产生时间；所述校验数据 C 可以但不限于为对挑战问题中的其它信息连接而成的数据进行杂凑运算后所得到结果中部分指定位置的数据。所述挑战问题可以但不限于由上述信息连接而成；其它备选方案中，也可以设置只在挑战问题中包括上述信息中任一种或其任意组合。
- [0154] 该备选方案的一种实施方式中，所述步骤 S205 前还可以包括：
- [0155] 所述客户端从所述挑战问题的明文中提取交易数据；
- [0156] 所述客户端显示所述交易数据；
- [0157] 所述客户端收到用户输入的确认信息后进行所述步骤 S205。
- [0158] 该实施方式中，所述客户端显示所述交易数据的步骤前还可以包括：
- [0159] 所述客户端从所述挑战问题的明文中提取起始时间；
- [0160] 所述客户端判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值；
- [0161] 如果大于，则所述客户端提示用户是否继续；
- [0162] 如果不大于，或接收到用户要求继续的指令则所述客户端进行所述显示交易数据的步骤。
- [0163] 所述步骤 S208 前还可以包括：
- [0164] 所述网络侧从所述挑战问题的明文中提取起始时间；所述起始时间为所述挑战问题的产生时间；

- [0165] 所述网络侧判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值；
[0166] 如果大于，则结束认证；
[0167] 如果不大于，则进行所述步骤 S208。
- [0168] 本实施例的一种备选方案中，所述步骤 S204 具体可以包括：
- [0169] 所述客户端采用首选密钥解密挑战问题的密文，如果解密成功则得到挑战问题的明文；如果失败，则采用次选密钥解密所述挑战问题的密文，如果解密成功则得到挑战问题的明文，将次选密钥作为首选密钥；如果解密失败则结束认证；
[0170] 如果采用首选密钥解密成功，则所述步骤 S205 前还可以包括：
[0171] 所述客户端将原先的首选密钥作为新的次选密钥。
[0172] 这里“原先的首选密钥”就是指解密挑战问题的密文成功时用的密钥；比如客户端最初的首选密钥为密钥 A，次选密钥为密钥 B；如果步骤 S204 中采用密钥 A 时解密成功，则在进行步骤 S205 前，将次选密钥也替换为密钥 A，步骤 S205 中是根据密钥 A 和挑战问题的明文产生新的首选密钥。如果步骤 S204 中采用密钥 A 解密不成功，采用密钥 B 解密成功，则以密钥 B 作为首选密钥，由于此时的次选密钥就是密钥 B，因此不用再更新次选密钥；步骤 S205 中是根据密钥 B 和所述挑战问题的明文生成新的首选密钥。
[0173] 在其它备选方案中，也可以保存解密成功时所使用的密钥，在生成动态密码后将解密成功时所使用的密钥作为次选密钥。
[0174] 当采用首选密钥和次选密钥都无法解密挑战问题的密文时，说明密钥与网络侧不同步，密钥有可能被盗；可以进一步提示用户联系厂家更新密钥。
[0175] 该备选方案中，所述客户端在得到挑战问题的明文后还可以利用所述校验数据 C 验证所得到的挑战问题的明文是否有效；如果有效则进行步骤 S205；如果无效且采用的是首选密钥解密，则使用次选密钥尝试解密后再验证所得到的挑战问题的明文是否有效；如果无效且采用的是次选密钥解密，则说明首选密钥和次选密钥都不正确，结束认证。
[0176] 本实施例的一种备选方案中，所述步骤 S205 和步骤 208 中，是采用基于杂凑算法的 MAC 生成算法对所述挑战问题的明文及首选密钥进行计算，将计算结果作为新的首选密钥。其它备选方案中，也可以采用其它算法或处理过程来得到新的首选密钥，客户端和网络侧采用的算法或处理过程需相同。
[0177] 本实施例的一种备选方案中，所述步骤 S206 和步骤 208 中根据新的首选密钥产生动态密码的步骤具体可以包括：
[0178] 采用杂凑算法对所述新的首选密钥进行计算；
[0179] 截取计算结果中的部分数据；
[0180] 将截取的数据对 10 的 N 次方取模；其中 N 为动态密码的位数。
[0181] 其它备选方案中，也可以采用其它算法或处理过程来得到动态密码，客户端和网络侧采用的算法或处理过程需相同。
[0182] 实施例四，一种动态密码认证方法，应用于网络支付情况下的认证；其它情况下的认证也可以参照本实施例进行。
[0183] 本实施例涉及以下设备：
[0184] 交易系统 (Transcation Server, 简写 TS)，具体业务系统，如：网上银行系统、购物网站等需要认证用户身份的系统。

[0185] 认证服务器 (Authentication Server, 简写 :AS), 重要的核心服务, 为交易系统提供动态密码的管理和验证功能, 功能如下 :

[0186] 认证策略管理, 包括动态密码长度、挑战问题有效期长度、认证失败锁定次数和时间等;

[0187] 批量产生用户共享密钥, 用户共享密钥是预先产生的, 根据设定的策略, 启动批量产生密钥任务, 调用随机数算法, 生成共享密钥, 并加密保存到后台数据库;

[0188] 用户共享密钥管理, 提供密钥与用户账户绑定与解除绑定、信息查询统计、激活、冻结、解冻、作废管理等功能。

[0189] 所述交易系统需要用到认证服务器的功能有 :

[0190] 获取新手机动态令牌密钥, 与账号绑定;

[0191] 获取二维码数据, 当需要认证用户身份时, 执行此操作, 将账户、交易内容提交给认证服务器, 得到二维码数据, 调用二维码图片产生库函数, 生成二维码图片, 并在页面显示;

[0192] 验证动态密码, 将账号、交易内容、动态密码提交给认证服务器, 并获取认证结果, 根据认证结果, 执行交易内容。

[0193] 在认证时, 认证服务器根据传入的账号、交易数据, 组织挑战问题, 并用账号对应的首选密钥加密, 形成二维码图片数据; 根据传入的账号、交易内容、动态密码等, 进行合法性检查, 更新该账号对应的首选密钥后根据新的首选密钥计算产生动态密码, 与用户输入动态密码比对, 并返回认证结果。

[0194] 客户端 (Mobile Application, 简写 MA), 可安装在智能手机或其它终端上。具有以下功能 :

[0195] 利用二维码, 导入用户密钥, 安全保护密钥;

[0196] 利用摄像头对电脑屏幕中二维码图片拍照, 解码得到密文的挑战问题;

[0197] 解密挑战问题的密文并验证其有效性;

[0198] 从挑战问题中提取交易数据并显示, 提示用户确认;

[0199] 更新手机内保存的密钥, 根据更新后的密钥产生动态密码。

[0200] 本实施例的一个例子中, 用户通过电脑连接交易系统, 进行网上支付; 通过安装了所述客户端的手机产生用于认证的动态密码。该例子的认证过程如图 3 所示, 包括步骤 S301 ~ S320。

[0201] S301、用户输入账号和登录密码, 登录交易系统。

[0202] 本例子的交易系统为每个用户分配两个密码 :a、登录密码, 初步验证用户身份, 即使丢失也不能造成大的影响 ;b、支付密码, 当用户进行下订单或转账时, 涉及资金转移时认证用户身份的密码。在该种交易系统中, 动态密码为支付密码。

[0203] S302、交易服务器验证用户身份, 显示交易页面。根据交易系统不同, 后续用户的操作也不同。

[0204] S303、当用户在交易系统中需要进行支付操作时, 如 :付款、转账等, 交易系统进入支付环节, 进行步骤 S304。

[0205] S304、交易系统需要再次认证用户身份, 根据该用户已有的账户信息, 结合交易内容, 向认证服务器发出“获取二维码”操作;

[0206] S305、认证服务器根据账号查询数据库, 获取该用户的首选密钥, 生成挑战问题 (CQ)。

[0207] 挑战问题是服务器向客户端提出的问题, 客户端利用首选密钥, 采用约定的算法, 生成动态密码, 来“回答”问题, 证明身份。

[0208] 本例子中挑战问题 CQ 包括已认证次数 S、起始时间 T、交易数据 D、校验数据 C ;
 $CQ = S | T | D | C$; 其中, “|”表示数据追加, 如 : “ab” | “cd” = “abcd”。

[0209] 本例子中, 认证次数 S 表示用户认证成功的次数, 长度为两字节。

[0210] 起始时间 T 可以但不限于是认证服务器产生挑战问题时的时间。客户端设置超时时间窗, 当扫描二维码时, 检查二维码图片中包含的时间与手机系统时间差值, 若超出时间窗范围, 则警告用户, 挑战问题可能已过期。由于用户手机时间不一定准确, 有可能是由于用户手机内置时钟不正确导致的超时, 所以这里仅提醒, 用户可选择继续向下进行。另外, 加入时间信息后, 即使交易内容相同, 由于每次交易的时间不同, 因此挑战问题 CQ 也是不同的, 避免出现相同的 CQ。

[0211] 交易数据 D 指用户在业务进行中个性化操作内容。如 : 登录网上银行中, 转账操作中的对方银行账户、姓名、转账金额等; 登录购物网站中, 选购的商品名称、店铺名称、收货地址等; 其他网站预留的个性化信息等。交易数据将会在手机客户端显著位置显示, 并提示用户确认, 用户需手动按“确认”按钮后, 才能产生验证码, 防止被篡改。

[0212] 校验位 C, 由认证次数 S、起始时间 T、交易数据 D 三部分计算得出, 对应解密得到的挑战问题, 用来验证挑战问题是否合法。

[0213] $C = \text{Truncate}(\text{Hash}(S | T | D), 4)$;

[0214] 其中, $\text{Truncate}(P1, P2)$ 表示从指定数据 P1 中截取部分内容, 长度由 P2 决定。如 : 设 $S = “abcde”$, 则 $\text{Truncate}(S, 2) = “de”$ 。截取方式有多种, 如从 P1 的最前面开始截取, 或者从 P1 的末尾开始截取, 也可以根据某个字节内容, 确定开始位置, 进行截取。为了简单处理, 本例子中是从 P1 的末尾截取。

[0215] S306、认证服务器使用该用户的首选密钥 (FK), 采用对称加密算法加密挑战问题 (CQ), 得到挑战问题的密文 (ECQ), 该密文就是二维码图片数据, 即 :

[0216] $ECQ = \text{Encrypt}(FK, CQ)$;

[0217] Encrypt 是对称加密算法中的加密操作, 如 : DES、TripleDES、AES 等。

[0218] ECQ 是用首选密钥加密后的挑战问题密文, 也是二维码图片数据, 以二维码图片形式展现。手机通过扫描二维码图片, 解码得到此数据, 实现了将交易系统的数据“传输”到手机客户端软件中过程, 而这个过程, 手机和电脑之间无须存在任何形式的物理连接, 最大限度保证了电脑与手机的隔离, 大大提高安全性。

[0219] S307、认证服务器发送 ECQ 给交易系统。

[0220] S308、交易系统根据 ECQ, 生成二维码图片并在页面显著位置显示, 提示用户打开手机客户端, 进行拍照扫描。

[0221] S309、用户打开手机中客户端软件, 扫描二维码图片 ;

[0222] S310、客户端软件解码二维码图片得到挑战问题的密文, 即 ECQ ; 使用所述用户的 FK(首选密钥)解密 ECQ, 得到挑战问题的明文, 验证挑战问题的明文的有效性, 若有效则进入步骤 S311 ;

[0223] 如果采用首选密钥无法解密,则采用 SK(次选密钥)解密 ECQ,得到挑战问题的明文,验证挑战问题的明文的有效性,若有效则将次选密钥作为首选密钥,进入步骤 S311;

[0224] 挑战问题的明文 CQ 为:

[0225] $CQ = \text{Decrypt}(FK, ECQ)$, 或 $CQ = \text{Decrypt}(SK, ECQ)$;

[0226] Decrypt 是对称加密算法中的解密操作,如:DES、TripleDES、AES 等。

[0227] 如果采用次选密钥也无法解密,说明密钥与服务器不同步,密钥有可能被盗,提示用户联系厂家更新密钥,认证结束。

[0228] 最初的首选密钥由认证服务器随机产生,并导入到手机客户端。作用:1、加密挑战问题;2、与挑战问题一同计算,得到新的首选密钥。本例子中,首选密钥是变化的,是当前最新产生的密钥;每次认证成功,双方将同步更新首选密钥。次选密钥是最新密钥产生前的上一个密钥。

[0229] 在服务端,只需要保留最新密钥,每次认证成功,重新计算并更新;而在手机客户端,每次产生动态密码,也会生成新密钥,即:首选密钥,但是旧密钥还不能丢,因为此时动态密码还没有经过服务器认证,而服务器只有对这个动态密码验证通过后,才能将密钥更新到与手机客户端相同的值,即“密钥同步一致”,而用户生成动态密码后,处理提交服务器进行认证,并认证成功外,还有可能认证失败(若经过长时间才输入认证),或者根本就不提交到服务器,这样的话,服务器保存的还是旧密钥,而手机客户端已经更新了一代密钥,若再次进行交易,重新获取挑战问题时,双方使用的密钥将不一致,因此,为了保持一致,手机客户端需要保存两个版本的密码:最新密钥(即首选密钥),上一次使用的解密密钥(即次选密钥),解密二维码数据时,先用首选密钥解密,若解密失败,再用次选密钥解密,只要有一个解密成功就行;将解密成功的密钥作为首选密钥,供后面使用。

[0230] S311、客户端软件从 CQ 中提取起始时间,检查 CQ 是否在有效期内,若超时,则提醒用户该二维码已失效;若在有效期内,则进行步骤 312。

[0231] S312、手机屏幕显示从 CQ 中提取的交易数据 D,并提示用户核对。

[0232] S313、用户查看交易数据,并确认。

[0233] S314、客户端软件更新密钥 FK 和 SK,并产生动态密码 DP,显示到手机屏幕上;其中:

[0234] $SK = FK$;

[0235] $FK = \text{Hmac}(FK, CQ)$;

[0236] $DP = \text{Truncate}(\text{Hash}(FK), 4) \bmod 10^n$;

[0237] Hash 为消息杂凑算法,可选择 MD5、SHA1、SHA256 等算法;Hmac 是基于 Hash 算法的 MAC 生成算法,可选择 Hmac-SHA1 或 Hmac-SHA256 等算法。Mod 表示计算余数,如: $134 \bmod 100 = 34$ 。

[0238] 动态密码 DP,也称认证密码。是用户使用手机扫描二维码图片并确认交易后得到的一串数字,用来向交易系统表明身份,由认证服务器来检查是否正确。计算产生过程中,由于加入交易内容要素,因此安全性大大提高。动态密码计算过程:先对计算首选密钥 FK 的 Hash 值,从里面截取部分数据,转换成大整数,最后对一个大整数取模,这里的大整数一般为 10 的 n 次方,n 为动态密码的长度,比如:动态密码长度是 6,则对 1000000(10 的 6 次方)取模,截取数据长度和动态密码位数可调整。

[0239] $DP = \text{Truncate}(\text{Hash}(FK), 4) \bmod 10^n$;

[0240] 动态密码的取值除了数字外,还可以包含其他字符,如字母、数字、特殊符号等。计算时:1、将所有取值看作是数组(取值数组,将所有取值排序,每个取值对应一个下标);2、截取数据转换成大整数,对取值数组长度取模 Mod 运算,余数作为下标(index)去取值数组中取出对应的值,就是动态密码中一位;3、将大整数整除数组长度的商值作为下一次运算的大整数,重复第 2 步操作,产生动态密码中下一位。依次循环,直到得到要求长度的动态密码。

[0241] S315、用户将所显示的动态密码在电脑上的交易页面中输入,发送给交易系统。

[0242] S316、将该用户的账户、交易信息、动态密码传给认证服务器。

[0243] S317、认证服务器提取用户认证记录,核对交易信息是否一致;检查挑战问题是否超时。一致且未超时的话,进行步骤 S318。

[0244] S318、认证服务器根据该用户的首选密钥和挑战问题的明文生成新的首选密钥,根据新的首选密钥产生动态密码,并与用户输入的动态密码比对;如果一致,则认证结果为完成认证,将认证次数 S 加 1;如果不一致,则认证结果为未认证。

[0245] S319、认证服务器将认证结果返回给交易系统。

[0246] S320、交易系统接收认证服务器返回的认证结果,若认证结果为完成认证,则执行交易内容,在电脑的交易页面上显示交易成功;若认证结果为未认证,则在电脑的交易页面上显示交易失败。

[0247] 实施例五、一种客户端,包括:

[0248] 接收单元,用于接收挑战问题的密文;

[0249] 解密单元,用于解密挑战问题的密文,得到挑战问题的明文;将成功解密挑战问题所使用的密钥作为首选密钥;

[0250] 更新单元,用于根据所述挑战问题的明文及首选密钥产生新的首选密钥;

[0251] 动态密码生成单元,用于根据所述新的首选密钥产生动态密码并显示。

[0252] 本实施例的一种备选方案中,所述接收单元从网络侧接收挑战问题的密文是指:

[0253] 所述接收单元扫描网络侧生成的二维码图片,该二维码图片通过对挑战问题的密文编码产生;对所述二维码图片解码得到挑战问题的密文。

[0254] 本实施例的一种备选方案中,所述挑战问题中包括:已认证次数 S、起始时间 T、交易数据 D、校验数据 C;还可增加其他信息。所述起始时间为所述挑战问题的产生时间;所述校验数据 C 可以但不限于为对挑战问题中的其它信息连接而成的数据进行杂凑运算后所得到结果中部分指定位置的数据。所述挑战问题可以但不限于由上述信息连接而成;其它备选方案中,也可以设置只在挑战问题中包括上述信息中任一种或其任意组合。

[0255] 该备选方案的一种实施方式中,所述客户端还包括:验证单元,用于在所述更新单元根据挑战问题的明文及首选密钥产生新的首选密钥前,从所述挑战问题的明文中提取交易数据,显示所述交易数据;收到用户输入的确认信息后,指示所述更新单元根据挑战问题的明文及产生新的首选密钥。

[0256] 该实施方式中,所述挑战问题中至少包括起始时间;所述起始时间为所述挑战问题的产生时间;

[0257] 所述验证单元还用于在显示所述交易数据前,从所述挑战问题的明文中提取起始

时间；判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值；如果大于，则提示用户是否继续；如果不大于，或接收到用户要求继续的指令则显示交易数据。

[0258] 该备选方案中，所述验证单元还可以用于在得到挑战问题的明文后利用所述校验数据 C 验证所得到的挑战问题的明文是否有效；如果有效则指示所述更新单元根据挑战问题的明文及产生新的首选密钥；如果无效且采用的是首选密钥解密，则使用次选密钥尝试解密后再验证所得到的挑战问题的明文是否有效；如果无效且采用的是次选密钥解密，则说明首选密钥和次选密钥都不正确，结束认证。

[0259] 本实施例的一种备选方案中，所述解密单元解密挑战问题的密文，得到挑战问题的明文，将成功解密挑战问题所使用的密钥作为首选密钥是指：

[0260] 所述解密单元采用首选密钥解密挑战问题的密文，如果解密成功则得到挑战问题的明文；如果失败，则采用次选密钥解密所述挑战问题的密文，如果解密成功则得到挑战问题的明文，将次选密钥作为首选密钥；如果解密失败则结束认证；

[0261] 所述更新单元还用于当所述解密单元采用首选密钥解密成功时，在根据所述挑战问题的明文及首选密钥产生新的首选密钥前，将原先的首选密钥作为新的次选密钥。

[0262] 这里“原先的首选密钥”就是指解密挑战问题的密文成功时用的密钥。

[0263] 在其它备选方案中，解密单元也可以保存解密成功时所使用的密钥，在生成动态密码后将解密成功时所使用的密钥作为次选密钥。

[0264] 其它实现细节可参考实施例一、三。

[0265] 实施例六、一种认证系统，包括：

[0266] 生成单元，用于当需要对用户进行认证时，产生对应于待认证用户的挑战问题；

[0267] 加密单元，用于根据该待认证用户对应的首选密钥加密所述挑战问题；

[0268] 通信单元，用于发送挑战问题的密文，接收所述待认证用户输入的动态密码；

[0269] 认证单元，用于当所述通信单元接收到动态密码后，根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥；根据该新的首选密钥生成动态密码，并与接收的动态密码比对；如果一致，则完成认证。

[0270] 本实施例的一种备选方案中，所述通信单元发送挑战问题的密文是指：

[0271] 所述通信单元根据挑战问题的密文进行编码，生成二维码图片数据；发送所生成的二维码图片数据。

[0272] 本实施例的一种备选方案中，所述挑战问题中包括：已认证次数 S、起始时间 T、交易数据 D、校验数据 C；还可增加其他信息。所述起始时间为所述挑战问题的产生时间；所述校验数据 C 可以但不限于为对挑战问题中的其它信息连接而成的数据进行杂凑运算后所得到结果中部分指定位置的数据。所述挑战问题可以但不限于由上述信息连接而成；其它备选方案中，也可以设置只在挑战问题中包括上述信息中任一种或其任意组合。

[0273] 该备选方案的一种实施方式中，所述认证系统还可以包括：

[0274] 判断单元，用于在所述认证单元根据所述待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥前，从所述挑战问题的明文中提取起始时间，判断当前时刻和所述起始时间的时间间隔是否大于预定时间阈值；如果大于，则结束认证；如果不大于，则指示所述认证单元根据待认证用户的首选密钥、和对应于该待认证用户的挑战问题生成该待认证用户的新的首选密钥。

[0275] 其它实现细节可参考实施例二、三。

[0276] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块 / 单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本申请不限制于任何特定形式的硬件和软件的结合。

[0277] 当然，本申请还可有其他多种实施例，在不背离本申请精神及其实质的情况下，熟悉本领域的技术人员当可根据本申请作出各种相应的改变和变形，但这些相应的改变和变形都应属于本申请的权利要求的保护范围。

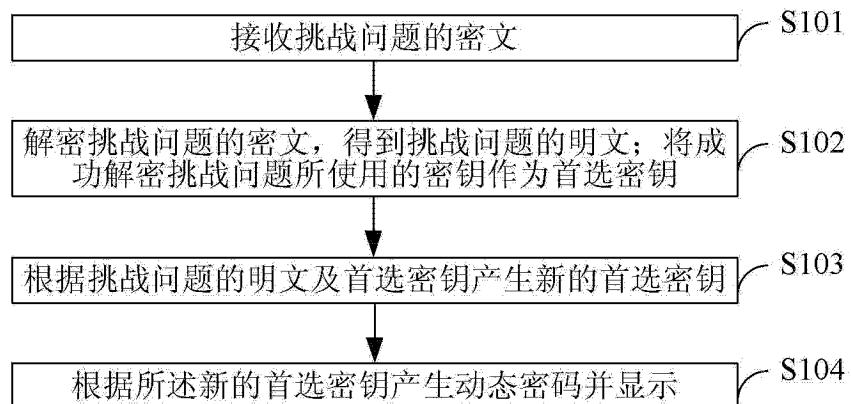


图 1



图 2

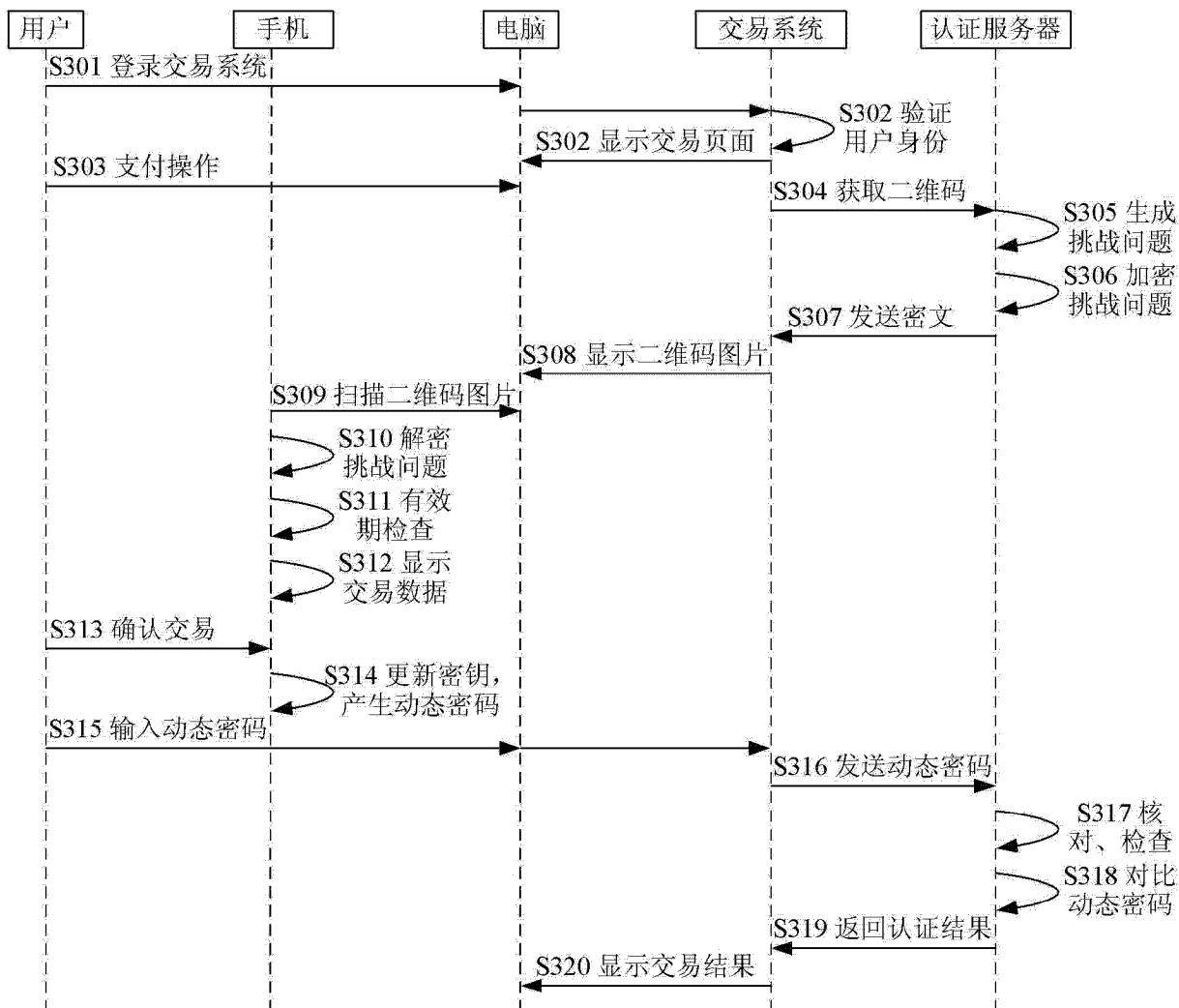


图 3