



(12) 发明专利

(10) 授权公告号 CN 101371241 B

(45) 授权公告日 2012.09.12

(21) 申请号 200780002623.0

(22) 申请日 2007.01.19

(30) 优先权数据

60/760,475 2006.01.20 US

(85) PCT申请进入国家阶段日

2008.07.18

(86) PCT申请的申请数据

PCT/US2007/060744 2007.01.19

(87) PCT申请的公布数据

W02007/084973 EN 2007.07.26

(73) 专利权人 美国唯美安视国际有限公司

地址 美国加利福尼亚

(72) 发明人 R·T·库拉考维斯基 D·S·怀特

(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 董莘

(51) Int. Cl.

G06F 15/16(2006.01)

(56) 对比文件

US 2006/0010199 A, 2006.01.12, 说明书第0015段, 第0017段, 第0035段, 第0064-0066段, 第0075段, 第0075段、权利要求1.

US 2003/0163693 A1, 2003.08.28, 说明书第0011-0013段, 第0029-0033段, 第0051段、附图1-2.

CN 1308275 A, 2001.08.15, 全文.
全文.

审查员 邹予婷

CN 101371241 B

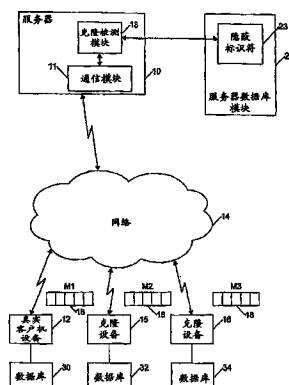
权利要求书 3 页 说明书 27 页 附图 11 页

(54) 发明名称

网络安全系统和方法

(57) 摘要

在用于与客户机设备进行网络通信的安全系统中,每一个客户机设备都具有用于通过网络与至少一个服务器进行通信的通信模块,用于存储客户机设备上的一个或多个操作事件的一个或多个隐蔽数据值的数据存储模块,以及基于存储的隐蔽数据值创建至少一个隐蔽标识符的隐蔽标识符生成模块。在发往服务器的,或以别的方式发送到服务提供商的一个或多个网络消息中提供了隐蔽标识符,并可以响应通过网络接收到的特定请求,或例行地在通常涉及网络通信的一个或多个消息中提供隐蔽标识符。服务器比较从具有相同客户机标识符的客户机设备接收到的隐蔽标识符,以便检测可能的克隆。



1. 一种用于检测通过网络进行通信的克隆的客户机设备的方法，包括：
在服务器上存储在服务器上注册凭证的客户机设备的至少一个隐蔽标识符；
在所述服务器上从客户机设备接收消息，所述消息包含从所述客户机设备的至少一个操作事件中得到的隐蔽标识符；
确定在所述消息中接收到的隐蔽标识符是否匹配在所述服务器上存储相同凭证的所述客户机设备的隐蔽标识符；以及
如果所述消息中的所述隐蔽标识符的至少一部分不匹配存储在所述服务器中的所述客户机设备的隐蔽标识符，则报告检测到真正客户机设备的克隆。
2. 根据权利要求 1 所述的方法，其中所述隐蔽标识符包括在客户机设备中由操作事件生成的隐蔽数据值，如果从客户机设备接收到的隐蔽标识符中的所述隐蔽数据值不匹配存储在所述服务器中的隐蔽标识符中的任何隐蔽数据值，则报告检测到真正客户机设备的克隆。
3. 根据权利要求 1 所述的方法，其中所述隐蔽标识符包括基于由客户机设备中的不同操作事件生成的隐蔽数据值的代码。
4. 根据权利要求 1 所述的方法，其中所述隐蔽标识符至少部分地基于由所述服务器向所述客户机设备所提供的至少一个令牌。
5. 根据权利要求 1 所述的方法，其中所述隐蔽标识符基于由所述客户机设备生成的隐蔽数据值。
6. 根据权利要求 1 所述的方法，其中所述隐蔽标识符基于由所述服务器生成的、并由所述服务器在消息中向所述客户机设备所提供的隐蔽数据。
7. 根据权利要求 1 所述的方法，其中所述隐蔽标识符基于由所述客户机设备和所述服务器生成的隐蔽数据值。
8. 根据权利要求 1 所述的方法，进一步包括基于预定的事件触发器，在客户机设备上定期更新所述隐蔽标识符，并在消息中向所述服务器提供所更新的隐蔽标识符。
9. 根据权利要求 8 所述的方法，其中至少一个事件触发器包括在客户机设备上安装更新的固件。
10. 根据权利要求 8 所述的方法，其中至少一个事件触发器包括从所述服务器接收到预定数量的特定类型的消息。
11. 根据权利要求 8 所述的方法，其中至少一个事件触发器包括从所述客户机设备发送预定数量的特定类型的消息。
12. 根据权利要求 8 所述的方法，其中至少一个事件触发器包括在所述客户机设备中的预定数量的信道变换。
13. 根据权利要求 2 所述的方法，其中在所述服务器上存储至少一个隐蔽标识符的步骤包括：
在从客户机设备接收到预定的消息时，在所述服务器上存储第一隐蔽数据值，当从具有相同凭证的客户机设备接收到随后的预定消息时，存储更新的第二隐蔽数据值，
确定在来自客户机设备的随后消息中接收到的隐蔽标识符是否匹配以前存储的隐蔽标识符的步骤包括：
将所述消息中的隐蔽数据值与存储在所述服务器中的所述第一和第二隐蔽数据值进

行比较,其中如果所述随后消息中的隐蔽数据值不匹配所述第一和第二隐蔽数据值中的至少一个隐蔽数据值,则报告检测到使用相同凭证的克隆客户机设备。

14. 根据权利要求 13 所述的方法,其中所述隐蔽数据值基于发送所述预定消息的时间。

15. 根据权利要求 13 所述的方法,其中存储在所述服务器中的所述隐蔽数据值基于在来自至少一个客户机设备的消息中接收到的隐蔽数据值。

16. 根据权利要求 2 所述的方法,进一步包括:

基于客户机设备中的不同操作事件,定期将至少一个隐蔽数据值改变为不同隐蔽数据值。

17. 根据权利要求 1 所述的方法,其中所述隐蔽标识符至少部分地基于由所述服务器向所述客户机设备所提供的至少一个加密密钥。

18. 根据权利要求 1 所述的方法,其中所述隐蔽标识符至少部分地基于由所述服务器向所述客户机设备所提供的至少一个加密密钥,

其中所述客户机将所述服务器提供的加密密钥用于所述客户机和所述服务器之间的加密通信。

19. 根据权利要求 1 所述的方法,进一步包括:

基于预定事件触发器,在客户机设备上定期添加附加的隐蔽标识符,其中所述附加的隐蔽标识符被添加到以前的隐蔽标识符中。

20. 根据权利要求 1 所述的方法,其中所述隐蔽标识符基于在所述客户机设备中发生的事件的时刻。

21. 一种用于检测网络上的克隆客户机设备的系统,包括:

具有通过网络与客户机设备进行通信的通信模块的服务器;

与所述服务器关联的数据存储模块,用于存储与向所述服务器注册服务的至少一个真正客户机设备关联的客户机标识符,以及从具有相同客户机标识符的客户机设备上的至少一个操作事件得到的且从所述具有相同客户机标识符的客户机设备接收到的至少一个隐蔽标识符;以及

与所述服务器和数据存储模块关联的克隆检测模块,用于将从客户机设备接收到的消息中的至少一个隐蔽标识符和与所述相同客户机标识符关联的存储的隐蔽标识符进行比较,如果所述隐蔽标识符不匹配,则创建克隆检测报告。

22. 根据权利要求 21 所述的系统,进一步包括:

通过所述网络与所述服务器进行通信的多个客户机设备。

23. 根据权利要求 22 所述的系统,其中所述客户机设备是智能卡。

24. 根据权利要求 22 所述的系统,其中至少一些客户机设备具有智能卡。

25. 根据权利要求 22 所述的系统,其中至少一些客户机设备是机顶盒。

26. 根据权利要求 22 所述的系统,其中至少一些客户机设备是移动通信设备。

27. 根据权利要求 22 所述的系统,其中至少一些客户机设备是个人计算机。

28. 根据权利要求 22 所述的系统,其中每一个客户机设备都具有隐蔽标识符生成模块,用于基于对应于所述客户机设备上的操作事件的至少一个隐蔽数据值,生成隐蔽标识符,用于存储隐蔽数据值的隐蔽数据存储模块,以及消息格式化模块,用于将所述隐蔽标识

符嵌入到通过所述网络发送到所述服务器的至少一个消息中。

29. 根据权利要求 28 所述的系统, 其中所述隐蔽标识符包括至少一个真实的隐蔽数据值。

30. 根据权利要求 28 所述的系统, 其中所述隐蔽标识符包括至少一个隐蔽数据值的转换后的版本。

31. 根据权利要求 28 所述的系统, 其中所述隐蔽标识符包括对应于所述客户机设备上的不同操作事件的多个隐蔽数据值。

32. 根据权利要求 28 所述的系统, 其中所述隐蔽标识符包括对应于所述客户机设备上的不同操作事件的多个隐蔽数据值的转换后的版本。

网络安全系统和方法

[0001] 相关申请

[0002] 本申请要求 2006 年 1 月 20 日申请的共同待审的美国临时专利申请 No. 60/760,475 的优先权，该专利申请的全部内容作为参考包含于此。

技术领域

[0003] 本发明涉及服务器和客户机设备之间的网络通信，具体地说，尤其涉及用于检测试图窃取服务而不支付费用或以别的方式模仿真正客户机设备的真正或正常地注册客户机设备的克隆的网络安全系统和方法。

背景技术

[0004] 在分布式计算环境中，盗版者通过创建具有与正当的客户机或合法用户相同的凭证的多个客户机来窃取服务，从而允许非付费的用户共享（窃取）付费合法用户的服务。由于凭证似乎是正当的，服务器向这样的克隆发送广播密钥或类似的东西，允许未经授权的用户查看广播，参与双向通信，或进行类似的操作。这样的克隆技术对网络提供商来说是严重的问题。盗版者还试图复制或克隆诸如经授权的个体作为信用卡或自动柜员机（ATM）卡，在移动电话中，作为高安全性标识和接入控制卡、公共交通卡，及其他用途的智能卡之类的客户机设备。克隆智能卡也会给这些服务的提供商以及经授权的卡用户带来严重问题。

[0005] 因此，所需要的是减少或克服在如上文所描述的常规系统中所发现的这些严重问题的系统和方法。

发明内容

[0006] 这里所描述的实施例可以向客户机设备和服务器之间的正常消息中添加隐蔽安全数据，以便服务器可以确定是否有一个以上的与网络进行通信的客户机设备具有相同的注册凭证或客户机标识符（客户机 ID），表示存在一个或多个克隆的客户机设备。

[0007] 根据一个方面，提供了用于检测克隆客户机设备的安全方法，包括：在服务器上从客户机设备接收消息，所述消息包含从所述客户机设备上的一个或多个操作事件得到的隐蔽标识符，确定所述隐蔽标识符是否匹配存储在所述服务器上的所述客户机设备的隐蔽标识符，以及，如果所述隐蔽标识符不匹配，报告检测到克隆的客户机设备。

[0008] 存储在服务器上的隐蔽标识符可以基于由服务器或由客户机设备或两者生成的一个或多个隐蔽数据项，并可能是在声称来自于同一个客户机设备的以前的消息中接收到的。如果消息始发于不同客户机设备，如真正客户机设备和克隆的客户机设备，隐蔽标识符不匹配，因为一个客户机设备上的操作事件的定时和数值与另一个客户机设备上的那些定时和数值不相同。隐蔽标识符可以是由一个或多个操作事件生成的数值，或基于一个或多个操作事件，例如，事件的发生时间，或在客户机设备上发生特定事件的次数，也可以是使用散列函数等等的一个或多个隐蔽数据值的转换后的版本。

[0009] 客户机设备可以是能够通过网络接收和 / 或发送数据的任何种类的计算设备, 如机顶盒 (STB)、个人计算机、游戏控制台、蜂窝电话、个人数字助理 (PDA)、视频设备、智能卡等等。为客户机设备生成的隐蔽标识符可以包括由客户机设备收集并存储的一个或多个隐蔽数据值, 或这种隐蔽数据值的转换后的版本, 并可以基于客户机设备的随着时间而变化的、并可以由客户机设备存储的、或由客户机设备和服务器存储的任何操作特征或事件。隐蔽标识符可以是由服务器所提供的令牌或数值, 也可以是客户机和服务器生成的隐蔽数据值的组合。这里所提及的客户机设备的操作特征是在客户机设备上发生的或与客户机设备关联地发生的、并且是该特定客户机设备所特有的事件, 如发生预定操作事件 (例如, 在客户机设备或服务器上发送或接收预定的消息) 的时间, 固件更新, 向网络发送消息和从网络接收响应之间的延迟时间, 在客户机设备上接收到第 n 个网络数据分组的时间, 发生某一操作事件的次数, 从服务器发送到客户机设备的令牌, 接收到的授权控制消息 (ECM) 数据分组的计数, 在预定时间客户机设备被调谐到的信道, 在预定时间内信道更换的次数, 在客户机设备中的芯片上包含的寄存器值等等。在智能卡的情况下, 用于生成隐蔽数据的操作特征例如可以是首次使用智能卡的时间, 当智能卡用于某一操作时的微秒时间, 由智能卡在某一时间处理的或在诸如广播事件触发器之类的某一事件中捕获的数据字节的总数, 或任何其他操作数据、计数, 或在使用智能卡过程中发生的事件。在移动电话的情况下, 电话上的呼叫日志可以用以生成隐蔽标识符, 利用散列函数对呼叫日志进行处理, 生成该电话所特有的标识符。操作特征是通过特定客户机设备的操作创建的, 因此, 不会轻易地被克隆的客户机设备“攻击”或复制, 例如, 发生某事件或发生某触发器或捕获新的数据的微秒时刻。可以使用新的操作事件定期更新隐蔽标识符, 以提供隐蔽数据值, 进一步降低被黑客成功地攻击的风险。

[0010] 可以用以创建客户机设备所特有的隐蔽标识符的可能隐蔽数据值的一些示例有: 最后一次从客户机设备发送或由客户机设备接收的特定类型的消息的时间, 发生特定事件的次数, 如购买的货品数量, 接收到的瞬时密钥更新的数量, 接收到某一类型的数据消息或网络数据分组的次数, 或客户机设备执行某一事件的次数, 当用于系统中时, 由动态主机配置协议 (DHCP) 服务器所使用的因特网协议 (IP) 地址, 从诸如电缆调制解调器之类的其他网络设备获得的数值或信号强度, 在发生了预定数量的事件之后客户机数据参数的数值等等。隐蔽数据值可以包括在来自服务器的消息中接收到的、并用于发往服务器的随后消息中的数据。可以由服务器在每一次随后通信中更新该数值。如此, 如果接收到不包含更新的隐蔽数据值的消息, 即, 系统上有一个以上的具有相同凭证的客户机设备, 则服务器认识到存在潜在的克隆设备。一个以上的隐蔽数据值可以用于每一个消息中的隐蔽标识符中, 以便增强安全性。在智能卡的情况下, 隐蔽标识符可以基于使用该卡的时间, 购买货品的数量等等。

[0011] 事件触发器可以用于某些实施例中, 以更新或修改隐蔽数据值或启动计数或定时器, 这会导致用于生成新的隐蔽标识符的更新的隐蔽数据值, 或修改客户机和服务器之间的消息中包含的消息收发协议或数据。

[0012] 在另一个方面, 提供了用于检测克隆客户机设备的安全系统, 包括: 网络服务器数据存储模块, 用于存储多个经过授权的或真正客户机设备的多个客户机凭证或客户机标识符 (ID) 的集合, 还存储基于在来自客户机设备的消息中接收的客户机设备的操作特征的

隐蔽标识符,以及隐蔽数据处理模块,它将从客户机设备接收到的消息中的隐蔽标识符与对应于相同客户机 ID 的以前存储的隐蔽标识符进行比较,如果隐蔽数据标识符不匹配,则创建克隆检测报告。

[0013] 如果网络是双向网络,则在正常的网络通信过程中交换基于收集的操作事件的隐蔽标识符。如果网络通常作为单向网络运行,但是对于某些客户机通信具有返回信道,则收集基于设备的使用状况的预定隐蔽数据值,并将其用于创建由客户机设备存储的隐蔽标识符。例如,当可用时,在周期性的续订过程中,隐蔽标识符通过返回信道在消息中发送到服务器。服务器为某一用户存储第一隐蔽标识符。如果以后接收到声称始发于同一个客户机设备的隐蔽标识符,则由服务器发出克隆检测报告。

[0014] 根据另一个方面,提供了客户机设备,包括隐蔽数据生成模块,用于基于通过客户机设备的操作而生成的数据,生成隐蔽标识符,以及用于存储该隐蔽标识符的隐蔽数据存储模块。如果客户机设备预定用于双向网络环境中,或用于对于某些通信具有返回信道的单向网络环境中,则客户机设备也可以包括消息生成模块,用于生成包含当前存储的隐蔽标识符的消息。随后,隐蔽标识符通过网络,在嵌入到消息中的隐蔽数据字段中,或响应于来自服务器的请求作为数据值,或其任何组合,发送到网络服务器。消息可以是通常以双向通信发送到网络的消息类型,或者,如果客户机设备通常只涉及与网络的单向通信,在消息中作为周期性的续订过程一部分,或其他标准消息。

[0015] 在没有用于单向网络服务的返回信道的情况下,客户机设备创建并存储客户机标识符,该客户机标识符可以基于客户机设备上的新的事件而被定期更新。客户机设备或网络服务器可以具有服务代码生成模块,用于以预定的时间间隔在客户机设备上生成服务代码消息。该消息可以要求用户呼叫服务中心或通过移动电话或因特网连接向服务中心发送短消息服务 (SMS),提供用户标识和客户机设备中的当前存储的隐蔽标识符。由于对于真正客户机设备和克隆的客户机设备,当前存储的隐蔽标识符是不同的,因为它们是以不同的方式操作的,因此,服务中心可以确定何时接收到具有相同客户机或用户标识,但是隐蔽标识符不同的消息。然后,服务中心可以采取附加的步骤,以确定哪一个客户机设备与合法用户关联,并只对该客户机设备续订,切断给使用相同用户或客户机标识的任何其他客户机设备的服务。

[0016] 隐蔽标识符是通过在客户机设备的实际操作过程中发生的操作事件生成的。因为操作事件是在制造客户机设备之后发生的并依赖于用户如何使用客户机设备的方式,因此,操作事件是特定客户机设备所特有的。甚至在克隆的客户机设备之间,这些操作事件也是不同的,因为在克隆的客户机设备接通电源之后它们做事的方式是不同的,这是用于生成隐蔽标识符的操作的差异。因此,隐蔽数据为特定客户机设备提供了由该客户机设备存储的唯一标识符,随后用于发往服务器的消息中。在客户机设备通常只用于单向网络通信中的情况下,可以在周期性的续订过程向网络提供唯一隐蔽标识符,或者,如果怀疑被克隆,则由网络服务器请求提供唯一隐蔽标识符。

[0017] 隐蔽数据生成模块可以集成到客户机设备的中央处理单元中,在某些情况下,如在智能卡、移动电话等等中,可以嵌入在同一个芯片(系统芯片或 SOC)。隐蔽数据存储模块也可以集成在中央处理单元(CPU)中或与中央处理单元关联的单独的数据库中,或 CPU 内部或外部的存储器中。

[0018] 一个实施例中的客户机设备消息格式包括消息标识符字段、隐蔽数据字段、以及包含要被传递到服务器的消息的至少一个另外的数据字段，如客户机标识字段或密钥请求，或作为消息或消息 ID 的一部分。消息类型可以是登录消息、广播密钥请求消息、电子商务购买消息、改变信道的请求、续订消息等等。如果消息类型是登录消息，则另外的数据字段包含用户名和密码。隐蔽数据字段包含隐蔽标识符，该隐蔽标识符可以包括一个或多个隐蔽数据值或项，或这样的隐蔽数据值的转换后的版本。在接收到消息时，隐蔽标识符可以被服务器用以确定是否有一个以上的客户机设备使用相同的凭证。可以有一个以上的消息类型包含隐蔽标识符。

[0019] 在一个实施例中，当前隐蔽标识符作为正常消息的一部分从客户机设备发送到服务器，如登录到系统、请求解密密钥、执行电子商务交易，或通常在系统内发生的其他消息和事件。用于创建隐蔽标识符的隐蔽数据值可以基于各种事件，而事件触发器可以用以定义触发以前存储的隐蔽标识符的更新或修改的事件。添加到客户机和服务器之间的正常消息中的隐蔽标识符不需要在客户机和服务器之间添加消息或添加确认，降低了黑客可以监视协议并确定如何攻击系统的概率。如此，试图通过克隆用户凭证，例如，机顶盒 (STB) 的凭证来窃取服务的黑客，也需要了解隐蔽标识符的含义和引起隐蔽标识符的变化的触发器，以确保可信的 STB 和克隆的 STB 具有相同的隐蔽标识符。可以使用一个以上的隐蔽数据值来创建隐蔽标识符，例如，可以使用两个或更多隐蔽数据值的客户机库来在发往服务器的每一个选定客户机消息中创建隐蔽标识符。定期更新隐蔽数据值的客户机库，使得克隆设备躲避服务器的检查更加困难。在替代实施例中，隐蔽标识符也可以与客户机和服务器之间的单独的消息一起发送。

[0020] 安全系统也可以包括被设计为识别怀疑的克隆设备的续订过程。可以响应由网络服务器生成的克隆检测报告来启动续订过程，也可以以周期性的时间间隔或当由于其他原因怀疑有克隆时执行续订过程。续订过程被设计为当有多个这样的设备使用相同的凭证时，只重新授权给单个客户机设备。

[0021] 在阅读了下列详细描述和附图之后，本发明的其他特征和优点对所属领域的技术人员将变得更加容易理解。

附图说明

[0022] 本发明的细节，无论其结构还是操作，通过对附图的研究得到，其中类似的附图标记表示相同的部件，在附图中：

[0023] 图 1 示出了在用于检测潜在的克隆客户机设备的安全系统的一个实施例中，具有与服务器进行通信的真正的或经过授权的客户机设备和一些克隆的客户机设备的网络的方框图；

[0024] 图 2A 示出了现有技术的用户登录消息中的数据字段的图形；

[0025] 图 2B 示出了在用于检测潜在的克隆客户机设备的安全系统的一个实施例中，在包含在服务器上使用的隐蔽标识符的用户消息的一个实施例中数据字段的图形；

[0026] 图 3 示出了根据一个实施例的被配置为在消息中插入隐蔽标识符的客户机设备的方框图；

[0027] 图 4 示出了检测克隆客户机设备的方法的一个实施例的流程图；

- [0028] 图 5A 和 5B 示出了克隆检测方法的一个实施例的流程图；
[0029] 图 6A 到 6F 示出了在图 5A 和 5B 的方法中的各个阶段生成的消息；
[0030] 图 7 示出了用于在客户机设备和服务器之间的消息中插入隐蔽标识符的方法的实施例的流程图；
[0031] 图 8 示出了使用隐蔽标识符的服务续订方法的一个实施例的流程图；以及
[0032] 图 9 示出了图 8 的方法的修改的流程图，用于从客户机设备没有返回信道的单向网络环境中。

具体实施方式

[0033] 这里所公开的某些实施例用于检测一个以上的客户机设备使用相同的凭证的情况。例如，这里所说明的一种方法和系统，用于使用在客户机设备和服务器之间的正常消息中添加的、基于客户机设备所特有的操作事件的数值的隐蔽标识符，检测潜在的克隆设备。

[0034] 在阅读该描述之后，在各种替代实施例和备选应用中如何实现本发明，对于本领域的技术人员来说将变得很清楚。然而，虽然这里描述了本发明的各种实施例，但是应该理解，这些实施例只是作为示例来呈现的，而不作为限制。如此，各种替代实施例的详细描述不应该被理解为对如所附的权利要求中阐述的本发明的范围作出限制。

[0035] 在下面的描述中，客户机设备可以是能够计算和从网络接收数据的任何类型的计算设备，如机顶盒 (STB)、个人计算机、游戏控制台、移动电话、个人数字助理 (PDA)、个人媒体播放器、视频设备，诸如数字视频接收器 (DVR)、数字视盘 (DVD) 播放器 (DVD)、压缩光盘 (CD) 播放器、智能卡等等。可信的或真实客户机设备是正常地向服务器注册以便通过网络接收服务，或诸如银行结算、购物等等通过网络授权的本地服务的设备，如在智能卡的情况下。克隆的客户机设备是与在网络上正常地注册了服务的真实客户机设备具有相同的凭证的设备，未经授权的或非付费用户用以未经授权企图获得金钱或服务。术语“隐蔽数据”、“隐蔽数据值”和“隐蔽数据项”被用以表示基于客户机设备的操作特征的唯一数据值，例如，通过特定客户机设备的操作或该设备与服务器的通信创建的数值，或基于客户机设备的操作的、由服务器所创建的并嵌入到发送到客户机设备的消息中的令牌或数值。这样的数值是隐蔽的，因为它们的特性使它们难以被黑客检测并在克隆的客户机设备中复制，因为该数据是在制造之后生成的。术语“隐蔽标识符”表示特定客户机设备所特有的标识符，它是基于与该设备的操作关联的隐蔽数据值生成的，并可以在某些实施例中包括一个或多个真实的隐蔽数据值，或者可以是这样的数据值的转换后的版本，转换是通过使用散列函数或播种随机数值进行的，或对数据执行某些其他转换。术语“事件触发器”被用以表示触发客户机设备和服务器之间的消息收发协议中包含的隐蔽标识符的更新或修改的事件。“事件计数器”计数由客户机设备执行的事件，并可以被用作当计数的事件的数量超过阈值时的事件触发器。

[0036] 图 1 是根据一个实施例的包括克隆检测的网络安全系统的方框图，其中服务器 10 通过网络 14 与真实的或经过授权的客户机设备 12 进行通信，若干个使用相同客户机凭证的克隆客户机设备 15、16 也通过网络 14 向服务器 10 发送消息。一个、两个或更多克隆设备可能试图通过佯装为客户机设备 12 在任何时刻使用网络服务。在计算环境中，盗版者常常通过创建具有相同凭证的多个客户机来窃取网络及其他服务，从而允许非付费的用户共

享或盗用付费的合法用户的服务。

[0037] 如图 1 所示出的,服务器 10 链接到服务器数据库 (DB) 20,该数据库具有数据存储模块 23,用于存储隐蔽标识符,该隐蔽标识符可以在消息中从客户机设备接收到,和 / 或由服务器生成。如上所述,每一个隐蔽标识符都基于特定客户机设备上的操作事件。服务器 10 具有用于控制网络通信的通信模块 11,以及克隆检测模块 13,用于将从客户机设备接收到的消息中的隐蔽标识符与模块 21 中的以前存储的隐蔽标识符进行比较,如下面比较详细地描述的。服务器 10 具有没有显示的另外的标准服务器处理和控制模块。

[0038] 在图 1 的系统中,客户机设备 12 向服务器 10 发送消息 M1,而克隆设备 15、16 向服务器发送类似的消息 M2 和 M3。这些消息可以以任何顺序发送,服务器可以检测一个或多个潜在的克隆的存在,不管消息 M1 到 M3 的传输次序如何。每一个消息都可以包括嵌入到消息的预定隐蔽数据字段或部分的隐蔽标识符 18。与服务器进行通信的客户机设备的隐蔽标识符与客户机设备的客户机凭证关联,并存储在隐蔽数据存储模块 23 中,以便与从具有相同凭证的一个或多个客户机设备接收的未来隐蔽标识符进行比较,如下面比较详细地描述的。每一个真正的和克隆的客户机设备都分别具有数据库或存储器设备 (RAM、ROM、FLASH、EEPROM) 或寄存器存储器 30、32、34,其中存储了隐蔽数据值,并由预定的事件触发器更新。虽然显示的数据库是与图 1 中的客户机设备分开的,但是,它也可以封装在客户机设备中,或者,也可以是客户机设备中的中央处理单元或系统芯片 (SOC) 的一部分,或诸如 RAM 存储器、FLASH 存储器、安全存储器等等设备存储器的一部分。

[0039] 图 3 中更详细地示出了客户机设备 (真实的或克隆的) 12、15 或 16。客户机设备可以是被配置为通过网络进行通信的任何客户机设备,如机顶盒、个人计算机、游戏控制台、移动电话、PDA、便携式媒体播放器、DVD 播放器、DVR 或智能卡等等。客户机设备具有关联的数据存储模块 30、32、34,它们是单独地显示的,但是,也可以与客户机设备的其他模块集成到同一个外壳中,或在某些情况下与其他模块集成同一个芯片上。客户机设备也具有用于控制与服务器 10 的网络通信的通信模块 17,用于基于隐蔽数据值、事件触发器或从服务器接收到的数据,创建隐蔽标识符的隐蔽标识符生成模块 19,以及消息格式化模块 28。客户机设备也包括标准的客户机设备处理和控制模块,图 3 中未示出。数据存储模块具有用于存储隐蔽数据值的当前集合的隐蔽数据表模块 29,如下面所描述的。在隐蔽标识符是隐蔽数据值的转换后的版本的情况下,当前隐蔽标识符或隐蔽数据值的矩阵或隐蔽数据值的组也存储在模块 29 中。

[0040] 在一个实施例中,消息格式化模块 28 可以将当前隐蔽标识符插入或嵌入在发送到服务器的一种或多种类型的消息中。在其中客户机设备只用于接收单向网络通信并且不能接入到网络的返回信道的另一个实施例中,消息格式化模块 28 被省略,隐蔽标识符生成模块被配置为以唯一标识代码的形式向与周期性的用户续订过程关联的客户机设备的用户显示当前存储的隐蔽标识符,如下面参考图 9 更加详细描述的。

[0041] 在一个实施例中,隐蔽安全性数据或标识符 18 基于从其中传输消息的设备的操作特征。这样的特征难以或不可能在客户机设备的克隆中复制,因为克隆的客户机设备不会与可信的或真实客户机设备相同地操作,诸如消息、更新等等操作事件在不同设备中是在不同的时间发生的。在现实世界的客户机设备中获取微妙的相同事件几乎是不可能的。客户机设备的操作特征是该特定客户机设备所特有的数值,该数值是基于客户机设备的操

作生成的,如发生预定操作事件(例如,在客户机设备或服务器上发送或接收预定的消息)的时间,固件更新,向网络发送消息和在网络接收响应之间的延迟时间,在客户机设备上接收到第n个网络数据分组的时间,在选定时间段内客户机设备执行某一操作事件的次数,从服务器发送到客户机设备的令牌,接收到的ECM数据分组的计数,在预定时间客户机设备被调谐到的信道,在预定时间内信道更换次数,在某一时间在客户机设备中的芯片上包含的寄存器值等等。结果是,有无限多个操作数据值可以用以生成隐蔽数据值(或客户机的操作所特有的数据值),因为准确的数据值不重要,而重要的是,基于两个相同设备的操作而数据值不同的似然率是比较高的。如果使用相同凭证的两个或更多客户机设备通过网络进行通信,这样的操作特征从一个客户机设备到其他客户机设备是不相同的,并且通过用户对特定客户机设备的操作唯一地创建的。因此,这样的操作特征和基于这样的特征的隐蔽标识符不能轻易地被克隆的客户机设备“修改”或复制。克隆的客户机设备的操作员不太可能能够获取真正或可信客户机设备的这样的特征,并且通常甚至不能察觉到哪些特定操作特征被用以创建隐蔽标识符,在一个实施例中,隐蔽数据值在客户机软件的不同版本之间是不同的。

[0042] 服务器提取发自具有某些凭证的设备的消息中接收到的隐蔽标识符,并将此标识符与显然源自同一个设备的以前消息中接收到的标识符进行比较。如果没有匹配,则很可能有人在使用一个或多个克隆,服务器可以向系统操作员提供可能克隆检测的适当通知,以便采取进一步的行动。由于服务器不能确定发送消息的具有相同的凭证的多个客户机设备中的哪些是克隆的设备,因此,除向操作员提供克隆检测通知之外,还向设备提供被请求的服务。

[0043] 在一个实施例中,隐蔽标识符是在客户机和服务器之间交换的普通消息中传输的。例如,假设客户机需要登录到系统,并定义了登录消息。标准的登录消息包括用户名和密码。在一个实施例中,除用户名和密码之外,登录消息还包括隐蔽标识符18。当客户机设备试图登录到系统时,客户机设备提供诸如用户名和密码之类的标准登录信息,隐蔽标识符被嵌入到构成了登录命令的登录消息中(或任何消息或所有消息),该登录命令包括了隐蔽标识符,作为标准登录消息的一部分。登录消息包含用户名、密码,以及包含隐蔽标识符的附加的数据字节。在一个实施例中,隐蔽标识符中包含的或用于生成隐蔽标识符的数据项或数值基于客户机内的操作事件在不同的时间变化,或基于时刻而变化,或基于在某一事件之后经历的时长而变化,以便可以通过在特定时间改变隐蔽数据值或者通过向以前的隐蔽数据项添加新的隐蔽数据项(本质上提高了特定客户机的隐蔽数据项的数量),来更新隐蔽标识符。

[0044] 客户机设备和服务器之间的任何标准消息(如初始登录消息)交换都可以用于检测克隆。隐蔽标识符可以与正常消息和/或事件组合起来,如当客户机登录到系统中时。除在登录中通常发现的信息(如客户机用户名和密码)之外,还可以向登录消息中添加某一客户机设备的操作特定的隐蔽标识符,如用户最后一次登录到网络的时间,或当前登录和前一次登录之间的时间差。隐蔽数据可以应用于通信系统中的所有消息或只应用于选定的消息,如登录消息或其他类型的消息。

[0045] 图2A示出了当前使用的消息协议的常规日志。此消息包括消息标识符字段(ID)21,该字段根据系统上支持的一组消息定义消息类型,对于系统中的每一个消息通常

是唯一的。它还可以包括可选序列号字段 22，其中包含系统中的任何类型的每一个消息的唯一编号，通常是增量式计数，允许系统在处理消息之前通过验证序列号为新的，来消除消息重放攻击。当消息是初始登录消息时，它还具有用户名字段 24，其中包含在系统上注册了服务的用户或客户机设备的用户名，或者与服务提供商的用户帐户关联的用户名，以及密码字段 25，密码字段 25 包含与帐户或服务关联的用户的密码。当用户首次预订或向系统或服务提供商注册时，提供密码，在随后由用户请求服务时，服务器验证该密码。只有在密码保护的系统中正确地提供密码之后，才可以接入服务，或者用户才可以使用服务购买货品。此外，对于每一个客户机，隐蔽数据还可以用作密码盐析 (salting) 过程的一部分，服务器端察觉到用于盐析密码或数据的隐蔽数据，或者，服务器端下载加密密钥或将密钥盐析到客户机中。这样的密码有时也被黑客获得，并与克隆设备一起使用，企图不支付报酬地获取服务。

[0046] 图 2B 示出了修改的初始登录消息的实施例，在正常的登录消息结构中包含隐蔽数据字段 18 中的隐蔽标识符。ID 字段、序列号字段 22、用户名 24，以及密码 25 与图 2A 的对应的字段相同，但是，消息被修改，以在字段 22 和 24 之间的数据字段 18 中提供隐蔽标识符。在其他实施例中，可以在消息中的其他位置提供隐蔽数据字段 18，也可以在不同类型的消息中提供，如在请求广播密钥消息、电子商务购买消息、改变信道消息等等中。可以只在设备和服务器之间的一种特定类型的消息中提供隐蔽标识符，也可以在由设备发送的每一个消息中提供，或间歇地在各种消息中提供。隐蔽标识符的间歇传输可以使这样的标识符更难以让潜在的黑客跟踪。由于加密消息始终比客户机和服务器之间的非加密消息收发更安全，因此，在一个实施例中，隐蔽数据是通过加密的连接传输的，如互联网协议安全 (IPSec)，或安全套接字层 (SSL) 或客户机和服务器之间的其他形式的加密。

[0047] 如图 1 所示出的，每一个消息 M1、M2 和 M3 都在字段 18 中具有隐蔽标识符，但是，消息 M2 和 M3 中的隐蔽标识符通常不匹配消息 M1 的隐蔽标识符。这是因为，在一个实施例中，隐蔽标识符基于由客户机设备的操作特征或操作事件生成的隐蔽数据值，如在客户机设备或服务器上发送或接收某些消息的时间，接收到某一类型的数据消息或网络数据分组的次数等等。隐蔽标识符可以包括隐蔽数据字段的不同区域中包含的以不同操作方式生成的隐蔽数据值，也可以包括这样的隐蔽数据值的转换后的版本。这样的数值在克隆客户机设备中大不可能与真实客户机设备上的隐蔽数据值相同，因为克隆客户机设备的操作通常不匹配客户机设备或另一个克隆客户机设备的操作。例如，隐蔽数据字段的第一段可以包含以微秒为单位的客户机设备的第一次接通电源的时间。在某一时间段或若干个事件之后，隐蔽数据字段的第二段可以向第一次接通电源的时间添加该设备的随后接通电源的时间（例如，T1, T2）。尽管服务器不知道第二次接通电源的时间是由客户机设备添加的还是由克隆的客户机设备添加的，但是，原始接通电源的时间 T1 对于两个设备来说是非常不可能相同的，向客户机和服务器之间交换的隐蔽数据添加的第二和随后的隐蔽数据项被设计为在多个客户机之间是唯一的，因为附加的隐蔽数据项是在客户机的连续操作过程中生成的，因此，隐蔽数据相同的似然率非常低。

[0048] 服务器从可信的和 / 或克隆客户机设备接收消息，并将与被授权用户的客户机凭证关联的最近隐蔽标识符保存在服务器隐蔽数据存储模块 23 中。当显然是从与相同客户机凭证关联的设备中接收到随后消息时，服务器将隐蔽标识符与该客户机的以前存储的隐

蔽标识符进行比较。如果在一个或多个隐蔽标识符中没有发现匹配，则与服务器进行通信的其中一个设备很可能是克隆设备，服务器向操作员报告已经检测到克隆。然后，操作员可以启动确定哪一个设备是正当的或经过授权的客户机设备，哪一个设备是克隆的过程。

[0049] 图 4 示出了使用图 1、2B 和 3 的系统检测网络上是否存在克隆客户机设备的方法的一个实施例的流程图。在步骤 40 中，客户机设备向服务器发送在隐蔽数据字段 18 中包含隐蔽标识符的消息。该消息例如可以是图 2B 中所示出的格式，也可以是任何其他类型的标准网络通信消息，在该消息中所选择的数据字段插入了包括一个或多个隐蔽数据值的隐蔽标识符，或一个或多个隐蔽数据值的转换后的版本的标识符。服务器接收该消息，并从消息中提取隐蔽标识符 (42)，然后，将隐蔽标识符与对应于与注册的客户机设备（看来似乎从该注册客户机设备始发了消息）关联的客户机凭证的存储的隐蔽标识符进行比较 (步骤 44)。服务器基于该比较确定是否有匹配 (步骤 45)，即，确定在存储的隐蔽标识符的任何一部分和消息中的隐蔽标识符之间是否有匹配。如果找到匹配，则当适合于客户机设备时，服务器发送消息应答 (步骤 48)，存储新的隐蔽标识符，并进行所需的服务或交易。如果没有找到匹配，即，在隐蔽标识符的任何一部分之间没有匹配，则服务器向操作员生成报告，指出已经检测到潜在的克隆 (步骤 46)，并可以在存储器中设置可选标志。如果隐蔽标识符是通过转换隐蔽数据值创建的多位代码，则匹配意味着，接收到的隐蔽标识符与存储的隐蔽标识符相同。如果隐蔽标识符是基于正在进行的事件的一个或多个隐蔽数据值，则接收到的隐蔽标识符可以只匹配以前存储的隐蔽标识符的一部分，而它还包括在发往服务器的最后消息之后添加的新的隐蔽数据值。如果接收到的隐蔽标识符的一部分匹配存储的隐蔽标识符，仍然找到匹配，但是，如果在隐蔽标识符的任何一部分没有匹配，则不会找到匹配。

[0050] 当检测到潜在的克隆时，服务器可以继续与发送该消息的设备进行通信，因为还没有确定该设备是否是克隆客户机设备，即，服务器没有足够的信息确定与服务器进行通信的两个客户机设备中的哪一个是克隆。在最后一个步骤中，可以中止向被发现是克隆的设备提供的服务，或向所有设备停止服务，让合法用户与服务提供商进行接触，以使它们的服务继续。

[0051] 在一个实施例中，隐蔽标识符所依据的隐蔽数据值可以由客户机设备上的某些操作事件生成。由操作事件生成的可能隐蔽数据值的一些示例有：

[0052] a) 客户机执行某一事件的次数，如请求密钥或初始化与服务器的会话，或执行电子商务交易。

[0053] b) 由用户以前购买的货品的数量。

[0054] c) 由客户机接收到的瞬时密钥更新的数量。

[0055] d) 最后一次固件更新的时间。

[0056] e) 客户机的最后一次进行密钥请求的时间。

[0057] f) 最后一个特定类型的消息的时间，或接收到某一消息的次数的计数，或从服务器接收到的当前消息和以前消息之间的延迟。

[0058] g) 由客户机接收到某一类型的消息时的时间。

[0059] h) 从客户机接收到某一类型的消息的时间。

[0060] i) 接收到某一类型的数据消息或网络数据分组的次数的计数，示例包括视频 ECM（授权控制消息），不同的 MPEG2PID 值的计数，特定 TCPIP 端口号上的数据分组的计数

等等。

- [0061] j) 请求消息被发送到网络和从服务器接收返回的响应之间的时间延迟。
- [0062] k) 最后一次执行多播联接的时间,或最后一个多播联接的数值。
- [0063] l) 当系统中使用了 DHCP 时,由动态主机配置协议 (DHCP) 服务器所提供的 IP 地址。
- [0064] m) 当系统中使用了 DHCP 时, DHCP 租约的剩余时间。
- [0065] n) 从其他网络设备获得的数值,如电缆调制解调器的参数范围,或在运行新的客户机 3 天之后网络的信号强度。
- [0066] o) 在某一时间长度之后生成的数据更改或新消息,例如,客户机设备从服务器接收到隐蔽数据值,向客户机设备指示客户机设备应该在多少分钟内与服务器接触。
- [0067] p) 在若干个事件 (如当发生了 57 次信道更换时电视频道号) 之后的客户机数据参数的数值。
- [0068] q) 从利用创建新的隐蔽数据值的功能处理的以前使用的隐蔽数据值得到的新的隐蔽数据值。
- [0069] r) 根据客户机设备上的芯片内的数据生成的隐蔽数据值,或根据客户机设备中的芯片或硬件插件板或卡或安全存储器中的处理的或定标的数据生成的隐蔽数据值。
- [0070] s) 从服务器接收到的诸如令牌或密钥之类的隐蔽数据值,客户机设备将它们保留,并用作在与服务器的随后消息中包含一个或多个隐蔽数据值或数据项的隐蔽标识符的一部分。从服务器接收到的隐蔽数据可以被客户机设备转换,转换后的版本可以返回到服务器,作为随后消息中的隐蔽标识符。这就使得服务器在客户机和服务器之间的正常消息中将令牌或密钥传递到客户机,作为正常的系统消息的一部分。用于客户机隐蔽标识符中的服务器提供的令牌可以在单独的消息中发送,但是,优选的消息是在正常消息中从服务器传递隐蔽数据值。
- [0071] t) 当接收到第 12000 个网络数据分组时的时刻。
- [0072] 上文所列出的一些值可以另外地或者被替代地用作触发客户机设备和服务器之间的消息收发协议中包含的隐蔽标识符的更新或修改的事件触发器或事件计数器。例如,操作事件可以触发计数了连续的操作事件,例如,诸如客户机设备上的信道更换的数量,并当用户更换信道达到了预定次数时记录隐蔽数据值的计数器。隐蔽数据值可以是当到达预定的计数值的时刻,或在到达预定计数之前所花的时间长度。可以以同样的方式计数其他类型的操作事件,以提供事件触发器,如由客户机设备发送或接收到的某一类型的消的数量,购买的货品数量等等,或事件本身的数量也可以直接用作隐蔽数据值。其他可能的事件触发器可以是发生操作事件的时间,如固件更新。这样的事件触发器可以用以基于不同的操作事件,将以前的隐蔽数据值集合改变为一组新的隐蔽数据值,然后,使用新的隐蔽数据值来创建隐蔽标识符。这使得黑客确定哪些特定操作事件被用以生成隐蔽标识符难得多。
- [0073] 隐蔽数据 18 可以以表来构建。下面的表 1 示出了可能的隐蔽数据表的一个实施例。在下面显示的表中,使用两个隐蔽数据项或数值来构建隐蔽数据表。一个隐蔽数据项是当发出最新的广播密钥请求 (BKEY) 消息时的时刻 (TOD),另一个是由诸如机顶盒 (STB) 之类的客户机设备或其他客户机设备获取的瞬时密钥更新的数量。在替代实施例中可以使

用基于操作特征的其他隐蔽数据项，为增强安全性，可以使用两个以上的隐蔽数据项。最初，表 1 中的两个值都是 0，而初始隐蔽标识符可以是 0,0。下面的表 1 只是可以一起在客户机软件版本的一个版本中的两个数据值的示例。可以预见，其他隐蔽数据值也可以用以创建隐蔽标识符，在不同的软件版本之间可以使用不同的数据值。例如，在该示例中，使用了瞬时密钥更新的数量，但是，在软件的另一个版本中，可以使用最后的瞬时密钥更新的时刻 (TOD)，也可以使用第一和第二瞬时密钥更新之间的秒数。

[0074]

隐蔽数据	描述
第一 BKEY 请求的 TOD	客户机设备作出第一或第 n 个广播密钥 (BKEY) 请求的时刻。最初，这被设置为 0。
瞬时密钥更新的数量	客户机设备更新其瞬时密钥的次数。最初，这被设置为 0。

[0075] 表 1- 隐蔽数据表

[0076] 图 5A 和 5B 示出了使用如上面的表 1 中的隐蔽数据检测克隆设备的实施例的一个示例中的方法步骤的流程图。下面的表 2 示出了在图 5A 和 5B 中的各种步骤中服务器和客户机设备或克隆客户机设备中存储的隐蔽数据值的一个可能的示例，而图 6A 到 6F 示出了在图 5A 和 5B 的示例中的各种阶段生成的消息。在表 2 和图 5 中，术语“真实客户机设备”用以表示与在服务器上注册的客户机设备凭证关联的原始或可信客户机设备，而术语“克隆的客户机设备”表示作为具有相同凭证的真实客户机设备的完全相同副本的客户机设备。在图 5A 的步骤 100 中，安装的是真实的或可信的客户机设备，并注册为将用户与服务器 10 所提供的服务关联，服务器 10 将用户客户机设备的凭证保存在数据库 20 中。在客户机设备 14 第一次接通电源时（步骤 101），隐蔽标识符被初始化为服务器数据库和客户机设备数据库中的已知初始值（步骤 102）。在该情况下，隐蔽标识符包括隐蔽数据值的集合，如下面的表 2 所示。在该示例中，隐蔽标识符中所使用的至少一个隐蔽数据值是客户机设备作出广播密钥 (BKEY) 请求的时刻 (TOD)，虽然在其他实施例中可以使用任何其他隐蔽数据值来代替 BKEY 请求 TOD 或与 TOD 一起使用。

[0077] 在接收到任何 BKEY 请求之前存储在服务器数据库 20 中的初始隐蔽数据值有：Acknowledged(Acked) TOD = 0, Not Acknowledged(NotAcked) TOD = 0，即，该客户机在服务器上的隐蔽数据或标识符是 0,0，而当它第一次接通电源时存储在客户机设备上的初始隐蔽数据值是 TOD = 0。因为这是安装客户机设备之后的第一次电源使用，对于广播密钥请求的 TOD 事件触发器是零，因为客户机设备还没有请求广播密钥。在客户机设备第一次接通电源时，和 / 或在服务器上在从客户机设备接收到第一个消息之前，任何或所有隐蔽数据都可以设置为初始状态，如 0。在替代实施例中，当用户的客户机设备在服务器上进行注册时的注册过程中，可以生成一个或多个非零的隐蔽数据值，并用以创建初始隐蔽标识符，或除了最初设置为 0 的一个或多个隐蔽数据值之外，包括在隐蔽标识符中。

[0078] 在表 2 中，在服务器中存储的隐蔽数据项的未确认 (NotAcked) 值是由服务器向在源自客户机设备的消息中还没有被确认的客户机设备（真实的或克隆的）发出的最后一个

值。当客户机返回 NotAcked 值或由客户机设备从 NotAcked 值导出的值时,NotAcked 值移到存储在服务器上的数值的确认 (Acked) 列。在一个实施例中,客户机可以在下一个消息中向服务器返回 NotAcked 值,如表 2 和图 5 和 6 所示。在替代实施例中(未显示),客户机设备在接收到新的 NotAcked 值时,向服务器发送特定确认消息,确认 NotAcked 值已经成功地存储在客户机设备数据库中。此时,NotAcked 值替换服务器中的 Acked 值。然而,该替代方案对于黑客来说比较容易获取隐蔽数据值。图 5A 和 5B 所示的方法更加隐蔽,其中当指定的类型的下一个消息被发送到服务器时,进行对 NotAcked 值的唯一一次确认。

[0079] 在初始化之后,客户机设备 14 在步骤 104 中向服务器发送对于广播密钥的请求 (BKEY 请求)。在一个实施例中,该请求包含隐蔽标识符或隐蔽安全性数据 18。在该情况下,BKEY 消息中的隐蔽标识符如下:

[0080] TOD 最后一个 BKEY 请求 = 0

[0081] 瞬时密钥更新 = 0。

[0082] 换句话说,BKEY 请求中的隐蔽标识符是 0、0,图 6A 示出了此消息 M1 的格式。

[0083] 服务器接收 BKEY 请求(步骤 105),并从该请求中提取隐蔽标识符中的隐蔽数据值,然后,对照存储在服务器中的对应数值检查这些数值。下面只对于消息系列中的 BKEY TOD 隐蔽数据值来描述该比较,但是,对于隐蔽标识符中的其他隐蔽数据值,如基于瞬时密钥更新的数值,也可以进行类似地比较。由于这是源自使用这些客户机凭证的任何客户机设备的第一个消息,BKEY TOD 数据匹配(步骤 108),服务器向客户机设备返回 BKEY(步骤 110),并带有服务器确定的 TOD 值 T1,即,在服务器上收到来自此客户机的第一个 BKEY 请求的时刻。图 6B 示出了 BKEY 应答消息 R1 的格式的一个实施例,其中在消息 ID 和 SN 之后的消息字段中提供了新的 TOD 值 T1。在替代实施例中,可以由客户机设备本地读取消息的 TOD 值,代替在来自服务器的消息中进行接收。在其他备选实施例中,从服务器接收到的 TOD 值可以替换为从服务器发送的任何类型的数据值或令牌。

[0084] 在下面的表 2 中提供的示例中,TOD 值 T1 是 8437,在步骤 114 中被作为 NotAcked TOD 添加到服务器数据库中,因为还没有从客户机设备接收到确认收到该数值的确认。正如上文所指出的那样,在替代实施例中,客户机设备可以被编程为发送确认收到 TOD 值 T1 的确认,但是,在该实施例中,直到下一个 BKEY 消息之前没有发送这样的确认,如此,TOD 值 T1 直到并且除非它在连续的 BKEY 消息中被确认,仍保持为 NotAcked 值,这是更加隐蔽的选项。此时,在该示例中,保存在服务器上的客户机标识符中的 TOD 值是 Acked TOD = 0,NotAcked TOD = T1 或 8437。

[0085] 表 2- 图 5 中的各种步骤中的隐蔽数据值的示例

[0086]

步骤	服务器操作	服务器 DB	客户机中的隐蔽数据值	客户机 / 克隆设备操作
101, 102	客户机设备的初始隐蔽数据值被初始化为已知初始值。	Acked TOD = 0 NotAcked TOD = 0	TOD = 0	初始状态 (0,0) 下的所有隐蔽数据

[0087]

112, 114	服务器返回具有由服务器确定的时刻 (TOD) 值的 BKEY。服务器向服务器 DB 添加最近的隐蔽数据值, 作为未确认的数值。DB 包含最后一个已知好的数值 (在该示例中, 为 0), 加上最后一个未确认的数值 (当前 TOD = 8437)	Acked TOD = 0 NotAcked TOD = 8437. 注意, 8437 是由服务器向客户机提供的新的 TOD。		
115, 116			TOD 现在等于 8437。	真实客户机设备保存在 BKEY 提供过程中从服务器传递的最后一个 BKEY 的 TOD

[0088]

步骤	服务器操作	服务器 DB	客户机中的隐蔽数据值	客户机 / 克隆设备操作
				非易失性存储器中的消息
122		Acked TOD = 0 NotAcked TOD = 8437	TOD = 0	BKEY 请求中的克隆的客户机设备隐蔽数据如下： TOD 最后一个 BKEY 请求 = 0, 瞬时密钥更新 = 0

126, 130	服务器返回具有由服务器确定的新的时刻 (TOD) 值的 BKEY。服务器向服务器 DB 添加最近的隐蔽数据值, 作为未确认的数值。DB 包含最后一个已知好的数值 (在该示例中, 为 0), 加上最后一个未确认的数值 (当前 TOD)	Acked TOD = 0 NotAcked TOD = 9902. 注意, 9902 是由服务器向客户机提供的新的 TOD, 消除了在克隆的 STB 之前发送到请求了密钥的其他 STB 的 non-Acked 值 8437		
132			克隆中的 TOD 是 9902。	克隆的客户机设备保存在 BKEY 提供消息中的从服务器接收到的 TOD。
134		ACKedTOD = 0, notAckedTOD =	真实客户机设备中的 TOD 是 8437	真实的客户机发送 renewBKEY

[0089]

步骤	服务器操作	服务器 DB	客户机中的隐蔽数据值	客户机 / 克隆设备操作
		9902		具有最近的 BKEY 请求 = 8437 的 Acked TOD 的发往服务器的消息, 瞬时密钥更新 = 0
135	服务器接收 BKEY 请求, 并对照请求中的 TOD 检查 DB 中的 TOD。	ACKedTOD = 0 ; notAckedTOD = 9902	AckedTOD = 8437	
140, 142	服务器将 notAckedTOD 更新为 11305, 并将 BKEY 和 TOD 发送到 STB	ACKedTOD = 0 notAcked TOD = 11305	真实客户机设备中的 TOD 是 11305	

[0090] 在步骤 115 中, 真实客户机设备接收源自服务器的应答中的广播密钥, 以及新的

TOD 值 T1(在该示例中为 8437)。然后,客户机设备存储新的 TOD 值(步骤 116),使用广播密钥对诸如广播数据之类的加密数据进行解密(步骤 118)。在所示出的示例中,克隆的客户机设备在由真实客户机设备接收到第一个广播密钥之后并且在真实客户机设备将连续的广播密钥请求发送到服务器之前的某一时间通电(120)。此事件序列不会在所有情况下发生,只是与服务器进行通信的真实的和克隆的客户机设备的顺序的一个可能的示例。克隆的客户机设备向服务器发送广播密钥请求(122),其中包含隐蔽标识符,隐蔽标识符包括初始隐蔽数据值 0,0,图 6C 中示出了此消息 M2 的一个可能的格式。在该实施例中,从任何克隆的客户机设备发送的第一个消息与源自可信的或真实客户机设备的第一个消息具有相同的隐蔽标识符,即,0,0。如果此消息是由服务器在真实客户机设备已经确认源自服务器的新的 TOD 值之前接收到,则服务器仍没有办法知道存在克隆的客户机设备。如果它是在最初请求 BKEY 的同一个客户机设备已经确认了新的 TOD 值之后接收到的,则服务器知道在系统上有两个使用相同的凭证的客户机设备,并生成克隆检测报告,如图 4 所示。

[0091] 在图 5A 和 5B 的示例中,在真实客户机设备已经确认从服务器收到新的 TOD 值之前,克隆的客户机设备向服务器发送第一个 BKEY 请求。在接收到 BKEY 请求时,服务器提取隐蔽数据值 0,0,并将这些数值与为具有相同凭证的真实客户机设备存储的隐蔽数据值进行比较(步骤 124)。此时,发现了隐蔽数据匹配(步骤 125),即,接收到的隐蔽数据是正确的,因为还没有从客户机设备接收到收到 NotAckedTODT1(例如,8437)的特定确认。在此特定示例中,服务器不知道是否由于某种原因(如网络故障或客户机设备被关闭)是否客户机设备决不会接收到包含 TOD 消息,因此不会认为有任何克隆的设备存在。服务器数据库包含 TOD 的最后一个已知的好数值(在该情况下,0)加上最后一个未确认的 TOD 值 T1。由于确认的数值是一个匹配项,服务器在应答消息中(在一个实施例中,可以具有图 6D 中所示出的格式)向克隆的客户机设备发送具有新的 TOD 值 T2 的广播密钥(步骤 126)。在上面的表 2 中提供的特定示例中,值 T2 是 9902。同时,在步骤 30 中,服务器上的 NotAcked TOD 变为 T2(或在该示例中,9902),如图 5B 所示,消除了以前存储的 NotAckedTODT1(或表 2 的示例中的 8437)。

[0092] 克隆的客户机从服务器接收 BKEY 消息以及消息中的新的 TOD 值 T2,并保存新的 TOD 值 T2(步骤 132),并继续对从服务器接收到的诸如广播数据之类的数据进行解密(步骤 133)。在图 5B 中所示出的示例中,在步骤 132 之后与服务器的下一次通信是从请求广播密钥(BKEY 请求)的真实客户机设备发送的消息,因为真实客户机设备需要续订其 BKEY(步骤 134)。此消息可以具有图 6E 中所示出的格式,并包含隐蔽标识符,该隐蔽标识符包括当前存储在真实客户机设备上的隐蔽数据值,具体地说,来自此客户机设备的最后一个 BKEY 请求的 TOD(T1 或 8437),以及瞬时密钥更新编号(在该示例中为 0)。在步骤 135 中,服务器从真实客户机设备接收新的 BKEY 消息,将当前存储的 Acked 和 NotAcked TOD 值(具体地说,0 和 T2 或 9902)与在源自客户机设备的隐蔽标识符中接收到的 TOD 值 T1 或 8437 进行比较。由于从客户机设备接收到的数值 T1 不等于存储在服务器上的 Acked 值 0 或者存储在服务器上的 NotAcked 值 T2(步骤 136),因此,服务器向系统操作员报告克隆检测情况,以便采取进一步的行动(步骤 138)。可以在此时进行其他服务器端处理,以检测克隆设备。服务器不会拒绝服务,因为它不能确定发送消息的两个客户机设备中的哪一个是真实的或可信的客户机设备,因此,在应答消息中向真实客户机设备发送 BKEY 和新的 TOD

值 T3(上面的表 2 的示例中的 11305)(步骤 140), 该应答消息可以具有图 6F 中所示出的格式。然后, 服务器将新的 TOD 值 T3 作为 NotAcked 值存储在服务器数据库中(步骤 142), 并且真实客户机设备也存储新的 TODT3。

[0093] 图 5A 和 5B 的方法示出了一种可能的方法以及事件序列, 其中在真实客户机设备从服务器接收到其第一个 BKEY 之后, 但是在真实客户机设备从服务器请求续订的 BKEY 之前, 克隆的客户机设备向服务器发送一个消息。这样的事件可以以不同的顺序发生, 取决于真正的以及克隆的客户机设备的使用情况, 在相同的时间段, 可能有两个以上的具有相同凭证的客户机设备向服务器发送消息。克隆客户机设备可以在任何时间并以相对于从真实客户机设备发送的类似消息的任何顺序向服务器发送消息。不管顺序如何, 服务器都可以确定克隆的客户机设备的存在, 因为来自真实客户机设备或者一个或多个克隆客户机设备的消息中的隐蔽数据值不匹配服务器上的一个或多个当前存储的数值。例如, 参考图 5A 和表 2 的步骤 122, 在克隆的客户机设备发送任何消息之前, 如果在此阶段真实客户机设备向服务器发送连续的 BKEY 请求, 那么, 在表 2 的特定示例中, BKEY 请求中的隐蔽数据值是 T1、0 或 8437、0。接收到此消息的服务器注意到来自客户机设备的 TOD 值和保存在其数据库中的 notAcked TOD 之间的匹配, 并将 Acked TOD 从 0 改变为 T1。然后, 在应答中将新的 notAcked TODT2 发送到客户机设备中。随后与服务器进行通信的克隆的客户机设备发送 $TOD = 0$, 因为它是从该设备到服务器的第一次通信。该 TOD 不匹配存储在服务器上的 Acked TOD(T1) 或者 NotAcked TOD(T2), 并由服务器生成克隆检测报告。当有一个以上的使用相同凭证的客户机设备与服务器进行通信时, 在任何消息顺序中的某个点会发生类似的匹配故障, 不管服务器与真实客户机设备和克隆的客户机设备之间的通信的顺序如何。

[0094] 在图 5 和 6 的实施例, 以及上面的表 2 中概述的该实施例的特定示例中, 每一个消息中的隐蔽标识符都包括两个或更多隐蔽数据值。然而, 隐蔽标识符可以包括基于这样的隐蔽数据值生成的代码, 例如, 通过使用散列函数等等, 对这些数值进行转换。在上面的实施例中, 包含隐蔽标识符的消息是广播密钥请求, 而客户机设备从服务器接收广播。在该情况下, 客户机设备是诸如电视机机顶盒、个人计算机之类的媒体播放器, 或能够播放诸如电视广播之类的广播的任何其他客户机设备。服务器可以是向客户机分发广播电视频道解密密钥的服务器。然而, 其他类型的客户机设备和服务提供商可以在不同类型的的消息中使用相同的隐蔽数据技术。正如上文所指出的那样, 上面的实施例的隐蔽数据技术可以应用于任何类型的网络服务提供商和链接到服务提供商的服务器的任何类型的客户机设备, 如个人计算机、蜂窝电话、个人数字助理 (PDA)、视频设备 (TIVO、DVD、CD 等等), 以及任何其他类型的客户机设备, 并用于任何类型的服务, 如网上银行、电子商务、数据日志记录、消息通信系统等等。在上面的实施例中, 广播电视频道解密密钥 (BKEY) 是对加密的广播电视频道进行解密所需的密钥, 如通常用于诸如 Home Box Office (HBO) 或 MovieChannel1 的收费电视频道的那样。收费电视频道是有线电视或因特网协议 (IP) TV 用户可以选择购买的可选频道。这里所描述的技术也适用于那些密钥被分发给客户机设备以允许对各种网络服务进行接入的任何加密技术, 或者, 也可以用于服务器和客户机设备之间的不同类型的消息中, 除解密密钥请求消息之外, 或代替解密密钥请求消息。

[0095] 因为存在着在接收到消息响应之前由于网络故障或由于客户机设备被关闭, 导致真实客户机设备不会从服务器接收到消息的可能性, 因此, 图 5A 和 5B 的实施例可以包括服

务器侧处理,以降低生成的假的克隆检测警告的数量,从而,克隆检测警告是已经检测到具有与另一个客户机相同的客户机凭证的客户机的指示。在一个替代实施例中,如上文所提及的,每当更新隐蔽标识符中所使用的隐蔽数据项时,都会从客户机设备发送一个引伸的客户机确认,而服务器基于源自客户机的关于服务器提供的隐蔽数据项已经被成功地接收到并且被客户机存储的确认,协调服务器数据库中的预计的隐蔽数据项。通过使用客户机和服务器之间的表示源自服务器的隐蔽数据令牌已经被客户机存储,或者客户机隐蔽数据项已经被服务器确认的直接确认消息,可以改善克隆的检测,但是,产生了由服务器处理的并且会被黑客截取的附加消息。

[0096] 在一个实施例中,服务器向客户机设备发送唯一隐蔽数据项或令牌,以便用于连续的消息中。服务器可以发送到客户机设备的数据项或数值的示例包括当客户机和服务器进行通信时由服务器定期改变的临时数据值,从客户机发送到服务器的临时密钥等等。在一个实施例中,服务器将临时或瞬时加密 / 解密密钥发送到客户机,瞬时密钥变为在对客户机和服务器之间的消息进行加密时所使用的密钥环的一部分。通过使用瞬时密钥,可以防止克隆的客户机与服务器进行通信,因为只有一个客户机包含适当密钥,用以在客户机和服务器之间实现加密的通信。瞬时密钥可以通过基于会话的加密的通信信道发送,如通过 SSL 提供的或通过 Diffie Hellman 类型的密钥交换所提供的,如此,包含由服务器所提供的已更新的瞬时密钥不能被获得了相同瞬时密钥更新消息的克隆设备进行解密。这样的基于会话的加密可以用于任何类型的通信。在一个实施例中,服务器向客户机设备发送一个令牌或多个令牌,这些令牌被客户机设备存储起来,并用于随后的客户机与服务器之间传送的消息中。服务器可以在随机的时间或每隔固定的时间间隔向客户机设备提供唯一的令牌。

[0097] 在表 2 的示例中,示出了两个隐蔽数据值。然而,一个、两个或更多隐蔽数据值可以与由服务器唯一地提供的数值一起使用,和 / 或与客户机基于客户机设备的操作唯一地确定的数值一起使用。在一个实施例中,客户机设备中的隐蔽数据模块 29 可以包括非易失性存储器,隐蔽数据的某些部分或全部可以本地存储在客户机设备上的非易失性存储器(硬盘、闪存等等)中。真实的和克隆的客户机设备的接通电源的顺序,或者它们连接到网络的顺序,或者它们与服务器进行第一次连接的顺序并不重要,上文所描述的技术不需要客户机设备以任何顺序通电。如此,图 5A 和 5B 中的第一个通电的客户机设备可能是克隆的客户机设备而不是真实客户机设备,而真实的和克隆的客户机设备可以以任何顺序和在任何时间与服务器进行通信。不管消息的顺序如何,该实施例都允许服务器当接收到其中的隐蔽数据值不匹配服务器上的隐蔽数据值的消息(表明真实客户机设备已经被克隆)时,确定何时有一个以上的使用相同客户机凭证的客户机设备。

[0098] 图 5A 和 5B 示出了使用从服务器发送到客户机设备的以来自客户机设备的最后一个请求的时刻(TOD)的形式存在的单一隐蔽数据项的隐蔽克隆检测过程。在替代实施例中,可以使用一个或多个隐蔽触发器。隐蔽触发器是在发生了若干个事件之后产生的触发器,它们通过修改用于产生隐蔽标识符的隐蔽数据,或提供可以被服务器跟踪的新的隐蔽数据来作出响应。在客户机设备的正常操作中有很多可能的隐蔽触发器,隐蔽触发器或事件可以基于多种事件类别,如时间(客户机设备处于活动状态的总小时数,在安装或更新客户机设备之后的随机小时数),消息(接收到的视频授权控制消息或 ECM 的总数,总的信

道更换次数),或内部数据处理(例如,对第100,000个视频数据分组进行解密时的TOD)。隐蔽触发器的其他示例包括,当诸如机顶盒(STB)之类的客户机设备转换信道100或200次时发生的触发器,或当发生一定数量的客户机事件时发生的触发器,当触发器发生时,触发器会保存客户机时刻(或其他参数)。另一个示例是接收到的第15000个ECM数据分组的实际值,或当接收到的第15000个ECM数据分组时的时刻(TOD)或两个数据值的散列。触发产生隐蔽数据值的事件在具有相同的凭证的两个客户机设备上(可信的/真实的和克隆的客户机设备)是以不同速率发生的,以致可信的或真实客户机设备和克隆的客户机设备具有不同的隐蔽数据,因此具有不同的隐蔽标识符。隐蔽标识符在服务器侧使用,以检测在网络上运行的多个客户机。

[0099] 在一个实施例中,保存的隐蔽值的客户机库被定期变为保存新的或不同的隐蔽数据值,而这些隐蔽数据值又用以生成隐蔽标识符。如此,可能已经获得了一个客户机库的黑客不知道创建隐蔽标识符中所使用的隐蔽数据值的新的事件可能发生在客户机库已经更新之后。黑客需要使所有克隆的客户机设备与网络断开,以避免客户机库软件更新之后的检测,以便尝试确定哪些隐蔽触发器被编程到客户机库中,何时发生触发器,以及响应触发器,哪些隐蔽数据存储在客户机库中。这样的更新可以由服务器生成,并可以使用客户机设备内包含的安全处理功能。可以使用用于更新客户机库的客户机固件下载方法,对代码图像进行数字签名,以使客户机对下载内容进行验证。前端软件可以具有应用程序编程接口(API)功能或用于下载客户机软件的数据轮播接口。

[0100] 在一个实施例中,隐蔽标识符包含对于若干个请求可以是静态的数据,然后,用于生成隐蔽标识符的隐蔽数据基于隐蔽触发器而变化,或者,某一类型的每个消息的隐蔽标识符都变化,如以前的消息请求的时刻或TOD。隐蔽标识符中所使用的隐蔽数据可以在客户机设备内产生,或者作为消息收发的一部分从服务器发送,或者,也可以是客户机/服务器数据的组合。隐蔽标识符可以包括由客户机或服务器处理的数据,如将当前隐蔽数据值应用到数学转换或加密散列。

[0101] 在一个实施例中,隐蔽标识符中所使用的隐蔽数据值也可以基于服务器以若干种不同方式中的一种对请求作出响应而变化。在一个示例中,头10个广播密钥请求接收隐蔽数据一个值,而10之外的连续的请求接收到不同的响应,其中隐蔽数据已变化或加扰或两种情况都有。变化可以在客户机上产生或在服务器端产生,或两种情况都有。隐蔽标识符作为在正常的系统处理过程中处理的正常消息的一部分,包含在消息斑点(blob)或字段中,消息斑点可以在客户机软件的两个不同的代码版本之间有所不同。此外,消息斑点还可以具有作为数据白化剂应用的无意义的随机数据。在一个实施例中,数据斑点具有三个到五个隐蔽数据值,隐蔽数据值基于在不同的时间发生的不同的事件或触发器而变化。

[0102] 在上文参考图5和6所描述的实施例中,在广播密钥请求消息等等中提供了基于消息的时刻的隐蔽标识符。下面的表3示出了在包括移动电话的客户机设备中创建的转换后的隐蔽标识符的示例。

[0103] 表3-移动电话隐蔽标识符

[0104]

	真实的电话			克隆1			克隆2		
手机ID (ESN)	100-4452			100-4452			100-4452		
呼叫日志	#	TOD	时长	#	TOD	时长	#	TOD	时长
	N1	8:22	1:06	N3	23:45	7:45	N5	16:41	3:16
	N2	9:11	0:23	N4	1:02	3:36	N6	21:42	10:44
隐蔽标识符	391740			457492			112208		

[0105] 在表 3 中,一个电话是真实的,而其他两个是克隆,每一个电话都基于电话的操作创建了隐蔽标识符。在上面的示例中,只使用头两个呼叫项来生成唯一隐蔽标识符 (ID)。利用加密散列型函数,处理每一个电话的呼叫日志,生成每一个电话的唯一隐蔽 ID,导致每一个电话所特有的标识符,甚至对于完全克隆的电话也是如此。因为电话是在制造时克隆的,随着时间的推移,使用每一个电话的方式也稍微不同,因此,隐蔽标识符非常难以复制,即使电话的所有者尝试创建相同的呼叫日志来生成相同的隐蔽标识符。这是因为需要获取微秒相同的事件,才能创建完全相同的呼叫日志,在现实世界的设备中是不可能的。

[0106] 客户机和服务器之间的隐蔽标识符可以是加密的,以便增强安全性,加密密钥在客户机之间是唯一的,但是,在其他实施例中隐蔽标识符可以是非加密的隐蔽数据值。在某些实施例中,也可以在客户机和服务器之间实现无密钥的安全性,只使用隐蔽数据值或基于这样的数值的隐蔽标识符来标识客户机设备。然而,当客户机 / 服务器通信被加密时,安全性增强。隐蔽数据或隐蔽标识符可以以多种方式使用,以在操作上标识客户机,无需使用一对加密密钥。事实上,上文所描述的隐蔽数据方案可以在所有消息事务中使用,在系统中不需要安全性特定的消息。这意味着,这里所描述的隐蔽数据技术可以用以增强对客户机的验证,可以使用或不使用诸如 X.509 证书之类的安全性凭证、加密密钥,以及类似的安全性特定的密钥。在一个实施例中,在不需要加密特定的密钥的情况下,客户机和服务器之间的,或两个计算机设备之间的所有通信都可以通过这里所描述的技术来增强。实施例可以适用于在系统中运行的软件和固件的所有类型,包括应用软件、系统中间件、记帐软件,任何类型的电子商务交易、任何类型的客户机 / 服务器通信,以及客户机和服务器之间的或在客户机需要被标识的情况下任何类型的消息收发。

[0107] 在一个实施例中,隐蔽安全性数据可以用以在对于客户机设备和网站或服务器之间的通信不使用安全性或加密的系统中提供无密钥的安全性,并可以进行克隆的客户机设备检测。图 7 的流程图中示出了该实施例。在第一个步骤 150 中,客户机设备与网站或服务器接触,以注册服务。在注册过程中,客户机设备向服务器发送唯一地标识该客户机设备的初始隐蔽标识符 (步骤 152)。该实施例中的隐蔽标识符包括隐蔽数据值的系列,但是在其他实施例中也可以包括这样的数值的转换后的版本。隐蔽标识符中所使用的初始隐蔽数据值可以是任何客户机设备特定的数据,包括难以克隆的这里所描述的隐蔽数据。当进行注册时,客户机可以发送有点难以克隆的客户机信息作为隐蔽标识符,如中央处理单元 (CPU) 序列号 (如果可用的话),磁盘驱动器卷 ID,或其他硬件特定的信息。注册过程本身可以在服务器端或客户机创建更加难以克隆的新的隐蔽数据值,如在 CPU 或计算机硬件设备中的

一个或多个寄存器的数据,发送的消息和由客户机接收到的响应之间的以纳秒为单位的时间延迟,存储器的一部分的校验和或 crc 值,等等。在注册过程中,由客户机设备和服务器捕获和存储初始隐蔽数据的集合或表(步骤 154)。此时,隐蔽数据是注册的客户机设备所特有的,客户机 - 服务器通信是使用基于此数据的隐蔽标识符进行的,以验证客户机设备(步骤 155)。在该情况下,用于检测克隆的客户机设备的方法如图 4 所示。如果服务器接收到声称来自于注册的客户机设备的通信但是没有匹配存储在服务器上的该客户机设备的初始隐蔽数据值的隐蔽数据值,则由服务器生成克隆的设备检测报告。

[0108] 因为黑客可能能够入侵到系统中,并获得初始的隐蔽数据值的集合,或基于该数据的隐蔽标识符(进行了转换),随着客户机设备的继续运行,基于操作特征创建新的隐蔽数据(步骤 156)。新的隐蔽数据被添加到服务器和客户机设备之间的连续通信中的初始的隐蔽数据值的集合中(步骤 158),新的隐蔽数据值被添加到服务器和客户机设备上的该客户机设备的以前存储的隐蔽数据值中(步骤 160)。可以通过定时的事件或计数的事件,创建新的隐蔽数据,添加在注册之后创建的附加的隐蔽数据,以标识客户机。可选地,服务器可以在消息收发过程中的各种时间创建隐蔽数据,并将隐蔽数据提供到客户机设备,给客户机设备提供对于此客户机设备唯一的附加的隐蔽数据。随着客户机设备继续运行,继续添加新的隐蔽数据,以致于没有用于任何延长的时间周期的静态的隐蔽数据集,使得黑客入侵和克隆难得多。在任何阶段,如果在从声称是真实客户机设备接收到的消息中的隐蔽数据不匹配为该客户机设备在服务器上存储的当前的隐蔽数据集合,则生成克隆检测报告。

[0109] 图 7 的方法允许没有安全措施的系统基于不能容易地被黑客获取的隐蔽数据创建客户机唯一标识符。对于某些应用,隐蔽数据技术独自就可以提供适当的安全性,或者,可以将隐蔽数据技术添加到那些客户机 / 服务器的消息收发是使用最佳类型的加密技术(利用这里所描述的隐蔽数据方法增强)来保证安全的系统中,例如,如参考图 5 和 6 以及表 2 所描述的。

[0110] 当也使用加密密钥对计算机设备之间的消息进行加密或使用密钥来安全地标识网络上的计算机时,上文所描述的隐蔽数据技术可以用以提高安全性。当创建了克隆客户机设备时,克隆的设备与经过授权的可信的或真实客户机设备具有相同的密钥,并可以对在经过授权的可信的真实客户机设备和服务器之间发送的所有消息进行解密。然而,在操作上,随着时间的推移,真实客户机设备和克隆的客户机设备执行某些功能的方式是不同的,或具有不同的操作计数器值(处理的 ECM 的数量、发生第 10 次信道更换时的时刻,等等),以致如上所述,真实客户机设备和克隆的客户机设备生成的隐蔽数据是不同的。

[0111] 在很多情况下,隐蔽数据的实际值不重要,而重要的是,当与可信客户机设备的克隆副本相比时,诸如机顶盒之类的客户机设备的操作行为在正常操作条件下是不同的。这意味着,该隐蔽数据值在客户机之间是不同的,甚至当客户机设备具有与真实客户机设备相同的克隆客户机凭证时也是如此。在某些实施例中,这些操作差异用以检测可信客户机设备和克隆客户机设备之间的不同的隐蔽数据值或基于这样的数值的隐蔽标识符,上面利用图 5 和 6 以及表 2 说明了这样的方法的一个实施例。此外,隐蔽数据值还可以是“计数器值”,利用定标因数,赋予这些“计数器值”权重,要求客户机设备在值变化之前操作一段时间内,如此,提供了在几天、几个星期或几个月的操作时间内,固定在单一值的数据值。在一

个实施例中,一个或多个隐蔽数据值被用作在客户机设备和服务器之间的消息收发中的隐蔽标识符。在一个实施例中,一个以上的隐蔽数据值和导致各种隐蔽数据值以不同速率变化的不同阈值或触发器一起使用。下面的表 4 示出了叫做“GetKey Message”的消息中的三个隐蔽数据值或项的示例,以及隐蔽数据项随着时间的变化。

[0112] 图 5A 和 5B 以及表 2 的实施例使用了广播密钥或 BKEY 来发送隐蔽数据值,下面在表 4 中所描述的针对 Get Key Message 的相同技术可以用于广播密钥或 BKEY 请求示例中或在客户机设备和服务器之间所使用的任何其他消息中。还要注意,隐蔽数据项或数值可以在客户机设备上,在服务器上,或者同时在两者上始发,隐蔽数据值可以是通过处理数据值(如通过使用散列函数,或播种随机数值,或者对被用作隐蔽数据方案的一部分的数据值执行转换)而获得的结果。

[0113] 表 4Get Key Message(GKM) 和随着时间的隐蔽数据

[0114]

消息字段	上电复位之后的 GKM 消息	2 天之后的 GKM 消息	在计数器 1 触发器之后的 GKM 消息	1 星期之后的 GKM 消息	9 天之后的 GKM 消息	2 星期之后的 GKM 消息	3 星期之后的 GKM 消息
GKM 消息 ID	1	1	1	1	1	1	1
隐蔽数据项 1	0	0	0	0	0	31	31
隐蔽数据项 2	0	0	0	0	88359	88359	88359
隐蔽数据项 3	0	0	7190	7190	7190 的平方	7190 的平方	7190 的平方

[0115] 上面的表 4 中的示例示出了 Get Key Message(GKM) 中的三个隐蔽数据值或项 1、2、3 如何随着时间而变化。上面的表中的作为 T 的数值所示出的 GKM 消息 ID 将消息标识为 Get Key Message。可以预见的是,在每一个固件修订之后,为诸如获得密钥请求之类的功能(或诸如电子商务交易或其他交易之类的任何其他事件),作为客户机/服务器通信的一部分发送的隐蔽标识符包含不同于以前的固件版本的隐蔽数据项,使以前的固件黑客攻击在系统上无用。在上面的示例中,隐蔽数据项是在客户机设备或服务器上生成的不同的操作值,可以是上文所描述的可能的隐蔽数据项或数值中的任何一个,或从客户机设备的操作得到的任何其他唯一数据。如果服务器在任何时间接收到不匹配为特定客户机设备存储的当前 GKM 消息的 GKM 消息,则它生成克隆的客户机设备检测报告。

[0116] 在上面的示例中,Get Key Message 的消息 ID 不需要变化,被视为静态消息 ID 值,以表示在客户机和服务器之间传递的若干个消息类型中的一个。然而,消息 ID 可以在不同的客户机固件版本之间变化,当实现了客户机固件更新时,黑客将需要很大力气对新消息

ID 进行反向工程。在消息 ID 中可以包含固件修订号，以允许服务器与不同的客户机固件版本协同工作。

[0117] 在一个实施例中，为各种固件版本收集的隐蔽数据项在不同的版本之间是不同的。下面的表 5 示出了三个不同的固件版本的可能的隐蔽数据字段的实施例。该表示出了版本号为 1.0、1.1 和 1.2 的三个不同的固件版本的三个隐蔽数据字段的内容，例如，在一年的时期内产生各种版本。客户机设备和服务器之间的，或服务器和客户机设备之间的，或同时在两者之间的消息中的隐蔽标识符包括三个隐蔽数据项，隐蔽数据项的特征取决于所使用的当前固件版本。该表沿着每一列向下读而被读取。固件的版本 1.0 的三个隐蔽数据项是来自服务器的第四消息令牌，定标的 ECM 数据分组计数，以及接收到的特定类型的第三消息的时刻。在版本 1.1 中，这些项变为客户机设备已经运行的总小时数的定标后的计数，在发往服务器的特定类型的第六消息之后从服务器接收到的令牌，以及当由客户机设备接收到特定类型的第 10000 个消息时的时刻。在版本 1.2 中，所有三个隐蔽数据项再次发生变化，隐蔽数据项 2 变为零，其他隐蔽数据项变为当接收到特定类型的第 150 个消息时的时刻，在安装新的固件当天在 8:37pm 客户机设备被调谐到的信道号的数值。

[0118] 表 5 不同的固件版本中的隐蔽数据值的示例

[0119]

消息中的隐蔽数据项编号	版本 1.0 中的隐蔽数据的数值	版本 1.1 中的隐蔽数据的数值	版本 1.2 中的隐蔽数据的数值
1	在发往服务器的第四消息之后从服务器接收到的令牌	客户机设备已经运行的总小时数的定标的计数	当接收到特定类型的第 150 个消息时的时刻
2	接收到的 ECM 数据分组的定标的计数	在发往服务器的第六个消息之后从服务器接收到的令牌	始终设置为 0，永不变化
3	当接收到特定类型的第三个消息时的时刻	当接收到特定类型的第 10,000 个消息时的时刻	客户机在 8:37 被调谐到的信道号的数值

[0120] 在一个实施例中，用于任何单一固件版本的隐蔽数据项也可以在预定时间或响应预定的触发器而改变。例如，假设在 3 月份发布了代码的某一修订本，并加载到客户机设备上。对于加载修订本之后的头两个月，隐蔽数据项 2 是更新固件时的时刻。然后，在超过两个月之后，隐蔽数据项 2 变为由服务器所提供的数据值。然后，在此固件版本操作四个月之后，数据项 2 在加载该修订本的四个月之际变为客户机设备上的芯片中包含的注册值。在该实施例中，在头四个月的操作过程中，隐蔽数据项的数值变化三次，以便黑客更加难以成功地运行客户机设备的克隆。当预先存储的隐蔽数据项的数值在特定时间变化时，服务器察觉到该时期，并适当地调节其数据库。例如，假设在操作 90 天之后客户机库被设计为生成全新的隐蔽数据表或矩阵，那么，服务器察觉到在使用 90 天之后客户机会报告新的隐蔽数据。事实上，甚至使克隆设备同步以清空它们的旧隐蔽数据表并同时刷新为新的数据，会

给黑客带来逻辑问题,特别是当黑客可能不会预想到隐蔽数据值要发生变化。

[0121] 通过客户机设备操作、与客户机设备进行通信的服务器或两者,生成多个不同的可能隐蔽数据项和隐蔽数据触发器,可以用以在上文所描述的实施例中生成向消息添加的客户机标识符。一个或多个隐蔽数据项可以是由服务器作为消息响应的一部分向客户机设备提供的令牌或时间,服务器提供的数据项被客户机设备在稍后的时间返回到服务器(可以在客户机设备的下一个请求中),例如,如上文参考图5和6和表2所描述的。这就使得服务器生成被用作识别克隆的隐蔽数据的令牌。隐蔽数据也可以是由客户机设备处理的消息的数量或由客户机设备向消息日志中或消息队列中写入的消息的数量的计数,或第10次对客户机API函数的API调用的数值,或其他类似的通常将在甚至具有相同的凭证的客户机设备之间变化的事件。

[0122] 在很多情况下,客户机设备可能不知道或者甚至关心隐蔽数据的含义是什么,因为它是在服务器侧用以检测克隆的信息,或者它是由服务器所提供的用于检测克隆的信息。在一个实施例中,一些隐蔽数据值是基于一次性的事件生成的,如在新的客户机设备操作了特定时间段(例如,操作了23:49:33(小时:分钟:秒))之后客户机设备被客户机设备调谐到什么信道。其他的隐蔽数据值可以使用网络或系统操作值来生成,如电缆调制解调器范围参数、DHCP租用时间等等。还有其他的隐蔽数据值可以由服务器提供。其他隐蔽数据值还可以通过客户机设备和服务器之间的消息收发或在产品的环境中通常发现的其他参数来产生。例如,PC可以具有与无线电话不同的隐蔽数据值。

[0123] 使用由如上面的实施例所描述的客户机设备操作事件生成的隐蔽数据的安全系统还可以被设计为包括用户授权续订过程,要么当系统检测到克隆的或盗版的客户机设备时或由于其他理由而怀疑时,或以预定的时间间隔,不管是否怀疑的克隆客户机设备。图8示出了双向网络或具有返回信道的单向网络的续订过程的实施例。任何形式的永久的或不持久的(偶尔可用的)返回信道,如偶尔的拨号调制解调器连接,或当移动电话连接到诸如STB之类的客户机设备时形成的返回信道,都可以用于续订,如图8中那样。类似的处理也可以用于没有返回信道的单向网络上,图9的流程图示出了这样的处理过程的一个实施例。

[0124] 图8的过程可以用于与双向网络有关或具有返回信道的单向网络有关的续订过程中。如图8所示出的,由服务器通过网络向单个的客户机(在双向网络上)或向所有客户机设备(在单向网络上)发送对于隐蔽标识符的请求。服务器向客户机发送续订消息(181)。假设有返回信道可用(182),客户机设备被编程为通过向服务器发回当前隐蔽标识符来作出响应(步骤184)。如果返回信道不可用(即,客户机设备在没有返回信道的单向网络上操作),过程如图9所示出的那样持续,下面将比较详细地对其进行描述。

[0125] 在步骤184中为具有返回信道的网络发回的隐蔽数据标识符基于由特定客户机设备收集的隐蔽数据,而隐蔽数据又与该客户机设备上的操作事件关联。由于在每一个客户机设备中隐蔽标识符刚刚被更新,黑客必须重新开始他们的入侵以查找紧随在步骤179中接收更新代码之后真实客户机设备的隐蔽标识符,并试图复制任何克隆设备中的隐蔽标识符。这样的黑客入侵企图不太可能在包含每一个客户机设备的隐蔽标识符的响应在步骤184中从每一个客户机设备自动地发回之前来得及复制隐蔽标识符。在一个实施例中,隐蔽数据标识符是从收集到的隐蔽数据值生成的八位代码,并且不包含与用户相关的行为

信息或与隐私相关的信息。然而，在替代实施例中，可以生成基于隐蔽数据值的其他代码。然后，服务器确定是否接收到具有相同客户机标识符但是隐蔽数据不同的一个以上的响应（步骤 185）。如果只接收到一个响应，则由服务器创建基于从客户机设备接收到的隐蔽标识符的续订解锁代码（步骤 186），并传输到客户机设备（步骤 188）。如果只接收到一个响应，最有可能在网络上没有真实客户机设备的克隆，真实客户机设备对续订代码进行解锁，并续订为其提供的服务。然而，如果由于某种原因真实客户机设备没有发送响应，或者克隆的客户机设备没有发送响应，则一个以上的客户机设备可能仍会接收到续订解锁代码，因为此代码被广播到在相同客户机标识符或凭证下工作的所有客户机设备。只有具有相同隐蔽数据标识符的客户机设备才能够对续订代码进行解锁，并通过网络为其续订服务。使用同一个客户机标识符的任何其他客户机设备不能够对续订代码进行解锁，并被阻止接收服务。如果被续订的客户机设备实际是克隆，则真实的用户会被阻止，并呼叫服务提供商，提出投诉。在该情况下，克隆的设备被阻止，给真实用户的客户机设备的服务被续订。图 8 中未显示的步骤 181 之前的可选步骤将是向客户机发送隐蔽标识符更新消息，让客户机此时获取再一个新的隐蔽数据值，并将它添加到在步骤 184 中返回的隐蔽数据表中。然后，接收到该消息的每一个客户机设备都为捕获的隐蔽数据的特定段，基于特定设备的当前操作特征，更新隐蔽标识符。

[0126] 如果在步骤 185 中接收到一个以上的带有隐蔽标识符的客户机设备响应，则识别真实客户机设备（步骤 189）。步骤 189 中的真实客户机设备的识别可以包括如 2006 年 7 月 20 日申请的共同待审的申请系列号 No. 11/489, 779 所描述的网络用户身份验证方法，该专利申请的全部内容作为参考包含于此。在此方法中，合法用户与客户机设备的物理连接的位置关联，在步骤 189 中对网络进行探测，以确定哪一个客户机设备位于合法用户的正确的物理网络位置。当定位了正确的或真实客户机设备时，在步骤 190 中创建基于从该客户机设备接收到的隐蔽数据的续订解锁代码，并在步骤 192 中通过网络广播到单向网络上的具有相同客户机标识符的所有客户机设备，并唯一地递送到双向网络上的客户机。到所有这样的客户机设备的服务被阻止，只有真实客户机设备才能够对续订代码进行解锁，并续订服务。

[0127] 如果服务提供商没有基于真实客户机设备的物理位置或物理连接标识符的验证过程，则可以通过其他技术，如让服务运营商呼叫用户以及让用户查找真实客户机设备上的隐蔽标识符，并以 SMS 消息或通过电话向服务提供商提供该标识符，定位真实客户机设备。

[0128] 图 9 示出了可以用于客户机设备在没有返回信道的单向网络上与隐蔽数据安全系统的连接中的周期性的续订过程中的步骤。此续订过程使用与图 8 中所示出的相同的初始步骤 179、180 和 181。然而，响应于服务代码续订消息，客户机设备上的中央处理器被编程为在客户机设备的屏幕上显示服务代码或续订消息（步骤 193）。此消息包括客户机标识符和从隐蔽数据存储模块 29 中检索到的当前隐蔽标识符。客户机设备的客户机标识符，对于真实客户机设备和克隆客户机设备来说是相同的，但是，对于每一个客户机设备，存储在客户机设备上的当前隐蔽标识符是不同的。服务代码消息包括让用户向显示在屏幕上的电话号码发送两个 ID，电话号码可以是服务提供商的 800 号码。

[0129] 在步骤 194 中，客户机设备的用户向服务提供商提供客户机标识符和隐蔽数据

ID, 作为发往屏幕上的电话号码的 SMS 消息, 或者通过发往服务提供商的操作员的语音电话呼叫。在此阶段, 服务提供商可以基于存储在服务器上的个人信息或安全信息, 如合法用户的电话号码, 确定消息的发件人或呼叫者是否是合法用户。如果确定呼叫者是合法用户, 则服务器或服务提供商在步骤 195 中基于从用户接收到的唯一隐蔽数据 ID, 生成续订解锁代码, 并将续订解锁代码发送或广播到网络上具有相同客户机标识符的所有客户机设备(步骤 196)。如果接收到该代码的客户机设备能够正确地处理解锁代码(步骤 197), 则对于该设备, 续订服务(198)。如果接收到该代码的客户机设备不能正确地处理该解锁代码, 因为存储在该客户机设备上的隐蔽数据不匹配解锁代码中的隐蔽数据, 对该客户机设备的服务被阻止(步骤 199)。如果系统不正确地确定被请求消息的呼叫者或发件人是合法用户, 而用户实际使用的是克隆设备, 以致真实客户机设备不能处理续订解锁代码, 被授权的用户呼叫服务提供商, 因为它们的服务已经被阻止。然后, 可以基于真实客户机设备上的隐蔽数据, 生成进一步的续订解锁代码, 并广播到客户机设备, 以便阻止以前续订的设备, 为真实客户机设备续订服务。

[0130] 上文参考图 8 和 9 所描述的续订过程可以以预定的时间间隔, 或当怀疑网络上存在一个或多个克隆客户机设备, 或同时出现两种情况时进行。如图 8 和 9 所描述的续订过程可以使用隐蔽数据表的任何一部分或隐蔽数据表的多段来生成客户机设备特定的解锁代码, 从而, 具有不同隐蔽数据值的克隆客户机不能够生成适当的密钥用以对解锁代码进行解密。Diffie Hellman 是这样的客户机特定的密钥管理方案的示例。也可以使用其他类型的密钥交换机制。例如, 通过使用 Diffie Hellman, 隐蔽数据(任何数据或全部数据)被用作用于生成客户机侧唯一密钥的播种机制的一部分, 或用于提供服务器侧兼容的密钥的数据的一部分, 以便具有不同隐蔽数据值的克隆客户机不能在其他克隆设备之间生成相同的唯一密钥对(Diffie Hellman 密钥对)。可以实现续订过程的另一种方式是通过让服务器使用以已知方式为客户机接收到的隐蔽数据, 以便以诸如 Diffie Hellman 的算法播种或生成共享的成对的密钥, 本质上, 生成只能由包含适当的隐蔽数据的客户机重新创建的唯一密钥对。进行客户机设备续订的另一种可选方法是使用隐蔽数据的一部分, 作为加密/解密密钥数据, 因为每一个客户机都具有唯一隐蔽数据, 该唯一隐蔽数据对服务器是已知的。隐蔽数据的片段或全部或隐蔽数据的散列后的或转换后的版本可以应用于生成加密/解密密钥数据或用于利用诸如 Diffie Hellman 的算法生成共享的密钥的密钥或种子数据或因子。还可以预期, 隐蔽数据可以用以加扰或转换在客户机和服务器之间, 或在续订过程中在服务器和客户机之间发送的密钥种子或密钥因子数据。例如, 隐蔽数据可以被客户机散列, 然后被用作当对发送到服务器的数据进行加密时的密钥。并且, 因为服务器知道隐蔽数据, 因此, 服务器可以执行相同的散列, 以生成解密密钥。

[0131] 再以 Diffie Hellman 作为示例, 隐蔽数据库 Key Exchange 可以按如下方式工作:

[0132] 1. Alice chooses a random large integer X and sends Bob $X = (g^A \text{ mod } n)$ encrypted with Covert Data

[0133] 2. Bob chooses a random large integer Y and sends Alice $Y = (g^B \text{ mod } n)$ encrypted with Covert Data

[0134] 3. Alice decrypts Bob's encrypted Y and computes $K = Y^A \text{ mod } n$

[0135] 4. Bob decrypts Alice's encrypted X and computes $K' = X^B \text{ mod } n$

[0136] 根据DiffieHellman, K 和 K' 相等, 隐蔽数据被用作用于传输数据的加密密钥。隐蔽数据不仅可以用作加密密钥数据, 还可以用作随机大整数计算的种子数据或适用于用以算法计算中的数据和数值的散列。

[0137] 在上面的实施例中, 唯一隐蔽标识符是基于在操作或使用客户机设备的过程中发生的操作事件生成的, 基于客户或用户使用客户机设备的方式生成的。这些操作事件在真实客户机设备和克隆的客户机设备之间是不同的, 因为他们的用户对克隆的客户机设备的操作方式与真实客户机设备或其他克隆客户机设备的用户的操作方式是不同的。这样的操作是非常难以复制的。隐蔽标识符可以用以检测克隆的客户机设备, 还用于周期性的续订过程中, 可以消除对克隆客户机设备的服务。

[0138] 本领域的技术人员将理解, 各种说明性逻辑单元、模块、电路、以及参考这里所说明的实施例所描述的算法步骤, 常常可以作为电子硬件、计算机软件, 或两者的组合来实现。为清楚地显示硬件和软件的互换性, 上文已经一般就其功能而言描述了各种说明性组件、单元、模块、电路以及步骤。这样的功能是作为硬件还是作为软件来实现取决于特定的应用以及施加于整个系统的设计约束。本领域的技术人员可以对于每一个特定应用以各种方式来实现所描述的功能, 但是这样的实现方式的判定不应该被解释为导致偏离本发明的范围。此外, 对一个模块、单元或步骤内的功能的分组也只是为了描述方便。在没有偏离本发明的情况下, 特定功能或步骤可以从一个模块或单元中删除。

[0139] 参考这里所说明的实施例所描述的各种说明性逻辑单元和模块可以利用通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其他可编程逻辑器件、分离的门电路或晶体管逻辑、分离的硬件组件, 或被设计为执行这里所描述的功能的其任何组合来实现或执行。通用处理器可以是微处理器, 但是在备选方案中, 处理器可以是任何处理器、控制器、微控制器或状态机。处理器也可以作为计算设备的组合来实现, 例如, DSP 和微处理器的组合、多个微处理器、和 DSP 核心结合在一起的一个或多个微处理器, 或任何其他这样的配置。

[0140] 参考这里所说明的实施例所描述的方法或算法的步骤可以直接以硬件, 由处理器执行的软件模块, 或以两者的组合来实现。软件模块可以驻留在 RAM 存储器、FLASH 存储器、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动磁盘、CD-ROM, 或任何其他形式的存储介质中。示范性存储介质可以连接到处理器, 以便处理器可以从存储介质中读取信息, 并向存储介质中写入信息。在备选方案中, 存储介质可以与处理器集成在一起。处理器和存储介质可以驻留在 ASIC 中。

[0141] 各种实施例还可以主要以硬件的方式来实现, 例如使用诸如专用集成电路 (“ASIC”) 或现场可编程门阵列 (“现场可编程门阵列”) 之类的硬件组件。实现能够执行这里所描述的功能的硬件状态机, 对于本领域的技术人员来说也是很显然的。各种实施例还可以使用硬件和软件两者的组合来实现。

[0142] 提供了所说明的实施例的上述描述, 以允许任何本领域的技术人员实施或使用本发明。对这些实施例的各种修改方案对所属领域的技术人员是很显然的, 在不偏离本发明的精神或范围的情况下, 这里所描述的一般原理可以应用于其他实施例。如此, 应该理解的是, 这里所呈现的描述和附图代表本发明的目前优选的实施例, 因此, 代表本发明广泛地预期的主题。应该进一步理解, 本发明的范围完全包含对所属领域的技术人员是显而易见的。

其他实施例，本发明的范围相应地应当由所附权利要求进行限定。

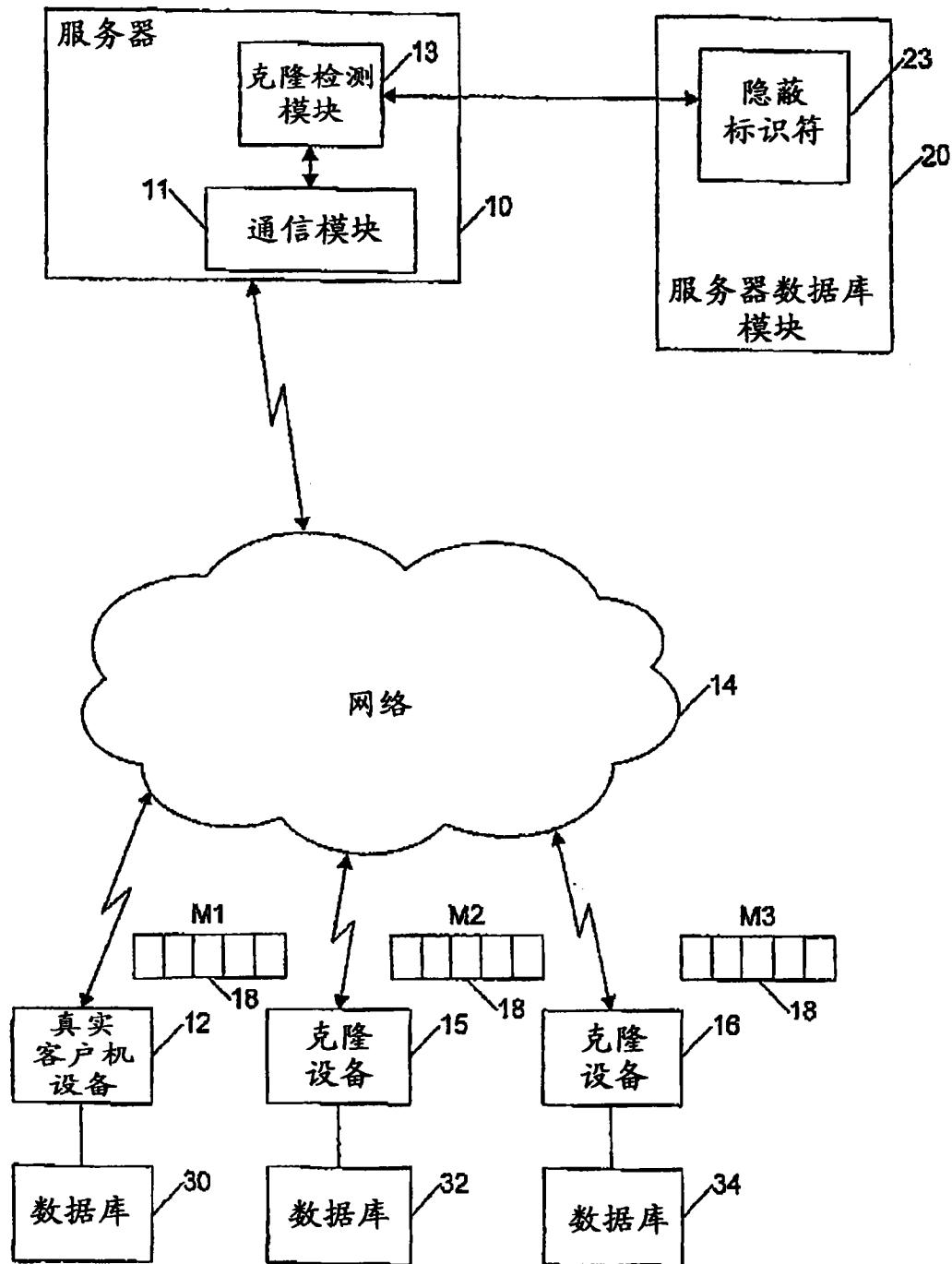


图 1

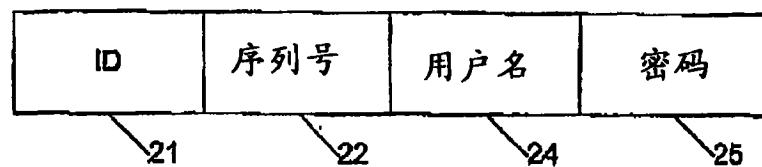


图 2A (现有技术)

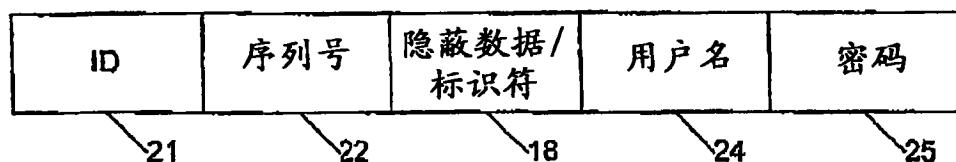


图 2B

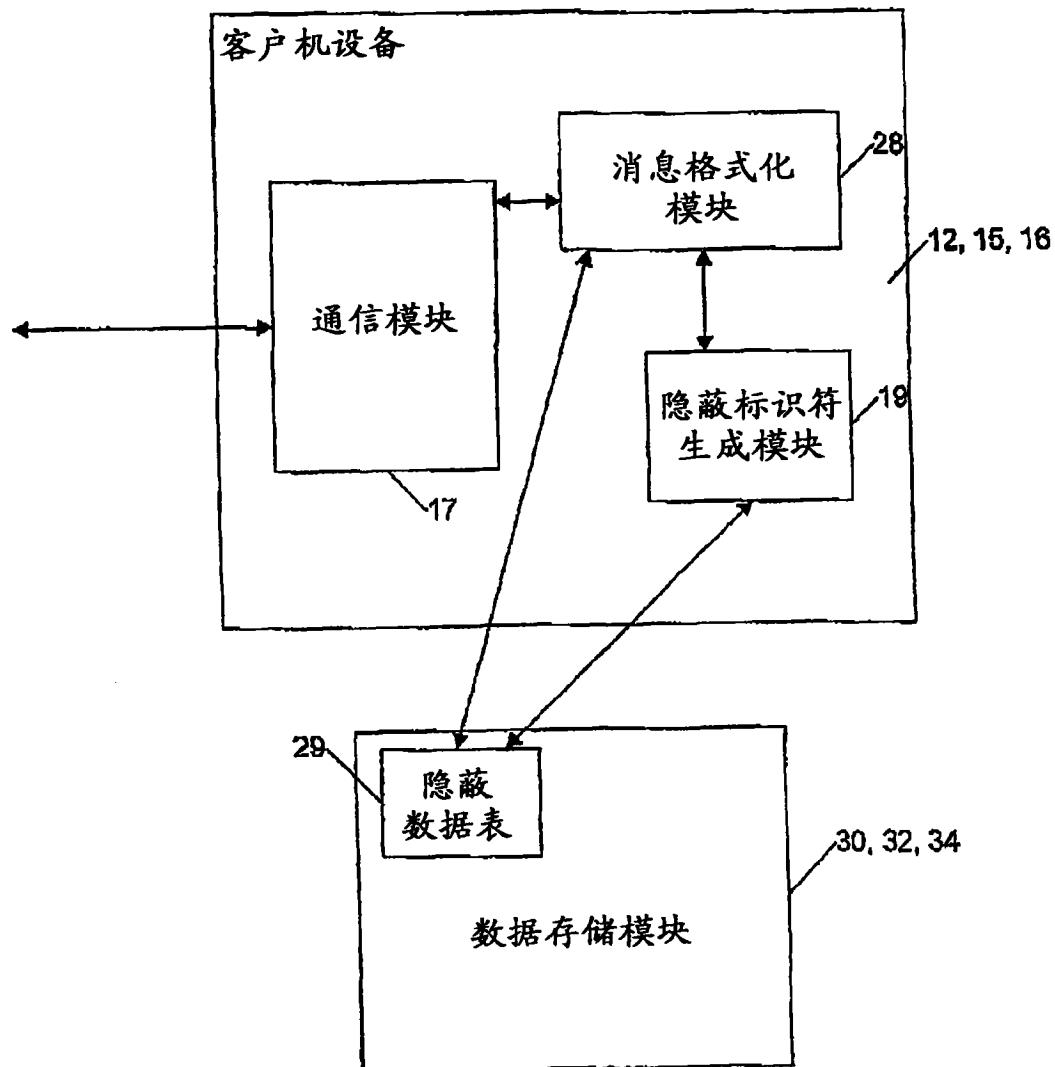


图 3

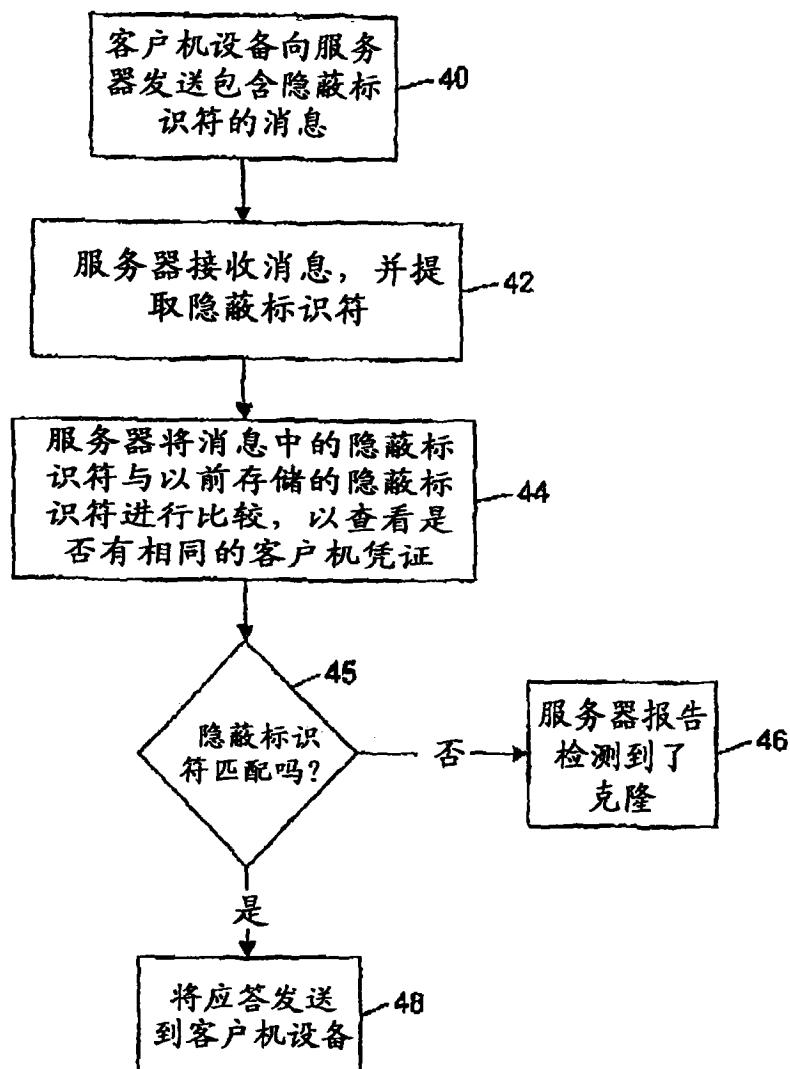
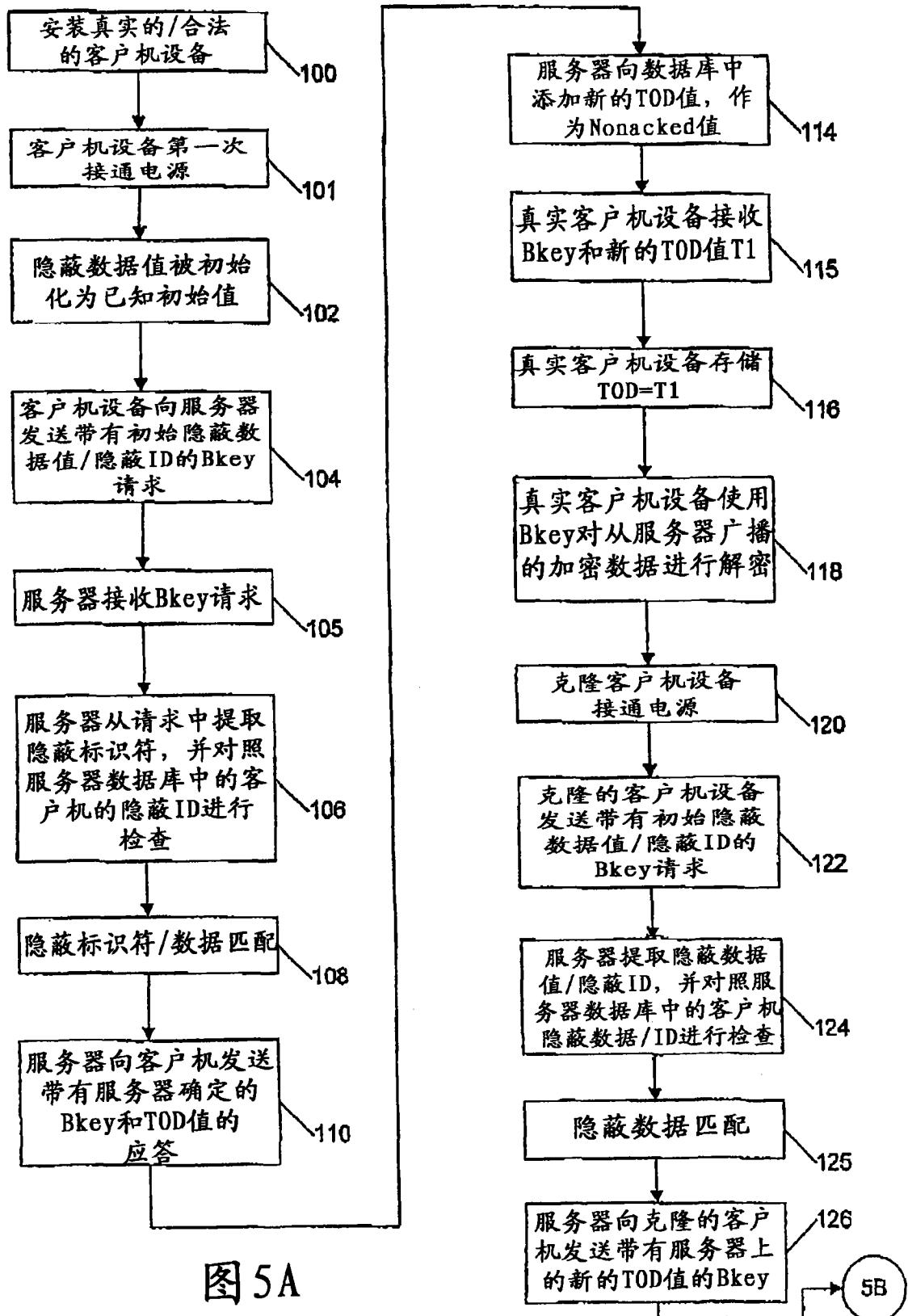
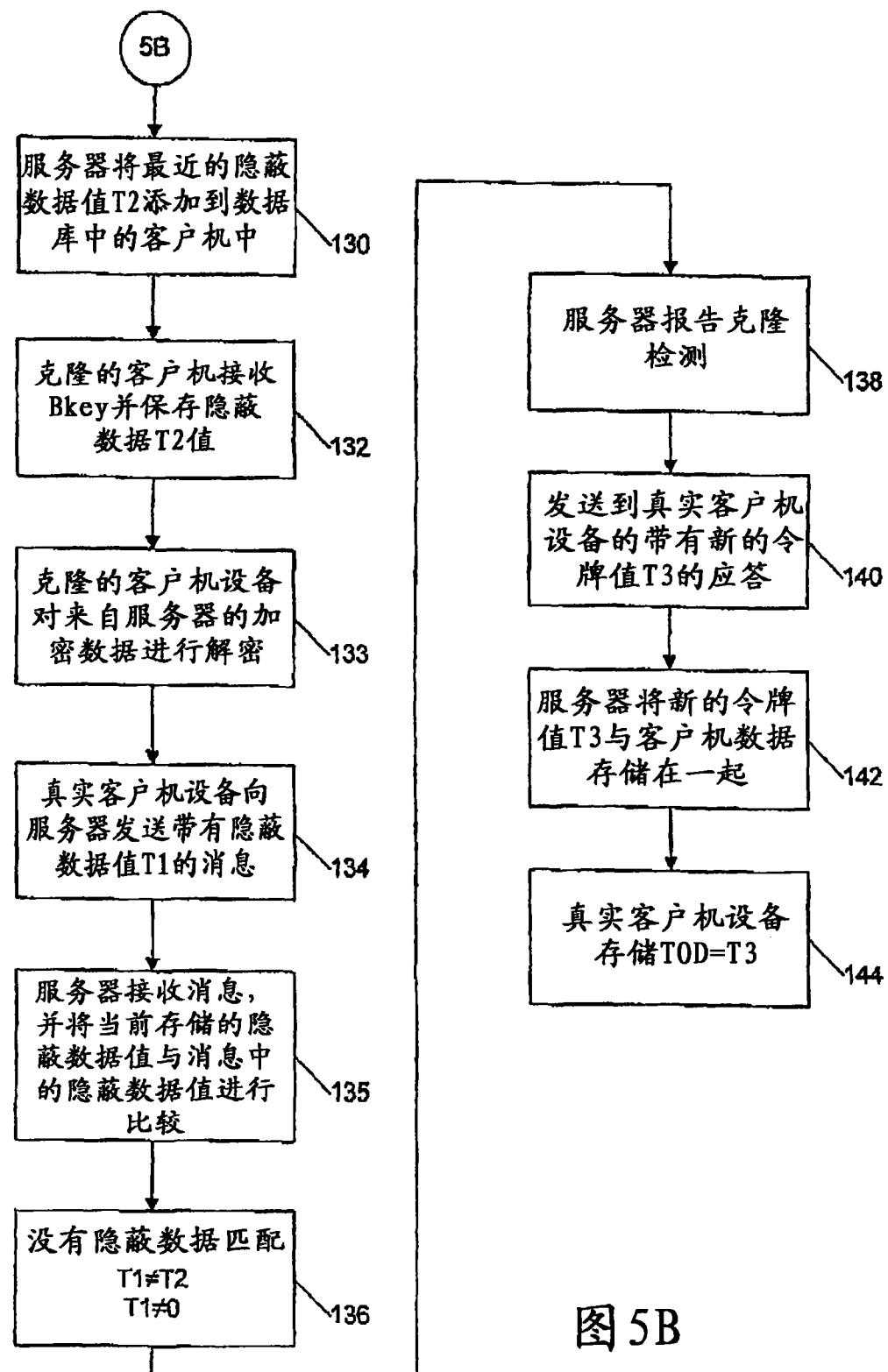


图 4





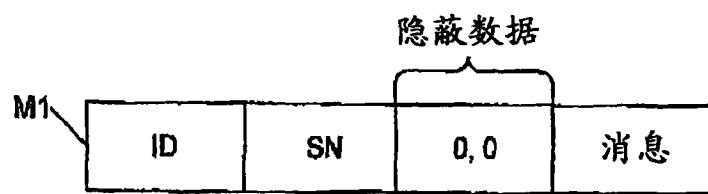


图 6A



图 6B

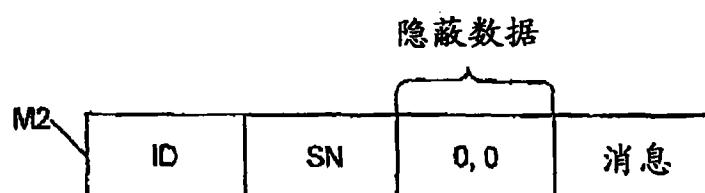


图 6C

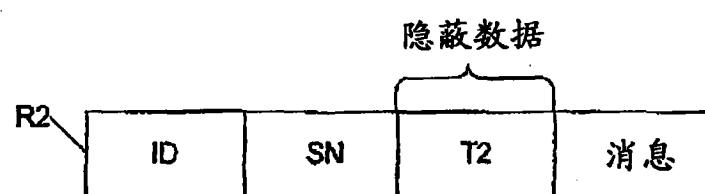


图 6D

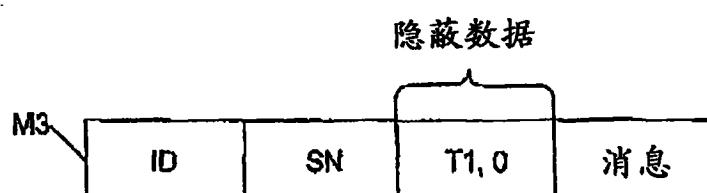


图 6E

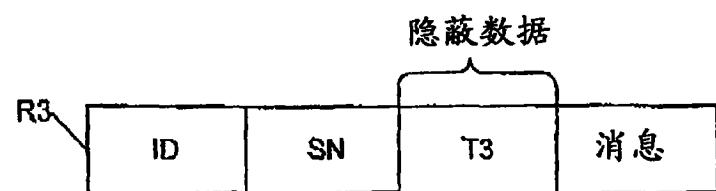


图 6F

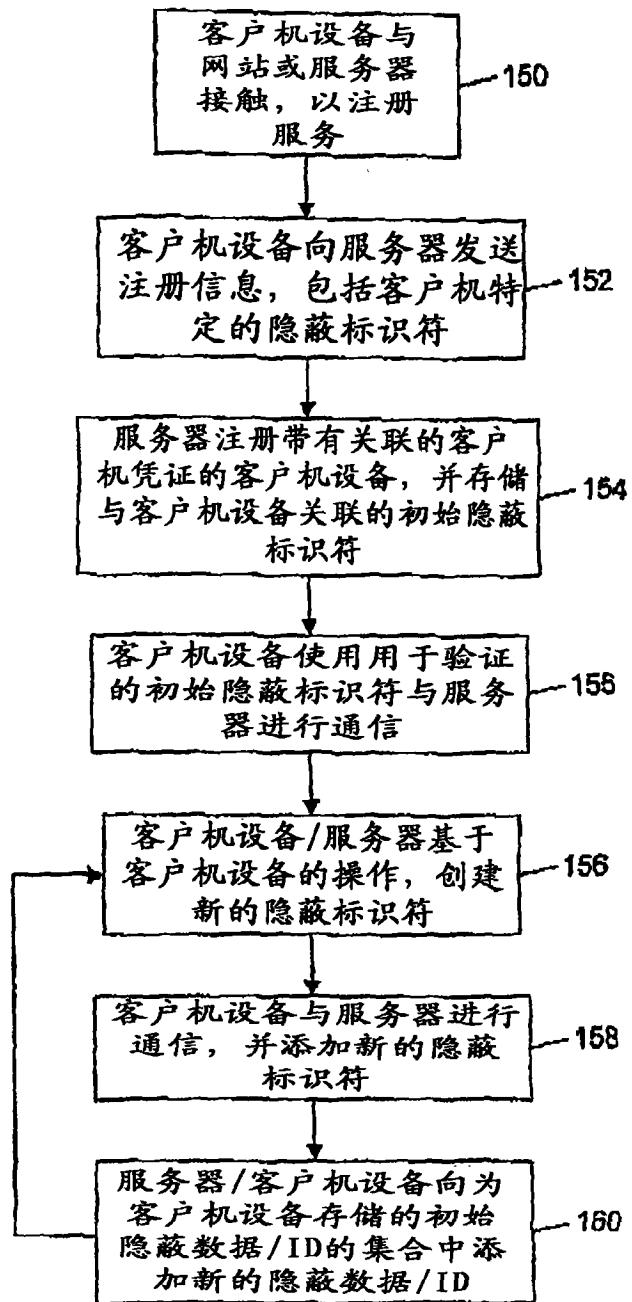


图 7

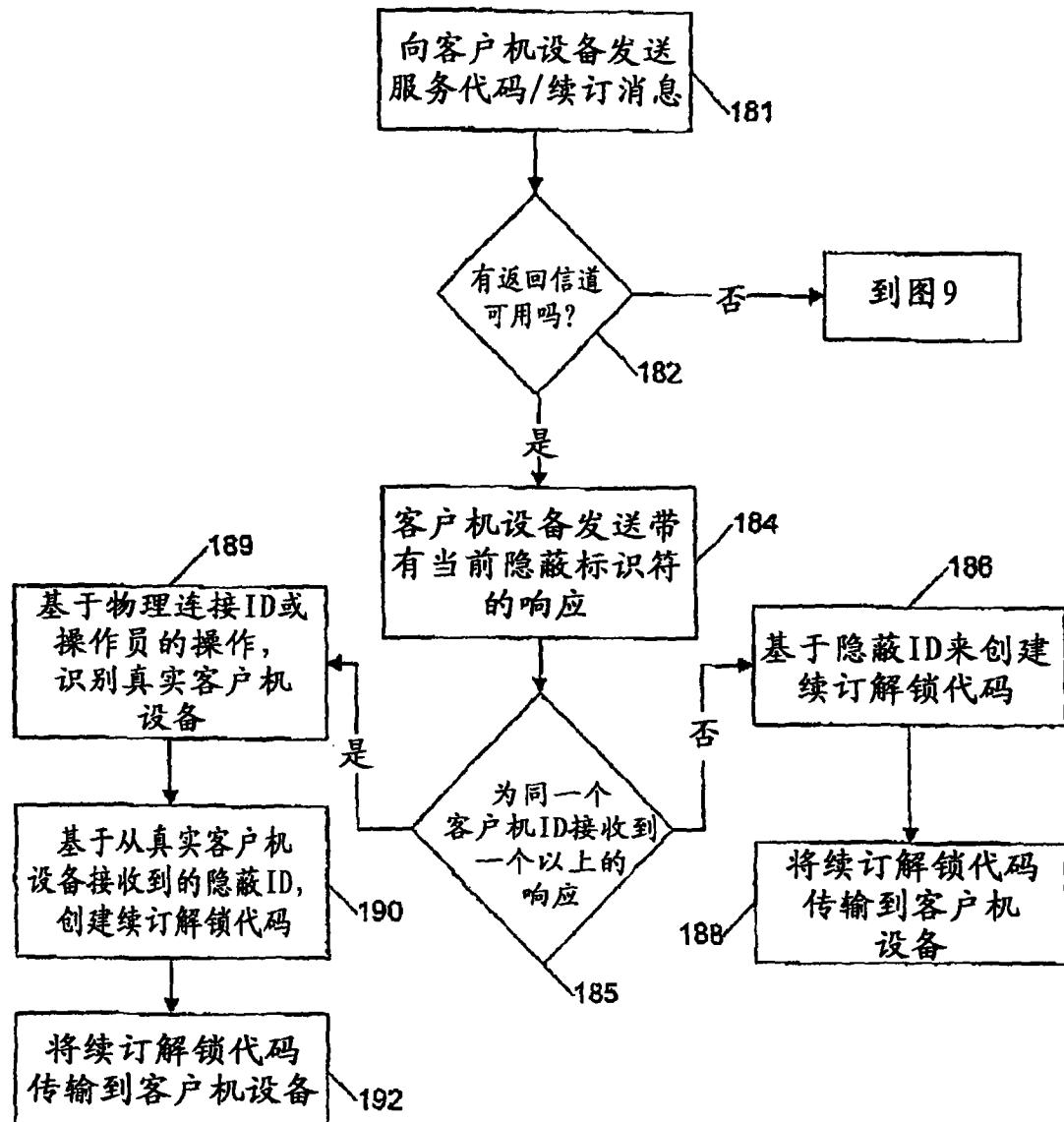


图 8

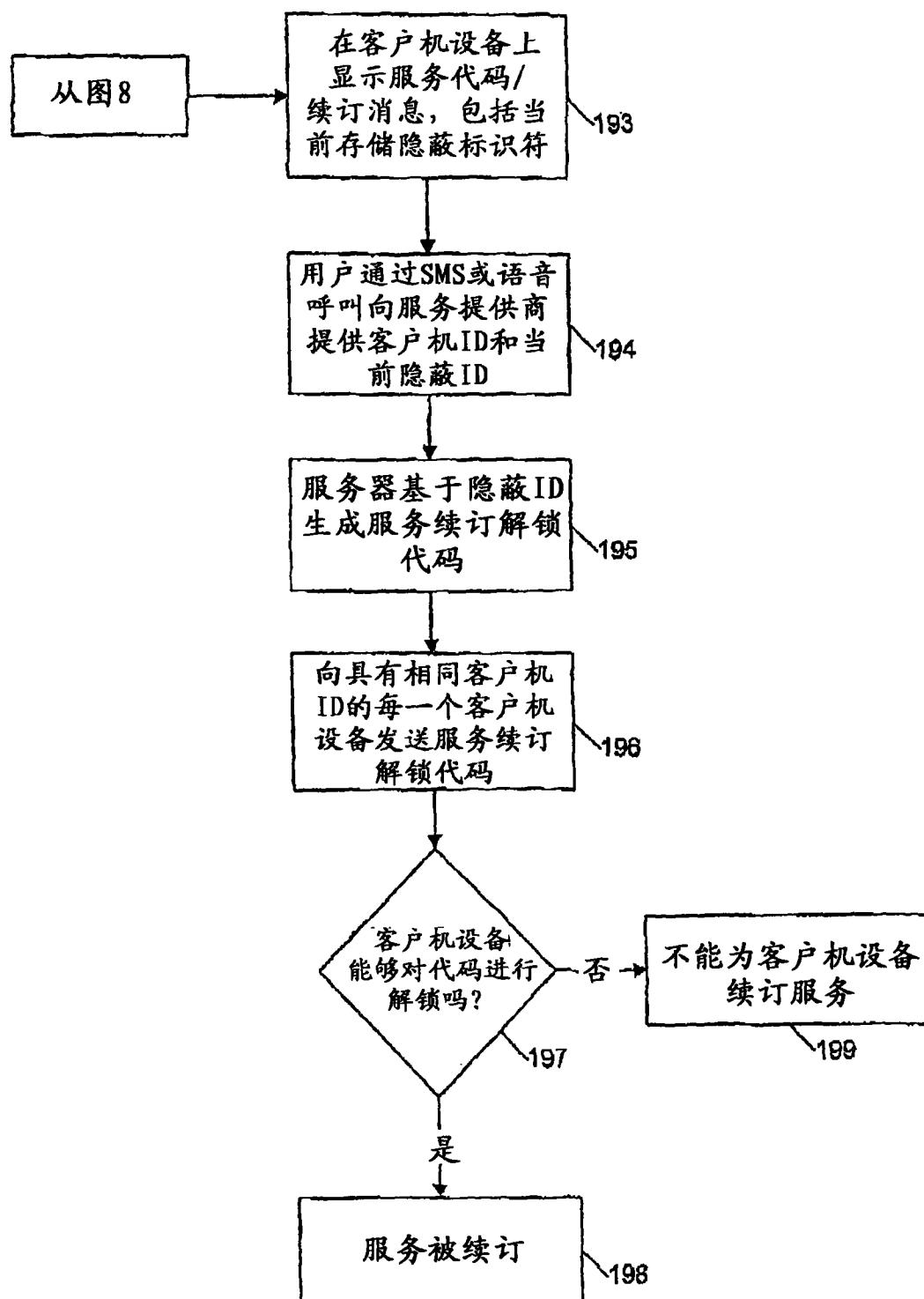


图 9