[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
H04L 29/06 (2006.01)
G06F 17/30 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480013320.5

[45] 授权公告日 2009 年 8 月 19 日

[11] 授权公告号 CN 100530207C

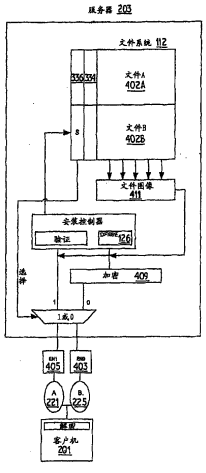
[22] 申请日 2004.4.15
[21] 申请号 200480013320.5
[30] 优先权
[32] 2003.5.22 [33] US [31] 10/443,675
[86] 国际申请 PCT/GB2004/001629 2004.4.15
[87] 国际公布 WO2004/104902 英 2004.12.2
[85] 进入国家阶段日期 2005.11.15
[73] 专利权人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 苏珊·M·基奥恩
杰拉尔德·F·麦克布里尔蒂
肖恩·P·马伦
杰西卡·K·莫里洛
约翰尼·M-H·希
[56] 参考文献
US2003/0028761A1 2003.2.6
CN1225186A 1999.8.4
CN1164074A 1997.11.5
CN1354936A 2002.6.19
Cryptographic file system for Unix. BLAZE MATT. ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. 1993
JFS:a secure distributed file system for network computers. O´CONNELL M ET AL. EUROMICRO CONFERENCE. 1999
PHP course:Redirection. . 2003
审查员 王 亮
[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临 王志森
权利要求书 4 页 说明书 10 页 附图 6 页

[54] 发明名称

分布式文件系统网络安全扩展

[57] 摘要

当请求访问在联网的文件系统上的敏感文件时，动态地执行文件系统的增强安装安全的安全协议。当客户机系统的用户试图访问特殊标签的敏感文件时，主管所述文件系统的服务器执行软件代码，所述软件代码终止当前的安装并且重新配置所述服务器端口，以便经由更安全的端口来接收来自客户机的重新安装(mount)。服务器重新配置的服务器端口提供了客户机的 IP 地址，并且在重新安装操作期间匹配所述 IP 地址。以无缝的方式来完成安全安装的转换，以便不在耗资的加密和其他资源密集的安全特征而使得服务器陷入困境的情况下，授权的用户可以访问敏感文件。用户不会经历大的延迟，同时在向客户机系统的传输期间使得敏感文件不被未经授权的用户捕获。



1. 一种为至少第一文件的传输提供安全的方法，所述方法用于数据处理系统，所述数据处理系统包括（1）存储介质，其上存储了所述至少第一文件，所述第一文件具有预设访问许可，（2）至少第一标准端口和第二安全端口，用于将所述数据处理系统连接到外部客户机系统，（3）用于经由所述第一标准端口和所述第二安全端口而选择性地路由至少一个文件的传输的逻辑部件，和（4）用于配置支持所述客户机系统的安装的所述第一标准端口和所述第二安全端口的重新配置逻辑部件，所述方法包括:

响应所述外部客户机系统对所述第一文件访问的请求，检查所述第一文件的所述预设访问许可；以及

当所述第一文件的所述预设访问许可表示对于所述第一文件需要安全访问时，经由所述第二安全端口动态地路由所述第一文件向外部客户机系统的传输，所述动态地路由步骤包括:

首先配置所述第二安全端口以支持从所述客户机系统接收的重新安装操作;

终止所述客户机系统在所述第一标准端口上的当前安装；以及

存储所述当前安装的会话参数以使能在所述第二安全端口上的会话无缝继续。

2. 按照权利要求 1 的方法，还包括:

当所述预设访问许可表示正常的访问是足够时，经由所述第一标准端口路由所述第一文件的传输。

3. 按照权利要求 1 的方法，还包括:

使能经由所述第一标准端口的所述数据处理系统的第一安装；以及

仅当所述第一文件要求安全访问时，使能经由所述第二安全端口的所述数据处理系统的第二安装。

4. 按照权利要求 1 的方法，其中，所述数据处理系统还包括与所述第二安全端口相关联的加密模块，所述动态路由步骤包括:

首先使用所述加密模块来加密所述第一文件。

5. 按照权利要求 4 的方法，其中，所述配置步骤包括:

提取所述客户机系统的 IP 地址;

将所述IP地址置于所述第二安全端口的配置中，其中，所述第二安全端口自动识别来自所述客户机系统的重新安装操作，并且重新建立与所述客户机系统的会话。

6. 按照权利要求1的方法，其中，所述预设访问许可是在链接到所述第一文件的元数据内的一个比特，并且所述方法还包括读取所述比特的值以评估所述第一文件是否需要安全访问。

7. 按照权利要求1的方法，其中，所述预设访问许可包括识别哪些特定用户被允许经由安全访问而访问所述第一文件，所述方法还包括：

将所述客户机系统的用户与具有访问所述文件的许可的所述特定用户相比较；以及

当所述用户是所述特定用户之一时，自动启动经由所述第二安全端口重新路由所述第一文件的传输。

8. 按照权利要求1的方法，其中，所述第一标准端口经由第一非安全网络连接到所述客户机系统，并且所述第二安全端口经由第二安全网络来连接到所述客户机系统。

9. 按照权利要求1的方法，其中：

所述数据处理系统是在网络内的服务器，所述网络具有：第一子网，它将所述第一标准端口连接到所述客户机系统；以及第二子网，它将所述第二安全端口连接到所述客户机系统；

所述第一文件被存储在文件系统内；

所述检查步骤包括访问所述文件系统并且定位所述第一文件；以及

所述路由步骤包括：当所述文件要求安全访问时，经由所述第二子网来传输所述文件，并且当所述第一文件不要求安全访问时，经由所述第一子网来传输所述第一文件。

10. 一种为至少第一文件的传输提供安全的系统，用于数据处理系统内，所述数据处理系统包括（1）存储介质，其上存储了所述至少第一文件，所述第一文件具有预设访问许可，（2）至少第一标准端口和第二安全端口，用于将所述数据处理系统连接到外部客户机系统，和（3）用于经由所述第一标准端口和所述第二安全端口而选择性地路由所述至少一个文件的传输的逻辑部件，所述为至少第一文件的传输提供安全的系统包括：

检查逻辑部件，用于响应于由所述外部客户机系统做出的对所述第一文

件访问的请求，检查所述第一文件的所述预设访问许可；

重新配置逻辑部件，用于配置所述第一标准端口和所述第二安全端口，以支持通过所述客户机系统的安装；以及

动态路由逻辑部件，用于当所述第一文件的所述预设访问许可表示对于所述第一文件需要安全访问时，经由所述第二安全端口而动态地路由所述第一文件向外部客户机系统的传输，所述动态路由逻辑部件包括：

配置逻辑部件，用于首先配置所述第二安全端口以支持从所述客户机系统接收的重新安装操作；

逻辑部件，用于终止所述客户机系统在所述第一标准端口上的当前安装；以及

逻辑部件，用于存储所述当前安装的会话参数以使能在所述第二安全端口上的所述会话的无缝继续。

11. 按照权利要求 10 的系统，还包括：

逻辑部件，用于当所述预设访问许可表示正常的访问是足够时，经由所述第一标准端口路由所述第一文件的传输。

12. 按照权利要求 10 的系统，还包括：

逻辑部件，用于使能经由所述第一标准端口的所述数据处理系统的第一安装；以及

逻辑部件，用于仅仅当所述第一文件要求安全访问时，使能经由所述第二安全端口的所述数据处理系统的第二安装。

13. 按照权利要求 10 的系统，其中，所述数据处理系统还包括与所述第二安全端口相关联的加密模块，所述动态路由逻辑部件包括：

逻辑部件，用于首先使用所述加密模块来加密所述第一文件。

14. 按照权利要求 10 的系统，其中，所述动态路由逻辑部件中的所述配置逻辑部件包括：

逻辑部件，用于提取所述客户机系统的 IP 地址；

逻辑部件，用于将所述 IP 地址置于所述第二安全端口的配置中，其中，所述第二安全端口自动识别来自所述客户机系统的重新安装操作，并且重新建立与所述客户机系统的会话。

15. 按照权利要求 10 的系统，其中，所述预设访问许可是在链接到所述第一文件的元数据内的一个比特，所述为至少第一文件的传输提供安全的系

统还包括读取所述比特的值以评估所述第一文件是否要求安全访问。

16. 按照权利要求 10 的系统，其中，所述预设访问许可包括识别哪些特定用户被允许经由安全访问而访问所述第一文件，所述为至少第一文件的传输提供安全的系统还包括：

逻辑部件，用于将所述客户机系统的用户与具有访问所述文件的许可的所述特定用户相比较；以及

逻辑部件，用于当所述用户是所述特定用户之一时，自动启动经由所述第二安全端口重新路由所述第一文件的传输。

17. 按照权利要求 10 的系统，其中，所述第一标准端口经由第一非安全网络连接到所述客户机系统，并且所述第二安全端口经由第二安全网络连接到所述客户机系统。

18. 按照权利要求 10 的系统，其中：

所述数据处理系统是在网络内的服务器，所述网络具有：第一子网，它将所述第一标准端口连接到所述客户机系统；以及第二子网，它将所述第二安全端口连接到所述客户机系统；

所述第一文件被存储在文件系统内；

所述检查逻辑部件包括用于访问所述文件系统并且定位所述第一文件的部件；以及

所述动态路由逻辑部件包括：用于当所述文件要求安全访问时，经由所述第二子网来传输所述文件，当所述第一文件不要求安全访问时，经由所述第一子网来传输所述第一文件的部件。

分布式文件系统网络安全扩展

技术领域

本发明一般地涉及网络系统，具体涉及分布式文件系统。更具体而言，本发明涉及访问分布式文件系统的安全特性。

背景技术

在通用计算系统中，诸如支持各种版本的 Unix 操作系统（OS）的那些计算系统，应用程序可以通过一组包括文件系统的操作系统服务而访问在盘驱动器上存储的数据（Unix 是注册商标，由开放组（Open Group）排它许可）。文件系统可被计算机系统使用来将大的文件集合组织为独立的文件和文件目录，并且将那些文件映射到诸如盘的存储器件。文件系统包括两个主要组件，控制文件的物理表示的程序和被存储在盘上的文件本身。

在分布式计算环境中，可以通过通信网络或其他耦接设施来相互连接多个计算系统，并且所述多个计算系统可以通过分布式文件系统来共享文件。通常在服务器节点（控制对包含文件系统数据的盘的访问的计算系统）上执行文件系统输出程序，而通常在客户机节点（用于访问盘上的文件的其他计算系统）上执行文件系统输入程序。在客户机节点上的用户对于共享文件的访问被称为“远程”访问。由在服务器节点上的用户进行的对于共享文件的访问被称为“本地”访问。

网络文件系统被存储在网络的服务器或节点上，并且所述服务器或节点是通常远程链接到网络的客户机终端（即，用户计算机）可访问的。实际链接可以是标准的基于以太网的局域网（LAN）那样的有线链接或诸如蓝牙虚拟专用网络（VPN）之类的无线链接。经由客户机终端访问文件系统的过程被称为“安装文件系统（mounting a filesystem）”。当安装文件系统时，所述文件系统的控制程序从盘读取关于文件系统对象的布局的特定信息。根据这个信息，所述文件系统的构造被称为“虚拟文件系统”或 Vfs 的数据结构。每次打开文件或使得可以访问，所述文件系统建立被称为“vnode”的数据结构，它链接到 vfs。

每个 vnode 包含关于给定文件的信息，并且包括对于物理文件系统数据结构的引用。所述物理文件系统数据结构包含信息，诸如文件的拥有者、文件大小、文件建立日期和时间以及文件块在盘上的位置。文件系统包括管理文件的内部数据，它被称为元数据。元数据可以包括用于表示下列的数据：文件的每个数据块存储的位置；存储文件的存储器修改版本的位置；以及文件的许可和拥有者。

随着越来越多的公司使用远程/网络可访问的分布文件系统来电子存储和随后检索文件/文档——一些包括敏感信息，分布式文件系统的安全性变得越来越重要。标准的 IP 安全（IPSec）套件被引入，并且提供了两个主要的安全特征：验证和加密。换句话说，IPSec 保证发送和接收机确实是它们声称的内容，IPSec 使得能够在运行中加扰数据，因此如果被截取，则所述数据将是不可理解的。

因此，大多数系统在初始安装期间需要验证用户，这通常包括验证用户口令等。但是，口令保护和类似的安全措施由于对于非法闯入是开放的而声名狼藉，并且可能容易泄密，所以这个产业已经认识到：一旦获得对于文件系统的一般访问，则口令保护系统对于敏感文件提供了很小的保护。

更高级的黑客也通过在被授权的安装期间窃取传输和在从文件系统向客户机系统传输数据时来简单地复制数据获得对存储在文件系统上的文件的访问。这种情况发生的原因是：对于大多数口令保护的分布式文件系统，一旦完成了安全登录的几个级（口令验证等），则文件根据文件系统的实际传输以明文出现。因此，当所述传输包括很敏感的数据时，需要另外的安全措施来保证不能通过简单地在传输期间复制文件而获得明文数据。

通过这后一种方法可协调敏感信息的安全性的容易程度在一定程度上取决于授权的用户利用安装/访问文件系统的介质。例如，无线访问/传输通常比有线网络介质更易于被窃取和非法闯入。但是，甚至标准的以太网也可能容易地被破坏而不能被检测，因此，标准以太网对路由敏感数据也是不安全的选择。

如上所述，产业界通过在安装文件系统期间对所有被传输的数据应用强的加密来对传输介质上安全性增长的需求作出响应。当前，存在几种被设计来为在客户机系统/节点和主管所述文件系统的服务器之间传输的安全提供的加密算法和标准（例如，无线传输层安全）。利用强的加密要求对于所有的

业务在客户机系统和服务器上施加沉重的处理负担。系统的整体性能变差，并且希望实现对它们的文件系统访问的全系统加密的公司产生大的花费。加密被内置在通信机制中，并且虽然大多数业务可能不需要那个安全级（例如，非敏感信息/文件），但是加密被施加到客户机系统和服务器之间的所有业务。

随着公司向可能是移动用户提供远程访问并且希望远程连接网络，访问文件系统的无线系统的利用正在增加。但是，无线连接比有线连接更容易受到非法闯入的影响。一些无线用户使用 WTLS，但是这个安全特征被公知为较弱的安全级。一种解决方案需要虚拟专用网络（VPN）数据封装/加密来访问敏感数据，即使当多数客户机正在经由令牌网访问文件系统时也是如此。当服务器加密和解密所有数据时，这个 VPN 数据封装进一步负面地影响服务器的速度。

也可能配置多个 VPN 或在 VPN 上的服务器来识别 IP 地址或子网，并且仅仅需要对于特定的子网进行加密。这个解决方案的一个问题是分布式文件系统服务器的管理员必须知道不在网络内的每个无线节点。如果在它们的部门中的组织建立无线网络，则需要使得服务器管理员了解所述无线网络，以便可以向 IP 地址的 VPN 列表增加所述子网。

2000 年 6 月的 MSDN 杂志中的 Keith Brown 的 “Web Security: Putting Secure Front End on your COM+ Distributed Applications” 公开了要求使用 HTTPS 协议的 IIS metabase 的使用。IIS metabase 用于指令客户机使用 HTTPS 协议。

根据上述情况，本发明意识到有希望具有一种方法、系统和数据处理系统，用于当请求访问在分布式文件系统上的敏感文件时动态地实现增强的安装安全。每当在进行会话期间要访问敏感文件/数据时，自动提供安全安装的方法和系统将是受欢迎的改进。还期望如果以无缝的方式完成了安全安装，则授权的用户接受对于敏感文件的访问而不经历连接断开和重新安装验证处理，同时通过经由更安全的安装来路由敏感文件而防止了敏感文件未经授权而被捕获。

发明内容

所公开的是一种方法、系统和计算机程序产品，其当请求访问联网的文件系统上的敏感文件时动态地实现文件系统的增强的安装安全性。客户机系

统启动对于文件系统的文件的访问的标准安装和验证处理。当客户机系统的用户试图访问特殊标签的敏感文件时，服务器执行终止当前安装的软件代码。服务器被重新配置以将重新安装服务器的任何企图从与客户机相关联的IP地址路由到安全端口。当服务器终止会话时，客户机系统被编程来自动尝试重新安装服务器。服务器在重新安装操作期间识别客户机的IP地址，并且将客户机路由到所述安全端口。

因此，每当根据标准安装启动的正在进行的会话期间要访问敏感文件/数据时自动提供安全安装。因此，以无缝的方式来完成经由安全安装的路由，以便授权的用户接收对于敏感文件的访问而不经历大的延迟或可视的断开连接，即，要求用户启动的重新安装和验证处理。同时，通过经由所建立的更安全的安装而路由敏感文件来防止未经授权地捕获敏感文件。

附图说明

现在参照附图而仅仅举例来说明本发明，其中：

图1A是可以实现本发明的特征的数据处理系统的方框图；

图1B是按照本发明的一个实施例的、具有表示所需要的安全级的安全标签的、表示图1A的文件系统内的文件的方框图；

图2是是按照本发明的一个实施例的、可以实现本发明的特征的分布式网络的方框图；

图3A是按照本发明的一个实施例的、客户机在经由标准安装的访问期间被提供访问敏感文件的处理的流程图；

图3B和3C是按照本发明的一个实施例的、服务器监视和控制客户机请求访问敏感文件以保证经由安全信道路由那些文件的访问的处理的流程图；

图4是图解按照本发明的一个实施例的、用于无缝地完成在单个连续会话期间、在文件系统上的客户机会话从标准的非安全信道向安全信道的转换的逻辑部件的方框图。

具体实施方式

现在参照附图，并且特别是参照图1A，图解计算机系统的方框图，所述计算机系统可以被用作主管分布式文件系统的服务器或用于安装主管分布式文件系统的服务器的客户机系统。计算机系统100包括处理器102和存储器

104，其经由系统总线/互连线 110 而连接。计算机系统 100 也包括输入/输出（I/O）信道控制器（CC）109，它耦接到互连线 110。I/O CC 109 提供到包括盘的冗余阵列（RAID）114 的 I/O 器件 106 的连接。RAID 114 存储在必要时由被处理器执行的应用程序安装到存储器的指令和数据。按照所述说明性实施例，RAID 114 为构成文件系统 112 的多个文件提供存储介质。

计算机系统 100 还包括网络连接器件 108，它可以在其中包括有线调制解调器、无线调制解调器和以太网卡。通过 I/O 信道控制器（I/O CC）109 来路由向／从 I/O 器件 106 和网络连接器件 108 的访问，所述 I/O 信道控制器（I/O CC）109 包括当需要时经由“安全”路径/信道/端口来完成自动重新建立到计算机系统 100 的安装或来自计算机系统 100 的安装的逻辑部件，如下进一步说明。

计算机系统 100 包括操作系统(OS)122、文件系统软件应用程序 124、安装代码 125 和分布文件系统网络安全扩展（DFNSE）126。当计算机系统 100 正被用来主管文件系统 112 时，文件系统软件应用程序 124 提供文件系统 112 的基本的访问、维护和更新。

当在客户机系统内时，文件系统软件应用程序 124 包括安装代码 125 的客户机版本，用于完成主管文件系统的服务器的安装和自动重新安装。在图解的实施例中，每当在客户机未完成服务器的卸装的情况下服务器的已建立的安装被破坏/丢失的时候，由客户机系统实现自动重新安装处理。在所述的实施例中，服务器可以发出 FYN 命令以终止当前的安装，因此迫使客户机启动服务器的重新安装。响应对于要求特殊安全保护的特定文件的访问而发出 FYN 命令，如下更详细地说明。

返回图 1A，并且说明文件系统软件应用程序 124，当在服务器内执行时，文件系统软件应用程序 124 包括用于接收、维护和验证各种用户和客户机系统的证书信息的代码、用于维护文件系统 112 的代码和用于选择性地启动安全软件和相关的响应的代码，它们被称为分布式文件系统网络安全扩展（DFNSE）126。DFNSE 126 在此提供了本发明的特征的主干，并且下面参照图 3A-3C 和 4A 来说明在服务器上执行 DFNSE 126。在基本级，DFNSE 126 确定对于文件系统 112 的特定文件允许/授权什么级的安全访问以及何时启动的本发明的增强安全措施。

现在参见图 2，其图解了包括多个互连的计算机系统的示例网络，它可

与图 1 的计算机系统 100 被类似地配置，其有益地用于提供服务器或客户机功能，以便分别主管或访问分布式文件系统。网络 200 包括在三个（或更多）互连服务器 203 上主管的分布式文件系统 202。网络 200 也包括经由网络干线 210 而连接到分布式文件系统 202 的多个客户机系统 201。网络干线 210 包括一个或多个网络连接系统（或子网），其可以按照诸如以太网或令牌网之类的网络协议来配置。这些子网可以例如是有线或无线的局域网（LAN）或广域网（WAN），诸如因特网。另外，子网也可以包括光纤网络。

分布式文件系统 202 经由在至少一个服务器 203 上的一个或多个端口（未示出）而直接耦接到网络干线 210。客户机系统 201 可以或者直接耦接到网络干线（有线）或经由无线天线 207 图示的无线介质而通信地连接。客户机系统 201 经由各种可用介质之一而访问分布式文件系统 202，所述可用介质利用各种网络配置之一，每个具有对非法闯入的不同级的敏感度。因此，客户机系统 201 可以经由非安全的无线网络 227 而访问和安装文件系统 202，或者客户机系统 201 可以利用安全光纤网络 225 来安装文件系统 202。为了以简单方式说明本发明，将假定无线网络 227 是没有加密的标准的非安全网络，而假定光纤网络 225 是具有加密的特殊的安全连接。每个连接经由服务器 203 可用的端口的不同的一个而路由，在此支持文件系统 202 的安装。

图 1B 图解了具有包括文件系统 202 的文件的更详细的描述的、文件系统 202 的方框图。如图所示，文件系统 202 包括控制块 131 和多个文件 132a-n，其中每个包括元数据标签 112，它具有首标/标识符字段 334 和安全字段 336。首标/ID 字段 334 包含关于文件 ID 和访问文件的用户的信息。安全字段是单比特字段，它表示可归因于那个文件的安全级，以及结束允许的用户访问的类型。按照所述说明性实施例，要求最高安全级，并且被限制为只在安全安装时被访问的特定文件（例如，文件 1 和 3）在它们各自的元数据的安全字段 336 中被标签为“1”。不这样加标签（即，标签为 0）的其他文件是普通的文件（例如，文件 2），并且可以被任何授权的用户访问，而不用特殊的安全安装。

如上所述，本发明引入了一种增强的安全机制，它在所述说明性实施例中被称为 DFNSE（分布文件系统网络安全扩展）。对于 DFNSE，网络系统服务器能够从文件或目录相关联的文件许可推断当提供特定用户访问文件时所需要的网络安全的级别。DFNSE 是服务器级的文件系统安全增强应用程序和

/或规程。因此，对于 DFNSE，仅仅服务器需要了解网络连接或由服务器使用的适配器。

在能够向文件系统提供安装以实现 DFNSE 的每个服务器中，提供了特定硬件、逻辑部件和软件部件。图 4 是图解一些这些部件的方框图。如在图 4 中所示，服务器 203 可以包括两个以太网网络适配器（或端口）：en0 403，它是安全的；以及 en1 405，它是不安全的。在一个实施例中，在这些适配器之后的网络拓扑是一致的。即，所选择的子网本身提供了安全，并且服务器能够动态地根据所要求的安全级在子网之间选择。在另一个实施例中，向安全的适配器 en0 403 提供了附加的加密或其他安全特征。

En0 403 连接到对所有敏感数据路由所用的光纤网络 225，而 en1 405 连接到基于标准以太网的有线网络 221，并且用于路由传送所有其他（非敏感）数据通信。En1 405 是用于安装文件系统的服务器的默认端口。所述示例实施例假定标准以太网可以被破坏而没有检测到的容易性使得以太网成为路由敏感数据的不安全选择。在安装文件系统期间，详细了解每个文件的文件许可 334 和安全级 336 的服务器跟踪用户访问，并且根据适于被访问的文件的文件许可来确定何时迫使客户机转换到安全网络。按照所述说明性实施例，网络拓扑对于安全和不安全路由是一致的，以便在从非安全到安全子网的转换期间不需要附加的硬件和/或路由协议更新来用于不同的拓扑。

图 4 的服务器 203 也包括安装控制器 407，它对于文件系统 202 执行传统的安装支持和卸装操作以及按照本发明的特征的重新安装配置。安装控制器 407 包括 DFNSE 126 并且优选地被体现为在服务器 203 上执行的软件代码。DFNSE 126 操作来触发安装控制器 407 以经由或者标准端口 En1 405 或安全端口 En0 403 将安装请求路由。当在安全端口上实现加密时，服务器 203 也包括加密模块 409，它与 DFNSE 126 和 En0 403 结合使用。

在文件系统访问期间，当在服务器 203 接收对敏感操作的访问的请求时，安装控制器 407 将客户机的 IP 地址标注为需要访问数据的 IP 地址。服务器 203 然后断开当前的连接（即，服务器向客户机传输 FYN）。客户机试图自动重新连接，并且安装控制器 407 在重新安装期间识别客户机 IP 地址。客户机的会话然后转向安全 SSL 端口。因此，当经由标准端口来提供主要访问时，当需要访问敏感数据/文件时访问动态地转换到 SSL 安全端口。

现在转向图 3B，图解了一个处理的流程图，通过所述处理，在主管文件

系统的服务器的上述硬件/逻辑配置内实现软件实现的 DFNSE 安全特征。所述处理以在服务器的标准端口从客户机接收的标准安装请求开始，如在块 321 所示。用户被提示输入验证数据（口令等），并且从数据分组检索客户机系统的 IP 地址，如在块 323 所示。在标准端口打开会话，并且 IP 地址和用户的验证数据被存储在与特定会话链接的参数文件内，如在块 325 所示。一旦建立了所述会话，即，与访问许可等相关联的服务器逻辑部件监控如块 327 所示的用户的交互和在块 329 做出的是否用户请求访问敏感文件的判定。

使用在远程客户机上的用户的授权/证书和被访问的文件的许可来编程满足对于文件的客户机请求的服务器。如果被访问的文件不是敏感的，则在标准端口向用户提供正常的访问，如在块 331 所示。但是，当被客户机请求的文件是在被允许访问之前要求更安全的信道的敏感文件时，在块 333 进行下一个判断用户是否具有访问文件的合适访问许可。如果用户没有合适的访问许可，则拒绝所述请求，如在块 335 所示。但是，如果用户的证书表示用户具有访问特定文件的许可，则使 DFNSE 安全协议有效，如在块 337 所示。DFNSE 的有效使得服务器通过下述方式来迫使客户机的卸装，即，向客户机发出 FYN，并且同时配置更安全的端口以从接受具有使用会话参数存储的 IP 地址的客户机的重新安装。服务器然后经由所述安全端口来向文件提供安全访问，如在块 339 所示。

图 3A 是主要从用户/客户机系统的角度来看的本发明的实现方式中涉及的处理的流程图。当用户（经由客户机系统）首先如在块 302 所示安装用于主管文件系统的服务器、并且如块 304 所示请求访问所述文件系统时，所述处理开始。当客户机初始安装 NFS 文件系统时，按照默认、通过标准 TCP 连接来完成所述安装。例如，所述连接可以是公知的 NFS 端口 2048。服务器具有被绑定到这个端口的监听套接字（listening socket），并且按照标准（非安全）协议来操作。注意，在所述说明性实施例中，通过 DFNSE 协议来增强标准协议，当请求访问敏感文件时实现所述 DFNSE 协议。

当从客户机请求连接时，服务器的监听套接字基本上复制其本身，并且将所述连接引向远程客户机。所述监听套接字然后保持开放以处理其他的连接请求。客户机的验证被启动，如在块 306 所示，并且在块 308 确定是否客户机的验证成功。如果客户机/用户验证处理是不成功的，则拒绝对文件系统的访问，并且如在块 310 所示断开安装。然后，处理结束，如在块 311 所示。

否则，打开一个会话，并且用户访问文件系统，如在块 309 所示。

如在块 312 所示，客户机系统对于断开的连接监控连接，并且如块 314 所示，确定所述连接是否变为无响应，或者在服务器端被过早断开（即，理想上是在接收到服务器发出的 FYN 时）。当所述连接变得无响应或断开时，客户机启动被路由到由服务器表示的端口的重新安装，如在块 316 所示。

值得注意地，虽然实际的端口可能是客户机系统不知道的，但是在服务器的安全端口进行响应于服务器启动的卸装的重新连接。利用 DFNSE 的安全协议并且基于对于哪个端口是安全的并且会话是否要求安全端口的了解，服务器能够请求所述客户机在安全端口重新安装。例如，可以使得客户机利用运行加密套接字层的端口来重新安装。注意，不需要用户行为来完成重新安装和端口转换过程。对于服务器端的卸装和随后的重新安装的监控全部作为客户机系统的背景过程而发生，并且使得用户（客户机）不知道向更安全端口转换。

通过图 3C 的流程图来图解经由在服务器端的更安全端口而重新路由所需要的内部处理的更详细的情况。当 DFNSE 识别对于敏感文件的访问时，所述处理开始，如块 351 所示。服务器检查当前的端口安全，如块 352 所示。在块 354 确定当前端口安全对于访问所请求的文件是否是足够的（取决于文件有多敏感，在所述说明性实施例中，这是通过读取文件的安全位来推断的）。如果当前的端口安全对于访问所请求的文件是足够的，则提供访问，如块 356 所示。

在一个替代实施例中，可以选择性地自动化重新安装功能，并且处理需要接着确定是否使能了自动重新安装的特征。对于这个替代实施例，如果不使能自动重新安装能力，则实际上向用户提示经由安全安装而重新安装。

返回图 3C 的图解实施例，当端口安全不足时，服务器通过选择用于会话的更安全的端口（例如 En0）来响应，如块 358 所示。服务器提取包括客户机的 IP 地址的会话的验证和安装参数的快照（snapshot），并且向更安全的端口的控制逻辑部件传送这些参数，如块 360 所示。所述传送以很小的延迟发生，并且所述更安全的端口因此被自动配置来从客户机接收重新安装，并且继续支持进程中的会话。在已经配置了所述安全端口后，向安装控制器提供对应的端口号与客户机的 IP 地址。服务器终止在第一标准端口的安装，并且当从客户机接收到重新安装时，经由所述更安全的端口来重新建立所述会话，

如块 362 所示。

需要注意，响应于服务器终止初始的安装，客户机启动重新安装，用户将所述重新安装引导到第二安全链路。这重新建立了客户机的初始会话。但是经由第二端口。重新建立所述连接涉及检查客户机 IP 地址，并且将其匹配到被建立来接收来自那个 IP 地址的连接的端口。整个处理在后台中发生，因此从用户角度来看完成了端口的无缝转换。

在一个替代实施例中，通过访问特定文件的用户（或所选择的客户机系统）来确定特定文件的安全级。因此，如果文件访问许可仅仅被限制到文件系统管理员，则安全级高，而提供给普通雇员的文件访问许可表示所需要的安全性为较低级。当用户初始建立文件并且向那个文件分配访问许可时，完成文件的安全级的确定。一旦文件置于文件系统内，则所述文件自动继承适当的网络安全保护。对于这种实现方式，对于在文件系统内的文件的现有文件许可（例如，用户、组、其他的 UNIX –rwx，rwx）包进在此提供的安全模型内，而不要求广泛的系统管理和配置。因此，本发明消除了在每个文件基础上重新配置现有文件系统的需要。对于本发明，也不需要将敏感文件移动到安全服务器。

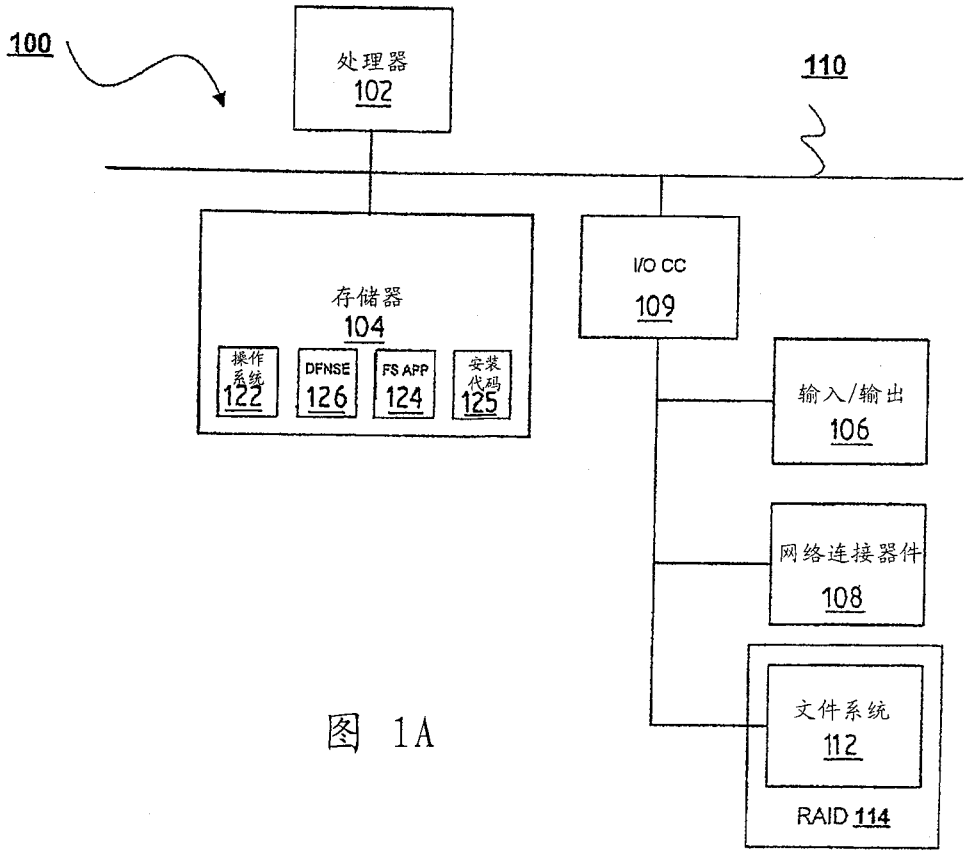

100
处理器
102
110
存储器
104
操作系统
122
DFNSE
126
FS APP
124
安装代码
125
I/O CC
109
输入/输出
106
网络连接器件
108
文件系统
112
RAID 114

图 1A

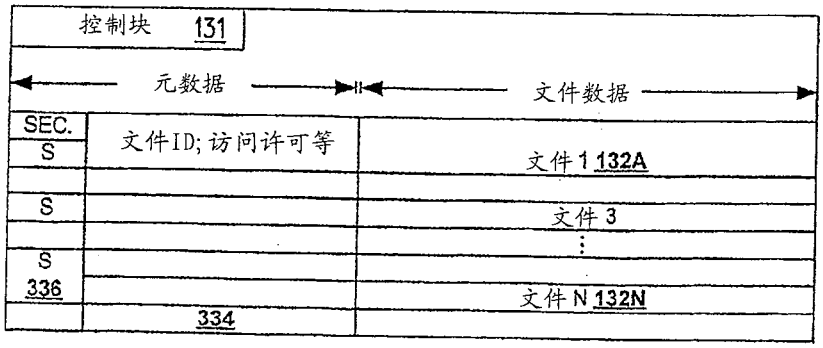

控制块 131
元数据
文件数据
SEC.
S
文件ID;访问许可等
文件1 132A
S
文件3
S
336
文件N 132N
334

图 1B

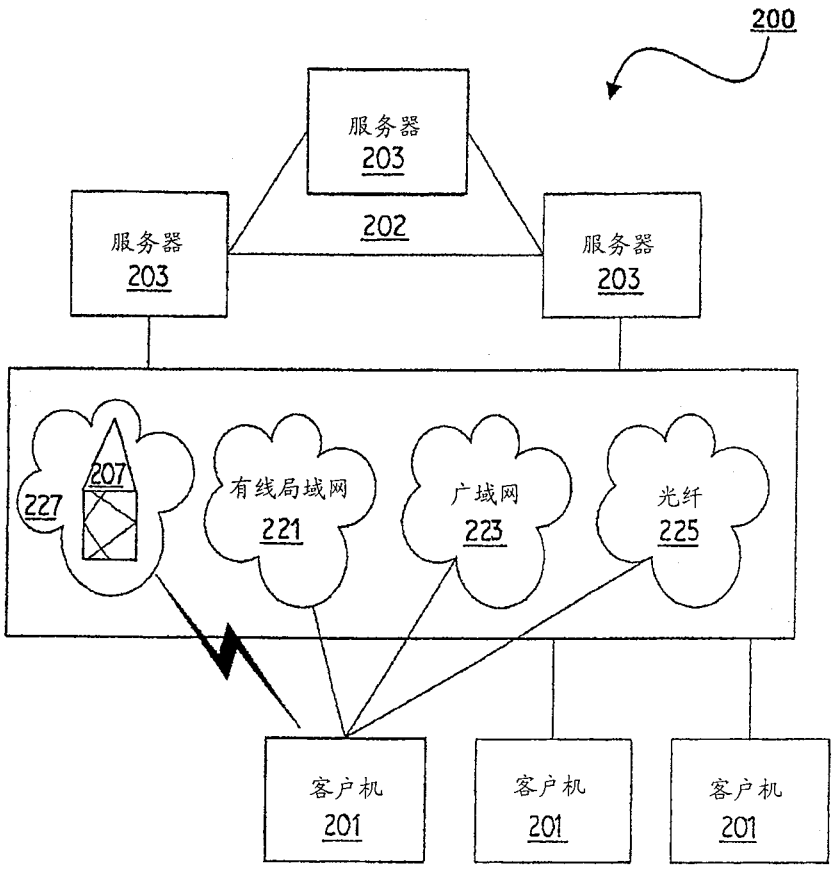

200
服务器
203
202
服务器
203
服务器
203
207
227
有线局域网
221
广域网
223
光纤
225
客户机
201
客户机
201
客户机
201

图 2

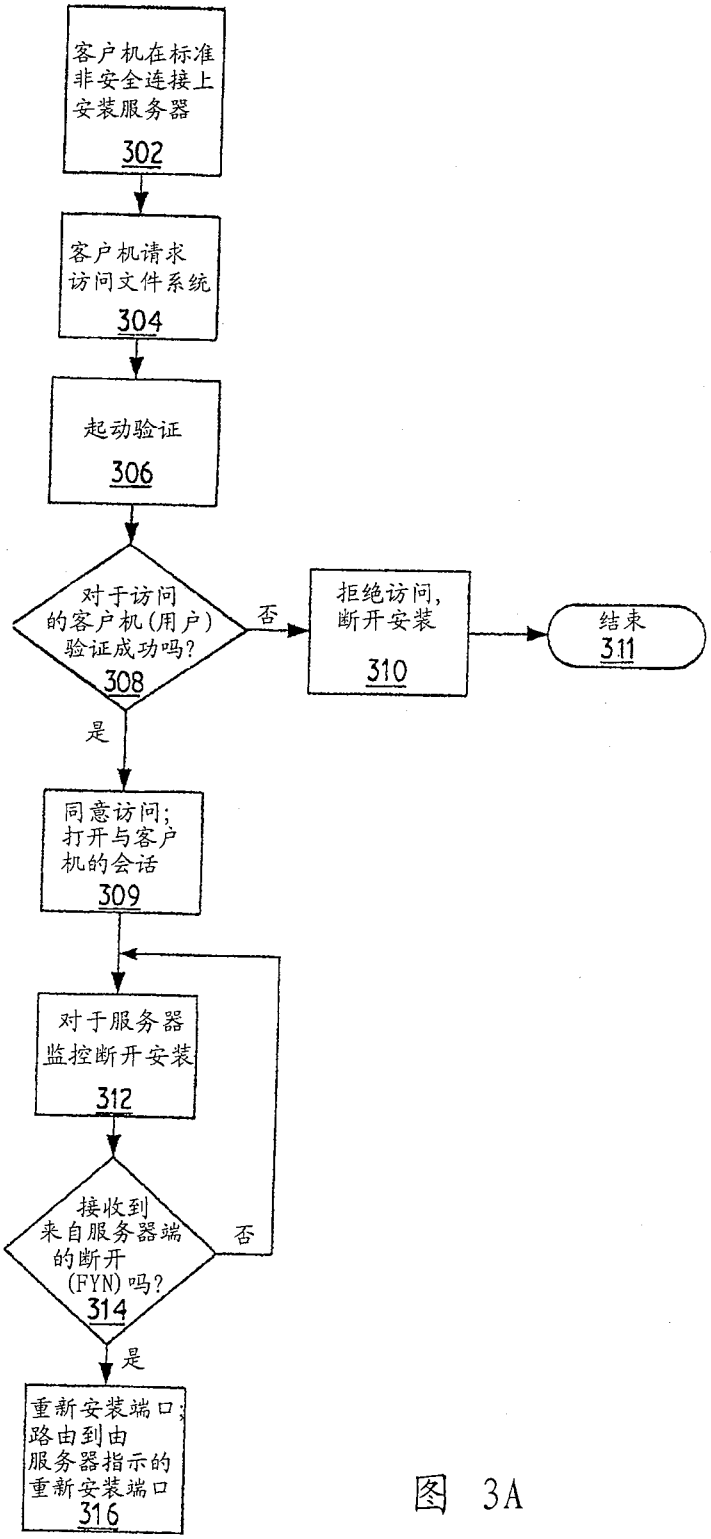

客户机在标准非安全连接上安装服务器
302
客户机请求访问文件系统
304
起动验证
306
对于访问的客户机(用户)验证成功吗?
308
否
拒绝访问,断开安装
310
结束
311
是
同意访问;打开与客户机的会话
309
对于服务器监控断开安装
312
接收到来自服务器端的断开(FYN)吗?
314
否
是
重新安装端口;路由到由服务器指示的重新安装端口
316

图 3A

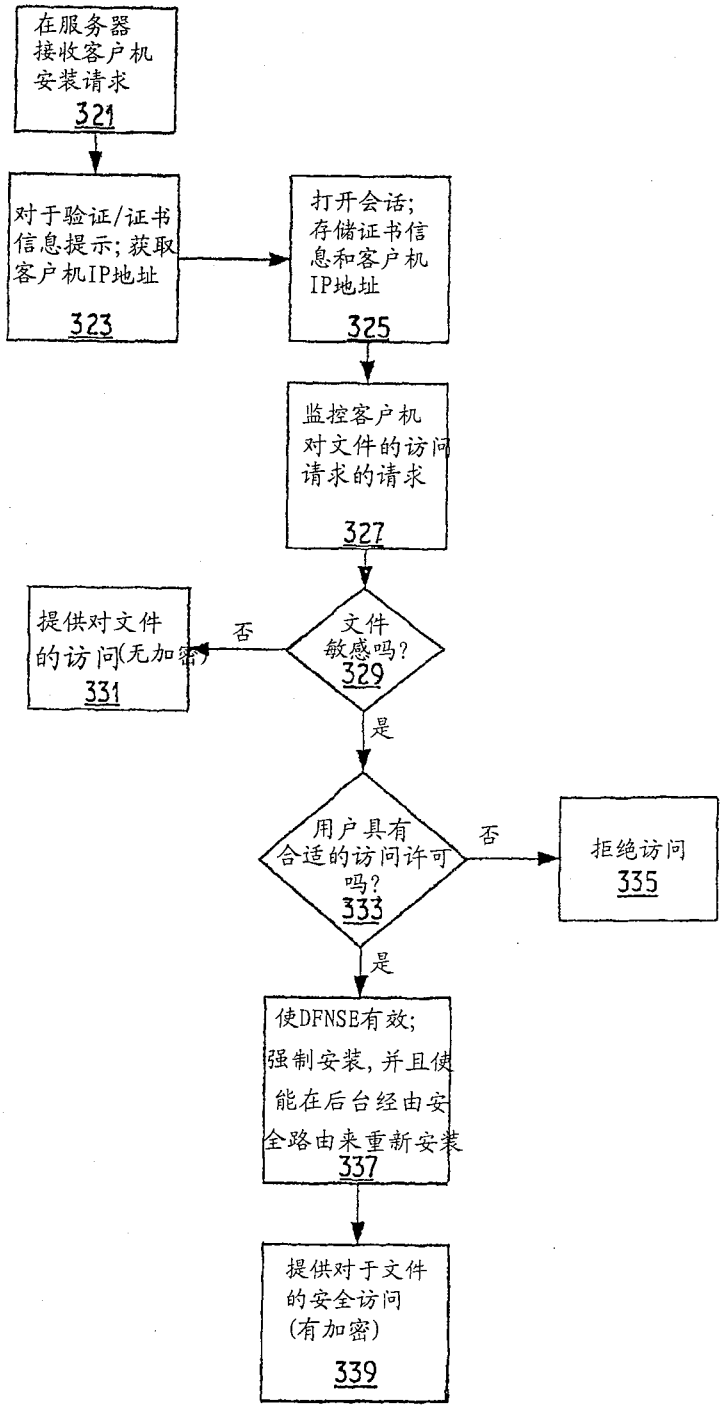

在服务器接收客户机安装请求
321
对于验证/证书信息提示；获取客户机IP地址
323
打开会话；存储证书信息和客户机IP地址
325
监控客户机对文件的访问请求的请求
327
文件敏感吗?
329
否
提供对文件的访问(无加密)
331
是
用户具有合适的访问许可吗?
333
否
拒绝访问
335
是
使DFNSE有效；强制安装，并且使能在后台经由安全路由来重新安装
337
提供对于文件的安全访问(有加密)
339

图 3B

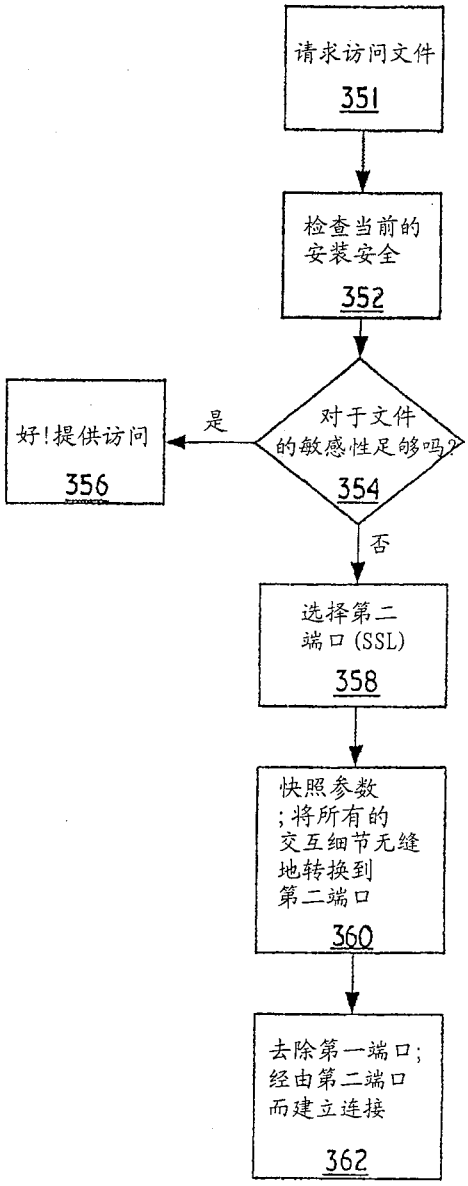

请求访问文件
351
检查当前的安装安全
352
对于文件的敏感性足够吗?
354
是
好!提供访问
356
否
选择第二端口(SSL)
358
快照参数;将所有的交互细节无缝地转换到第二端口
360
去除第一端口;经由第二端口而建立连接
362

图 3C

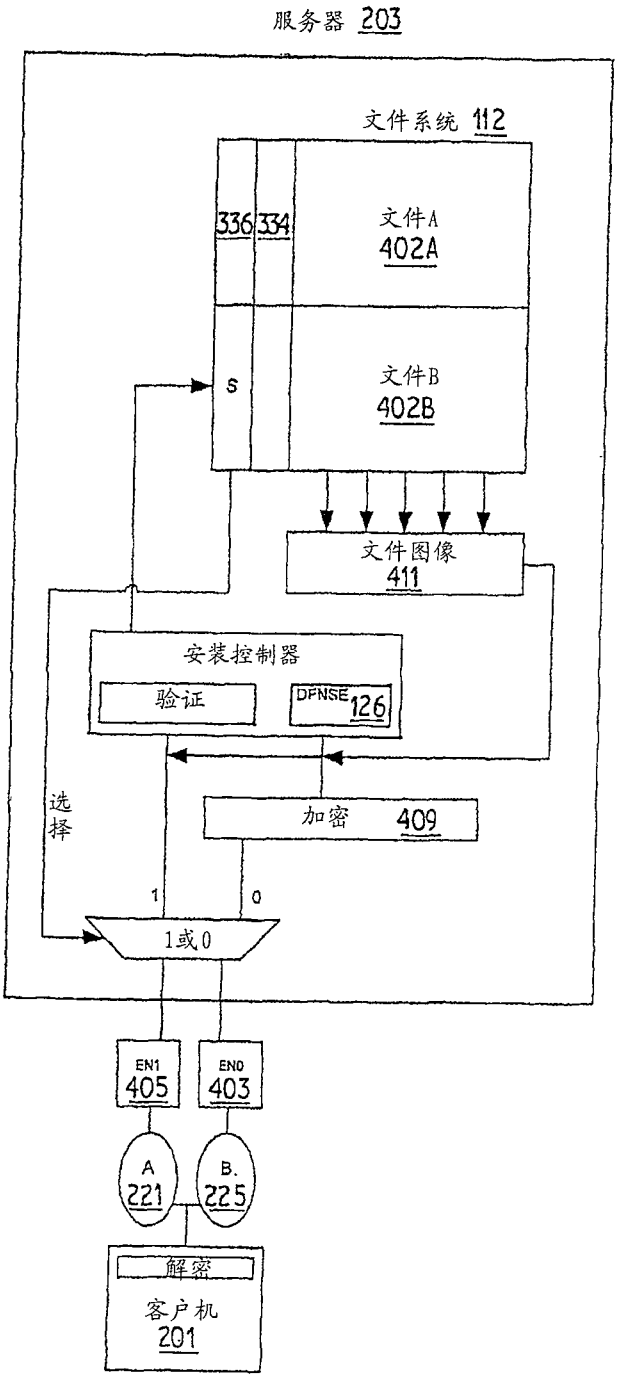

服务器 203
文件系统 112
336
334
文件A
402A
S
文件B
402B
文件图像
411
安装控制器
验证
DFNSE 126
选择
加密 409
1
0
1或0
EN1
405
EN0
403
A
221
B.
225
解密
客户机
201

图 4