[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00

[12] 发明专利申请公开说明书

[21] 申请号 200410061884.8

[43] 公开日 2005 年 2 月 9 日

[11] 公开号 CN 1578214A

[22] 申请日 2004.6.25
[21] 申请号 200410061884.8
[30] 优先权
[32] 2003.6.27 [33] US [31] 10/609，152
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 W·G·米勒
[74] 专利代理机构 上海专利商标事务所
代理人 谢喜堂

权利要求书 3 页 说明书 11 页 附图 3 页

[54] 发明名称 从服务器发送到客户机的启动文件的三向确认和验证

[57] 摘要

一种从服务器向具有预安装的环境的客户机传输启动文件的方法和系统。所述服务器验证所述客户机。所述客户机验证所述服务器。所述启动文件从所述已验证的服务器传输到所述已验证的客户机。所述客户机可以在执行所述启动文件来创建操作系统之前验证该启动文件。

ISSN1008-4274

1．一种从服务器向客户机传输启动文件的方法，其特征在于，它包括：

所述服务器验证所述客户机；

所述客户机验证所述服务器；以及

从所述已验证的服务器向所述已验证的客户机传输所述启动文件。

2．如权利要求1所述的方法，其特征在于，它还包括所述已验证的客户机验证所述传输的启动文件。

3．如权利要求2所述的方法，其特征在于，它还包括所述已验证的客户机执行所述已验证的启动文件。

4．如权利要求1所述的方法，其特征在于，其证书无效或已吊销的客户机不被所述服务器验证或应答。

5．如权利要求1所述的方法，其特征在于，其证书无效或已吊销的服务器不被所述客户机确认。

6．如权利要求1所述的方法，其特征在于，所述客户机接收到的未正确签名的启动文件不被所述客户机执行。

7．如权利要求1所述的方法，其特征在于，所述传输的启动文件包括一签名，其中所述客户机核实所述签名。

8．一种用于通过网络从服务器向具有预操作系统环境的客户机传输网络启动文件的方法，其特征在于，它包括：

在客户机上安装客户机可信性证书；

所述客户机通过网络请求所述服务器向所述客户机发送所述启动文件；

所述客户机通过网络发送所述已安装的客户机可信性证书；

所述服务器通过所接收的客户机可信性证书验证所述客户机；以及

从所述服务器向所述已验证的客户机传输所述启动文件。

9．如权利要求8所述的方法，其特征在于，它还包括：

所述已验证的客户机验证所述传输的启动文件；以及

所述已验证的客户机执行所述已验证的启动文件。

10．一种通过网络从服务器向具有前操作系统环境的客户机传输启动文件的方法，其特征在于，它包括：

在客户机上安装客户机可信性证书；

所述客户机通过网络请求所述服务器向所述客户机发送所述启动文件；

所述客户机通过网络发送所述已安装的客户机可信性证书；以及

所述客户机从服务器接收所述启动文件。

11．如权利要求10所述的方法，其特征在于，它还包括：

所述已验证的客户机验证所传输的启动文件；以及

所述已验证的客户机执行所述已验证的启动文件。

12．一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法，其特征在于，它包括：

所述客户机通过网络请求所述服务器向所述客户机传输启动文件；

所述服务器通过网络向所述客户机发送服务器可信性证书；

所述客户机通过所接收的服务器可信性证书验证所述服务器；

所述客户机通过网络请求所述已验证的服务器向所述客户机传输所述启动文件；以及

从所述已验证的服务器向所述客户机传输所述启动文件，作为对所述客户机请求的响应。

13．一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法，其特征在于，它包括：

所述服务器通过网络从所述客户机接收要所述服务器向所述客户机传输所述启动文件的请求；

所述服务器通过网络从所述客户机接收先前安装的客户机可信性证书；

所述服务器通过所述接收的客户机可信性证书验证所述客户机；

所述服务器通过网络向所述已验证的客户机发送所述启动文件。

14．一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法，其特征在于，它包括：

所述客户机通过网络请求所述服务器向所述客户机传输所述启动文件；

所述客户机通过网络从所述服务器接收服务器可信性证书；

所述客户机通过所述接收的服务器可信性证书验证所述服务器；

所述客户机通过网络请求所述已验证的服务器向所述客户机传输所述启动文件；以及

作为对所述客户机的请求的响应，接收从所述已验证的服务器到所述客户机的所述启动文件。

15. 如权利要求 14 所述的方法，其特征在于，其证书无效或已吊销的服务器不被所述客户机确认。

16. 如权利要求 16 所述的方法，其特征在于，所传输的启动文件包括一签名，其中，所述客户机验证所述签名。

17. 如权利要求 14 所述的方法，其特征在于，所述客户机接收的未正确签名的启动文件不被所述客户机执行。

18. 一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法，其特征在于，它包括：

所述客户机通过网络请求所述服务器向所述客户机传输启动文件；

作为对所述客户的所述请求的响应，从所述服务器向所述客户机传输所述启动文件；

所述客户机验证所传输的启动文件；以及

所述已验证的客户机执行所述已验证的启动文件。

19. 如权利要求 18 所述的方法，其特征在于，所传输的启动文件包括一签名，其中，所述客户机验证所述签名。

20. 如权利要求 19 所述的方法，其特征在于，所述客户机接收的未正确签名的启动文件不被所述客户机执行。

从服务器发送到客户机的启动文件的三向确认和验证

技术领域

本发明涉及客户机、服务器和启动文件的确认和验证领域，尤其涉及对于预操作系统（pre-operating system）环境中通过网络连接至服务器的客户机的启动文件的确认和验证。

背景技术

预操作系统（pre-OS）个人计算机（PC）的网络启动的一个关键问题是很难和/或无法确认这类 PC 对服务器的安全性。另外，许多服务器无法验证其客户机，并且许多客户机无法确认服务器和/或由服务器提供给客户机的启动文件的完整性。而且，当启动新的或被损坏的未安装操作系统的 PC 时有很大的限制。尤其是在预操作系统环境中，需要确认客户机、服务器或启动文件的完整性。也需要允许客户不论操作系统的状态如何都能够安全地启动，以提供一种更安全且健壮的方法来启动客户机并展开操作系统。

发明内容

通过在客户机上设置预安装的环境，并在预安装环境中装置能够确认客户机、服务器或启动文件的完整性的组件，本发明提供了一种更安全且健壮的方法来启动客户机并展开操作系统。另外，允许客户不论操作系统的状态如何都能够安全地启动，提供了一种更安全且健壮的方法来启动客户和展开操作系统。因此，本发明满足了对提供能用来确认这三个组件－客户机、服务器、（多个）启动文件的任一个或全部的完整性的预安装环境的非常驻组件的系统和方法的需求。

一般而言，本发明是一种用于确认和验证网络化环境中启动的操作系统的系统和方法。传统的基于网络的启动不包括对服务器/客户机的确认和验证组件。本发明提供一种用于服务器/客户机验证和确认的三向验证框架。本发明在客户机和服务器组件上同时使用确认装置，如数字证书。通过交换确认装置，客户机能够向服务器验证其自身，服务器能够向客户机验证其自身，并且客户机能够核实由服务

器发送的启动文件已适当地被确认。

依照本发明的一个方面，一种方法通过网络从服务器向具有预操作系统环境的客户机传输启动文件。该方法包括在客户机上安装客户机的可信性证书；客户机通过网络请求服务器向客户机传输启动文件；客户机通过网络发送已安装的客户机可信性证书；服务器通过接收的客户机可信性证书来验证客户机；服务器通过网络向客户机发送服务器可信性证书，作为对服务器验证客户机的响应；客户机通过所接收的服务器可信性证书验证服务器；已验证的客户机通过网络请求已验证的服务器向已验证的客户机发送启动文件；从已验证的服务器向已验证的客户机传输启动文件，作为对已验证的客户机的请求的响应；已验证的客户机验证所传输的启动文件；以及已验证的客户机执行已验证的启动文件。

以另一种形式，本发明包括一种从服务器向客户机传输启动文件的方法，包括服务器验证客户机；客户机验证服务器；以及从已验证的服务器向已验证的客户机传输启动文件。

以另一种形式，本发明包括一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法。该方法包括在客户机上安装客户机可信性证书；客户机通过网络请求服务器向客户机传输启动文件；客户机通过网络发送已安装的客户机可信性证书；服务器通过所接收的客户机可信性证书验证客户机；以及从服务器向已验证的客户机传输启动文件。

以另一种形式，本发明包括一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法，包括在客户机上安装客户机可信性证书；客户机通过网络请求服务器向客户机传输启动文件；客户机通过网络发送已安装的客户机可信性证书；以及客户机从服务器接收启动文件。

以另一种形式，本发明包括一种通过网络从服务器向具有预操作系统环境的客户机发送启动文件的方法。该方法包括服务器通过网络从客户机接收服务器向客户机传输启动文件的请求；服务器通过网络从客户机接收先前安装的客户机可信性证书；服务器通过接收的客户机可信性证书验证客户机；以及从服务器向已验证的客户机传输启动文件。

以另一种形式，本发明包括一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法，包括客户机通过网络请求服务器向客户机传输启动文件；服务器通过网络向客户机发送服务器可信性证书；客户机通过接收的服务器可

信性证书验证服务器；客户机通过网络请求已验证的服务器向客户机传输启动文件；以及从已验证的服务器向客户机传输启动文件，作为对客户机的请求的响应。

以另一种形式，本发明包括一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法，包括服务器通过网络从客户机接收服务器向客户机传输启动文件的请求；服务器通过网络从客户机接收先前安装的客户机可信性证书；服务器通过所接收的客户机可信性证书验证客户机；以及服务器通过网络向已验证的客户机发送启动文件。

以另一种形式，本发明包括一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法，包括：客户机通过网络请求服务器向客户机传输启动文件；客户机通过网络从服务器接收服务器可信性证书；客户机通过所接收的服务器可信性证书验证服务器；客户机通过网络请求已验证的服务器向客户机传输启动文件；以及接收从已验证的服务器向客户机传输的启动文件，作为对客户机请求的响应。

以另一种形式，本发明包括一种通过网络从服务器向具有预操作系统环境的客户机传输启动文件的方法。该方法包括客户机通过网络请求服务器向客户机传输启动文件；从服务器向客户机传输启动文件，作为对客户机的请求的响应；客户机验证所传输的启动文件；以及已验证的客户机执行已验证的启动文件。

以另一种形式，本发明包括一种传输启动文件的系统，包括一客户机；一具有启动文件的服务器；向服务器验证客户机的软件；向客户机验证服务器的软件；以及从已验证的服务器向已验证的客户机传输启动文件的软件。

以另一种形式，本发明包括一种用于通过网络从服务器向具有预操作系统环境的客户机传输启动文件的计算机可读媒质。该媒质含有指令，这些指令用于客户机通过网络请求服务器向客户机传输启动文件、用于客户机通过网络发送先前安装的客户机可信性证书、以及用于客户机从服务器接收启动文件。

以另一种形式，本发明包括一种用于通过网络从服务器向具有预操作系统环境的客户机传输启动文件的计算机可读媒质。该媒质含有指令，这些指令用于服务器通过网络从客户机接收服务器向客户机传输启动文件的请求、用于服务器通过网络从客户机接收先前安装的客户机可信性证书、用于服务器通过接收的客户机可信性证书验证客户机、以及用于从服务器向已验证的客户机传输启动文件。

以另一种形式，本发明包括一种用于通过网络从服务器向具有预操作环境系

统的客户机传输启动文件的计算机可读媒质。该媒质包括指令，这些指令用于服务器通过网络从客户机接收服务器向客户机传输启动文件的请求、用于服务器通过网络从客户机接收先前安装的客户机可信性证书、用于服务器通过接收的客户机可信性证书验证客户机、以及用于服务器通过网络向已验证的客户机发送启动文件。

以另一种形式，本发明包括一种用于通过网络从服务器向具有预操作系统环境的客户机传输启动文件的计算机可读媒质，包括指令，这些指令用于客户机通过网络请求服务器向客户机传输启动文件、客户机通过网络从服务器接收服务器可信性证书；客户机通过接收的服务器可信性证书验证服务器、客户机通过网络请求已验证的服务器向客户机传输启动文件、以及作为对客户机的请求的响应接收从已验证的服务器传输到客户机的启动文件。

可选地，本发明也可以包括各种其它方法和装置。

以下将部分指出其它特征，并且能够部分清楚这些其它特征。

附图说明

图 1 所示是依照本发明的客户机和服务器之间的通信的结构图。

图 2 所示是依照本发明的系统的方法和操作的流程图。

图 3 所示是适合在其中实现本发明的计算系统环境的示例的结构图。

具体实施方式

本发明包括储存在要启动的客户机上的数字证书或其它数字校验或确认装置，以及储存在启动服务器上的另一数字证书或其它数字校验或确认装置。依照本发明的体系结构和方法允许三向验证。包含具有内建证书的预操作系统的客户机向服务器作出启动文件的请求（通过 PXE 或其它关联协议）。预启动执行环境（PXE）是一种工业标准客户机/服务器接口，允许尚未加载操作系统的联网计算机能够由管理员远程地配置并启动。PXE 代码通常在新计算机的只读存储器芯片或启动盘上传送，允许该计算机（客户机）与网络服务器进行通信，使得该客户机机器能够被远程地配置并且其操作系统能够被远程地启动。PXE 提供以下三项：

1）动态主机配置协议（DHCP），允许客户接收 IP 地址来获取向网络服务器的访问。

2）一组应用程序接口（API），由客户机的基本输入/输出操作系统（BIOS）

或下载的网络引导程序（NBP）使用，NBP 自动化了操作系统的启动和其它配置步骤。

3）初始化 PXE ROM 芯片或启动盘中的 PXE 代码的标准方法。

服务器和客户机之间的初始连接通常由来自客户的请求启动，尽管背景情况也加以考虑。在服务器和客户机之间的初始连接时，任一方向上都未建立信任，即，服务器的对客户机的信任或客户机的对服务器的信任。在服务器从客户机接收请求之后，客户机把其凭证或证书呈现出来。服务器然后确定客户机所呈现的证书是否有效且未被吊销。如果该证书是无效或已吊销的，则服务器不响应。如果该证书是有效的，服务器使用其自己的证书来响应。客户机然后执行类似的分析来确定服务器的可信性和吊销状态。如果客户机检验出服务器是可信的，则客户机作出对（多个）实际启动文件进一步的请求。服务器采用数字签名的文件响应。客户机将使用其自己的本地证书来检查该文件以确定该文件是否为可信地签名的。如果该数字签名是可信的，则客户机将执行（多个）启动文件。

图 1 所示是依照本发明的客户机和服务器之间的通信的框图。特别地，参考图 1，说明了一种通过网络 100 从服务器 104 向具有预操作系统环境的客户机计算机 106 传输启动文件 102 的系统和方法。一般而言，启动是开始或复位计算机的进程。当首次打开或复位时，计算机执行启动文件来加载并开始其操作系统和/或准备将计算机投入使用。

客户机 106 上传输的启动文件 108 可以由客户机执行来为客户机创建、重建、修改、扩展或增强操作系统。一般而言，依照本发明的验证包括以下的一个或多个：服务器 104 验证客户机 106；和/或客户机 106 验证服务器 104；和/或从已验证的服务器 104 向已验证的客户机 106 传输已验证的启动文件以在客户机 106 上创建传输的启动文件，该启动文件能够被验证并被执行来影响客户机 106 的操作系统 110。

图 2 所示是依照本发明的系统的方法和操作的流程图。参考图 1 和 2，说明了一种通过网络 100 从服务器 104 向具有预操作系统环境的客户机 106 传输一个或多个启动文件 102 的方法。最初在 102，在客户机 106 上安装客户机可信性证书 112。这一安装（以及客户机和服务器之间的任一其它通信）能够手动或通过网络 110 实现。如图 1 的箭头 114 所示，在 204，客户机 106 通过网络 100 请求服务器 104 向客户机 106 传输启动文件 102，并且在 206，客户机通过网络发送已安装的客户机可信性证书 112 以呈现其凭证。在 208，服务器 104 通过接收的客户机可信性证

书 112 验证客户机。如果客户机不可信（如，如果客户机证书是无效的、过期的或者已吊销的），则进程结束。

如图 1 的箭头 116 所示，如果客户机证书 112 与服务器 104 维护或可访问的预存可信客户机列表相匹配，则令客户机 106 对服务器 104 可信，在 210，服务器 104 通过网络 100 向客户机 106 发送服务器可信性证书 118，作为对服务器验证客户机的响应。

在 212，客户机 106 通过所接收的服务器可信性证书 118 来验证服务器。如果服务器 104 不可信（例如，如果服务器证书是无效的、过期的或已吊销的），则进程结束。客户机 106 可能以若干种方式之一来验证服务器的证书 118。例如，服务器的证书 118 可能对应于客户机的证书 112。另一方面，服务器证书 112 可能匹配客户机 106 所维护或可访问的预存可信服务器列表，令服务器对客户机 106 可信。如图 1 的箭头 120 所示，如果服务器证书 118 匹配或已检验，则客户机 106 向服务器 104 响应。特别地，在 214，已验证的客户机通过网络请求已验证的服务器向已验证的客户机传输启动文件 102。如图 1 的箭头 122 所示，服务器 104 通过向启动文件 102 添加签名来响应，并在 216 从已验证的服务器向已验证的客户机传输签名的启动文件，作为对已验证的客户机的请求的响应。

下一步，在 218，已验证的客户机通过确认启动文件具有与客户机证书和/或服务器证书相应的签名来验证传输的签名启动文件。特别地，所传输的启动文件应当包括与来自服务器的客户机可信性证书相应的签名，并且客户机检验签名对应于其可信性证书（见图 2 的 124）。如果启动文件未验证（如，如果启动文件是不正确地签名的、无效的、过期的或已吊销的），则进程结束。在 220，客户机执行验证的启动文件来创建操作系统 110。

也考虑依照本发明的系统和方法仅包括客户机授权。这一实施例如下实现。在客户机 106 上安装客户机可信性证书 112。这可以手动或通过网络 100 或由服务器 104 安装。客户机通过网络请求服务器向客户机传输启动文件。客户机通过网络发送已安装的客户机可信性证书。服务器通过接收的客户机可信性证书验证客户机并从服务器向已验证的客户机传输启动文件 102。可选地，启动文件可以是已签名的，并且已验证的客户机可以在执行启动文件之前验证所传输的签名启动文件。

从客户机一方来看，客户机授权系统和方法可包括安装在客户机上的客户机可信性证书。客户机具有请求服务器向客户机传输启动文件的软件（或通过手动提

示）。客户机通过网络发送已安装的客户机可信性证书，并从服务器接收启动文件。可选地，已验证的客户机可以在执行启动文件之前先对其进行验证。

从服务器一方来看，客户机授权系统和方法可包括服务器上的软件，用于通过网络从客户机接收服务器向客户机传输启动文件的请求。该软件也通过网络接收先前安装在客户机上的客户机可信性证书。服务器包括用于通过接收的客户机可信性证书验证客户机的软件。服务器的软件然后从服务器向已验证的客户机传输（可任选地签名的）启动文件。

也考虑依照本发明的系统和方法仅包括服务器授权。在该实施例中，客户机106通过网络100请求服务器104向客户机传输启动文件102。服务器通过网络向客户机发送服务器可信性证书118。客户机通过接收的服务器可信性证书验证服务器。客户机通过网络请求已验证的服务器向客户机传输启动文件。作为对客户机的请求的相应，通过网络从已验证的服务器向客户机传输启动文件。可选地，可以对启动文件签名，使它们能被客户机验证。

从服务器一方来看，服务器授权系统和方法包括用于通过网络从客户机接收服务器向客户机传输启动文件的请求的软件、通过网络从客户机接收先前安装的客户机可信性证书的软件、用于通过接收的客户机可信性证书验证客户机的软件以及通过网络向已验证的客户机发送（可任选地签名的）启动文件的软件。

从客户机一方来看，服务器授权系统和方法包括通过网络请求服务器向客户机传输启动文件的软件、通过网络从服务器接收服务器可信性证书的软件、通过接收的服务器可信性证书验证服务器的软件、通过网络请求已验证的服务器向客户机传输启动文件的软件以及从已验证的服务器接收（可任选地签名的）启动文件作为对客户机的请求的响应的软件。

也考虑依照本发明的系统和方法可以仅包括启动文件授权。在该实施例中，客户机106通过网络100请求服务器104向客户机传输启动文件102。从服务器向客户机传输签名的启动文件作为对客户机的请求的响应。客户机验证传输的签名的启动文件并执行已验证的启动文件。

通过包括数字签名或其它数字校验装置作为由客户机使用来创建其操作系统的启动文件的一部分，可以对客户机、服务器和启动文件做全面确认。无论客户机软件存在于可读还是读/写计算机可读存储器（CRM）装置中，预安装的环境都能够：

确认服务器是可信的；

向服务器验证客户是可信的；以及

确认启动文件的完整性。

可选地，如上所述，可以实现不同的部分仅确认客户完整性、仅确认服务器完整性或仅确认（多个）启动文件的完整性，而得到不同层次的安全性。依照本发明的一种安全解决方案是要得到三者之全部，因此核实该进程的全部非安全步骤。

也可以实现以下在验证失败的情况下的准则来降低风险：

服务器不回应具有无效或已吊销证书的客户机。

客户机不应答具有无效或已吊销证书的服务器。

客户机不执行所接收到的非正确签名的启动文件。本发明尤其适用于网络配置团体和配置/管理团体。本发明着眼于保护网络启动协议，这是当前技术未满足的团体客户的需求。

图 3 以计算机 130 的形式示出了通用计算设备的一个示例，计算机 130 可以是客户机 106 或服务器 104。在本发明的一个实施例中，计算机，如计算机 130 适合在这里说明并描述的其它示图中用作服务器和/或客户机。计算机 130 具有一个或多个处理器或处理单元 132 以及系统存储器 134。在说明的实施例中，系统总线 136 将包括系统存储器 134 的各种系统组件耦合至处理器 132。总线 136 代表任意若干种总线结构的一个或多个，包括存储器总线或存储器控制器、外围总线、加速图形端口以及使用任一多种总线体系结构的处理器或本地总线。作为示例而非局限，这类体系结构包括工业标准体系结构（ISA）总线、微通道体系结构（MCA）总线、增强 ISA（EISA）总线、视频电子标准协会（VESA）本地总线以及外围部件互连（PCI）总线，也称为 Mezzanine 总线。

计算机 130 通常至少具有某些形式的计算机可读媒质。计算机可读媒质包括易失和非易失媒质、可移动和不可移动媒质，可以是可由计算机 130 访问的任一可用媒质。作为示例而非局限，计算机可读媒质包括计算机存储媒质和通信媒质。计算机存储媒质包括易失和非易失、可移动和不可移动媒质，以任一方法或技术实现来储存信息，如计算机可读指令、数据结构、程序模块或其它数据。例如，计算机存储媒质包括 RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘（DVD）或其它光盘存储、磁盒、磁带、磁盘存储或其它磁存储设备，或可以用来储存所期望的信息并可由计算机 130 访问的任一其它媒质。通信媒质通

常以诸如载波或其它传输机制的已调制数据信号中来实现计算机可读指令、数据结构、程序模块或其它数据，并包括任一信息传送媒质。本领域的技术人员熟悉已调制数据信号，该信号以某种方式设置或改变其一个或多个特征以对信号中的信息进行编码。有线媒质，如有线网络或直接连线连接，以及无线媒质，如声学、RF、红外和其它无线媒质，是通信媒质的示例。上述任一组合也包括在计算机可读媒质的范围之内。

系统存储器 134 包括可移动和/或不可移动、易失和/或非易失存储器形式的计算机存储媒质。在说明的实施例中，系统存储器 134 包括只读存储器（ROM）138 和随机存取存储器（RAM）140。基本输入/输出系统 142（BIOS），包含如在启动时帮助在计算机 130 内的元件之间传输信息的基本例程，通常储存在 ROM 138 中。ROM 140 通常包含处理单元 132 直接可访问和/或当前正在操作的程序模块。作为示例而非局限，图 3 说明了操作系统 144、应用程序 146、其它程序模块 148 以及程序数据 150。

计算机 130 也可包括其它可移动/不可移动、易失/非易失计算机存储媒质。例如，图 3 说明了对不可移动、非易失磁媒质进行读写的硬盘驱动器 154。图 3 也示出了对可移动、非易失磁盘 158 进行读写的磁盘驱动器 156、以及对可移动、非易失光盘 162，如 CD-ROM 或其它光媒质进行读写的光盘驱动器 160。可以在示例性操作环境中使用的其它可移动/不可移动、易失/非易失计算机存储媒质包括但不限于，磁带盒、闪存卡、数字多功能盘、数字录影带、固态 RAM、固态 ROM 等等。硬盘驱动器 154 以及磁盘驱动器 156 和光盘驱动器 160 通常通过非易失存储器接口，如接口 166 连接至系统总线 136。

以上描述并在图 3 中说明的驱动器或其它大容量存储设备及其关联的计算机存储媒质为计算机 130 提供了计算机可读指令、数据结构、程序模块和其它数据的存储。在图 3 中，例如，硬盘驱动器 154 被说明成储存操作系统 170、应用程序 172、其它程序模块 174 以及程序数据 176。注意，这些组件可以与操作系统 144、应用程序 146、其它程序模块 148 以及程序数据 150 相同，也可以与它们不同。这里对操作系统 170、应用程序 172、其它程序模块 174 以及程序数据 176 给予不同的数字来说明至少它们是不同的副本。

用户可以通过输入设备或用户接口选择设备，如键盘 180 和指向设备 182（如鼠标、轨迹球、输入笔或触摸板）向计算机 130 输入命令和信息。其它输入设备（未

示出）可包括麦克风、操纵杆、游戏板、圆盘式卫星天线、扫描仪等等。这些和其它输入设备通过耦合至系统总线 136 的用户输入接口 184 连接至处理单元 132，但是也可以通过其它接口和总线结构连接，如并行端口、游戏端口或通用串行总线（USB）。监视器 188 或其它类型的显示设备也通过接口，如视频接口 190 连接至系统总线。除监视器 188 之外，计算机经常包括其它外围输出设备（未示出），如打印机和扬声器，可通过输出外围接口（未示出）连接。

计算机 130 可以在使用到一台或多台远程计算机，如远程计算机 194 的逻辑连接的网络化环境中操作。远程计算机 194 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它普通网络节点，并通常包括上述与计算机 130 相关的元件的许多或全部。图 3 所示的逻辑连接包括局域网（LAN）196 和广域网（WAN）198，但也可包括其它网络。LAN 136 和/或 WAN 138 可以是有线网络、无线网络或其组合等等。这类网络环境常见于办公室、企业范围计算机网络、内联网和全球计算机网络（如因特网）。

当在局域网环境中使用时，计算机 130 通过网络接口或适配器 186 连接至 LAN 196。当在广域网环境中使用时，计算机 130 通常包括调制解调器 178 或其它用于通过 WAN 198，如因特网建立通信的装置。调制解调器 178 可以是内置的或外置的，通过用户输入接口 184 或其它合适的机制连接至系统总线 136。在网络化环境中，所描述的与计算机 130 相关的程序模块或其部分可以储存在远程存储器存储设备（未示出）中。作为示例而非局限，图 3 说明了远程应用程序 192 驻留在存储器设备中。可以理解，示出的网络连接是示例性的，也可以使用在计算机之间建立通信链路的其它装置。

一般而言，计算机 130 的数据处理器通过不同时间储存在计算机的不同计算机可读存储媒质中的指令来编程。例如，程序和操作系统通常分布在软盘或 CD-ROM 上。由此，它们被安装或加载到计算机的二级存储器中。在执行时，它们被至少部分地加载到计算机的一级电子存储器中。这里描述的本发明包括这些和其它不同类型的计算机可读存储媒质，这类媒质包含用于协同微处理器或其它数据处理器实现下文描述的步骤的指令或程序。当依照这里描述的方法和技术来编程时，本发明也包括计算机其本身。

为说明目的，这里说明程序和其它可执行程序组件，如操作系统，为离散的块。然而，应当认可，这类程序和组件在不同的时间驻留在计算机的不同存储组件

中，并由计算机的（多个）数据处理器执行。

尽管结合示例性计算系统环境，包括计算机 130 来描述，本发明可适用于众多其它通用或专用计算系统环境或配置。计算系统环境并非对本发明的适用或功能的范围的限制。此外，不应当将计算系统环境解释成具有关于示例性操作环境中说明的任一组件或其组合的依赖或需求。适合使用本发明的众所周知的计算系统、环境和/或配置的示例包括但不限于，个人计算机、服务器计算机、手持式或膝上设备、多处理器系统、基于微处理器的系统、机顶盒、可编程电子消费产品、移动电话、网络 PC、小型机、大型机、包括任一上述系统或设备的分布式计算环境等等。

本发明可以在计算机可执行指令的一般语境下描述，由一台或多台计算机或其它设备执行的计算机可执行指令如程序模块，。一般而言，程序模块包括但不限于，例程、程序、对象、组件以及数据结构，执行特定的任务或实现特定的抽象数据类型。本发明也可以在分布式计算环境中实践，其中，任务由通过通信网络连接的远程处理设备执行。在分布式计算环境中，程序模块可以位于本地或远程计算机存储媒质上，包括存储器存储设备。

在操作中，计算机 130 执行计算机可执行指令，如启动文件 102。

以下示例进一步说明了本发明。如果计算机 130 用作服务器 104，则其存储器包括如上所述的服务器可信性证书 118 和软件，用于与客户机 106 进行通信并用于验证客户机 106。如果计算机 130 用作客户机 106，则其存储器包括如上所述的客户机可信性证书 112 和软件，用于与服务器 104 进行通信、用于验证服务器 104、用于验证启动文件 102 并用于执行启动文件 102。

当介绍本发明或其（多个）实施例的元件时，冠词“一”、“一个”、“该”以及“所述”意指具有这些元件的一个或多个。术语“包括”、“包含”和“具有”是内含的，并意指除所列出的元件之外还有另外的元件。

从上述来看，可以发现，达到了本发明的若干目的，并且获得了其它有利的结果。

由于在不脱离本发明的范围的情况下可以对上述构造、产品和方法作出各种变化，所有包含在上述描述并在附图中示出的事物应解释为说明性的而非限制性的。

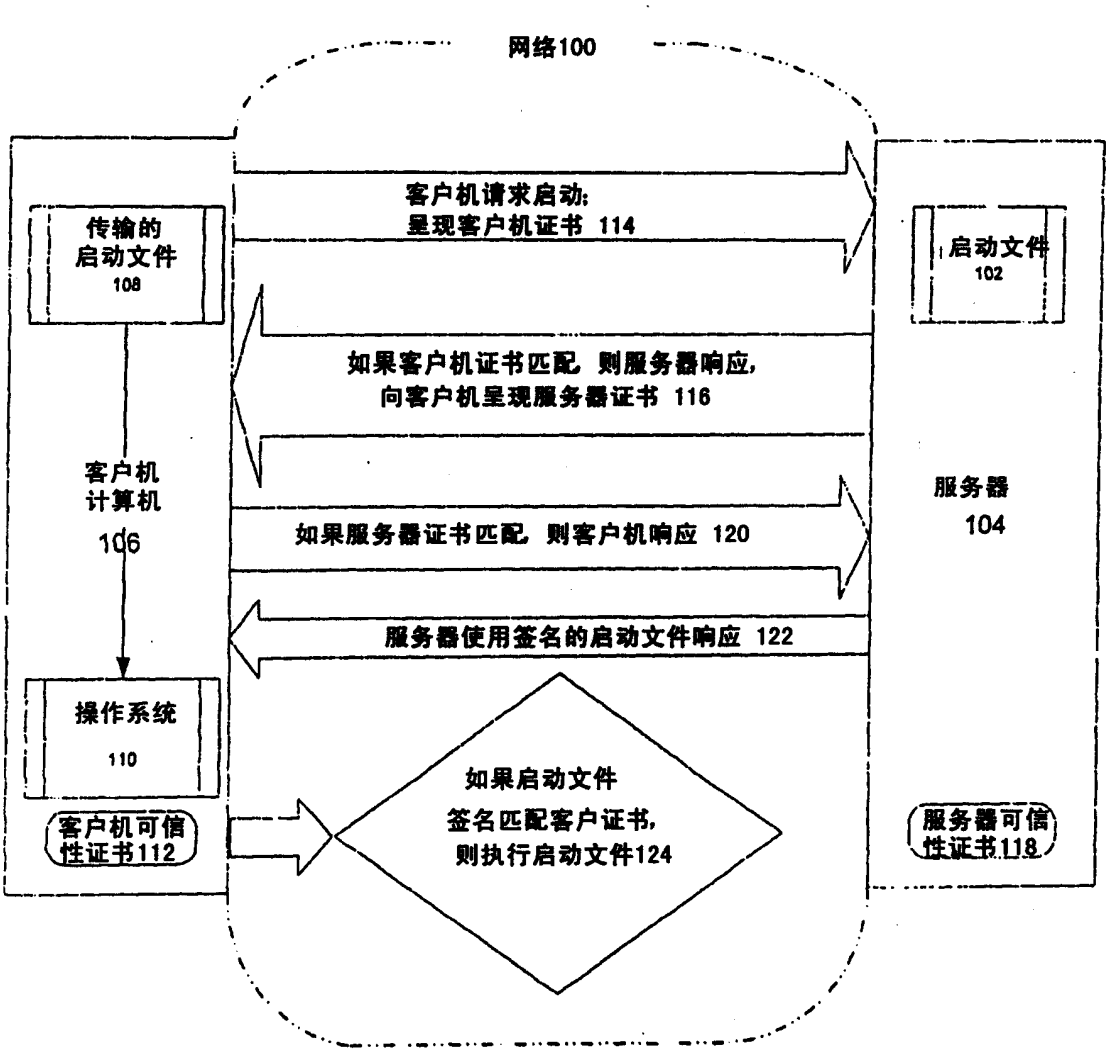
网络100
客户机请求启动;
呈现客户机证书 114
传输的
启动文件
108
启动文件
102
如果客户机证书匹配，则服务器响应，
向客户机呈现服务器证书 116
客户机
计算机
106
服务器
104
如果服务器证书匹配，则客户机响应 120
服务器使用签名的启动文件响应 122
操作系统
110
如果启动文件
签名匹配客户证书，
则执行启动文件124
客户机可信
性证书112
服务器可信
性证书118

图 1

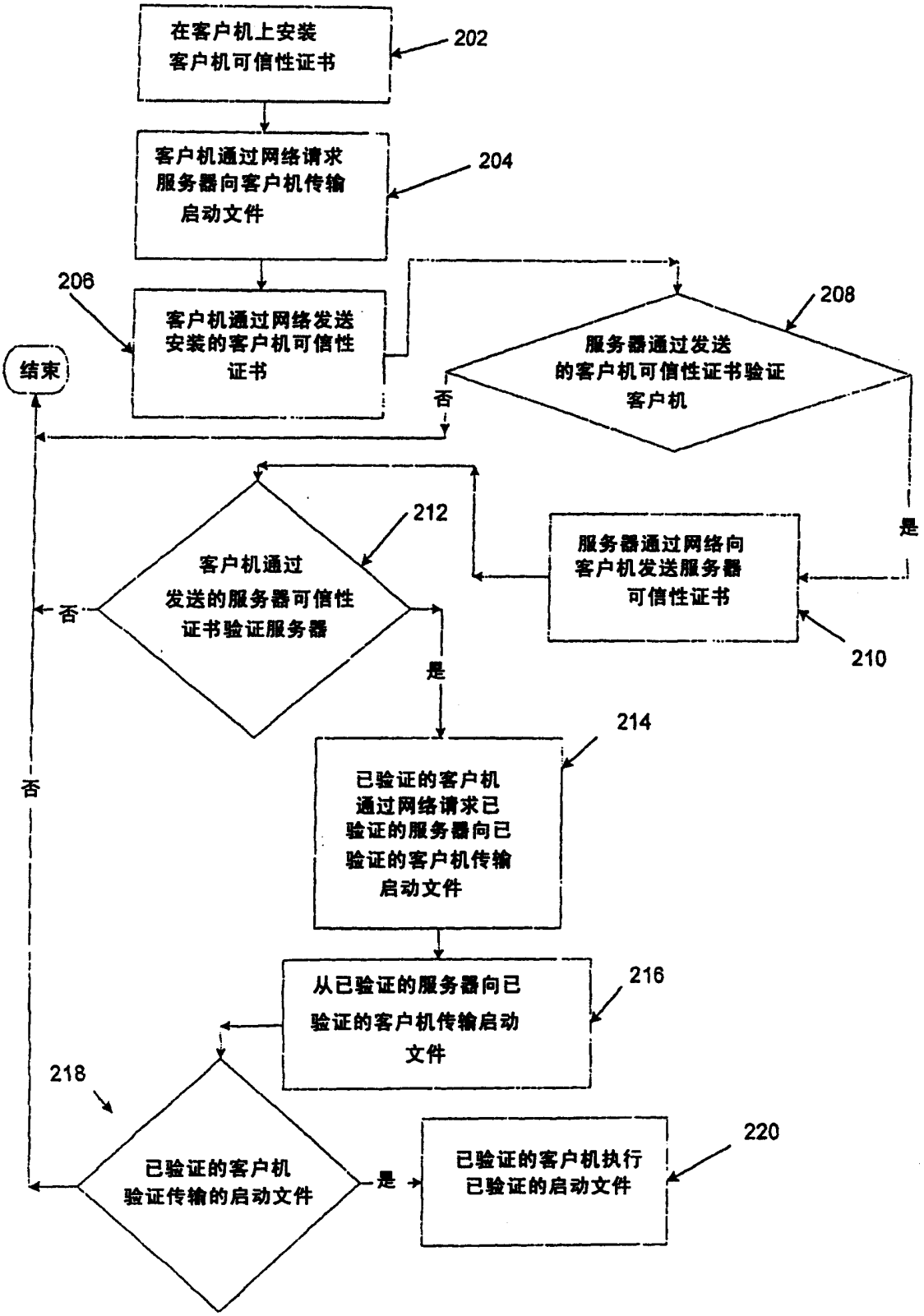
在客户机上安装
客户机可信性证书
202
客户机通过网络请求
服务器向客户机传输
启动文件
204
206
客户机通过网络发送
安装的客户机可信性
证书
结束
208
服务器通过发送
的客户机可信性证书验证
客户机
否
是
212
客户机通过
发送的服务器可信性
证书验证服务器
否
是
服务器通过网络向
客户机发送服务器
可信性证书
210
214
已验证的客户机
通过网络请求已
验证的服务器向已
验证的客户机传输
启动文件
216
从已验证的服务器向已
验证的客户机传输启动
文件
218
已验证的客户机
验证传输的启动文件
否
是
220
已验证的客户机执行
已验证的启动文件

图 2

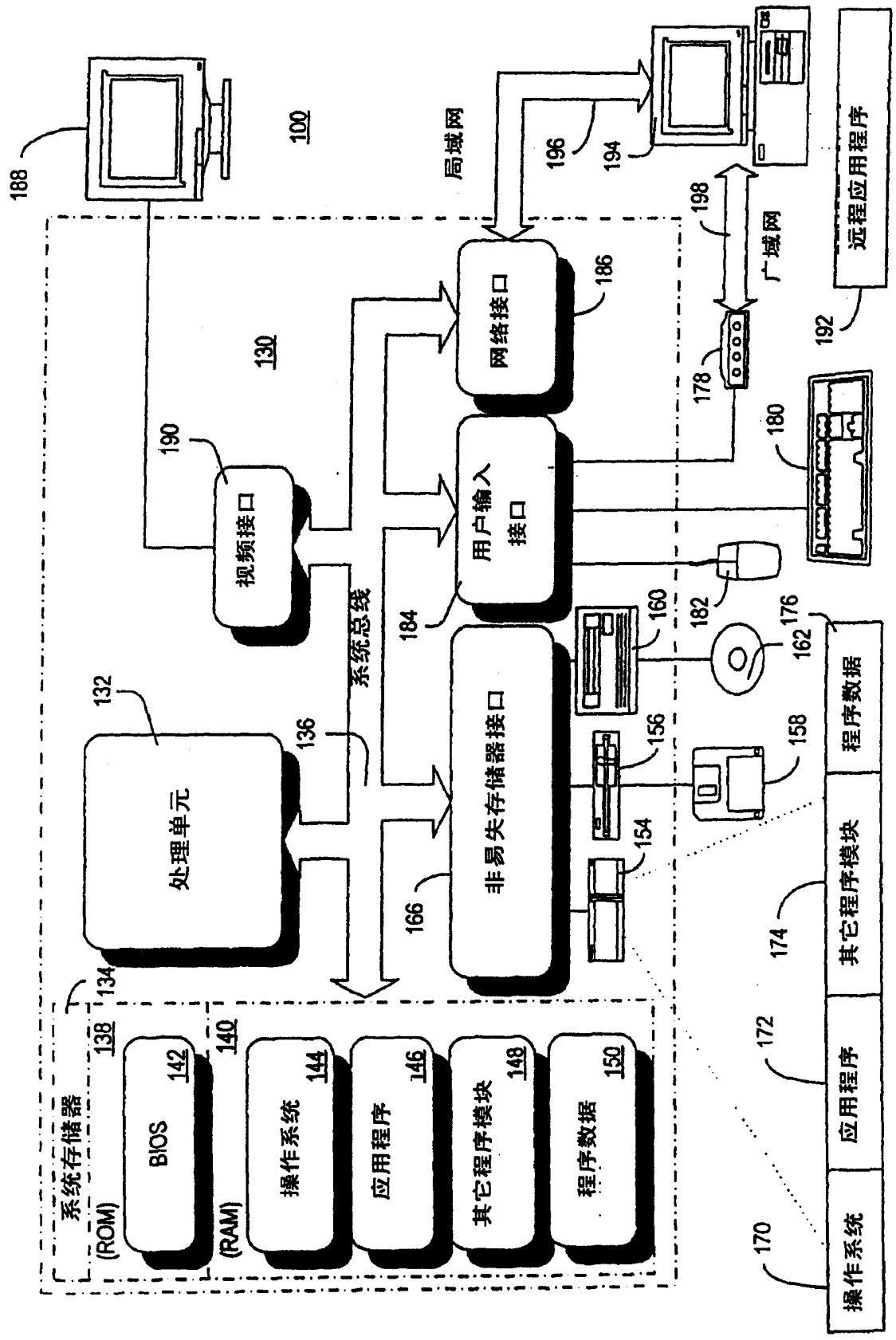
188
100
局域网
196
194
198
广域网
远程应用程序
192
130
190
视频接口
网络接口
186
178
180
用户输入接口
184
系统总线
160
182
176
162
132
处理单元
136
156
158
非易失存储器接口
154
166
134
系统存储器
138
(ROM)
BIOS
142
140
(RAM)
操作系统
144
应用程序
146
其它程序模块
148
程序数据
150
其它程序模块
174
程序数据
应用程序
172
操作系统
170

图 3