(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103095662 A
(43)申请公布日 2013.05.08

(21)申请号 201110346508.3

(22)申请日 2011.11.04

(71)申请人 阿里巴巴集团控股有限公司
地址 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 邓玉良

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

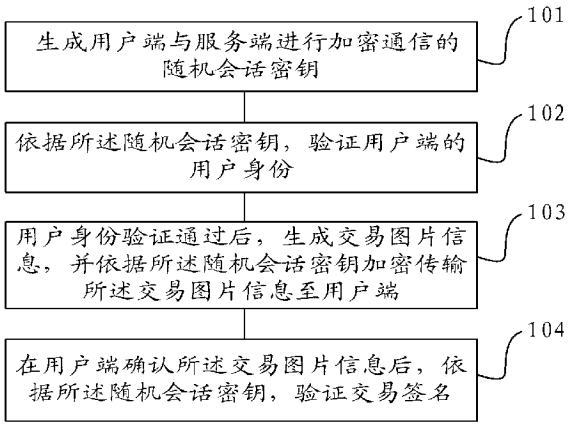
权利要求书3页 说明书13页 附图9页

(54)发明名称

一种网上交易安全认证方法及网上交易安全认证系统

(57)摘要

本申请提供了一种网上交易安全认证方法及网上交易安全认证系统，既能克服硬件存在的使用范围、使用寿命及技术升级的问题，又能解决当前网上交易面临的防范钓鱼、木马、木马钓鱼能力较差的问题。所述方法包括：生成用户端与服务端进行加密通信的随机会话密钥；所述服务器端依据所述随机会话密钥，验证所述用户端的用户身份；用户身份验证通过后，所述服务器端生成交易图片信息，并依据所述随机会话密钥加密传输所述交易图片信息至用户端；所述用户端确认所述交易图片信息后，所述服务器端依据所述随机会话密钥验证交易签名。



CN 103095662 A

1. 一种网上交易安全认证方法，其特征在于，包括：

生成用户端与服务端进行加密通信的随机会话密钥；

所述服务器端依据所述随机会话密钥，验证所述用户端的用户身份；

用户身份验证通过后，所述服务器端生成交易图片信息，并依据所述随机会话密钥加密传输所述交易图片信息至用户端；

所述用户端确认所述交易图片信息后，所述服务器端依据所述随机会话密钥验证交易签名。

2. 根据权利要求 1 所述的方法，其特征在于，所述生成用户端与服务端进行加密通信的随机会话密钥，包括：

在用户端生成随机数；

用预置的 RSA 公钥加密所述随机数；

发送所述加密的随机数至服务端；

在服务端依据所述加密的随机数生成随机会话密钥；

发送所述随机会话密钥至用户端。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述依据随机会话密钥验证用户端的用户身份，包括：

在用户端提取用户机器信息；

用所述随机会话密钥加密用户机器信息；

传送所述加密的用户机器信息至服务端；

在服务端验证用户机器信息匹配程度；

当用户机器信息匹配程度符合预置条件时，用户身份验证通过；

当用户机器信息匹配程度不符合预置条件时，用户身份验证失败。

4. 根据权利要求 3 所述的方法，其特征在于，还包括：

在服务端生成抓取因子，并发送至用户端；

则在用户端根据所述抓取因子提取用户机器信息，用所述随机会话密钥加密用户机器信息和抓取因子，并传送至服务端；

服务端依据所述抓取因子验证用户机器信息匹配程度。

5. 根据权利要求 3 所述的方法，其特征在于，当用户身份验证失败时，还包括：

用户端发送手机短信发送请求；

服务端收到所述请求后，获取用户信息，生成手机短信验证码，并发送所述手机短信验证码至用户绑定的手机；

用户收到手机短信验证码后，在用户端输入所述手机短信验证码，并发送至服务端；

服务端进行短信验证码验证，验证通过后，发送用户身份验证通过的结果至用户端。

6. 根据权利要求 1 所述的方法，其特征在于，所述生成交易图片信息，包括：

根据交易信息、随机会话密钥、时间和用户种子，生成交易验证码；

根据交易信息和随机会话密钥，生成摘要信息；

生成底图，并将摘要信息加入所述底图；

将所述交易信息和交易验证码加入所述包含摘要信息的底图，生成交易图片信息。

7. 根据权利要求 1 或 6 所述的方法，其特征在于，所述依据随机会话密钥验证交易签

名，包括：

在用户端输入交易验证码；

对交易图片信息和交易验证码用所述随机会话密钥进行数字签名；

发送所述数字签名至服务端；

服务端验证所述数字签名是否正确，并发送验证结果至用户端。

8. 一种网上交易安全认证系统，其特征在于，包括：OTP 控件、OTP 控件服务器和 OTP 认证平台，其中，

所述 OTP 控件和 OTP 控件服务器，用于生成 OTP 控件与 OTP 控件服务器进行加密通信的随机会话密钥，并依据所述随机会话密钥，验证 OTP 控件的用户身份；

所述 OTP 认证平台，与 OTP 控件服务器相连，用于在收到 OTP 控件服务器发送的用户身份验证通过的信息后，生成交易图片信息，并依据所述随机会话密钥加密传输所述交易图片信息至 OTP 控件；在 OTP 控件确认所述交易图片信息后，依据所述随机会话密钥验证交易签名。

9. 根据权利要求 8 所述的系统，其特征在于：

在生成随机会话密钥时，所述 OTP 控件用于生成随机数，用预置的 RSA 公钥加密所述随机数，并发送至 OTP 控件服务器；

所述 OTP 控件服务器用于依据所述加密的随机数生成随机会话密钥，并发送所述随机会话密钥至 OTP 控件。

10. 根据权利要求 8 或 9 所述的系统，其特征在于：

在验证 OTP 控件的用户身份时，所述 OTP 控件用于提取用户机器信息，用所述随机会话密钥加密用户机器信息，并发送至 OTP 控件服务器；

所述 OTP 控件服务器用于验证用户机器信息匹配程度，当用户机器信息匹配程度符合预置条件时，用户身份验证通过；当用户机器信息匹配程度不符合预置条件时，用户身份验证失败。

11. 根据权利要求 10 所述的系统，其特征在于：

所述 OTP 控件服务器还用于生成抓取因子，并发送至 OTP 控件；

则所述 OTP 控件根据所述抓取因子提取用户机器信息，用所述随机会话密钥加密用户机器信息和抓取因子，并发送至 OTP 控件服务器；

所述 OTP 控件服务器依据所述抓取因子验证用户机器信息匹配程度。

12. 根据权利要求 10 所述的系统，其特征在于，当用户身份验证失败时，还包括：

客户端脚本模块，用于发送手机短信发送请求；

所述 OTP 认证平台还用于收到所述请求后，获取用户信息，生成手机短信验证码，并发送所述手机短信验证码至用户绑定的手机；还用于进行短信验证码验证，验证通过后，发送用户身份验证通过的结果至客户端脚本模块。

13. 根据权利要求 8 所述的系统，其特征在于，所述 OTP 认证平台包括：

OTP 算法驱动模块，用于根据交易信息、随机会话密钥、时间和用户种子，生成交易验证码；

OTP 业务系统，用于根据交易信息和随机会话密钥，生成摘要信息；

图片服务器，用于生成底图，并将摘要信息加入所述底图；还用于将所述交易信息和交

易验证码加入所述包含摘要信息的底图，生成交易图片信息。

14. 根据权利要求 8 或 13 所述的系统，其特征在于：

在验证交易签名时，所述 OTP 控件用于输入交易验证码，对交易图片信息和交易验证码用所述随机会话密钥进行数字签名，并发送所述数字签名至 OTP 认证平台；

所述 OTP 认证平台用于验证所述数字签名是否正确，并发送验证结果。

一种网上交易安全认证方法及网上交易安全认证系统

技术领域

[0001] 本申请涉及安全认证领域，特别是涉及一种网上交易安全认证方法及网上交易安全认证系统。

背景技术

[0002] 在互联网日益发达和普及的今天，网上交易因其方便、快捷、高效、经济的优势已逐渐成为人们日常交易活动中重要的交易方式之一。但是，网上交易需要借助于互联网平台才能实现，在交易支付过程中用户需要通过计算机输入账户密码，如果这时遭到黑客的攻击，用户的账户密码就很容易泄露，使用户可能蒙受经济上的损失。

[0003] 当前比较流行的几种黑客攻击方式包括钓鱼、木马和木马钓鱼等，其中“钓鱼”是指黑客利用用户的弱点来骗取用户的密码；“木马”是指黑客通过向用户机器种植恶意程序，达到篡改用户交易的目的，让用户为黑客买单；“木马钓鱼”是指同时使用木马和钓鱼劫持用户交易，并在第三方网站创建交易，篡改用户交易显示，给用户展示用户想看到的交易，骗取用户输入密码，让用户为黑客在第三方网站上的交易买单。

[0004] 为了增加交易的安全性，人们开发了密码控件技术和动态口令 OTP(one time password，简称 OTP，即一次一密）技术，用来对用户的网上交易进行保护。但是，最初的密码控件技术仅仅是一个静态的密码保护插件，而第一代的 OTP 技术只是基于密码安全的角度设计的，对钓鱼和木马的防范能力较差；第二代的 OPT 技术虽然将交易信息作为一个外部输入来产生密码，此时的密码已经不再是基于密码安全的安全了，因此安全性能有所提升，但目前应用二代 OTP 技术的主要是一些硬件产品如 USB Key，而硬件产品在使用范围和使用寿命上都受到限制，特别是当技术升级时，硬件产品一般需要更换新的硬件才能实现。

[0005] 因此，需要本领域技术人员迫切解决的一个技术问题就是：如何通过软件的方式实现二代 OTP 技术，既能克服硬件存在的使用范围、使用寿命及技术升级的问题，又能解决当前网上交易面临的防范钓鱼、木马、木马钓鱼能力较差的问题。

发明内容

[0006] 本申请所要解决的技术问题是提供一种网上交易安全认证方法及网上交易安全认证系统，既能克服硬件存在的使用范围、使用寿命及技术升级的问题，又能解决当前网上交易面临的防范钓鱼、木马、木马钓鱼能力较差的问题。

[0007] 为了解决上述问题，本申请公开了一种网上交易安全认证方法，包括：

[0008] 生成用户端与服务端进行加密通信的随机会话密钥；

[0009] 所述服务器端依据所述随机会话密钥，验证所述用户端的用户身份；

[0010] 用户身份验证通过后，所述服务器端生成交易图片信息，并依据所述随机会话密钥加密传输所述交易图片信息至用户端；

[0011] 所述用户端确认所述交易图片信息后，所述服务器端依据所述随机会话密钥验证交易签名。

[0012] 优选的，所述生成用户端与服务端进行加密通信的随机会话密钥，包括：

[0013] 在用户端生成随机数；

[0014] 用预置的 RSA 公钥加密所述随机数；

[0015] 发送所述加密的随机数至服务端；

[0016] 在服务端依据所述加密的随机数生成随机会话密钥；

[0017] 发送所述随机会话密钥至用户端。

[0018] 优选的，所述依据随机会话密钥验证用户端的用户身份，包括：

[0019] 在用户端提取用户机器信息；

[0020] 用所述随机会话密钥加密用户机器信息；

[0021] 传送所述加密的用户机器信息至服务端；

[0022] 在服务端验证用户机器信息匹配程度；

[0023] 当用户机器信息匹配程度符合预置条件时，用户身份验证通过；

[0024] 当用户机器信息匹配程度不符合预置条件时，用户身份验证失败。

[0025] 优选的，所述方法还包括：

[0026] 在服务端生成抓取因子，并发送至用户端；

[0027] 则在用户端根据所述抓取因子提取用户机器信息，用所述随机会话密钥加密用户机器信息和抓取因子，并传送至服务端；

[0028] 服务端依据所述抓取因子验证用户机器信息匹配程度。

[0029] 优选的，当用户身份验证失败时，所述方法还包括：

[0030] 用户端发送手机短信发送请求；

[0031] 服务端收到所述请求后，获取用户信息，生成手机短信验证码，并发送所述手机短信验证码至用户绑定的手机；

[0032] 用户收到手机短信验证码后，在用户端输入所述手机短信验证码，并发送至服务端；

[0033] 服务端进行短信验证码验证，验证通过后，发送用户身份验证通过的结果至用户端。

[0034] 优选的，所述生成交易图片信息，包括：

[0035] 根据交易信息、随机会话密钥、时间和用户种子，生成交易验证码；

[0036] 根据交易信息和随机会话密钥，生成摘要信息；

[0037] 生成底图，并将摘要信息加入所述底图；

[0038] 将所述交易信息和交易验证码加入所述包含摘要信息的底图，生成交易图片信息。

[0039] 优选的，所述依据随机会话密钥验证交易签名，包括：

[0040] 在用户端输入交易验证码；

[0041] 对交易图片信息和交易验证码用所述随机会话密钥进行数字签名；

[0042] 发送所述数字签名至服务端；

[0043] 服务端验证所述数字签名是否正确，并发送验证结果至用户端。

[0044] 本申请还提供了一种网上交易安全认证系统，包括：OTP 控件、OTP 控件服务器和 OTP 认证平台，其中，

[0045] 所述 OTP 控件和 OTP 控件服务器，用于生成 OTP 控件与 OTP 控件服务器进行加密通信的随机会话密钥，并依据所述随机会话密钥，验证 OTP 控件的用户身份；

[0046] 所述 OTP 认证平台，与 OTP 控件服务器相连，用于在收到 OTP 控件服务器发送的用户身份验证通过的信息后，生成交易图片信息，并依据所述随机会话密钥加密传输所述交易图片信息至 OTP 控件；在 OTP 控件确认所述交易图片信息后，依据所述随机会话密钥验证交易签名。

[0047] 优选的，在生成随机会话密钥时，所述 OTP 控件用于生成随机数，用预置的 RSA 公钥加密所述随机数，并发送至 OTP 控件服务器；所述 OTP 控件服务器用于依据所述加密的随机数生成随机会话密钥，并发送所述随机会话密钥至 OTP 控件。

[0048] 优选的，在验证 OTP 控件的用户身份时，所述 OTP 控件用于提取用户机器信息，用所述随机会话密钥加密用户机器信息，并发送至 OTP 控件服务器；所述 OTP 控件服务器用于验证用户机器信息匹配程度，当用户机器信息匹配程度符合预置条件时，用户身份验证通过；当用户机器信息匹配程度不符合预置条件时，用户身份验证失败。

[0049] 优选的，所述 OTP 控件服务器还用于生成抓取因子，并发送至 OTP 控件；则所述 OTP 控件根据所述抓取因子提取用户机器信息，用所述随机会话密钥加密用户机器信息和抓取因子，并发送至 OTP 控件服务器；所述 OTP 控件服务器依据所述抓取因子验证用户机器信息匹配程度。

[0050] 优选的，当用户身份验证失败时，所述系统还包括：客户端脚本模块，用于发送手机短信发送请求；所述 OTP 认证平台还用于收到所述请求后，获取用户信息，生成手机短信验证码，并发送所述手机短信验证码至用户绑定的手机；还用于进行短信验证码验证，验证通过后，发送用户身份验证通过的结果至客户端脚本模块。

[0051] 优选的，所述 OTP 认证平台包括：

[0052] OTP 算法驱动模块，用于根据交易信息、随机会话密钥、时间和用户种子，生成交易验证码；

[0053] OTP 业务系统，用于根据交易信息和随机会话密钥，生成摘要信息；

[0054] 图片服务器，用于生成底图，并将摘要信息加入所述底图；还用于将所述交易信息和交易验证码加入所述包含摘要信息的底图，生成交易图片信息。

[0055] 优选的，在验证交易签名时，所述 OTP 控件用于输入交易验证码，对交易图片信息和交易验证码用所述随机会话密钥进行数字签名，并发送所述数字签名至 OTP 认证平台；所述 OTP 认证平台用于验证所述数字签名是否正确，并发送验证结果。

[0056] 与现有技术相比，本申请包含以下优点：

[0057] 第一，本申请基于 OTP 技术、密码控件技术、交易图片签名技术等软件技术实现了网上交易的安全认证，克服了硬件产品存在的使用范围、使用寿命和技术升级的难点；

[0058] 第二，本申请通过利用随机会话密钥安全地传输交易图片的方式，实现了用户交易的二次确认，即利用软件的方式实现了二代 OTP 技术，解决了现有的软件产品防范钓鱼、木马、木马钓鱼困难的问题；

[0059] 第三，本申请通过建立了 OTP 控件服务器和 OTP 认证平台，实现了 OTP 技术的批量化交易；

[0060] 第四，本申请提供的安全认证系统是基于软件技术构建的，易于推广，如能在第三

方系统（如第三方商家、第三方支付平台）中得到应用，可以增强整个行业的安全性。

附图说明

[0061] 图 1 是本申请实施例所述的一种网上交易安全认证方法流程图；

[0062] 图 2 是本申请实施例所述的生成用户端与服务端加密通信的随机会话密钥的流程图；

[0063] 图 3 是本申请实施例所述的通过用户机器信息验证用户身份的流程图；

[0064] 图 4 是本申请实施例所述的通过手机短信验证用户身份的流程图；

[0065] 图 5 是本申请实施例所述的手机短信信息内容示意图；

[0066] 图 6 是本申请实施例所述的获取交易图片信息的流程图；

[0067] 图 7 是本申请实施例所述的交易图片信息示意图；

[0068] 图 8 是本申请实施例所述的生成交易图片信息的流程图；

[0069] 图 9 是本申请实施例所述的验证交易签名的流程图；

[0070] 图 10 是本申请实施例所述的升级原密码控件用户为 OTP 控件用户的流程图；

[0071] 图 11 是本申请实施例所述的一种网上交易安全认证系统结构图；

[0072] 图 12 是本申请另一实施例所述的一种网上交易安全认证系统结构图；

[0073] 图 13 是本申请实施例所述的支付网站站内被钓鱼的示意图；

[0074] 图 14 是本申请实施例所述的用户被钓鱼到第三方外部商家的示意图；

[0075] 图 15 是本申请实施例所述的用户被钓鱼到第三方支付平台的示意图。

具体实施方式

[0076] 为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

[0077] 本申请利用软件的方式实现了一种网上交易安全认证方法和网上交易安全认证系统，既能克服硬件存在的使用范围、使用寿命及技术升级的问题，又能解决当前网上交易面临的防范钓鱼、木马、木马钓鱼能力较差的问题。

[0078] 下面通过图 1 至图 9 对本申请的内容进行详细说明。

[0079] 需要说明的是，图 1 至图 9 的流程中涉及到位于用户端的 OTP 控件、JS（一种计算机脚本语言 Javascript 的缩写）脚本和浏览器，以及位于服务端的网上支付网关、OTP 控件服务器（图中简称为控件服务器）、OTP 认证平台、业务系统和数据库。其中，OTP 控件安装在用户端的机器上，配合 OTP 控件服务器和 OTP 认证平台完成网上交易的安全认证。OTP 控件服务器主要用于验证 OTP 控件的用户身份，OTP 认证平台主要完成交易验证。网上支付 SSL 服务器是网上交易中用于完成网上支付的服务器，业务系统主要用于网上交易业务的数据处理。

[0080] 参照图 1，是本申请实施例所述一种网上交易安全认证方法流程图，具体步骤如下：

[0081] 步骤 101，生成用户端与服务端进行加密通信的随机会话密钥；

[0082] 所述生成用户端与服务端进行加密通信的随机会话密钥是指用户端与服务端进行会话密钥交互，由用户端生成随机数发送至服务端，由服务端根据随机数生成随机会话

密钥和抓取因子，并返回至用户端。

[0083] 参照图 2 所示，详细的过程如下：

[0084] S1，页面跳转至收银台；

[0085] S2，JS 脚本初始化 OTP 控件；

[0086] S3，JS 脚本生成会话密钥请求，并发送给 OTP 控件；

[0087] S4，OTP 控件生成 24 字节随机数；

[0088] S5，OTP 控件用预置的 RSA 公钥（一种公钥加密算法，名称来自三个发明者 Ron Rivest，Adi Shamirh，Leonard Adleman 的姓名）加密所述随机数；

[0089] S6，OTP 控件将加密的数据返回给 JS 脚本；

[0090] S7，JS 脚本调用浏览器发送会话密钥交互请求；

[0091] S8，浏览器发送会话密钥交互请求至网上支付网关；

[0092] S9，网上支付网关转发报文至 OTP 控件服务器；

[0093] 所述报文包含所述会话密钥交互请求；

[0094] S10，OTP 控件服务器解密报文，获取客户端随机数；

[0095] 具体的，OTP 控件服务器用 RSA 私钥解密得到 OTP 控件的 24 字节随机数；

[0096] S11，OTP 控件服务器生成 12 字节的随机数；

[0097] S12，OTP 控件服务器取 OTP 控件的 24 字节的前 12 字节和自己的 12 字节，变成一个 24 字节的随机会话密钥；

[0098] S13，OTP 控件服务器保存所述随机会话密钥到数据库；

[0099] S14，OTP 控件服务器生成抓取因子；

[0100] 所述抓取因子是随机抽取的 n 个随机数的集合，用于步骤 102 中抓取用户机器信息，并用于验证所抓取的用户机器信息，是本实施例的一种优选实现方式。

[0101] S15，OTP 控件服务器用 OTP 控件的 24 字节随机数作为密钥加密自己的 12 字节随机数和抓取因子；

[0102] S16，OTP 控件服务器发送会话密钥交互响应；

[0103] S17，网上支付网关转发响应报文至浏览器；

[0104] S18，浏览器接收响应报文，返回 JS 脚本调用；

[0105] S19，JS 脚本获取密文信息；

[0106] S20，JS 脚本向 OTP 控件发送机器信息验证请求；

[0107] S21，OTP 控件用自己的 24 字节随机数解密所述密文信息，获得 OTP 控件服务器的 12 字节随机数；

[0108] S22，OTP 控件用自己的 24 字节的前 12 字节和解密得到的 12 字节得到随机会话密钥，随后的报文用所述随机会话密钥加密传输；

[0109] S23，OTP 控件获取抓取因子。由上可知，控件和服务端之间生成了一个随机会话密钥，而且两边各自生成一半，因此非常安全。

[0110] 步骤 102，依据所述随机会话密钥，验证用户端的用户身份；

[0111] 所述验证用户端的用户身份包括两种方式，一种通过用户机器信息进行验证，如图 3 所示；另一种是当用户机器信息验证失败后，通过手机短信对用户身份进行验证，如图 4 所示。

[0112] 参照图 3 所示，所述通过用户机器信息进行验证的方式又可细分为下述步骤：

[0113] S1，JS 脚本将会话密钥响应报文传入 OTP 控件；

[0114] S2，OTP 控件获取随机会话密钥和抓取因子；

[0115] OTP 控件用自己的 24 字节解密服务端响应，并用解密得到的 12 字节替换 24 字节的后 12 字节，最终得到所述随机会话密钥。

[0116] S3，OTP 控件提取用户机器信息；

[0117] OTP 控件根据抓取因子提取用户机器信息。用户机器信息采取编号的形式，每个编号对应抓取因子中的一个随机数，假设某次的抓取因子包含 10 个随机数，则对应这 10 个随机数提取对应编号的机器信息。OTP 控件每次提取部分机器信息。

[0118] 由于抓取因子是随机的，因此每次根据抓取因子提取的用户机器信息也是不同的。例如，控件服务器在某一次下放的抓取因子为 16 个随机数，而随后在下一次下放的抓取因子又为 20 个随机数，那么对于同一个 OTP 控件和同一个用户机器，每次抓取的用户机器信息都是不同的，从而提高了用户身份验证的安全性，这也是本实施例的一种优选实现方式。其中，用户机器信息包含机器的硬件信息，也可以包含软件信息，如操作系统版本等。

[0119] S4，OTP 控件用随机会话密钥加密用户机器信息，并返回至 JS 脚本；

[0120] 如果采用抓取因子的方法，则 OTP 控件还会把抓取因子同用户机器信息一起加密发送。

[0121] S5，JS 脚本调用浏览器发送请求报文；

[0122] S6，浏览器发送请求报文至网上支付网关；

[0123] S7，网上支付网关转发报文至 OTP 控件服务器；

[0124] S8，OTP 控件服务器读取数据库信息；

[0125] S9，OTP 控件服务器根据抓取因子比对数据，逐个判断用户的机器信息是否变更；

[0126] 通过比对抓取因子对应的值，即将根据抓取因子抓取的用户机器信息和数据库中所述抓取因子对应的值进行比对，判断用户的机器信息是否变更。

[0127] S10，当用户机器匹配成功率符合预置条件时，认为此用户机器匹配成功；

[0128] 所述符合预置条件可以是，用户机器匹配成功率＞＝ 80％，此时认为用户身份验证通过；当用户机器匹配成功率＜ 80％时，认为用户身份验证失败。

[0129] S11，OTP 控件服务器返回成功报文至网上支付网关；

[0130] S12，网上支付网关转发成功报文至浏览器；

[0131] S13，浏览器接收成功报文，并返回 JS 脚本调用。

[0132] 参照图 4 所示，所述通过手机短信进行用户身份验证的方式又可细分为下述步骤：

[0133] 其中，S1 至 S9 与图 3 中的 S1 至 S9 相同，在此略，下面从 S10 开始说明；

[0134] S10，当用户机器匹配成功率不符合预置条件时，认为此用户机器匹配失败；

[0135] 如前所述，所述符合预置条件可以是，用户机器匹配成功率＜ 80％，此时认为用户身份验证失败。

[0136] S11，OTP 控件服务器返回失败报文至网上支付网关；

[0137] S12，网上支付网关转发失败报文至浏览器；

[0138] S13，浏览器接收报文，返回 JS 脚本调用；

[0139] S14，JS 脚本从业务系统获取短信验证码验证页面；

[0140] S15，JS 脚本展现所述页面；

[0141] 通常，所述页面提示用户输入手机号码或其他用户相关信息；

[0142] S16，JS 脚本发送短信发送请求至控件服务器；

[0143] 当用户在上述页面输入手机号码其他用户相关信息后，JS 脚本发送短信发送请求；

[0144] S17，控件服务器发送短信发送请求至 OTP 认证平台；

[0145] S18，OTP 认证平台从业务系统获取用户信息；

[0146] 所述用户信息可以是用户手机号码，也可以是用户名、电子邮箱、联系地址等其他相关信息；

[0147] S19，OTP 认证平台生成验证码；

[0148] OTP 认证平台是根据用户信息生成验证码；

[0149] S20，OTP 认证平台发送短信请求至业务系统；

[0150] S21，由业务系统发送短信给用户绑定的手机；

[0151] 其中，所述短信中包含了 OTP 认证平台生成的验证码，参照图 5 所示，是手机短信显示的信息内容示意图；

[0152] S22，用户收到所述短信后，在网页上输入短信验证码；

[0153] S23，JS 脚本发送短信验证请求至 OTP 控件服务器；

[0154] S24，OTP 控件服务器转发短信验证请求至 OTP 认证平台；

[0155] S25，OTP 认证平台对手机验证码进行验证；

[0156] S26，验证成功后，OTP 认证平台发送验证成功请求至 OTP 控件服务器；

[0157] S27，OTP 控件服务发送验证成功响应至 JS 脚本；

[0158] S28，JS 脚本向 OTP 控件发送抓取机器信息请求；

[0159] S29，OTP 控件抓取所有的机器信息；

[0160] S30，OTP 控件向 JS 脚本返回抓取的机器信息；

[0161] 其中，OTP 控件用随机会话密钥加密机器信息；

[0162] S31，JS 脚本调用浏览器提交抓取的机器信息；

[0163] S32，浏览器向网上支付网关发送请求报文；

[0164] S33，网上支付网关向 OTP 控件服务器转发报文；

[0165] S34，OTP 控件服务器更新用户机器信息；

[0166] S35，OTP 控件服务器向网上支付网关发送响应报文；

[0167] S36，网上支付网关向浏览器转发响应报文；

[0168] S37，浏览器向 JS 调用返回响应报文；

[0169] S38，JS 脚本收到响应报文，完成用户身份验证。

[0170] 步骤 103，用户身份验证通过后，生成交易图片信息，并依据所述随机会话密钥加密传输所述交易图片信息至用户端；

[0171] 由服务端生成交易图片信息，所述交易图片信息可参见图 7 所示，并由服务端将交易图片信息发给用户端。

[0172] 参照图 6 所示，用户端获取交易图片信息的过程具体包括：

[0173] S1，JS 脚本发送用户机器验证结果至 OTP 控件；

[0174] 当然，如果机器验证失败并采用手机短信验证方式，则可以将手机短信验证结果发送给 OTP 控件；

[0175] S2，OTP 控件发送交易图片信息获取请求至 JS 脚本；

[0176] S3，JS 脚本发送交易图片信息请求至浏览器；

[0177] S4，浏览器发送交易图片信息请求至网上支付网关；

[0178] S5，网上支付网关转发报文至 OTP 控件服务器；

[0179] S6，控件服务器发送获取交易图片请求至 OTP 认证平台；

[0180] S7，OTP 认证平台根据订单号获取交易信息；

[0181] OTP 认证平台从业务系统获取此次请求对应的订单号，并依据所述订单号获取对应的交易信息，所述交易信息包括交易内容、交易金额、交易时间等如图 7 所示的信息。

[0182] S8，OTP 认证平台根据交易信息生成图片要素；

[0183] 所述图片要素是指生成交易图片信息的要素，如交易验证码、摘要信息、底图等要素。

[0184] S9，OTP 认证平台生成交易图片信息；

[0185] 在 OTP 认证平台中，由图片服务器利用图片要素生成交易图片信息；

[0186] 其中 S8 和 S9 生成交易图片信息的详细过程可参见图 8 所示流程；

[0187] S10，OTP 认证平台用随机会话密钥加密交易图片信息，发送交易图片信息响应至 OTP 控件服务器；

[0188] S11，OTP 控件服务器发送交易图片信息响应至网上支付网关；

[0189] S12，网上支付网关转发响应报文至浏览器；

[0190] S13，浏览器接收报文，返回 JS 脚本调用；

[0191] S14，JS 脚本向 OTP 控件展示图片。

[0192] 参照图 8 所示，在 OTP 认证平台中生成交易图片信息的过程具体包括：

[0193] 1)OTP 算法驱动根据交易信息、随机会话密钥、时间和用户种子生成交易验证码；

[0194] 其中，所述时间是指交易时间，所述用户种子是一个 20 个字节的随机数，每个用户都有一个种子，而且都不一样。

[0195] 2)OTP 业务系统根据交易信息和随机会话密钥生成摘要信息，每一项交易对应唯一的摘要信息；

[0196] 3) 图片服务器生成底图；

[0197] 4) 将摘要信息加入底图，摘要信息与底图颜色一样；

[0198] 5) 将所述交易信息和交易验证码加入所述包含摘要信息的底图，生成交易图片信息。

[0199] 步骤 104，在用户端确认所述交易图片信息后，依据所述随机会话密钥验证交易签名。

[0200] 所述验证交易签名是指用户获取交易图片信息后，从交易图片中获取交易验证码，并输入交易验证码确认交易，OTP 控件对交易图片和交易验证码进行数字签名并发送至 OTP 认证平台，OTP 认证平台验证数字签名是否正确并返回交易签名认证结果至用户端。

[0201] 参照图 9 所示，具体包括：

[0202] S1，JS 脚本发送图片展现请求至 OTP 控件；

[0203] S2，OTP 控件展现交易内容信息，显示的交易图片信息参照图 7 所示；

[0204] S3，用户在 OTP 控件输入交易验证码；

[0205] S4，OTP 控件对交易图片和交易验证码利用随机会话密钥进行数字签名；

[0206] S5，OTP 控件发送签名验证请求至 JS 脚本；

[0207] S6，JS 脚本发送签名验证请求至浏览器；

[0208] S7，浏览器发送交易信息图片请求至网上支付网关；

[0209] S8，网上支付网关转发报文至 OTP 控件服务器；

[0210] S9，OTP 控件服务器发送交易签名验证请求至 OTP 认证平台；

[0211] S10，OTP 认证平台验证签名是否正确；

[0212] S11，OTP 认证平台发送交易签名验证结果至 OTP 控件服务器；

[0213] S12，OTP 控件服务器发送交易图片验证响应至网上支付网关；

[0214] S13，网上支付网关转发响应报文至浏览器；

[0215] S14，浏览器接收报文，返回 JS 调用；

[0216] S15，进行后续处理。

[0217] 综上所述，上述安全认证方法在传输过程中加入随机会话密钥，保证了整个传输过程的交易图片信息不会被篡改，同时图片信息变成在控件里面显示，并随着用户输入密码，控件对图片和密码签名，加密传输到服务端验证，这样就保证了整个交易过程中的安全性。

[0218] 以上所述的用户是指 OTP 控件用户，所谓 OTP 控件用户是指安装了 OTP 控件并进行实名认证和手机绑定的用户。对于原密码控件用户，参照图 10 所示，升级为 OTP 控件用户的流程具体包括：

[0219] 用户打开浏览器，输入支付网站网址，获取页面信息，网上支付网关下发带升级信息的脚本，通过浏览器显示，用户看到升级的提示，用户点击升级，向下载服务器提出下载请求，下载服务器将数据传输至浏览器，用户进行安装；更新后第一次支付，页面展现请求报文，网上支付网关查找用户类型，对于非实名认证用户，返回要求实名认证的页面，浏览器返回实名认证的页面，并展现给用户；用户登录身份信息和银行卡信息，浏览器发送实名认证请求，网上支付网关验证身份并打款，业务系统发送打款响应，网上支付网关转发报文至浏览器；用户输入打款和手机信息，浏览器发送验证请求，网上支付网关转发至业务系统，业务系统发送验证结果，浏览器展现验证结果给用户。

[0220] 对于新用户申请，用户在注册后，按照上述图 10 所示流程操作即可升级为 OTP 控件用户。

[0221] 此外，在步骤 102 验证用户身份的过程中，服务端首先通过用户机器信息验证用户身份，如果验证失败会再通过手机短信验证的方式验证用户身份，因此，用户绑定的手机号对安全支付来说是非常重要的信息。所以用户绑定的手机号变更需要通过以下两种方式之一才能完成：

[0222] 一种是采用往用户注册邮箱发邮件的方式，用户通过邮件链接验证身份，然后更新新手机号码；

[0223] 另一种是通过客服电话，有客服验证用户身份后，更新用户手机号码。

[0224] 基于上述方法实施例的说明，本申请还提供了相应的系统实施例。

[0225] 参照图 11，是本申请实施例所述的一种网上交易安全认证系统结构图。

[0226] 所述安全认证系统可以包括 OTP 控件 10、OTP 控件服务器 20 和 OTP 认证平台 30，其中，

[0227] 所述 OTP 控件 10 和 OTP 控件服务器 20，用于生成 OTP 控件 10 与 OTP 控件服务器 20 进行加密通信的随机会话密钥，并依据所述随机会话密钥，验证 OTP 控件 10 的用户身份；

[0228] 所述 OTP 认证平台 30，与 OTP 控件服务器 20 相连，用于在收到 OTP 控件服务器发送的用户身份验证通过的信息后，生成交易图片信息，并依据所述随机会话密钥加密传输所述交易图片信息至 OTP 控件 10；在 OTP 控件 10 确认所述交易图片信息后，依据所述随机会话密钥验证交易签名。

[0229] 其中，在生成随机会话密钥时，所述 OTP 控件 10 用于生成随机数，用预置的 RSA 公钥加密所述随机数，并发送至 OTP 控件服务器 20；所述 OTP 控件服务器 20 用于依据所述加密的随机数生成随机会话密钥，并发送所述随机会话密钥至 OTP 控件 10。

[0230] 其中，在验证 OTP 控件的用户身份时，所述 OTP 控件 10 用于提取用户机器信息，用所述随机会话密钥加密用户机器信息，并发送至 OTP 控件服务器 20；所述 OTP 控件服务器 20 用于验证用户机器信息匹配程度，当用户机器信息匹配程度符合预置条件时，用户身份验证通过；当用户机器信息匹配程度不符合预置条件时，用户身份验证失败。

[0231] 进一步优选的，所述 OTP 控件服务器 20 还用于生成抓取因子，并发送至 OTP 控件 10；则所述 OTP 控件 10 可以根据所述抓取因子提取用户机器信息，用所述随机会话密钥加密用户机器信息和抓取因子，并发送至 OTP 控件服务器 20；所述 OTP 控件服务器 20 可以依据所述抓取因子验证用户机器信息匹配程度。

[0232] 进一步优选的，如图 12 所示，当上述用户身份验证失败时，所述系统还可以包括：

[0233] 客户端脚本模块 40，用于发送手机短信发送请求；

[0234] 所述 OTP 认证平台 30 还用于收到所述请求后，获取用户信息，生成手机短信验证码，并发送所述手机短信验证码至用户绑定的手机；

[0235] 用户收到手机短信验证码后，在客户端脚本模块 40 中输入所述手机短信验证码，并发送至 OTP 认证平台 30；

[0236] 所述 OTP 认证平台 30 还用于进行短信验证码验证，验证通过后，发送用户身份验证通过的结果至客户端脚本模块 40。

[0237] 进一步优选的，所述 OTP 认证平台 30 具体可以包括：

[0238] OTP 算法驱动模块，用于根据交易信息、随机会话密钥、时间和用户种子，生成交易验证码；

[0239] OTP 业务系统，用于根据交易信息和随机会话密钥，生成摘要信息；

[0240] 图片服务器，用于生成底图，并将摘要信息加入所述底图；还用于将所述交易信息和交易验证码加入所述包含摘要信息的底图，生成交易图片信息。

[0241] 其中，在验证交易签名时，所述 OTP 控件 10 用于输入交易验证码，对交易图片信息和交易验证码用所述随机会话密钥进行数字签名，并发送所述数字签名至 OTP 认证平台 30；

[0242] 所述 OTP 认证平台 30 用于验证所述数字签名是否正确，并发送验证结果。

[0243] 对于上述安全认证系统实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0244] 为了更好地理解本申请的内容，下面再结合几个黑客攻击的具体案例分析利用本申请提供的方法和系统如何能防范钓鱼、木马、木马钓鱼。

[0245] 1、支付网站站内钓鱼

[0246] 站内交易替换是近期出现的一种木马病毒变种，木马在支付网站站内创建一笔即时到帐交易，如：我要付款，然后跳转回收银台让用户支付。

[0247] 站内交易替换的过程，参照图 13 所示：

[0248] ①用户在购物网站购买商品后，用户点击确认购买，浏览器跳转到支付网站收银台后，木马拦截正常的支付流程；

[0249] ②木马将浏览器导向支付网站即时到帐页面；

[0250] ③木马生成一笔“我要付款”订单，收款方为欺诈者的网上支付账号；

[0251] ④浏览器跳回支付网站收银台；用户看到自己需要支付一笔订单，这笔订单实际上会支付到欺诈者的网上支付账号；

[0252] ⑤用户选择付款；

[0253] ⑥用户支付木马生成的即时到帐订单，钓鱼过程结束。

[0254] 在本申请的方案中，因为用户的交易信息是以图片形式传入控件显示，而且整个过程是由应用层的随机会话密钥加密，即使黑客创建一笔新的交易，他也无法让这笔交易的图片传入控件，因为每个控件的随机会话密钥不一样，黑客的图片无法用用户控件的随机会话密钥解密。

[0255] 2、钓鱼到第三方外部商家

[0256] 此类型木马的钓鱼步骤参照图 14 所示：

[0257] ①用户机器感染木马后，木马会监听浏览器的 URL 地址栏；用户在购物网站购买商品后，用户点击确认购买；

[0258] ②浏览器跳转到支付网站收银台后，木马会拦截正常的支付流程，跳转至另一个第三方外部商户；

[0259] ③木马在用户客户端登录欺诈者的外部商户账号，然后生成一笔同样金额的订单，该订单使用支付网站进行付款；

[0260] ④浏览器会跳回支付网站收银台；这时候，用户看到自己需要支付一笔订单，这笔订单实际上会支付到欺诈者的外部商户账号；

[0261] ⑤用户选择付款；

[0262] ⑥用户实际支付了一笔外部商户订单，支付网站会付款给所述第三方外部商户，钓鱼过程结束。

[0263] 从以上流程可以看出，这种木马钓鱼不仅与支付网站的安全相关，而且与被钓鱼的第三方外部商家的安全性紧密相关。如果能将本申请的方案应用到第三方外部商家，因为绝大多数外部商家没有能力建设完善的安全体系，那么由支付网站提供客户端控件和服务端服务的方式，就可以防止这种木马。

[0264] 3、钓鱼到第三方支付平台

[0265] 此种木马钓鱼方式是用户通过在支付网站收银台的时候，木马去其他第三方支付平台生成一笔网银充值订单，诱骗用户进行网银充值付款。参照图 15，详细过程如下：

[0266] ①用户在收银台页面进行充值操作；这个操作可能由很多原因发起，如：用户在购物网站购买商品，进入收银台准备付款；用户发起一笔“我要付款”即时到帐交易；用户在个人版点击交易详情进行付款等；木马会监听浏览器的 URL，当用户准备付款时，木马就拦截正常的操作流程；

[0267] ②木马将浏览器导向其他第三方支付平台，并登录欺诈者的账号；木马可以使用下列方式将浏览器导向第三方支付平台：

[0268] (1) 修改浏览器的跳转地址，跳转至第三方支付平台；

[0269] (2) 修改网银订单提交表单的跳转地址；这种方式和图 15 中的流程稍有不同，需要木马在远程服务端动态生成一笔网银订单，然后远程发送给木马客户端，木马篡改页面中的表单信息；这种方式在木马出现初期较为常见；

[0270] (3) 其他形式；木马在短时间内做大量的 URL 跳转，比如木马会在用户点击去网银充值时，不直接进行拦截，而在浏览器跳转到网银页面后，再跳转去盛大；

[0271] ③无论木马在第二步会使浏览器跳转多少次，都会到第三方支付平台生成一笔网银充值订单；

[0272] ④用户在浏览器看到自己需要支付一笔网银订单，支付的银行和金额和正常交易流程相同，但是网银充值收款方不是支付网站；

[0273] ⑤用户没有注意充值收款方，进行了充值；

[0274] ⑥银行将钱充值进欺诈者的帐号，钓鱼过程完成。

[0275] 从以上流程可以看出，这种木马钓鱼不仅与支付网站的安全相关，而且跟被钓鱼的第三方支付平台的安全紧密相关。如果能将本申请的方案应用到第三方支付平台，由支付网站提供方案，第三方支付平台自建系统，方案被推广后，可以防止这种木马。

[0276] 综上所述，本申请包含以下优点：

[0277] 第一，本申请基于 OTP 技术、密码控件技术、交易图片签名技术等软件技术实现了网上交易的安全认证，克服了硬件产品存在的使用范围、使用寿命和技术升级的难点；

[0278] 第二，本申请通过利用随机会话密钥安全地传输交易图片的方式，实现了用户交易的二次确认，即利用软件的方式实现了二代 OTP 技术，解决了现有的软件产品防范钓鱼、木马、木马钓鱼困难的问题；

[0279] 第三，本申请通过建立了 OTP 控件服务器和 OTP 认证平台，实现了 OTP 技术的批量化交易；

[0280] 第四，本申请提供的安全认证系统是基于软件技术构建的，易于推广，如能在第三方系统（如第三方商家、第三方支付企业）中得到应用，可以增强整个行业的安全性。

[0281] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0282] 以上对本申请所提供的一种网上交易安全认证方法和网上交易安全认证系统，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明

书内容不应理解为对本申请的限制。

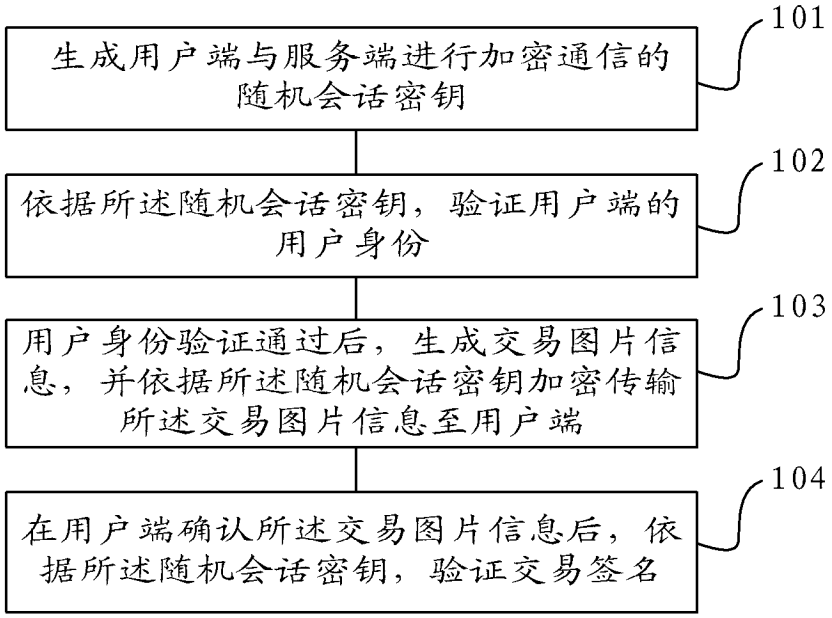

生成用户端与服务端进行加密通信的随机会话密钥
101
依据所述随机会话密钥，验证用户端的用户身份
102
用户身份验证通过后，生成交易图片信息，并依据所述随机会话密钥加密传输所述交易图片信息至用户端
103
在用户端确认所述交易图片信息后，依据所述随机会话密钥，验证交易签名
104

图 1

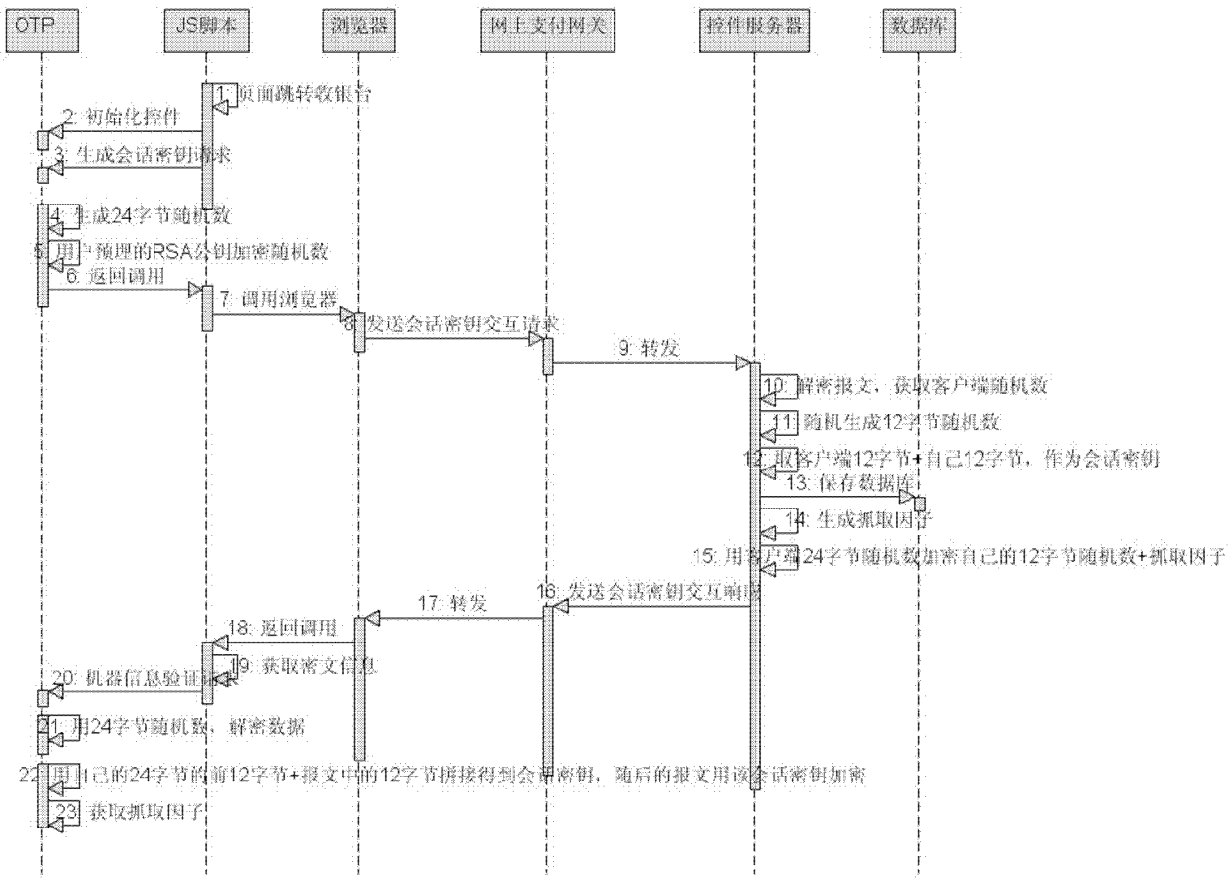

OTP
JS脚本
浏览器
网上支付网关
控件服务器
数据库
1: 页面跳转收银台
2: 初始化控件
3: 生成会话密钥请求
4: 生成24字节随机数
5: 用预埋的RSA公钥加密随机数
6: 返回调用
7: 调用浏览器
8: 发送会话密钥交互请求
9: 转发
10: 解密报文，获取客户端随机数
11: 随机生成12字节随机数
12: 取客户端12字节+自己12字节，作为会话密钥
13: 保存数据库
14: 生成抓取因子
15: 用客户端24字节随机数加密自己的12字节随机数+抓取因子
16: 发送会话密钥交互响应
17: 转发
18: 返回调用
19: 获取密文信息
20: 机器信息验证
21: 用24字节随机数，解密数据
22: 用自己的24字节的前12字节+报文中的12字节拼接得到会话密钥，随后的报文用该会话密钥加密
23: 获取抓取因子

图 2

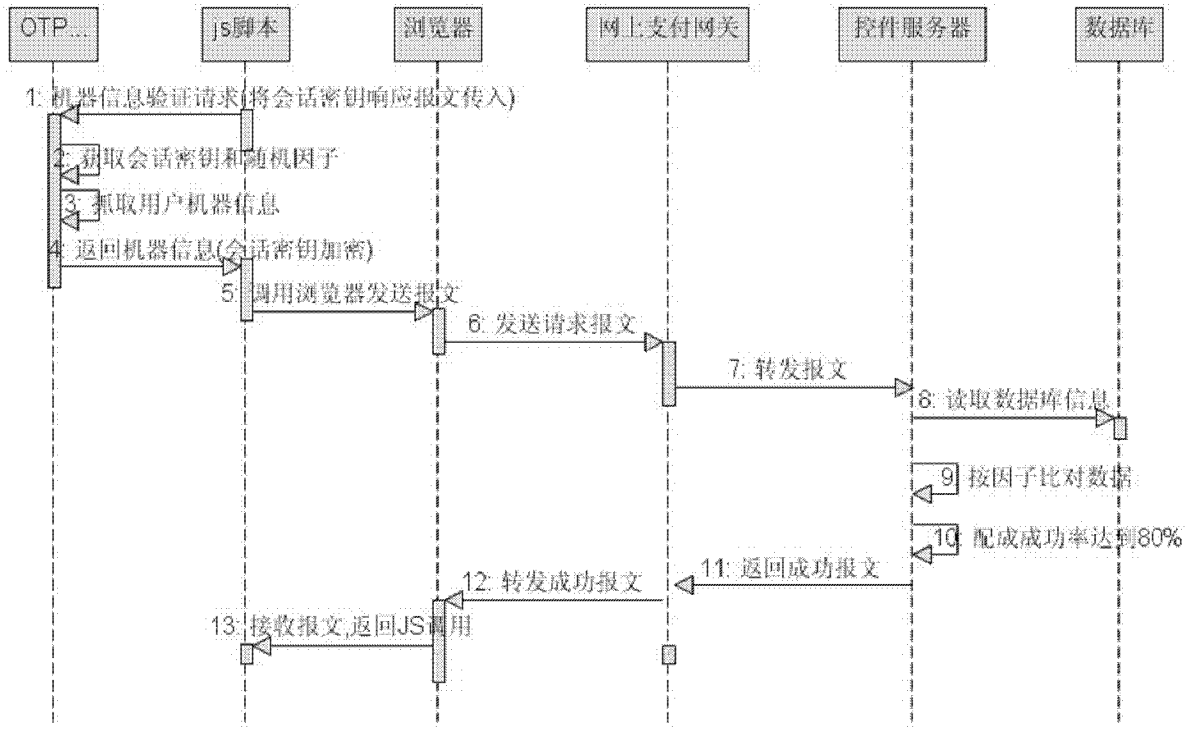

OTP...
js脚本
浏览器
网上支付网关
控件服务器
数据库
1: 机器信息验证请求(将会话密钥响应报文传入)
2: 获取会话密钥和随机因子
3: 抓取用户机器信息
4: 返回机器信息(会话密钥加密)
5: 调用浏览器发送报文
6: 发送请求报文
7: 转发报文
8: 读取数据库信息
9: 按因子比对数据
10: 配成成功率达到80%
11: 返回成功报文
12: 转发成功报文
13: 接收报文,返回JS调用

图 3

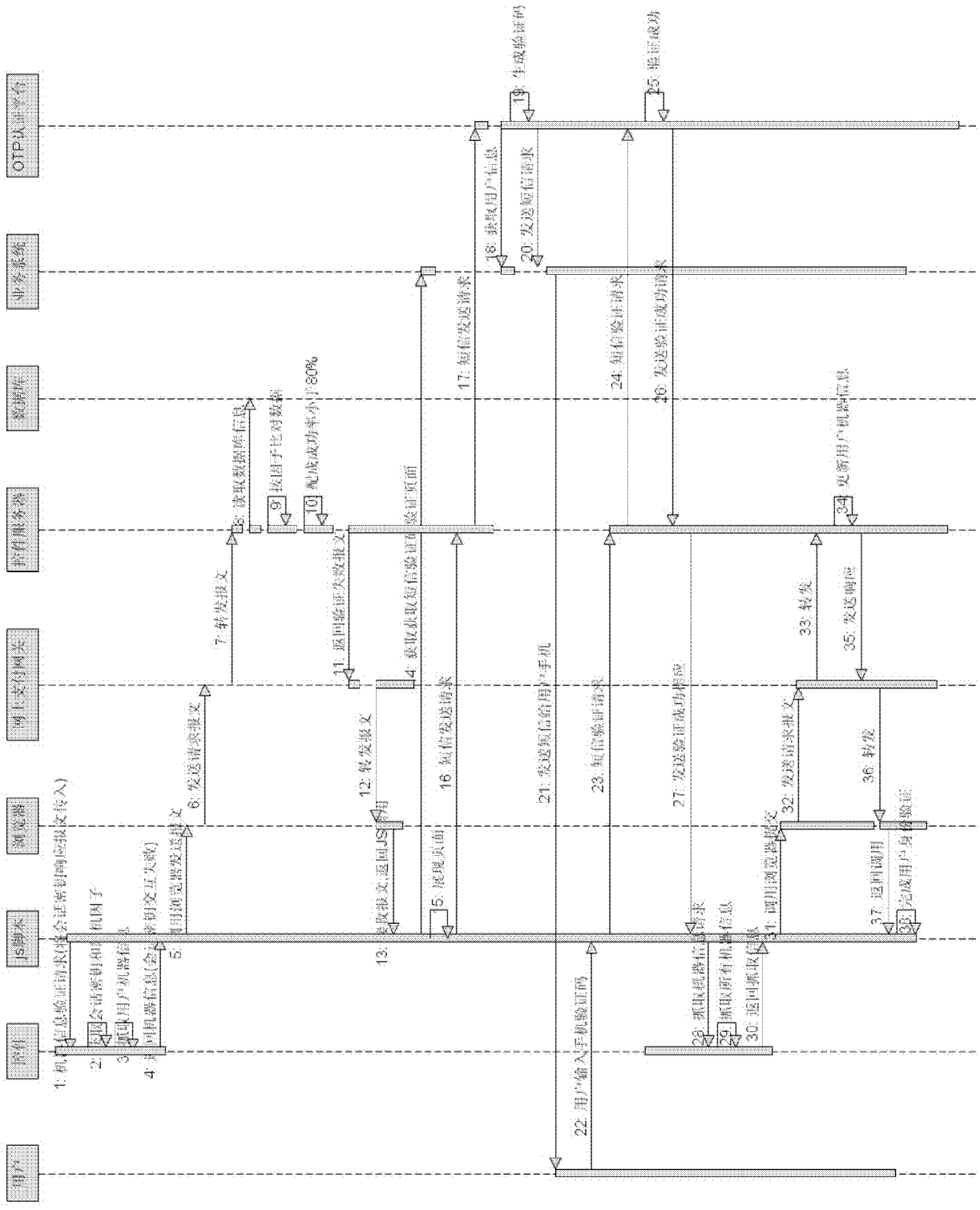

OTP认证平台
业务系统
数据库
操作服务端
网上支付网关
浏览器
JS脚本
控件
用户
19: 生成验证码
25: 验证成功
18: 获取用户信息
20: 发送短信请求
17: 短信发送请求
24: 短信验证请求
26: 发送验证成功请求
8: 读取数据库信息
9: 按因子比对数据
10: 配成成功率小于80%
34: 更新用户机器信息
7: 转发报文
11: 返回验证失败报文
4: 获取获取短信验证码页面
33: 转发
35: 发送响应
6: 发送请求报文
12: 转发报文
16: 短信发送请求
21: 发送短信给用户手机
23: 短信验证请求
27: 发送验证成功响应
32: 发送请求报文
36: 转发
14: 返回JS脚本
15: 展现页面
37: 返回调用
38: 完成用户身份验证
5: 调用浏览器发送报文
13: 返回报文
31: 调用浏览器报文
28: 获取机器信息请求
29: 获取所有机器信息
30: 返回获取信息
22: 用户输入手机验证码

图 4

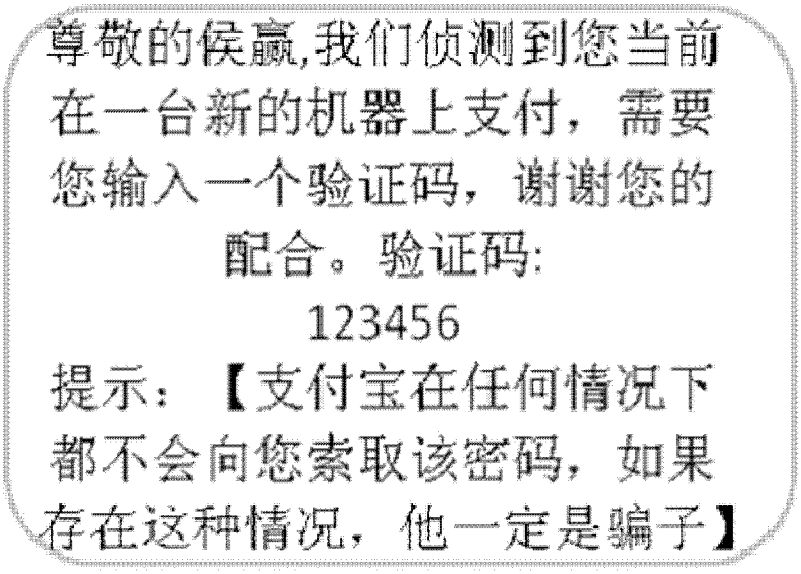

尊敬的侯赢,我们侦测到您当前在一台新的机器上支付，需要您输入一个验证码，谢谢您的配合。验证码:
123456
提示：【支付宝在任何情况下都不会向您索取该密码，如果存在这种情况，他一定是骗子】

图 5

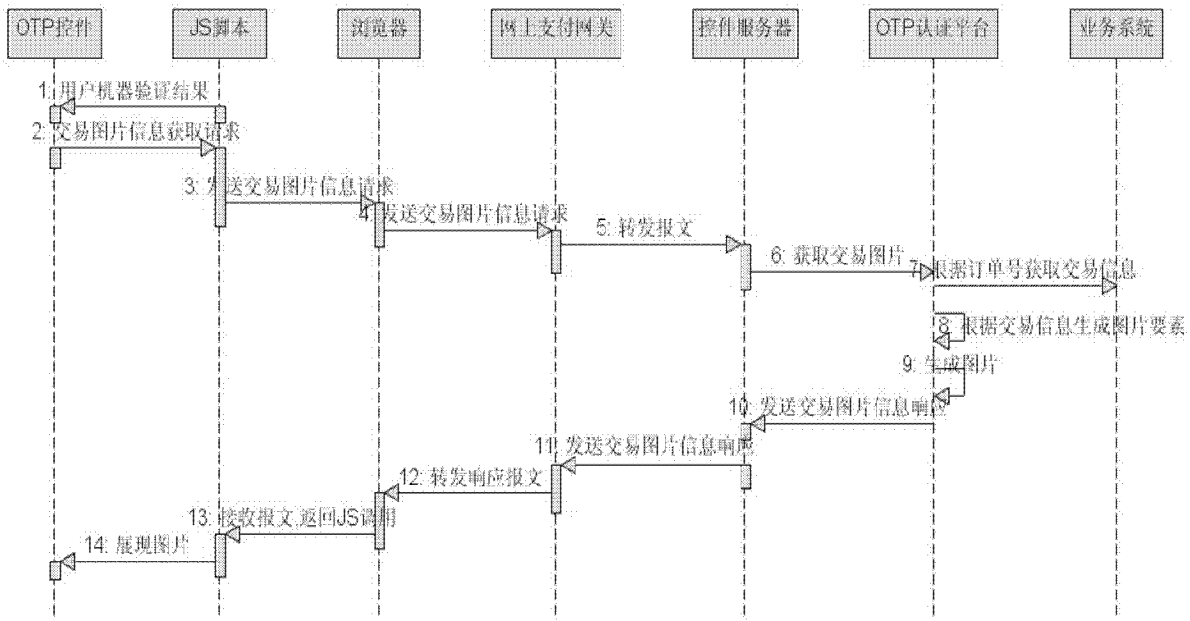

OTP控件
JS脚本
浏览器
网上支付网关
控件服务器
OTP认证平台
业务系统
1: 用户机器验证结果
2: 交易图片信息获取请求
3: 发送交易图片信息请求
4: 发送交易图片信息请求
5: 转发报文
6: 获取交易图片
7: 根据订单号获取交易信息
8: 根据交易信息生成图片要素
9: 生成图片
10: 发送交易图片信息响应
11: 发送交易图片信息响应
12: 转发响应报文
13: 接收报文,返回JS调用
14: 展现图片

图 6

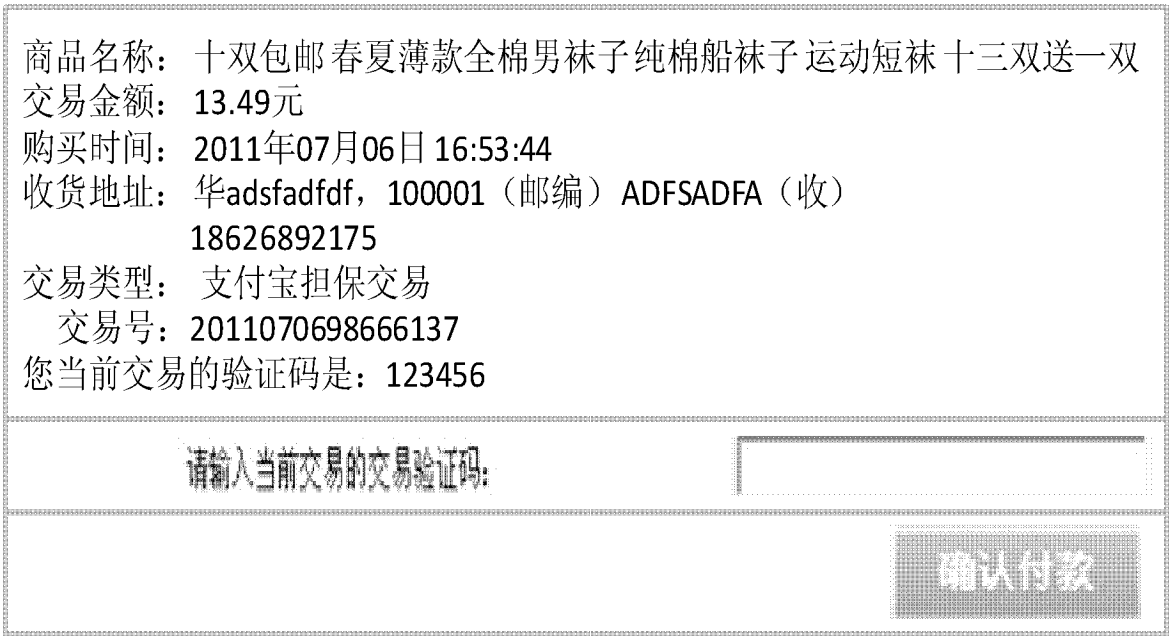

商品名称：十双包邮春夏薄款全棉男袜子纯棉船袜子运动短袜十三双送一双
交易金额：13.49元
购买时间：2011年07月06日 16:53:44
收货地址：华adsfadfdf，100001（邮编）ADFSADFA（收）
18626892175
交易类型：支付宝担保交易
交易号：2011070698666137
您当前交易的验证码是：123456
请输入当前交易的交易验证码：
确认付款

图 7


根据交易信息+会话密钥+时间+用户种子生成验证码
123456
OTP算法驱动
根据交易信息+会话密钥生成摘要
D125B2C4378C081CD3C48DE405807CC6
OTP业务系统
生成底图
图片服务器
摘要信息加入底图，
颜色跟底图一样
D125B2C4378C081CD3C48DE405807CC6
图片服务器
生成交易图片
商品名称：Esprit韩国男袜子男士彩色条纹短袜
船袜夏款个性棉袜sprit薄袜
交易金额：9.50元
购买时间：2011年07月03日 01:33:28
收货地址：华adsfadfdf，100001（邮编）
ADFSADFA（收）18626892175
交易类型：支付宝担保交易
交易号：2011070360403537
您当前交易的验证码：123456
图片服务器

图 8

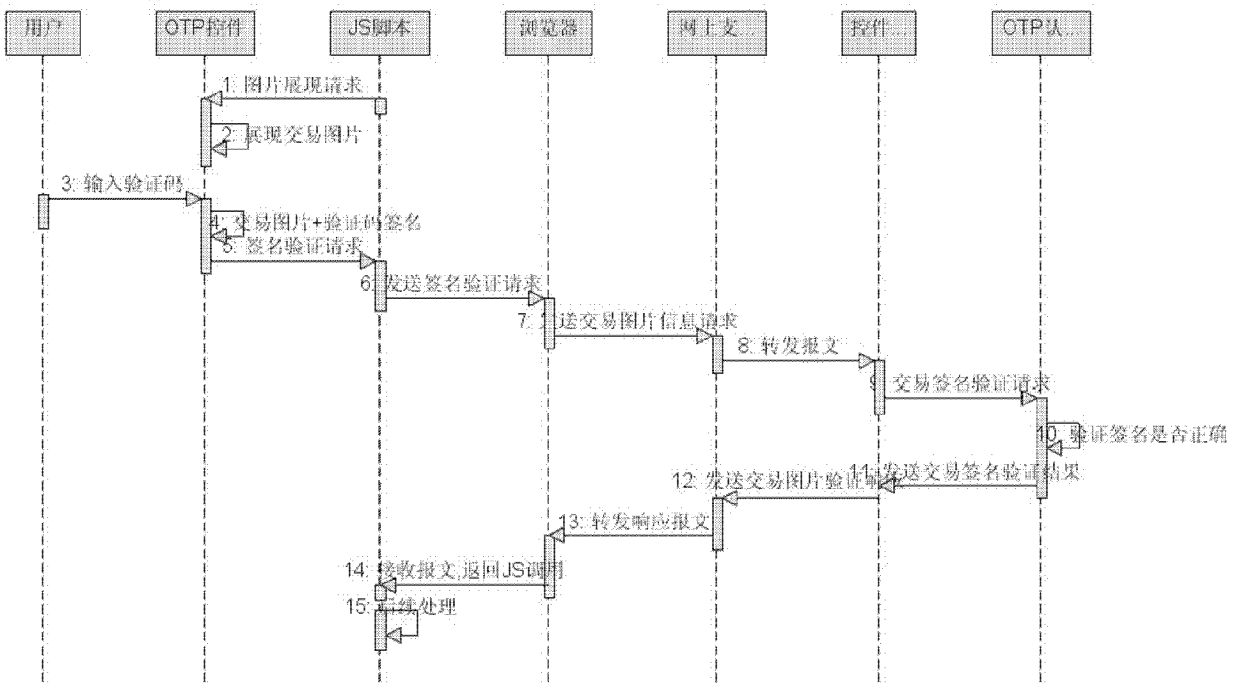

用户
OTP控件
JS脚本
浏览器
网上支
控件
OTP认
1: 图片展现请求
2: 展现交易图片
3: 输入验证码
4: 交易图片+验证码签名
5: 签名验证请求
6: 发送签名验证请求
7: 送交易图片信息请求
8: 转发报文
交易签名验证请求
10: 验证签名是否正确
11: 发送交易签名验证结果
12: 发送交易图片验证结
13: 转发响应报文
14: 接收报文,返回JS调用
15: 后续处理

图 9

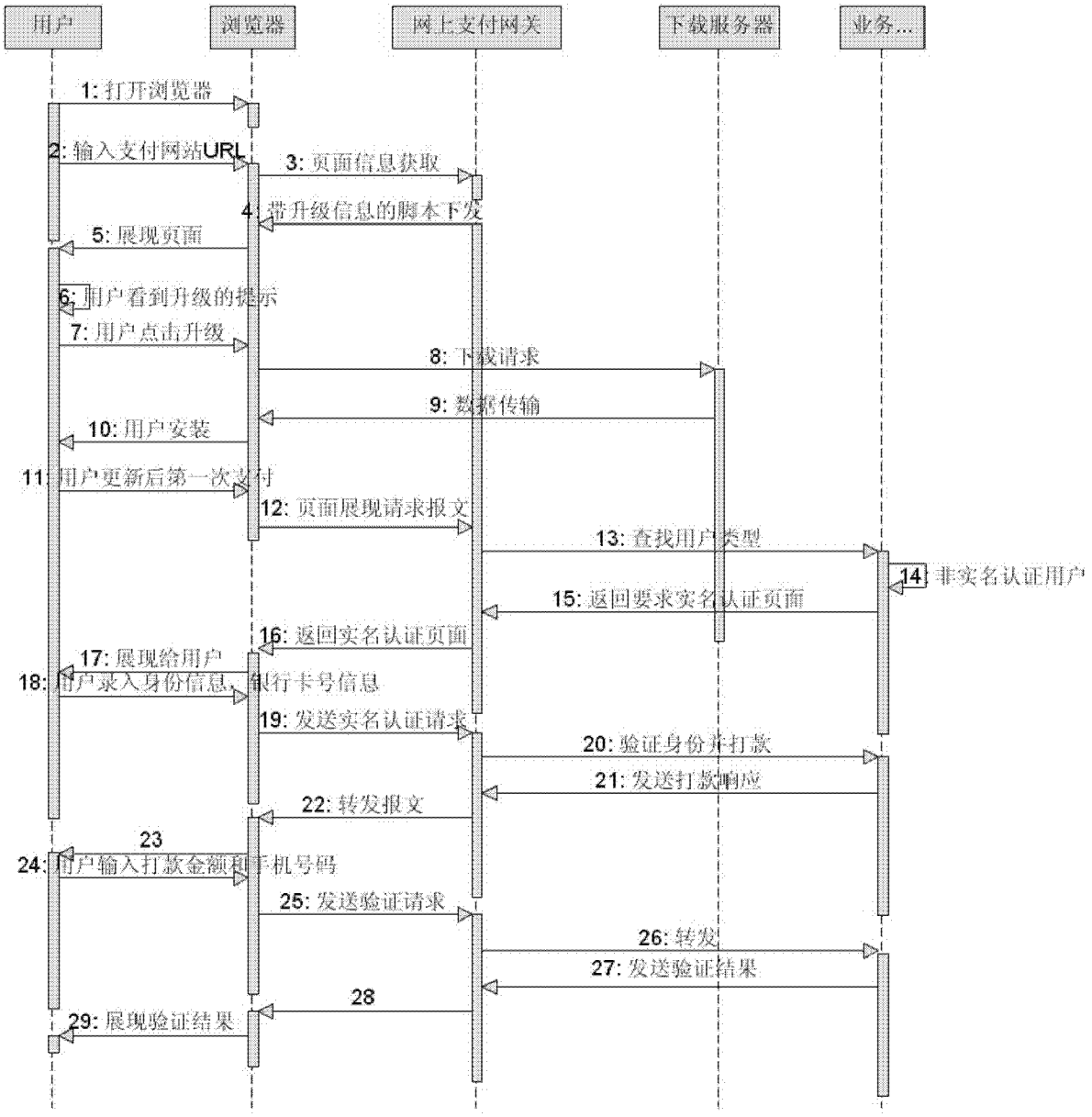

用户
浏览器
网上支付网关
下载服务器
业务...
1: 打开浏览器
2: 输入支付网站URL
3: 页面信息获取
4: 带升级信息的脚本下发
5: 展现页面
6: 用户看到升级的提示
7: 用户点击升级
8: 下载请求
9: 数据传输
10: 用户安装
11: 用户更新后第一次支付
12: 页面展现请求报文
13: 查找用户类型
14: 非实名认证用户
15: 返回要求实名认证页面
16: 返回实名认证页面
17: 展现给用户
18: 用户录入身份信息、银行卡号信息
19: 发送实名认证请求
20: 验证身份并打款
21: 发送打款响应
22: 转发报文
23
24: 用户输入打款金额和手机号码
25: 发送验证请求
26: 转发
27: 发送验证结果
28
29: 展现验证结果

图 10


OTP控件 10
OTP控件服务器 20
OTP认证平台 30

图 11


OTP控件 10
客户端脚本模块40
OTP控件服务器 20
OTP认证平台 30

图 12

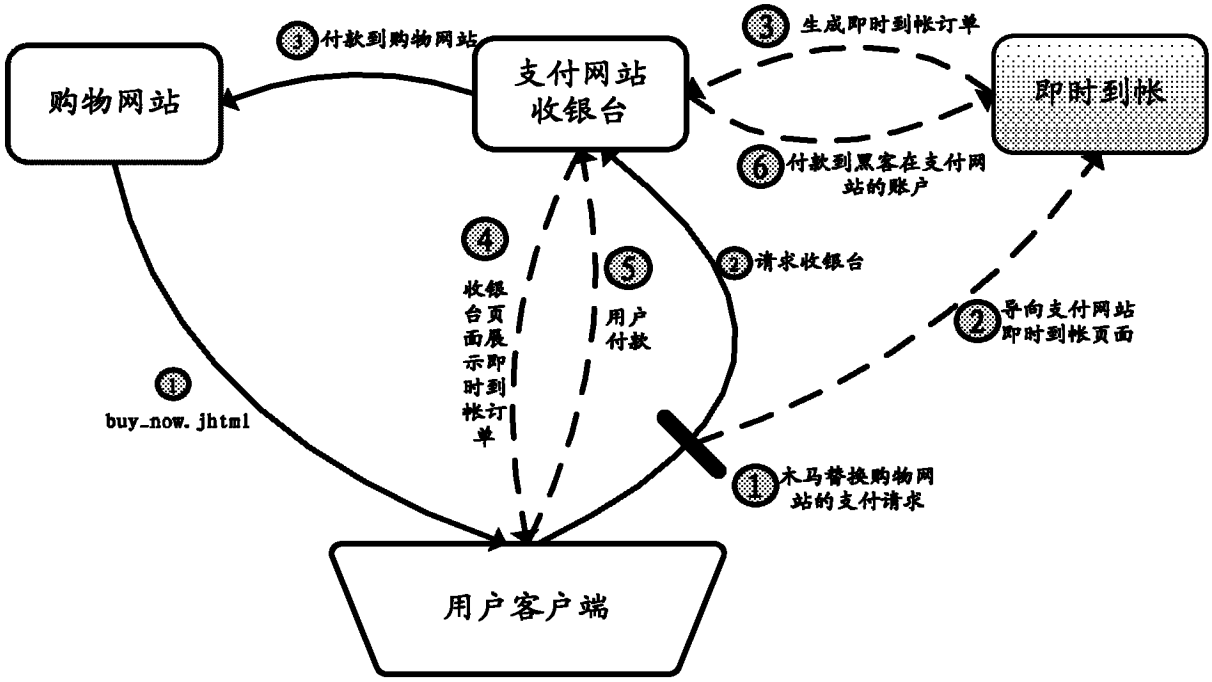

购物网站
支付网站
收银台
即时到帐
用户客户端
6 付款到购物网站
3 生成即时到帐订单
6 付款到黑客在支付网站的账户
4 收银台页面展示即时到帐订单
5 用户付款
2 请求收银台
2 导向支付网站即时到帐页面
1 buy_now.jhtml
1 木马替换购物网站的支付请求

图 13

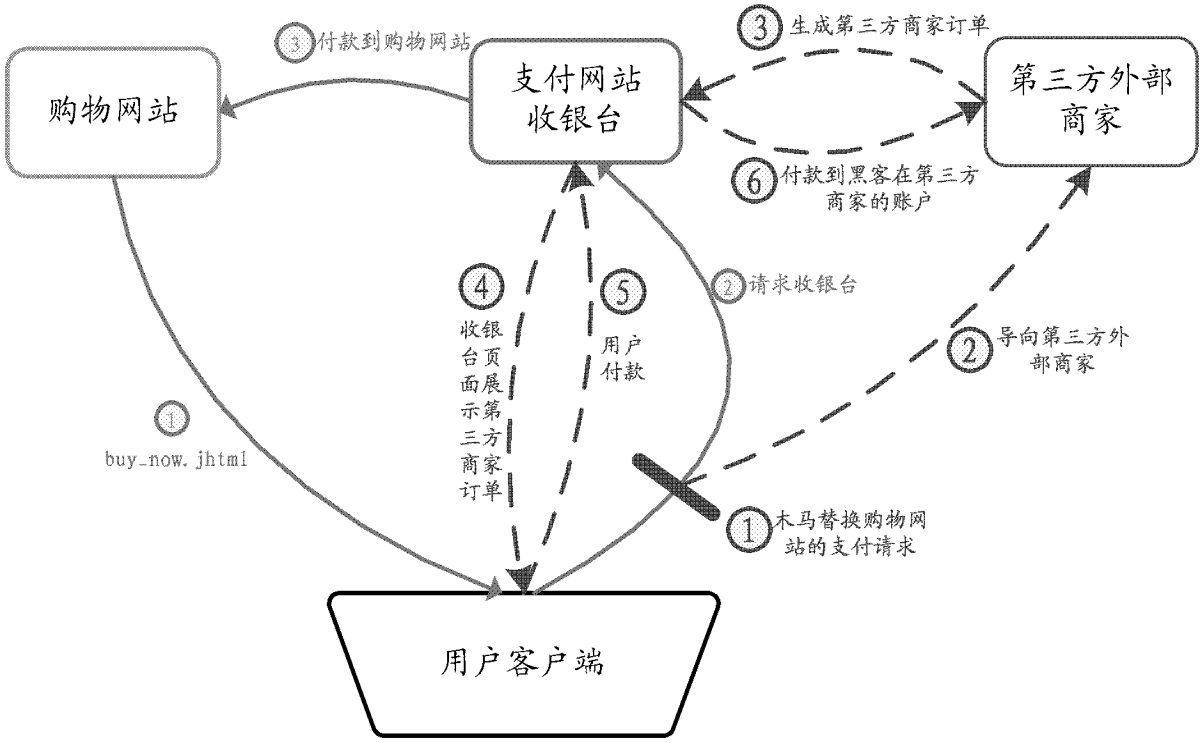

购物网站
支付网站
收银台
第三方外部
商家
3 付款到购物网站
3 生成第三方商家订单
6 付款到黑客在第三方
商家的账户
4 收银台页面展示第三方商家订单
5 用户付款
2 请求收银台
2 导向第三方外部商家
1 buy_now.jhtml
1 木马替换购物网站的支付请求
用户客户端

图 14

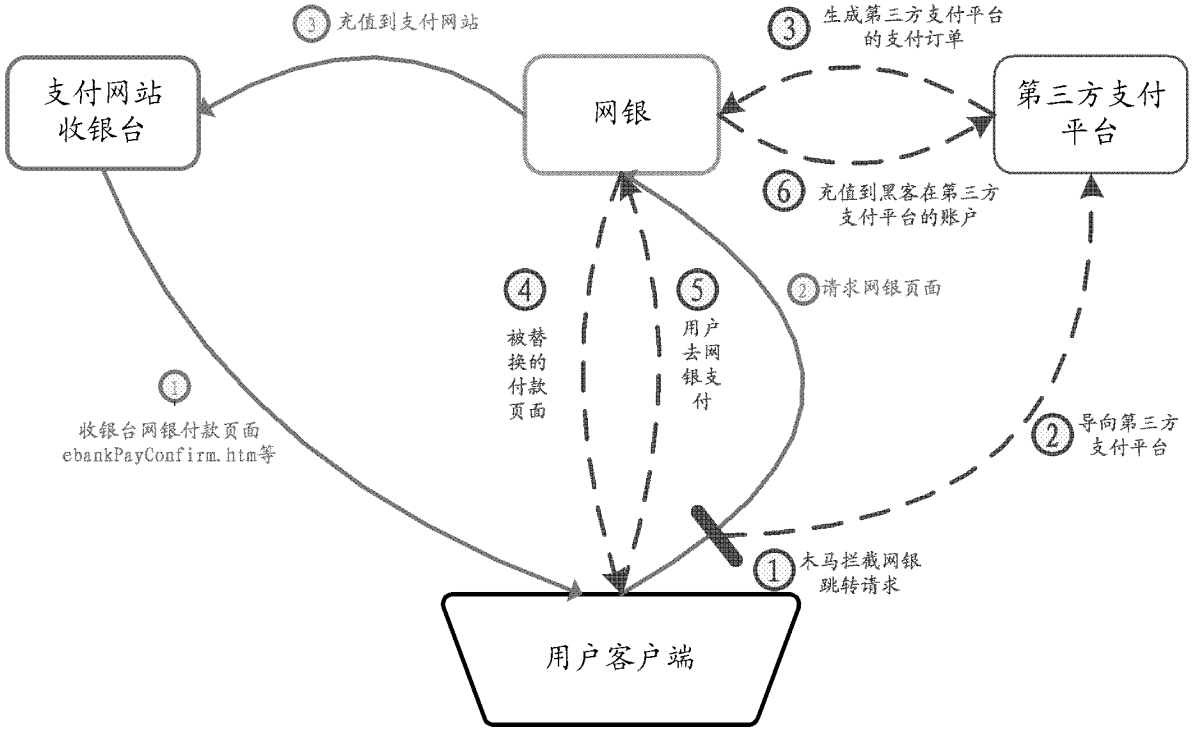

支付网站
收银台
网银
第三方支付
平台
3 充值到支付网站
3 生成第三方支付平台
的支付订单
6 充值到黑客在第三方
支付平台的账户
4 被替换的付款页面
5 用户去网银支付
2 请求网银页面
2 导向第三方
支付平台
1 收银台网银付款页面
ebankPayConfirm.htm等
1 木马拦截网银
跳转请求
用户客户端

图 15