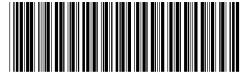


(19) 中华人民共和国国家知识产权局



(12) 发明专利

(10) 授权公告号 CN 101495956 B

(45) 授权公告日 2012.03.07

(21) 申请号 200680033466.5

(51) Int. Cl.

(22) 申请日 2006.08.10

G06F 7/04 (2006.01)

(30) 优先权数据

60/707,203 2005.08.11 US

(56) 对比文件

(85) PCT申请进入国家阶段日

US 2003046340 A1, 2003.03.06,
US 6161182 A, 2000.12.12,
US 6438539 B1, 2002.08.20,

2008.03.12

审查员 明媚

(86) PCT申请的申请数据

PCT/IL2006/000928 2006.08.10

(87) PCT申请的公布数据

W02007/017878 EN 2007.02.15

(73) 专利权人 晟碟以色列有限公司

地址 以色列萨巴

(72) 发明人 埃亚尔·贝奇科夫

(74) 专利代理机构 中国国际贸易促进委员会专

利商标事务所 11038

代理人 鲍进

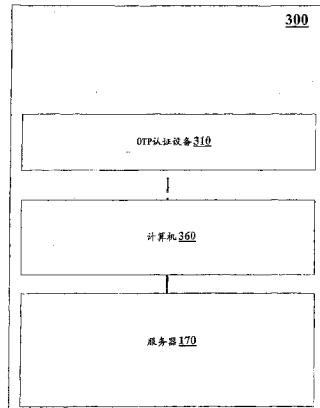
权利要求书 3 页 说明书 10 页 附图 10 页

(54) 发明名称

扩展一次性密码方法和装置

(57) 摘要

本发明披露了一种用于实现对客户机工作站进行认证以便通过因特网与服务器进行会话的OTP 令牌。将至少部分识别服务器的信息提供给OTP 令牌和 / 或客户机工作站，并使用该识别信息判定服务器是否是合法服务器。根据该判定，决定是否将表示会话 OTP 的数据从 OTP 令牌发送到客户机工作站。在某些实施例中，如果识别信息表示合法服务器，则将表示会话 OTP 的数据从 OTP 令牌发送到客户机工作站，否则，由客户机工作站拒绝表示会话 OTP 的数据。在各实施例中，表示会话 OTP 的数据可包括，从用户认证数据得出的多因素认证数据，或与用户认证数据无关的会话 OTP 数据。



B

CN 101495956

1. 一种处理与一次性密码 OTP 令牌的会话 OTP 传输的方法,所述 OTP 令牌经由网络与服务器和客户机工作站通信,所述方法包括以下步骤:

OTP 令牌利用在 OTP 令牌处的嵌入式安全浏览器打开 OTP 令牌和服务器之间的安全会话;

在打开安全会话之后,在 OTP 令牌处从服务器接收至少部分识别服务器的服务器信息;

OTP 令牌基于所接收的服务器信息判定所述服务器是否是合法的;

响应于判定所述服务器是合法的:

从 OTP 令牌发送内部生成的会话 OTP 的数据;以及

利用 OTP 令牌发起与服务器的客户机 - 服务器会话;以及响应于判定所述服务器不是合法的:

制止从 OTP 令牌发送内部生成的会话 OTP 的数据。

2. 根据权利要求 1 的方法,其中,所述内部生成的会话 OTP 的数据属于一
会话 OTP,并且,通过设备接口将所述数据从 OTP 令牌发送到客户机工作站。

3. 根据权利要求 1 的方法,其中,发送内部生成的会话 OTP 的数据包括:

在 OTP 令牌的显示屏幕上显示出所述会话 OTP 的数据。

4. 根据权利要求 1 的方法,其中,所述内部生成的会话 OTP 的数据包括至少部分基于用
户认证数据而得出的多因素认证数据。

5. 根据权利要求 1 的方法,其中,所述内部生成的会话 OTP 的数据不是从用户认证数据
得出的。

6. 根据权利要求 1 的方法,还包括:

响应于确定所述服务器不是合法的:

在 OTP 令牌内内部生成所述会话 OTP;以及

保持其中所述会话 OTP 保留在 OTP 令牌内的状态。

7. 根据权利要求 1 的方法,还包括:

在打开所述安全会话之后,将所述安全会话的客户机端从 OTP 令牌转移到客户机工作
站,

其中,所述客户机工作站执行所述接收至少部分识别服务器的服务器信息的步骤和所
述基于所接收的服务器信息判定所述服务器是否是合法的步骤中的至少一个。

8. 根据权利要求 1 的方法,其中,在 OTP 令牌从服务器接收到所述服务器信息时,所述
安全会话的客户机端保留在所述嵌入式安全浏览器处。

9. 根据权利要求 1 的方法,其中,由 OTP 令牌通过服务器与 OTP 令牌之间的通信链路执
行所述接收。

10. 根据权利要求 1 的方法,其中,在 OTP 令牌内执行对于所述服务器是否是合法的判
定。

11. 根据权利要求 1 的方法,其中,判定服务器是否是合法的包括:

查询驻留在 OTP 令牌内的数据库。

12. 根据权利要求 11 的方法,其中,客户机工作站查询所述数据库。

13. 根据权利要求 11 的方法,其中,驻留在 OTP 令牌内的客户机代码使得所述 OTP 令牌

查询所述数据库。

14. 根据权利要求 11 的方法,其中,所述数据库是不变数据库。

15. 根据权利要求 11 的方法,其中,所述数据库包括可接受 URL 的预定列表、可接受 IP 地址的预定列表和可接受证书字段值的预定列表中的一个。

16. 一种处理与一次性密码 OTP 令牌的会话 OTP 传输的方法,所述 OTP 令牌经由网络与服务器和客户机工作站通信,所述方法包括以下步骤:

在 OTP 令牌处从服务器接收至少部分识别服务器的服务器信息;

基于所接收的服务器信息判定所述服务器是否是合法的;

响应于判定所述服务器是合法的:

从 OTP 令牌发送内部生成的会话 OTP 的数据;以及

利用 OTP 令牌发起与服务器的客户机 - 服务器会话;以及响应于确定所述服务器不是合法的:

制止从 OTP 令牌发送内部生成的会话 OTP 的数据;

其中,根据接收到的一个通信的协议数据、在接收到的通信中发送的证书数据、IP 地址数据和 URL 数据的其中至少一个执行对于所述服务器是否是合法的判定。

17. 根据权利要求 16 的方法,其中,根据自所述服务器接收的证书的仅某些属性执行对于所述服务器是否是合法的判定。

18. 一种与客户机工作站一起使用的一次性密码 OTP 令牌,所述客户机工作站经由网络与服务器通信,所述 OTP 令牌包括:

人工输入设备,用于输入至少部分识别服务器的信息;

服务器合法性引擎,用于基于所述信息判定服务器是否是合法的;

OTP 发生器,用于生成会话 OTP;

OTP 发送决定引擎,用于决定是响应于确定所述服务器是合法的而从 OTP 令牌发送会话 OTP 的数据,还是响应于确定所述服务器不是合法的而制止发送会话 OTP 的数据;以及

嵌入在 OTP 令牌内的嵌入式安全浏览器,所述嵌入式安全浏览器用于打开在 OTP 令牌与服务器之间的安全会话。

19. 根据权利要求 18 的 OTP 令牌,还包括:

OTP 发送器,用于根据所述 OTP 发送决定引擎的决定,从 OTP 令牌发送表示会话 OTP 的数据。

20. 根据权利要求 19 的 OTP 令牌,还包括:

设备端口,其中,所述 OTP 发送器用于仅在判定所述服务器是合法的时,实现所述会话 OTP 的数据经由所述设备端口的设备间数据传送。

21. 根据权利要求 19 的 OTP 令牌,还包括:

数据显示器,其中,所述 OTP 发送器用于仅在判定所述服务器是合法的时,将所述会话 OTP 的数据发送到所述数据显示器。

22. 根据权利要求 18 的 OTP 令牌,其中,所述嵌入式安全浏览器用于在所述安全会话期间接收所述至少部分识别服务器的信息。

23. 根据权利要求 18 的 OTP 令牌,其中,所述服务器合法性引擎包括:

预定数据的数据库,其中,所述服务器合法性引擎用于根据所述数据库的内容判定所

述服务器是否是合法的。

24. 根据权利要求 23 的 OTP 令牌, 其中, 所述数据库是不变数据库。

25. 根据权利要求 23 的 OTP 令牌, 其中, 所述数据库包括可接受 URL 的预定列表、可接受 IP 地址的预定列表和可接受证书字段值的预定列表中的一个。

26. 一种与客户机工作站一起使用的一次性密码 OTP 令牌, 所述客户机工作站经由网络与服务器通信, 所述 OTP 令牌包括 :

人工输入设备, 用于输入至少部分识别服务器的信息 ;

服务器合法性引擎, 用于基于所述信息判定服务器是否是合法的 ;

OTP 发生器, 用于生成会话 OTP ; 以及

OTP 发送决定引擎, 用于决定是响应于判定所述服务器是合法的而从 OTP 令牌发送会话 OTP 的数据, 还是响应于判定所述服务器不是合法的而制止发送会话 OTP 的数据 ;

其中, 所述服务器合法性引擎用于根据来自服务器的通信的协议数据、在来自服务器的通信中发送的证书数据、IP 地址数据和 URL 数据中的至少一个判定服务器是否是合法的。

27. 根据权利要求 26 的 OTP 令牌, 其中, 所述服务器合法性引擎用于根据自所述服务器接收的证书的仅某些属性判定服务器是否是合法的。

28. 一种与客户机工作站一起使用的一次性密码 OTP 令牌, 所述客户机工作站经由网络与服务器通信, 所述 OTP 令牌包括 :

人工输入设备, 用于输入至少部分识别服务器的信息 ;

服务器合法性引擎, 用于基于所述信息判定服务器是否是合法的 ;

OTP 发生器, 用于生成会话 OTP ; 以及

OTP 发送决定引擎, 用于决定是响应于判定所述服务器是合法的而从 OTP 令牌发送会话 OTP 的数据, 还是响应于判定所述服务器不是合法的而制止发送会话 OTP 的数据 ;

其中, 所述 OTP 发生器用于根据用户认证数据生成所述会话 OTP, 从而生成所述会话 OTP 作为多因素认证数据。

29. 根据权利要求 28 的 OTP 令牌, 还包括 :

用户识别模块, 用于对所述用户认证数据进行认证。

30. 根据权利要求 29 的 OTP 令牌, 其中, 所述 OTP 发送决定引擎用于根据所述用户认证数据的认证, 决定是发送会话 OTP 的数据, 还是制止发送会话 OTP 的数据。

扩展一次性密码方法和装置

技术领域

[0001] 本发明涉及因特网 (Internet) 认证, 具体而言, 涉及使用一次性密码 (one-time password) 的认证。

背景技术

[0002] 许多因特网用户对其服务提供商, 公司网络, 付费服务, 或其银行或信用卡帐户具有特定访问权限。为了行使其权力, 这样的用户需对其自身进行认证。用于用户认证的大多数已知和常用方法是基于输入用户名和密码。

[0003] 随着因特网欺骗的不断增多和日益高级, 用户名和密码认证并不被视为是安全的, 这是因为通过通信网络, 能够很容易地截取数据, 从而, 被攻击者重新使用以冒充原用户的身份和权限。

[0004] 一次性密码 (此后称为“OTP”) 是常用的补救措施, 是由多个供应商提供, 用于克服用户名和密码方案的脆弱性。它是基于仅对单个登录或事务使用密码, 然后使该密码无效。任何其他登录或事务将需要不同的密码。从而, 即使某些人截取了密码, 那对于以后的事务是无用的。

[0005] 存在有三种用于生成和管理一次性密码的基本方法。一种方法是, 在纸制或电子文件上具有密码的长列表; 第二种方法是, 使用运行在其的个人计算机 (台式、膝上型、掌上型或智能电话) 上运行的软件, 生成这样的密码; 第三种方法是, 使用专用硬件设备生成密码。本发明的重点在于针对这样的硬件设备。

[0006] 图 1A 描述了现有技术的系统 100, 其使用专用 OTP 认证设备 110 (通常而言, 为 OTP “令牌”) 生成一次性密码。计算机 160 包括用于协同在服务器 170 上运行的服务器应用 182 运行客户机应用 168 的处理容量 (未示出), 以便获得目标功能, 如对信息或事务的访问。客户机应用 168 可为专用程序或通用 Web 浏览器。服务器应用 182 需要获得来自 OTP 验证器 178 的核准, 以便提供目标功能。OTP 验证器 178 是设计用于接收和检查来自服务器应用 182 的 (一次性) 密码的软件模块, 其再从客户机应用 168 接收这样的密码。在所考虑的配置中, 利用从 OTP 认证设备 110 生成和通过认证设备接口 164 接收的数据, 得出该密码。OTP 认证设备 110 是由用户携带的安全便携式设备, 其适用于与多个计算机 160 相接口。OTP 认证设备 110 的核心是 OTP 发生器 130, 它是基于微处理器的密码软件程序, 其被设计用于基于记录在 OTP 认证设备 110 中的触发器 120 和秘密用户密钥 132 生成一次性密码。一般而言, 将 OTP 设备 110 构造成具有抗篡改或防篡改性, 以防止访问和 / 或篡改秘密用户密钥 132 数据。

[0007] 触发器 120 是将 OTP 发生器 130 的一个密码生成操作改变到其他生成会话的元件, 因此提供密码的“一次性”方面。在现有技术中用于生成触发器 120 的三种常用方法是, 从服务器 170 接收随机询问 (random challenge) 120A, 从内嵌在 OTP 认证设备 110 中的精确实时钟 120B 接收全日期时间串, 或对于每次相继密码生成加 1 的计数器 120C。

[0008] 在所披露内容中, “会话 OTP 数据”指从触发器 120 和秘密用户密钥 132 得出的数

据。在 OTP 认证设备 110 和 / 或客户机工作站 160 内, 可将该会话 OTP 数据与用户认证数据 (即, 密码、生物学数据等) 进行组合以生成双因素 (或多因素) 认证数据。对于在 OTP 认证设备 110 内实现组合的特定情形, 双因素认证数据本身是“会话 OTP 数据”的形式。然而, 只要会话 OTP 数据是从用户密钥 132 和触发器 120 得出, 就不存在如从 OTP 设备 110 提供给客户机工作站 160 的“会话 OTP 数据”将是由用户提供数据 (即, 密码 /PIN 数据或生物学数据) 得出的多因素认证数据的明确要求。

[0009] 作为可选形式以及通常方式, 可将用户标识符 (或用户识别模块) 134 设置在 OTP 认证设备 110 中, 以防止发现或偷窃 OTP 认证设备 110 的一些人对其滥用。在许多实现方式中, OTP 发生器 130 不会生成 (或不会发送) 会话 OTP 数据, 除非用户标识符 134 提供肯定的用户识别。

[0010] 进行用户识别的常用方法是用于接收个人识别号 (PIN) 的小键盘、生物学传感器, 或检查 PIN 或自计算机 / 客户机工作站 160 接收 (通常来讲, 通过客户机工作站 160 的键盘输入到客户机工作站 160 中) 的其他数据的比较器。

[0011] OTP 接口 140 与认证设备接口 164 相接口, 以便在 OTP 认证设备 110 与计算机 160 之间交换 OTP 相关数据。特别是, 只要当 OTP 发生器 130 生成会话 OTP, OTP 发送器 (未示出) 就从 OTP 设备 110 “发送”(即, 显示和 / 或实现数据交换, 以便通过 OTP 接口 140 向计算机 160 提供会话 OTP 数据) 会话 OTP。

[0012] 用于 OTP 接口 140 的常用实现方式是: 显示器 140A, 用户利用它读取密码, 并将其人工输入到用作为认证设备接口 164 的键盘中 (那么, 优选的触发器 120 可为实时时钟 120B 或计数器 120C); USB 接口 140B (或其他“联系”接口), 与用作为认证设备接口 164 的匹配 USB 接口相接口, 以建立双向串行通信, 或 IR/RF 接口 140C (或其他“无线接口”), 与用作为认证设备接口 164 的可兼容红外 / 射频收发器相接口。在 USB 140B 和 IR/RF 接口 140C 的情形中, 用于触发器 120 的所有三种方法均可使用。

[0013] 应该注意, OTP 接口 140 应用显示器 140A 的情形并不需要在 OTP 认证设备 110 与计算机 160 之间的任何直接电子通信链路。在许多示例中, 用户将从显示器 140B 读取的会话 OTP 数据 140 以及用户认证数据 (即, 例如, 对于“双因素”认证的第二种方法而言, 为密码和 / 或生物学数据) 输入到客户机工作站 160, 在此将该数据进行组合, 以生成双因素认证密码 (其本身属于 OTP 类型)。

[0014] 仅当 OTP 验证器 178 核准时, 服务器 170 允许服务器应用 182 向客户机应用 168 提供目标服务。OTP 验证器 178 包括处理和密码装置, 用于对通过计算机 160 自 OTP 认证设备 110 接收的密码进行检查, 并考虑用户密钥 132 和触发器 120。用户密钥 132 是从用户数据库 176 检索得出, 用户数据库 176 包括合法用户的记录, 包括其用户名和密钥。触发器 120 的值通过 OTP 验证器 178 从触发器同步器 174 检索而得到, 其包含有分别对应于用于从询问 120A 中选出的触发器 120 的方法、实时时钟 120B 和计数器 120C 的询问发生器、实时时钟或计数器。

[0015] 图 1B 表示如图 1A 所示同一现有技术系统。在图 1B 中, 显式表示出 OTP 认证设备 110、计算机 160 (即, 客户机工作站) 和服务器 170 的部署。更具体而言, 如图 1B 所示, 客户机工作站 / 计算机 160 通过因特网接入链路 (例如, 宽带链路、拨号链路、SOHO 链路或任何其他 ISP (因特网服务提供商) 接入链路, 或用于蜂窝设备网上冲浪的蜂窝电话因特网接

入链路),利用由 ISP 提供的 WAN 网关 22(1SP 接入点)与广域网 20 相连。服务器 170 通过广域网 20(通常使用包交换协议)将对于会话 OTP 的请求发送到客户机工作站 160。当客户机工作站 160 接收该请求时,OTP 认证设备 110 将会话 OTP 发送(自动输入或由用户通过客户机工作站的键盘输入)到客户机工作站 160。该会话 OTP 数据可被直接转发到服务器 170,或者将其与认证数据(即,密码、PIN、生物学数据)进行组合,然后通过广域网(即,因特网)20 发送到服务器 170。

[0016] 图 2 描述了根据某些现有技术的如图 1A-1B 所示系统 100 的操作。在步骤 201 中,计算机 160 的用户启动客户机应用 168。客户机应用 168 需要与服务器应用 182 进行通信和交互,以便为用户提供所需目标功能,如对数据的访问或进行交易。在步骤 221 中,服务器应用 182 通过对使用 OTP 进行用户认证的请求,对客户机应用 168 进行响应。该请求被传输到 OTP 认证设备 110,在此,在步骤 221 中,OTP 发生器 130 由触发器部件 120 请求触发器生成 OTP。如果触发器为询问 120A,则服务器 170 在触发器同步器 174 中生成随机询问串,并将其通过计算机 160 提供给 OTP 发生器 130;如果触发器为实时时钟 120B 或计数器 120C 的任何一种,则在 OTP 认证设备 110 内将其自动生成。在步骤 231 中,OTP 发生器 130 对触发器 120 和用户密钥 132 进行处理,以生成 OTP。在步骤 241 中,将步骤 231 中生成的 OTP 从 OTP 设备 110 发送到客户机工作站 160,客户机工作站 160 将从 OTP 得出的数据转发到服务器 170。在步骤 251 中,OTP 验证器 178 基于从触发器同步器 174 检索出的触发器和从用户数据库 176 检索出的用户密钥,计算预期 OTP,并将其与通过计算机 160 从 OTP 认证设备 110 接收的 OTP 进行比较。如果验证结果是肯定的,则步骤 261 将流程进行到步骤 271,在此,客户机服务器会话开始通过在客户机应用 168 与服务器应用 182 之间的协作提供所需目标服务;如果验证结果是否定的,则步骤 261 将流程转到步骤 281,其中,服务器 170 拒决从计算机 160 接收的服务请求,并由计算机 160 向用户进行通知。

[0017] 以上所述系统使用现有技术的典型用户认证方法,重点强调通过服务提供商(其操作服务器 170)进行对用户(其使用计算机 160)进行认证。该单向认证方法在一定程度上保护服务提供商和用户避免遭受用户身份失窃,直至引入称为“网络钓鱼(phishing)”的新欺骗模式为止,这种欺骗模式甚至成为主流欺骗方法。在网络钓鱼中,通过假装成来自其银行或合法团体、著名因特网商业网站的电子邮件消息与用户打招呼。该消息邀请用户更新其详细信息或进行商业事务。在该过程期间,要求用户对其本人进行认证,罪犯利用用户提供的信息盗取用户身份,并以用户名义进行其他事务。用户名和密码的组合在网络钓鱼面前极其脆弱,这是由于罪犯将用户交出的用户名和密码用于更多事务。OTP 的使用,极大缩减了网络钓鱼的效果,但不会针对称为“中间人(man in the middle)”的网络钓鱼变型提供完全保护。在中间人攻击中,来自假站点的消息在用户看起来很像是合法金融或商业事务。在事务发生的同时,罪犯与实际站点进行其自己的事务。罪犯通过了基于 OTP 的认证会话,然后实施将金钱传输或将货物发送到他自己或其合伙人那里的事务。

[0018] 存在有许多关于在具有中间人攻击风险的环境中提高安全性的技术的公开文献。潜在相关专利和公开专利申请包括 US20010045451, US20060041759, US6141752, WO2005098630, WO06018647 和 WO06062838,所有这些申请其全部内容在此引作参考。

[0019] RSA Security 公司的白皮书“Enhancing One-Time Passwords for Protection Against Real-Time Phishing Attacks”披露了其中结合客户机工作站使用 OTP 设备(即,

电子令牌) 的技术。OTP 设备与客户机工作站进行通信(例如,“联系”OTP 设备通过 USB 接口进行通信,其中,通过 USB 接口提供触发器导出数据),或被将触发器导出 OTP 码(即,触发器导出数据)输入到客户机工作站的键盘中的人们使用。在客户机工作站处,将触发器导出 OTP 码(或自动提供,或从 OTP 令牌的屏幕拷贝)与输入到客户机工作站的密码/PIN 数据进行组合,以提供“双因素”密码。更具体而言,并非将该密码/PIN 数据输入到浏览器中以及直接将组合数据双因素认证数据在因特网上发送,而是在客户机工作站上提供驻留软件“密码保护模块(PPM)”(通常与浏览器相分离),以接收用户密码/PIN。在客户机工作站处,PPM 模块将用户密码/PIN 与 OTP 设备令牌提供的 OTP 数据进行组合。在从客户机工作站发送到服务器之前,根据请求服务器的身份由 PPM 对组合数据进行加密/散列化处理。这估计难以使“中间人”访问散列密码,以及学习 OTP 数据和/或双因素认证数据和/或用户认证数据。

[0020] 即使 PPM 通常是与易受攻击的浏览器相分离的应用,该现有技术的一个缺点在于,会话 OTP 数据总是从典型抗篡改 OTP 设备(由用户或通过设备接口)提供给潜在不安全客户机工作站,即使存在请求 OTP 认证的服务器不合法的一定风险也是如此。

[0021] 由于网络钓鱼和中间人攻击的威胁,非常需要用于保护 OTP 数据被授权方访问的改进型方法和装置。

发明内容

[0022] 本发明人在此披露用于扩展一次性密码(OTP)基本结构所提供的保护以有效阻止网络钓鱼攻击的系统和功能。具体而言,本发明人将披露,仅在存在某种迹象表明请求会话 OTP 的服务器是合法服务器时,向客户机工作站提供会话 OTP 数据可能有益。否则,如果未表明(或不足以表明)请求会话 OTP 数据的服务器是合法服务器时,OTP 设备拒绝来自客户机工作站/终端的会话 OTP 数据可能是有益的。

[0023] 尽管不是明确要求,在示例性实施例中,与判定请求服务器是否合法相关联的特定功能还可在抗篡改 OTP 设备内执行,从而,通过用于验证服务器身份的机制,提供防篡改(例如,由骇客和/或欺骗者和/或中间人实施)的进一步保护。或者或另外,该功能可在客户机工作站中执行。

[0024] 本发明首次披露用于处理会话 OTP 数据(例如,根据服务器生成的对于会话 OTP 的请求)传输的方法。目前所披露的方法可在这样的系统中执行,即该系统包括服务器、客户机工作站、OTP 令牌,其中,客户机工作站通过广域网(通常是因特网)与服务器进行通信,OTP 令牌通过设备接口(即,通过“联系”或“无线”接口)与客户机工作站相接口。本发明所披露的方法包括以下步骤:a)(由 OTP 设备和/或客户机工作站)从服务器接收至少部分识别服务器的信息;b) 判定识别信息是否表示合法服务器;以及 c) 根据判定,决定(即,由 OTP 令牌和/或客户机工作站作出决定)执行从包括以下行为的组中选出的一个行为:i) 从 OTP 令牌发送表示内部生成会话 OTP 的数据(即,在 OTP 令牌内而非在客户机工作站内生成的会话 OTP,根据触发器和秘密用户密钥以及可选择地根据用户认证数据生成的会话 OTP);以及 ii) 制止发送。仅在决定是肯定决定(即,决定发送表示会话 OTP 的数据)时,从 OTP 令牌发送表示会话 OTP 的数据。

[0025] 根据某些实施例,发送包括,仅在决定表示肯定时,执行表示数据通过接口从 OTP

令牌到客户机工作站的设备间数据传输。

[0026] 根据某些实施例,发送包括,仅在决定表示肯定时,在 OTP 令牌的显示屏幕上显示出表示会话 OTP 的数据。

[0027] 根据某些实施例,表示会话 OTP 的数据是从用户认证数据得出的多因素认证数据。

[0028] 或者,表示会话 OTP 的数据与用户认证数据无关。

[0029] 根据某些实施例,方法还包括 :d) 如果决定是否定决定,则 OTP 令牌制止生成会话 OTP。

[0030] 根据某些实施例,方法还包括 :d) 如果决定是否定决定 :i) 在 OTP 令牌内内部生成会话 OTP ;以及 ii) 保持其中会话 OTP 保留在 OTP 令牌内的状态。

[0031] 根据某些实施例,方法还包括步骤 :d) 在接收之前,使用在 OTP 令牌内的嵌入式安全浏览器,打开在 OTP 令牌与服务器之间的安全会话。

[0032] 根据某些实施例,方法还包括步骤 :e) 在打开会话之后,将会话的客户机端从 OTP 令牌转移到客户机工作站,其中,在客户机工作站处执行接收和判定的其中至少一个。

[0033] 根据某些实施例,在 OTP 令牌从服务器接收识别信息时,会话的客户机终点和 / 或客户机端保留在嵌入式浏览器处 (即,将客户机工作站用作为“数据管道”,并从 OTP 设备内对通信进行管理)。

[0034] 根据某些实施例,由 OTP 令牌 (即,嵌入在 OTP 令牌内的浏览器) 通过服务器与 OTP 令牌之间的通信链路执行接收,即,OTP 令牌是会话的客户端,将客户机工作站仅用作为“数据管道”,并从 OTP 设备内对通信进行管理。

[0035] 根据某些实施例,在 OTP 令牌内执行判定。在某些实施例中,这可提供由于在 OTP 令牌内环境的抗篡改和 / 或自由篡改 (tamper-free) 特性而导致的额外安全措施。

[0036] 根据某些实施例,判定包括执行对驻留在 OTP 令牌内的数据库的查询 (自客户机工作站和 / 或自驻留在 OTP 令牌内的数据库客户机代码)。

[0037] 根据某些实施例,数据库为不变数据库。从而,根据一个示例,金融机构或金融机构组对 OTP 设备发布嵌入在该设备内的合法服务器“白列表”(即,与金融机构或机构组有关)。该白列表将是不变的,尽管不提供“通用解决方案”可能对发布金融机构 (和 / 或其客户机) 是合适的。对服务器的合法性进行认证的数据库的不变特性还可提供对附加的安全措施。

[0038] 根据某些实施例,数据库包括以下其中之一 :可接受 URL 的预定列表、可接受 IP 地址的预定列表和可接受证书字段值的预定列表。

[0039] 根据某些实施例,判定的执行是根据以下内容的其中至少一个 :接收的一个通信的协议数据 (例如,通过从表示服务器 IP 地址的发送包数据中提取)、在接收到的通信中发送的证书数据、URL 数据和 IP 地址数据。

[0040] 根据某些实施例,判定根据自服务器接收的证书的仅某些属性执行。从而,在一个示例中,证书有许多字段,其中某些但非所有证书字段用于确定 / 判定服务器的合法性。在许多示例性情形中,这可能是有益的,例如,其中希望定义服务器或服务器参数的“家族 (family)”(从而,仅部分定义服务器的标识符)。例如,发行方 (例如,银行或安全服务器的其他运营者) 可与不止一个证书提供商一起工作,从而,可能不需要该字段用于对证书

进行验证。例如，银行可在特定组中部署多个服务器，可能不会使用表明组中哪个服务器正发出会话 OTP 请求的证书字段数据，而可能使用其他字段。这给发行方（例如，银行）提供了无需在对 OTP 设备发布（例如，包括不变数据库）时完全设定服务器标识参数的灵活性。
[0041] 应该注意，尽管“不变数据库”在某些情形中提供安全性，但并不对本发明构成限制。

[0042] 在示例性实施例中，将发送数据进行加密和 / 或散列化处理。

[0043] 下面，首次披露 OTP 令牌与通过广域网与服务器进行通信的客户机工作站一起使用。本发明所披露的 OTP 设备包括：(a) 设备端口（即，一个或多个设备端口 - 面向“联系”，如 USB 端口和 / 或无线端口），用于从客户机工作站接收包括至少部分识别服务器的信息的数据；b) 服务器合法性引擎，用于判定信息是否表示合法服务器；c) OTP 发生器，用于生成会话 OTP；以及 d) OTP 发送决定引擎，用于根据判定的结果，决定执行从包括以下行为的组中选出的一个行为：i) 从 OTP 令牌发送表示会话 OTP 的数据；以及 ii) 制止发送。

[0044] 在示例性实施例中，设备还包括 c) 用于发送表示会话 OTP 的数据的 OTP 发送器，其中，OTP 发送器是

[0045] 根据某些实施例，如果判定是肯定的，OTP 发送器用于通过数据端口将表示会话 OTP 的数据发送到客户机工作站。

[0046] 根据某些实施例，OTP 令牌还包括 :d) 数据显示器，其中，仅在引擎判定识别信息表示合法服务器时，OTP 发送器用于向数据显示器发送表示会话 OTP 的数据。

[0047] 根据某些实施例，OTP 令牌还包括 :d) 嵌入在 OTP 令牌内的嵌入式安全浏览器，嵌入式浏览器用于打开在 OTP 令牌与服务器之间的安全会话。

[0048] 根据某些实施例，嵌入式安全浏览器用于在安全会话期间接收识别信息。

[0049] 根据某些实施例，服务器合法引擎包括 :d) 预定数据的数据库，其中，服务器合法引擎用于根据数据库内容执行判定。

[0050] 根据某些实施例，数据库为不变数据库。这或许是有益的，例如，其中，分发用于与预定服务器组一起操作的特定 OTP 设备（而非通用 OTP 设备），期望的是提供附加安全性，以便欺骗者和 / 或罪犯和 / 或骇客不能够修改数据库以添加服务器。

[0051] 根据某些实施例，数据库包括以下之一：可接受 URL 的预定列表、可接受 IP 地址的预定列表和可接受证书字段值的预定列表。

[0052] 根据某些实施例，服务器合法性引擎用于根据来自服务器的通信协议数据和在通信中由服务器发送的证书数据的其中至少一个执行判定。

[0053] 根据某些实施例，服务器合法性引擎用于根据自服务器接收的证书的仅其中某些属性执行判定。

[0054] 根据某些实施例，OTP 发生器用于根据用户认证数据生成会话 OTP，从而生成作为多因素认证数据的会话 OTP。

[0055] 根据某些实施例，设备还包括 :e) 用户识别模块，用于对用户认证数据进行认证。

[0056] 根据某些实施例，OTP 发送决定引擎用于根据对用户认证数据进行认证的结果实现决定。

[0057] 下面，首次披露用于处理会话 OTP 数据传输的系统。本发明所披露的系统包括：a) 客户机工作站，通过广域网与服务器进行通信，b) OTP 令牌，与客户机工作站相接口，OTP

令牌包括 :i) 设备端口, 用于与客户机工作站相接口 ; 以及 ii) OTP 发生器, 用于生成会话 OTP ; 以及其中, OTP 令牌和客户机工作站的其中至少一个用于接收识别服务器的识别信息, 该系统还包括 :c) 服务器合法性引擎, 用于判定信息是否表示合法服务器, 服务器合法性引擎至少部分驻留在 OTP 令牌和客户机工作站的至少其中之一中 ; d) OTP 传输决定引擎, 用于根据判定结果决定执行从包括以下行为的组中选出的一个行为 :i) 从 OTP 令牌发送表示会话 OTP 的数据 ; 以及 ii) 制止发送, 其中, OTP 发送决定引擎至少部分驻留在 OTP 令牌和客户机工作站的其中至少一个中。

[0058] 下面, 首次披露一种计算机可读存储介质, 在所述计算机可读存储介质中嵌入有计算机可读代码, 所述计算机可读代码包括用于执行以下步骤的指令 :a) 由经由广域网与服务器进行通信的客户机工作站和与服务器相接口的 OTP 令牌的其中至少一个, 接收至少部分识别服务器的信息 ; b) 判定识别信息是否表示合法服务器 ; 以及 c) 根据判定, 决定执行从包括以下行为的组中选出的一个行为 :i) 从 OTP 令牌发送表示内部生成会话 OTP 的数据 ; 以及 ii) 制止发送。

[0059] 通过后面的详细描述和示例, 这些以及其他实施例将显而易见。

附图说明

[0060] 图 1A-1B(现有技术) 提供了示例性系统的各框图, 其中, 该系统包括 : 请求会话 OTP 的服务器 170、通过因特网 20 与服务器 170 进行通信的计算机 / 客户机工作站 160, 以及与客户机工作站 160 一起使用的 OTP 设备 / 令牌 110。

[0061] 图 2 提供了用于通过 OTP 设备 110 生成的 OTP 启动客户机服务器会话的现有技术程序的流程图。

[0062] 图 3A-3B 提供了根据本发明的某些实施例的示例性系统 300 的各框图, 其中, 系统 300 包括 : 请求会话 OTP 的服务器 170、通过因特网 20 与服务器 170 进行通信的计算机 / 客户机工作站 360, 以及与客户机工作站 160 一起使用的 OTP 设备 / 令牌 310。

[0063] 图 3C 提供了示例性 OTP 认证设备 / 令牌 310 的框图。

[0064] 图 3D 提供了示例性服务器合法性引擎 340 的框图。

[0065] 图 3E 提供了示例性客户机工作站 / 计算机 360 的框图。

[0066] 图 4A 提供了根据本发明的某些实施例的用于通过 OTP 设备 110 生成的 OTP 启动客户机服务器会话的程序的流程图。

[0067] 图 4B 提供了处理来自 OTP 令牌的会话 OTP 发送的程序的流程图。

[0068] 尽管在此以数个实施例以及示意性附图的示例方式描述了本发明, 但本领域技术人员应该理解, 本发明并不局限于所述实施例或附图。应该理解, 附图和详细描述并不意在将本发明局限在所披露的特定形式, 而是相反, 本发明涵盖属于本发明精神和范围的所有修改例、等效例和变型例。如本申请中所使用的, 词语 “可以或可能 (may) ” 用于允许含义 (即, 表示 “有这样的可能 ”), 而并非具有强制性含义 (即, 表示 “必须 ”) 。

具体实施方式

[0069] 现在将以具体、示例性实施例描述本发明。应该理解, 本发明不限于所披露的示例性实施例。还应该理解, 目前所披露的用于处理会话数据的装置、设备和计算机可读代码的

每一个特征，并非都是实现所附权利要求任一具体项要求保护的发明必不可少的。描述设备的多个元件和特征是为了使本发明完全能够得以实现。还应该理解的是，在本说明中，在表示或者描述处理或方法之处，方法的步骤可以按照任何顺序执行或者同时执行，除非从上下文中显然可以看出一个步骤依赖于首先执行的另一步骤。除非从上下文中明显看出是相反的，否则客户机工作站、服务器或 OTP 令牌的任何披露部件可以通过硬件和 / 或软件和 / 或固件的任何组合来实现。

[0070] 参照图 3A-3E，描述了根据本发明优选实施例构成的系统 300。注意，系统 300 的某些模块和功能与图 1A-1B 的系统 100 的相应模块和功能相同或者相似。因而，图 3A-3D 的 OTP 认证设备 310 包括触发器 120 和 OTP 发生器 330，OTP 发生器 330 根据用户密钥库 132 的内容和触发器 120 的输出生成会话 OTP 数据。可选择地，还根据用户认证数据（例如，由用户标识符 134 进行处理）生成会话 OTP 数据。或者，会话 OTP 数据不依赖于用户认证数据，仅依赖于触发器 120 的输出和用户密钥库 132（一般而言，其中驻留有用户密钥数据的抗篡改或防篡改非易失性存储器）的内容。

[0071] OTP 会话数据可通过 OTP 发送器 342，经由接口 140 从 OTP 令牌设备 310 发送给作为显示器接口 140A 的一部分的显示屏，或者经由联系接口 140B 或无线设备接口 140C 发送给客户机工作站 360。

[0072] 并非在每次接收到对于 OTP 会话的请求时都无条件地从 OTP 令牌 310 传输 OTP 会话数据。实际上，根据 OTP 发送决定引擎 344 作出的“进行 / 不进行”决定，执行发送。在图 3A-3E 中，将某些部件（例如，OTP 发送决定引擎 344，用户标识符 134，浏览器 350 和服务器合法性引擎 340）表述为驻留在 OTP 令牌 310 内，不过本发明人还设想了在实施例中将这些部件中的一个或多个部分或全部置于 OTP 令牌的外部。

[0073] 发送决定引擎 344 可根据一个或多个因素执行上面所述的“进行 / 不进行”发送决定。一般而言，只有当服务器合法性引擎 340 确定与对于会话 OTP 的请求相关联的服务器标识符表示请求服务器 170 可能合法（并且不太可能是欺骗者或网络钓鱼者或“中间人”）时，OTP 令牌 310 才从安全的 OTP 令牌发送会话 OTP（给安全性较差的客户机工作站 360 或显示屏）。

[0074] 因此，参照图 3D，注意在示例性实施例中，服务器合法性引擎 340 包括数据库 362 和逻辑 360，例如，用于“查询”数据库（其可以简单地为查询表）。数据库包括表示“可信赖服务器”的预定数据。因此，服务器合法性引擎 340 用于验证当前会话 OTP 将由合法服务器作出，而不是如典型网络钓鱼中那样由假装成合法服务器的伪装服务器作出。可信赖服务器的数据库 360 可由用于每个可信赖服务器的记录构成，所述记录包括例如 IP（因特网协议）地址，URL（统一资源定位器）或证书数据（例如，如发明内容中所讨论的‘局部’证书数据）中的至少一个。

[0075] 在示例性实施例中，由 OTP 认证设备 310 的提供方（例如，为其客户提供这种设备以便与其进行安全会话的银行），或者通过用户作出的表项，或者通过自可信赖方接收可信赖服务器的文件填充数据库。在有些实施例中，数据库是不变的，并且在 OTP 认证令牌 310 “发货（shipping）”之前配置该数据库。

[0076] 参照图 3E，注意计算机 360（即客户机“工作站”）可具有与图 1A-1B 所示计算机 160 相同的认证设备接口 164，并且客户机应用 368 可以类似于图 1A-1B 所示客户机应用

168, 其具有询问服务器 170 检索其身份 (使用本领域技术人员公知的标准识别服务, 以识别所连接方的 IP, URL 和 / 或证书), 并将该服务器身份作为输入发送给 OTP 认证设备 310 的服务器 ID 检验器 334 的附加功能。本发明无需对计算机 360 或服务器 170 进行任何改变。注意, 计算机 360 (“客户机工作站”) 可以是用于与服务器 170 进行通信的任何计算机化用户设备。例如, 计算机 360 可以是个人台式、膝上或掌上型计算机, 蜂窝电话或双向寻呼机。OTP 认证设备 310 是这样的自治、便携式设备 (电子“令牌”): 可与不止一个计算机 360 连接的, 并且可具有多种形式因素, 如, 具有显示器的密钥表链 (keyfob)、USB 令牌、具有令牌功能的 USB 盘、可移动卡 (例如, 安全数字卡、多媒体卡、存储棒, 或 SIM 卡) 等, 或者, 如果与诸如个人计算机之类的另一计算机结合使用的话, 它可为蜂窝电话。

[0077] 还应注意, 服务器 170 无需“知晓 (aware)”本发明。这可提供本发明所披露的、用于降低网络钓鱼攻击现有服务器 170 的风险的方法和装置之间的兼容性。

[0078] 图 4A 描述了根据本发明某些实施例的如图 3A-3E 所示系统 300 的操作。大部分步骤与图 2 相同, 其中添加了步骤 401, 411, 421 和 431。从而, 在步骤 201 中启动客户机应用 368 之后, 则在步骤 401 中, 在客户机应用 368 控制下, 由计算机 360 对服务器 170 的 ID 进行检索, 且其被发送到 OTP 认证设备 310, 以便在步骤 411 中由服务器 ID 检查器 334 与形成服务器 ID 检查器 334 的一部分的合法服务器的数据库进行验证。如果服务器得到肯定验证, 则步骤 421 将流程转到如图 2 所示步骤 211, 221, 231, 241, 251, 261, 271 和 281, 在此, 由 OTP 认证设备 310 的 OTP 发生器 330 生成 OTP, 并由服务器 170 进行验证, 以此作为运行客户机服务器会话的预条件。如果在步骤 411 中得到否定验证, 则步骤 421 将流程转到在步骤 431 处的拒绝, 其中, OTP 认证设备 310 的 OTP 发生器 330 不会生成有效的 OTP, 并且, 程序将由客户机应用 368 或服务器应用 182 终止。

[0079] 应该注意, 由于图 3 和 4 所示配置需要与 OTP 认证设备 310 进行双向通信, 从而, 最好使用 USB 140B 或 IR/RF 接口 140C。然而, 如果 OTP 接口 140 使用在 OTP 认证设备 310 与计算机 360 之间没有通信链路的显示器 140A, 则服务器 ID 的表项将使人工输入设备, 如键盘 (还可用于用户标识符 134 的 PIN 表项) 在 OTP 认证设备 310 中是强制的。从而, 在此情形中, 将通过计算机 360 的显示器上的消息向用户提示将服务器 ID (如在消息内显示的) 键入到 OTP 认证设备 310 中, 然后将显示器 140A 上显示的 OTP 键入到计算机 360 中。

[0080] 图 4B 描述在如图 4A 所示示例性认证程序的子程序。从而, 应该注意, 程序 4B 可在不同于如图 4B 所示的认证程序的情形中实现。

[0081] 参看图 4B, 首先, 接收 385 (在 OTP 设备 110 和 / 或客户机工作站 160) 至少部分地识别服务器的信息。然后, 判定 387 (例如, 通过服务器合法性引擎 340) 识别信息是否表示合法服务器 (即, 如果服务器 170 更有可能合法 / 真实 / 可信)。根据该判定结果, (例如, 通过 OTP 发送决定引擎 344) 作出“进行 / 不进行”发送决定 389 (用于将 OTP 会话数据发送到安全性较差的客户机工作站 - 没有必要作出关于将 OTP 会话数据通过广域网发送到服务器 170 的决定)。在肯定决定 (即, 发送) 的情形 391 中, “发送”(即, 通过设备接口或显示屏) 表示 OTP 会话的数据。否则, 制止 431 将 OTP 会话数据发送到在 OTP 令牌 310 外部的安全性较差环境。

[0082] 在本发明的描述和权利要求中, 动词“包括 (comprise 或 include)”和“具有 (have)”以及其变化的每一个均用于表示这些动词所涉及宾语或多个宾语没有必要是动词

主语的元件、组件、部件或部分的完全列表。

[0083] 在此引述的全部参考文献全部引作参考。关于参考文献的引述并非视为承认参考文献为现有技术。

[0084] 冠词“一 (a 或 an)”在此用于指一个或多个 (即, 至少一个) 名词所修饰语法对象。例如, “一元件 (an element)”表示一个或多个元件。

[0085] 术语“包括”在此用于表示语句“包括但不限于”, 并可与之互换使用。

[0086] 术语“或”在此用于表示术语“和 / 或”, 并可与之互换使用, 除非在某些情形明确表示其他含义。

[0087] 术语“例如 (或诸如)”在此用于表示语句“例如, 但不限于”, 并可与之互换使用。

[0088] 使用通过举例给出的对本发明实施例的详细描述, 描述了本发明, 这并非意在限制本发明的范围。所描述的实施例包括不同的特征, 在本发明的所有实施例中并非需要所有这些特征。本发明的有些实施例仅利用了某些特征或特征的可能组合。本领域技术人员可想到所述本发明实施例以及包括在所述实施例中表述的特征的不同组合的本发明实施例的变型。

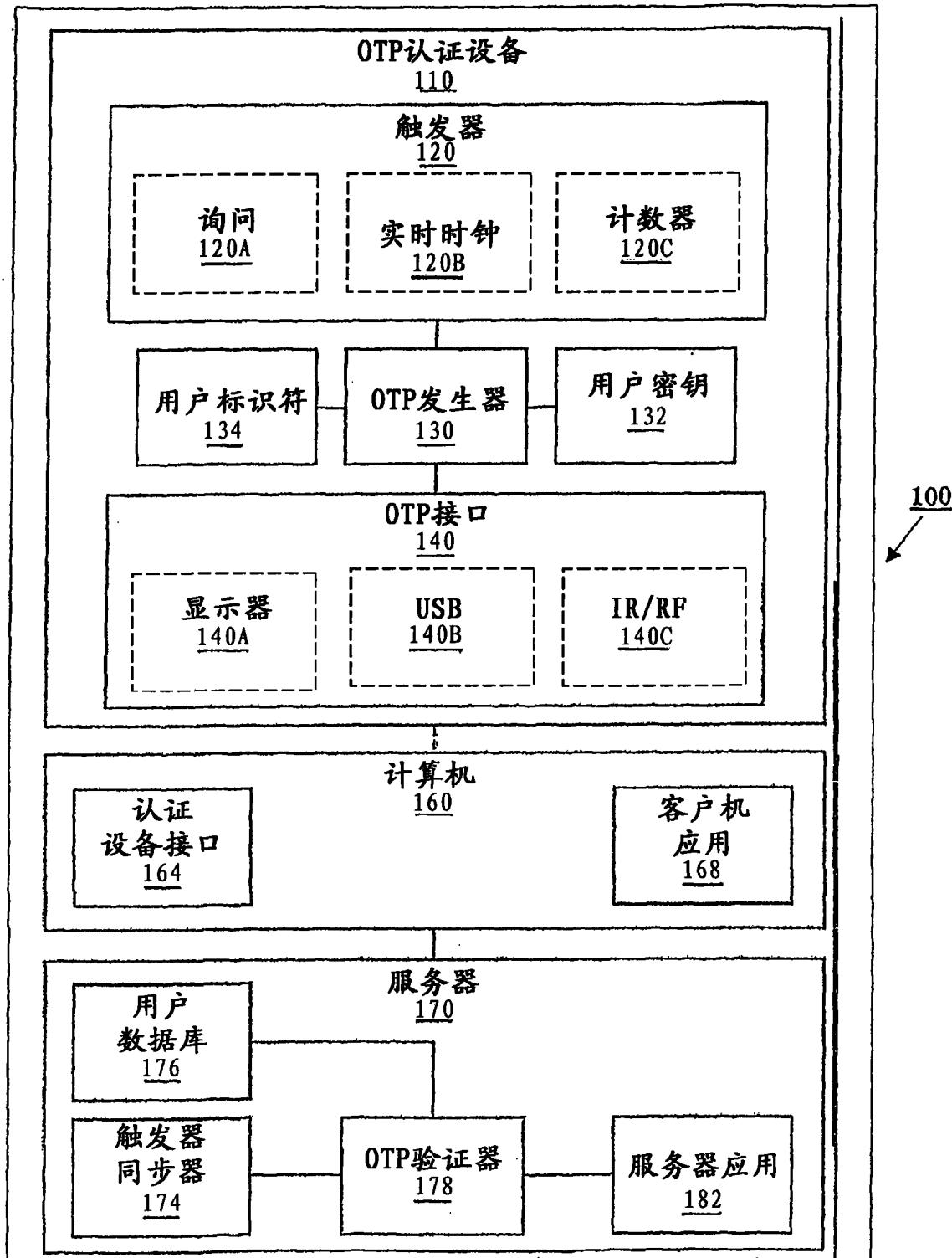


图1A (现有技术)

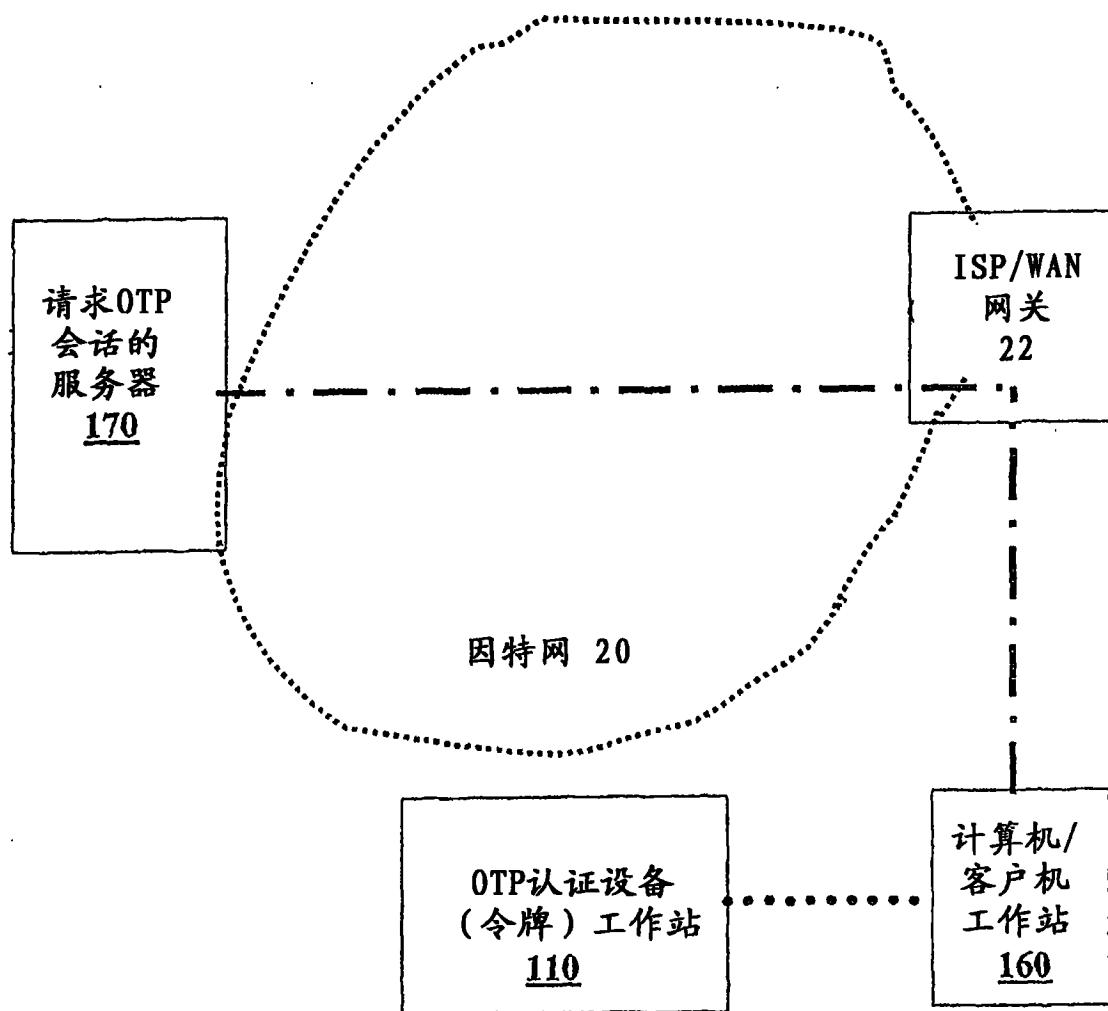


图1B (现有技术)

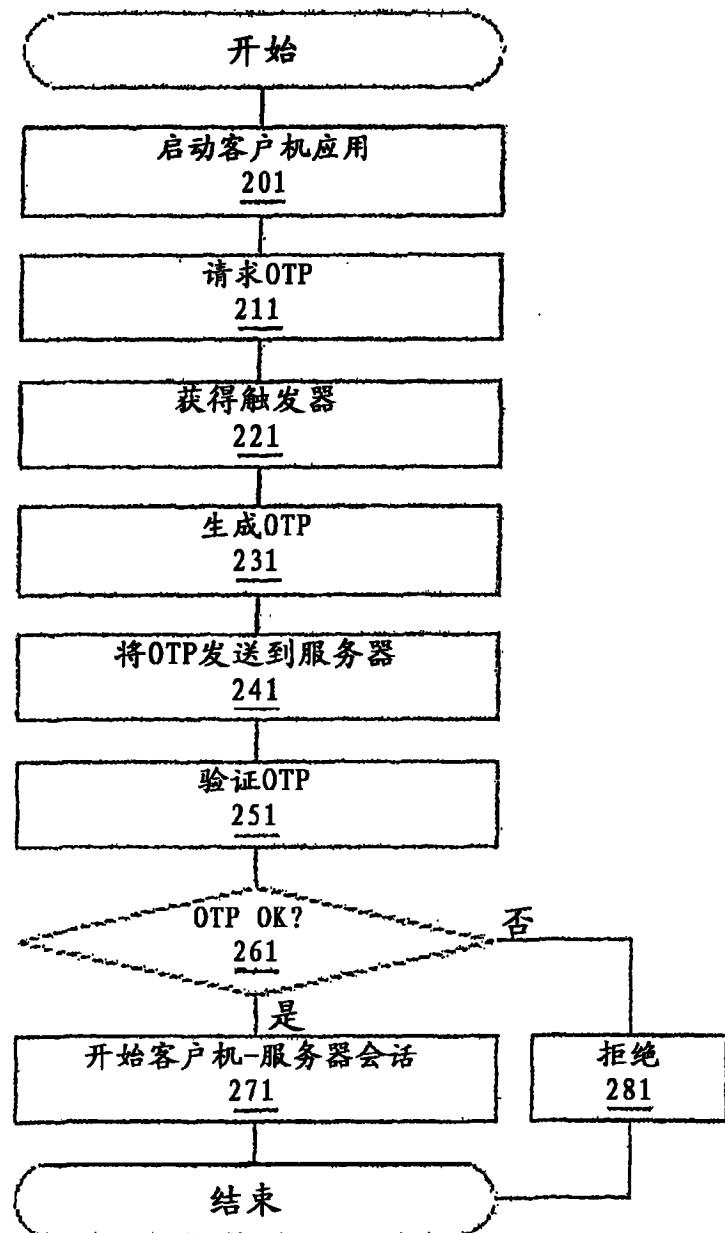


图2（现有技术）

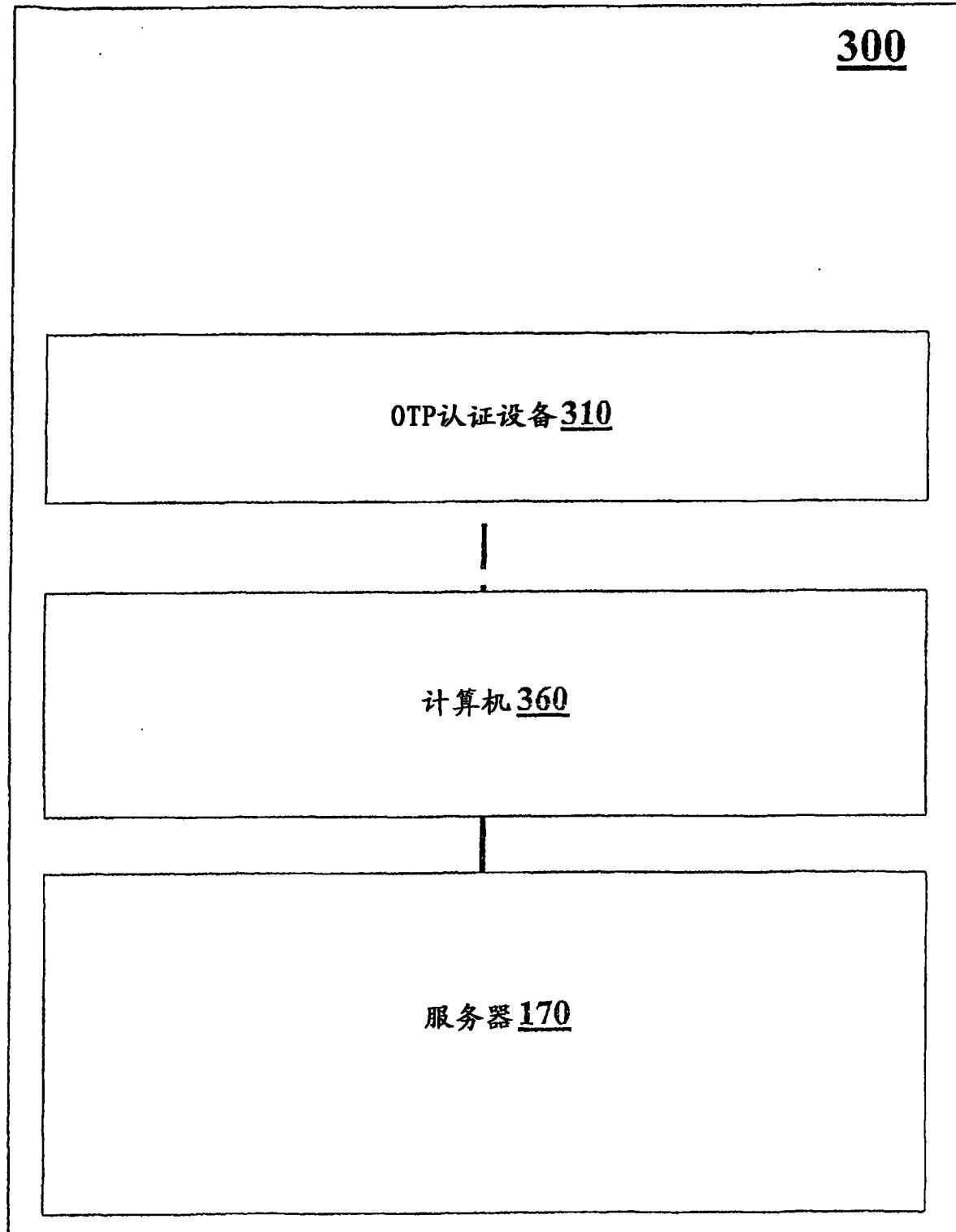


图 3A

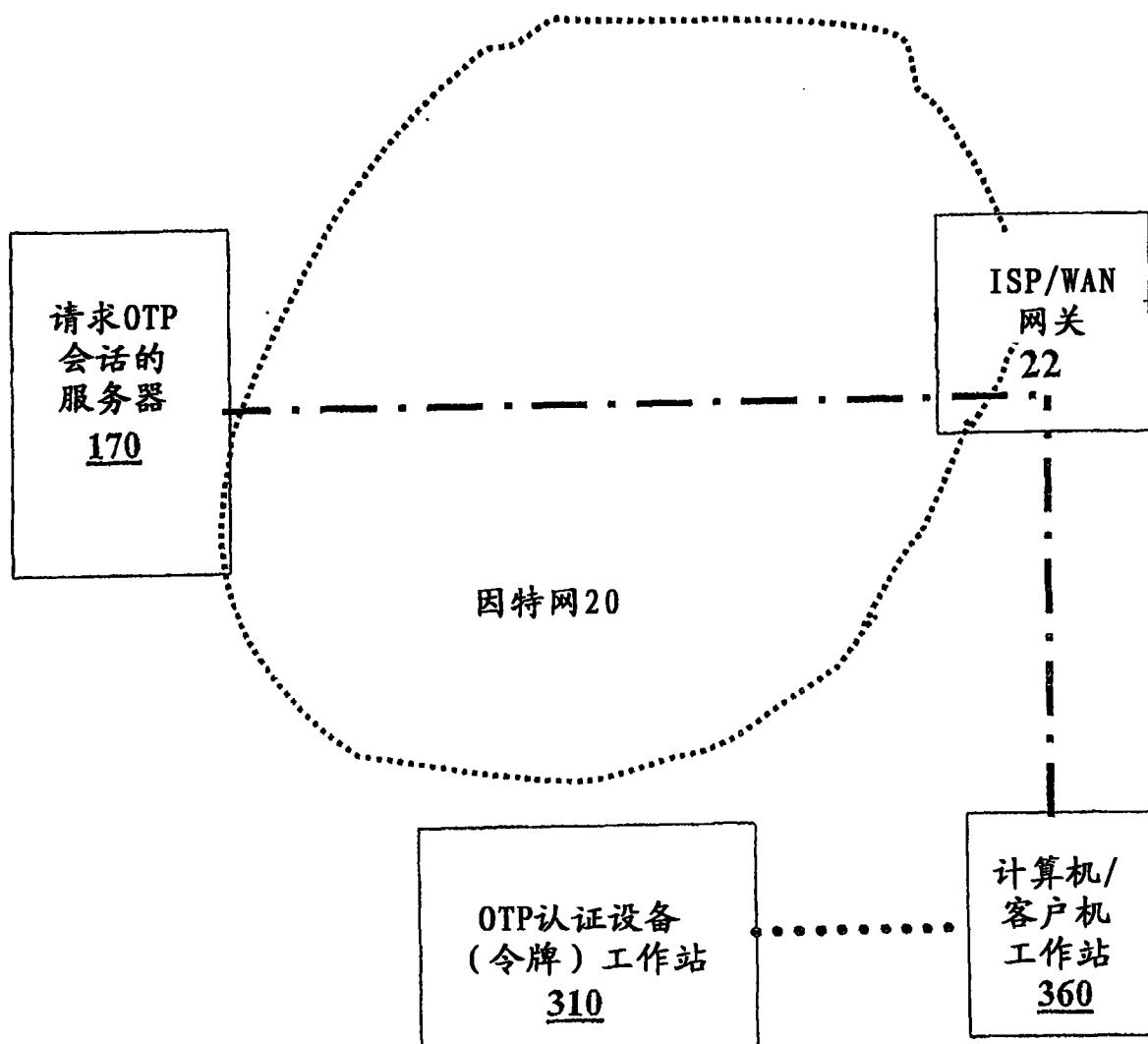


图 3B

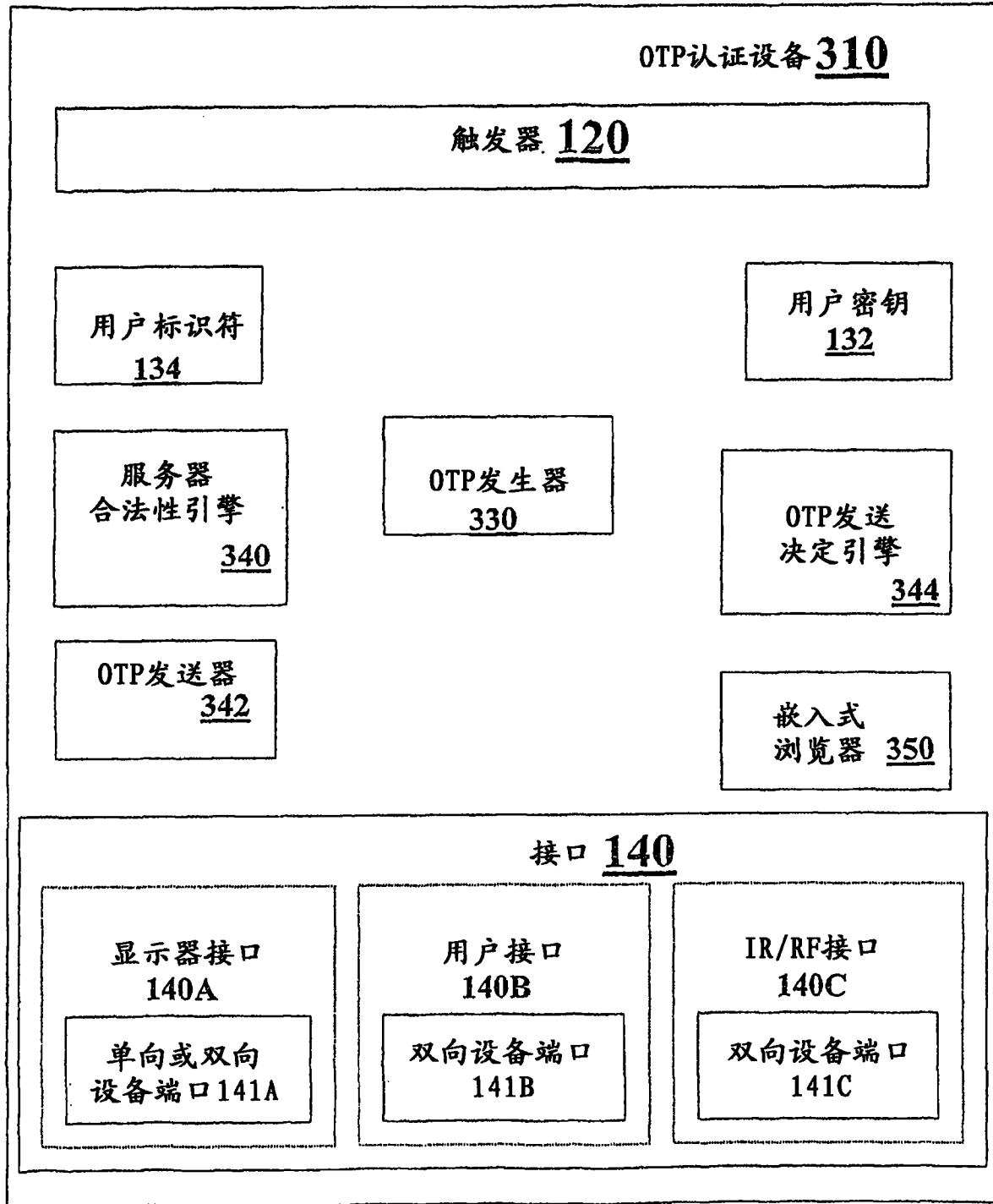


图 3C

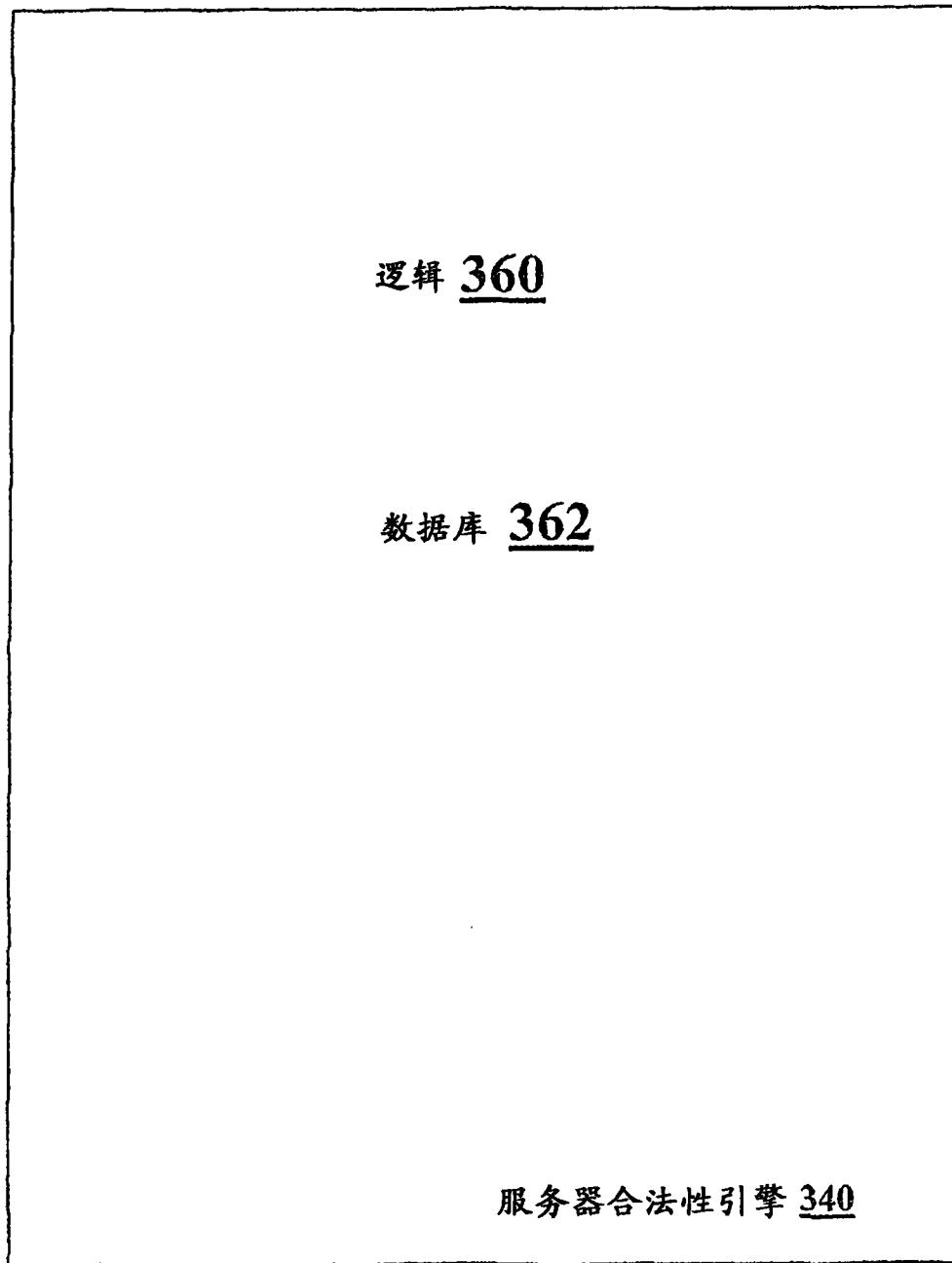


图 3D

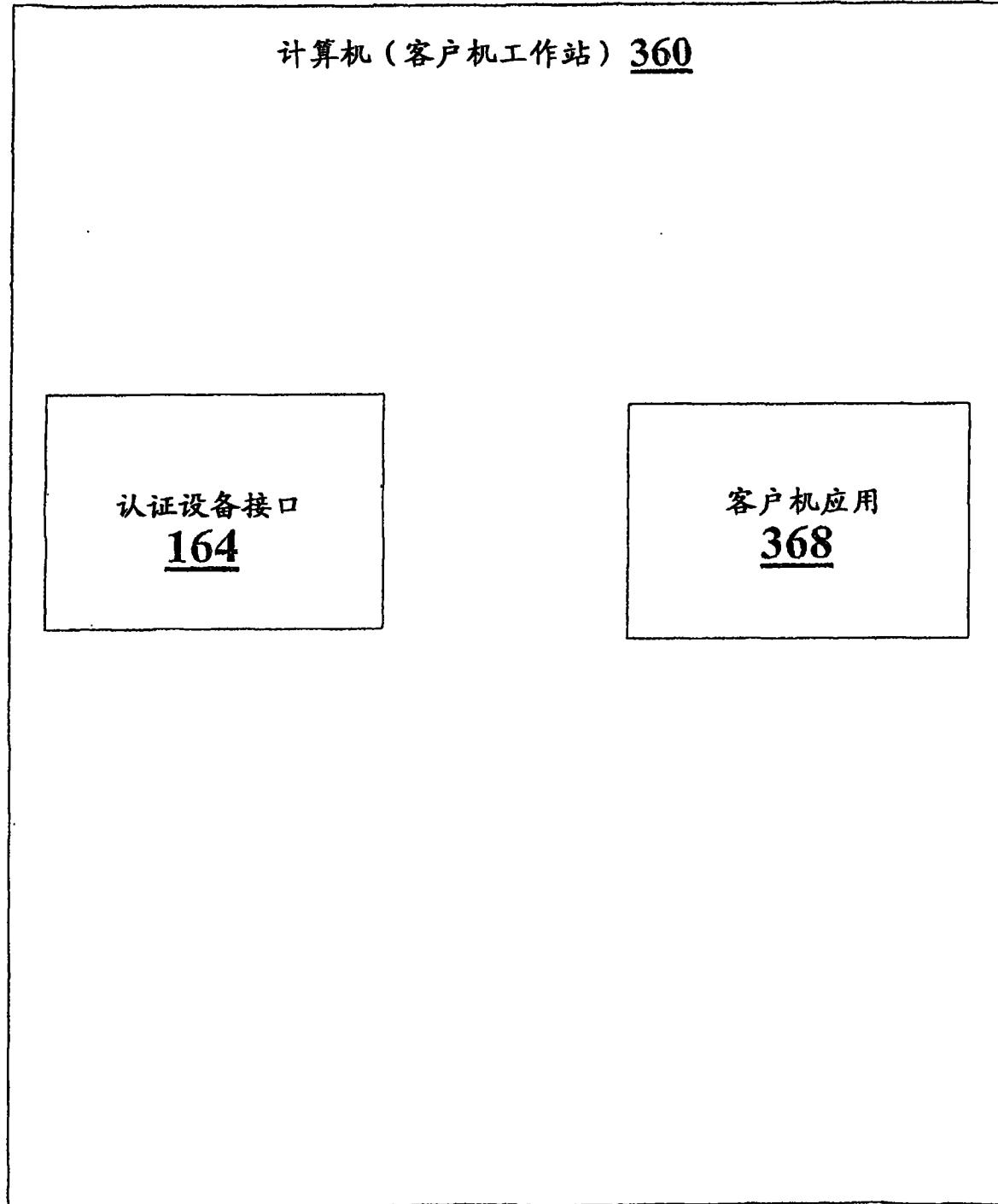


图 3E

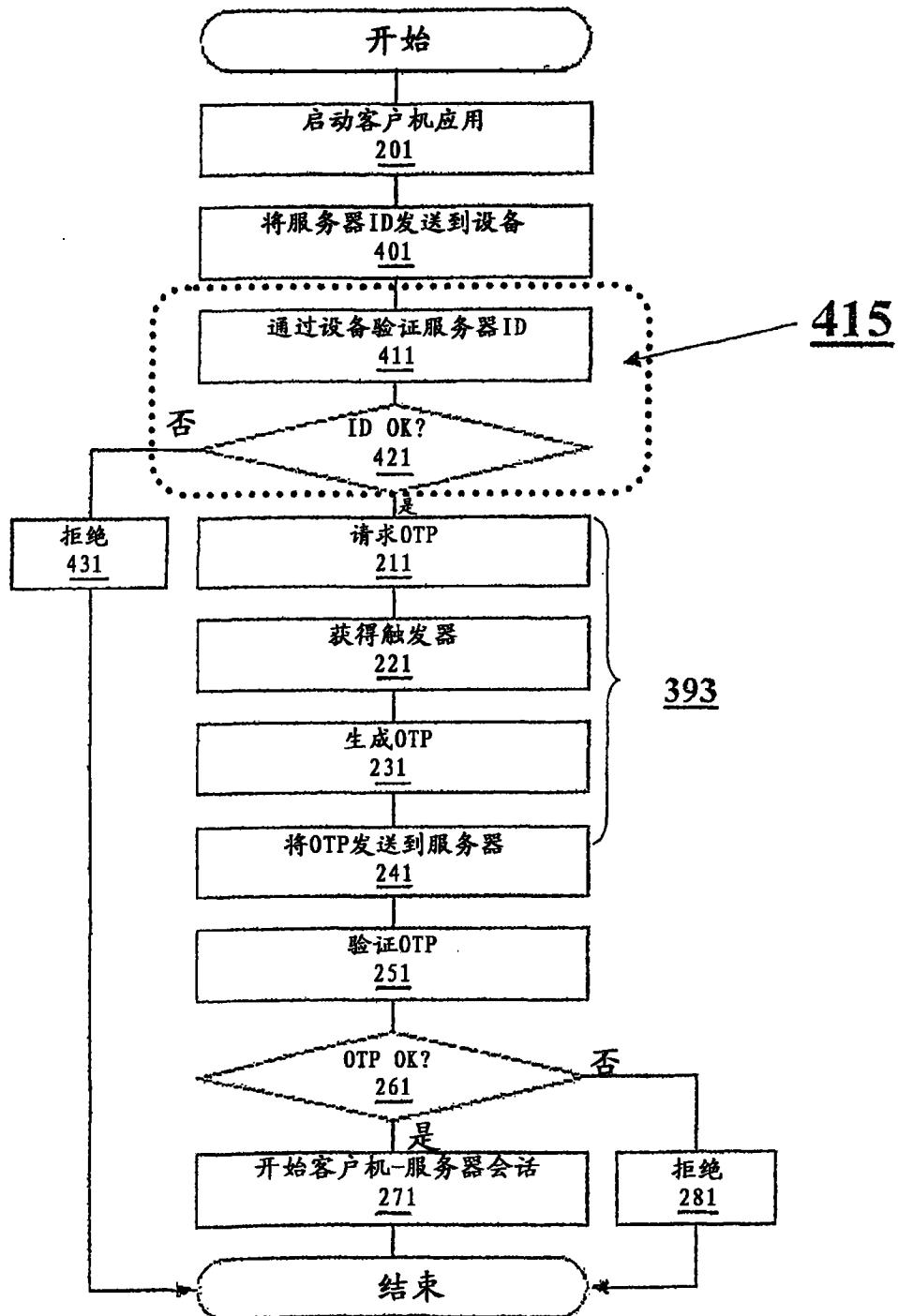


图 4A

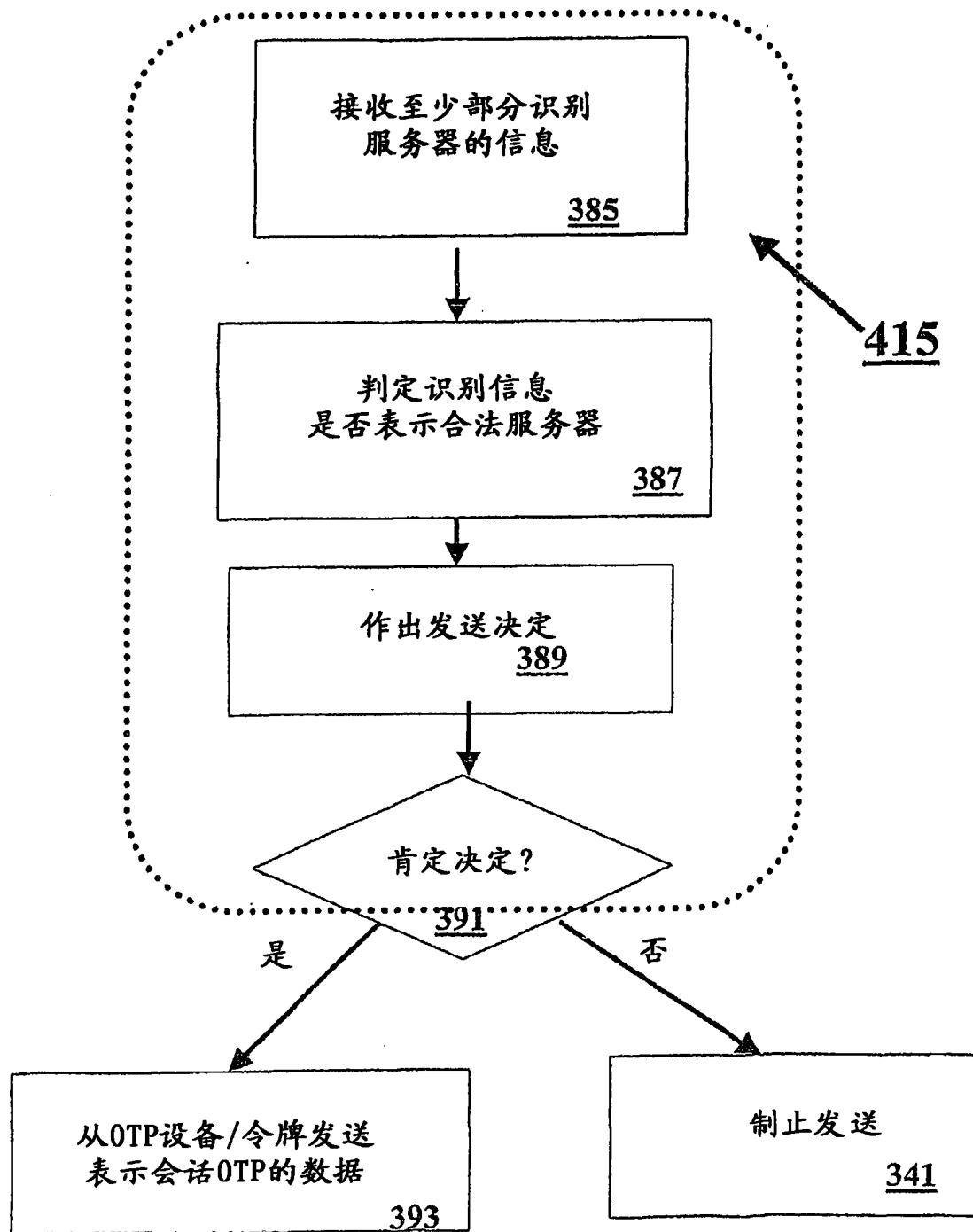


图 4B