(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 102265282 B
(45)授权公告日 2015.04.08

(21)申请号 200980153007.4
(22)申请日 2009.12.16
(30)优先权数据
10-2008-0134892 2008.12.26 KR
(85)PCT国际申请进入国家阶段日
2011.06.27
(86)PCT国际申请的申请数据
PCT/KR2009/007530 2009.12.16
(87)PCT国际申请的公布数据
WO2010/074449 KO 2010.07.01
(73)专利权人 SK电信有限公司
地址 韩国首尔
(72)发明人 权五綱 吴世铉 金玟锡 金星慎正金 南基善
(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 李辉 孙海龙
(51)Int.Cl.
G06F 21/12(2013.01)
(56)对比文件
WO 2008/147827 A2,2008.12.04,
US 2007/0185815 A1,2007.08.09,
CN 1740940 A,2006.03.01,
CN 1818919 A,2006.08.16,
审查员 李文浩

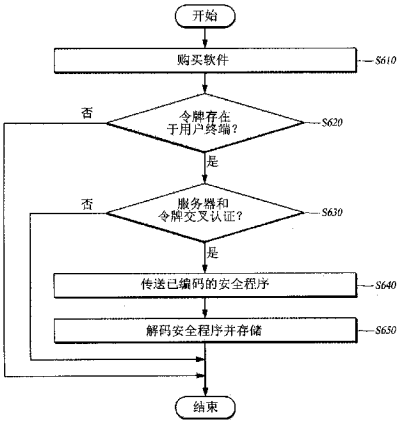
权利要求书2页 说明书8页 附图4页

(54)发明名称

用于保护软件许可的方法、用于保护软件许可的系统、服务器、终端以及计算机可读记录介质

(57)摘要

本发明涉及用于保护软件许可的方法、用于保护软件许可的系统、服务器、终端以及计算机可读记录介质。本发明提供用于保护软件许可的终端，所述终端包括：终端通信器，其连接至耦接的软件狗类型的令牌；终端控制器，其操作和控制特定的软件，检查用于驱动特定软件的安全程序是否存在于所述令牌中，如果存在，则向所述令牌传送用于执行所述安全程序的指令，并且从所述令牌接收执行结果以激活所述特定的软件；以及终端存储器，其用于存储所述特定的软件。本公开保护了软件许可，使其克服了易受反向工程的攻击的缺陷，并且避免了对因特网的依赖以及顾客的不便。



CN 102265282 B

1. 一种软件许可保护终端，所述软件许可保护终端包括：

终端通信器，其与耦接的软件狗类型的令牌协同操作；

终端控制器，其用于操作和控制特定的软件，其检查所述令牌是否具有运行所述特定的软件所必需的安全程序，如果有，则向所述令牌传送用于执行所述安全程序的执行指令，并且从所述令牌接收执行结果以激活所述特定的软件；以及

终端存储器，其用于存储所述特定的软件，

其中，当在运行所述特定的软件的过程中需要安全程序的识别路径的信息时，软件许可保护终端向令牌请求所述安全程序的识别路径的信息，并且在从所述令牌接收所述识别路径的信息时，所述软件许可保护终端识别出在所述令牌中存在所述安全程序。

2. 根据权利要求 1 所述的软件许可保护终端，其中，所述安全程序是包含有运行所述特定的软件所必需的组件的程序。

3. 根据权利要求 2 所述的软件许可保护终端，其中，所述安全程序包括：

标识部分，其包括用于区分所述安全程序的标识的字符串、图标和唯一的数字数据中的至少一个；

代码部分，其包括在所述令牌中运行的所述执行指令；

永久数据部分，其用于存储用作参考的永久数据；以及

动态数据部分，其用于存储执行所述安全程序的历史信息。

4. 根据权利要求 1 所述的软件许可保护终端，其中，所述终端控制器在通过收发经过所述特定的软件和所述令牌之间的共享密钥编码或解码的消息而确认了所述特定的软件和所述令牌之间具有公共的编码方案时，对所述令牌进行认证。

5. 根据权利要求 1 所述的软件许可保护终端，其中，所述终端控制器基于所述识别路径或所述安全程序的信息将输入参数和所述执行指令传送至所述令牌，将所述安全程序从所述令牌装载至可执行存储区域，并接着设置所述输入参数以接收执行相关代码的执行结果。

6. 一种软件许可保护方法，所述软件许可保护方法包括：

执行特定的软件；

在所关联的令牌中检查运行所述特定的软件的安全程序的存在，如果存在所述安全程序，则将用于执行所述安全程序的执行指令传送至所述令牌；以及

在接收到执行所述安全程序的结果时激活所述软件，

其中，传送执行指令的步骤包括：

当在执行所述软件的过程中需要所述安全程序的识别路径的信息时，向所述令牌请求所述安全程序的识别路径的信息；以及

在从所述令牌接收所述识别路径信息时，确认所述安全程序在所述令牌处的存在。

7. 根据权利要求 6 所述的软件许可保护方法，所述软件许可保护方法在所述安全程序识别之后还包括如下步骤：在通过收发经由所述特定的软件和所述令牌之间的共享密钥编码和解码的消息而确认所述特定的软件和所述令牌之间具有公共的编码方案时，对所述令牌进行认证。

8. 根据权利要求 6 所述的软件许可保护方法，其中，传送执行指令的步骤包括：基于所述识别路径或所述安全程序的信息将输入参数和所述执行指令传送至所述令牌。

9. 根据权利要求 8 所述的软件许可保护方法，其中，激活所述软件的步骤将所述安全程序从所述令牌装载至可执行存储区域，并接着对所述输入参数进行设置以接收执行相关代码的执行结果。

用于保护软件许可的方法、用于保护软件许可的系统、服务器、终端以及计算机可读记录介质

技术领域

[0001] 本公开涉及用于保护软件许可的方法、用于保护软件许可的系统、终端以及计算机可读记录介质。更明确地，本公开涉及软件许可保护方法、系统、服务器、终端以及计算机可读介质，其中将软件模块（以下称为安全 (secure)+ 小程序 (applet) ＝安全程序 (seculet)）提供给用于具体操作的软件的用户和购买者，所述软件模块是从服务器到具有内部计算能力的智能卡的令牌或到如耦接至用户终端的软件狗的特定软件的必要运行组件（包括压缩软件情况下的压缩算法、游戏软件中的计分规则、以及文档编辑软件中的对象配置逻辑），然后将鼓励用户检查在令牌软件狗中是否存在安全程序，并且如果存在，则向令牌传送指令以继续执行令牌中的安全程序，由此所接收到的执行结果激活特定的软件。

背景技术

[0002] 通常在包括 CD-ROM 和 DVD-ROM 的媒体上以离线的方式直接销售软件，或者通过软件制造商的因特网网点由顾客下载并支付。为了让软件购买者 / 用户安装产品并使用产品，必须在个人终端中输入所提供的拷贝认证 CD-key，软件制造商由此合法地授权产品的使用。

[0003] 然而，由于以普通文本形式的 CD-key 无遮掩地暴露，它们连同 CD-ROM 的内容一起被无助地反复拷贝以自由服务于非法的第三方个体。他们手头不需要 CD-key，而使用另外的非法 CD-key 生成程序或破解方法进入 CD-key 认证程序本身，以最终删改拷贝认证程序，甚至使得 P2P 站点不可控地在人群中进行分发，因此致命地挫败许多保护软件版权的努力。

[0004] 同时，常规技术中存在优于 CD-key 认证方案的编码（或加密）密钥方法的硬件狗，但是通过对其认证逻辑进行反向工程可以很容易将它们击败，并且缺点是软件的具体功能产出成本上的低效。

[0005] 响应于此，提供额外的硬件设备以附接至打印机的终端端口或 USB 端口，以便检查它的存在，或者将设备配置为存储编码 / 解码密钥值以及算法，直到已编码的代码在软件执行时被解码。然而，使执行的软件在可载入终端存储器之前被解码的结构上的限制允许越过保护方案以频繁侵入软件，并且甚至给非专业的普通公众提供开放的机会去使用可用的自动攻击工具以实际上从事违反版权保护技术的活动，特别是一旦它们变得更加普及。此外，使用虚拟环境（虚拟机）以挫败反向工程尝试并保护用于软件认证密钥的鉴别逻辑，并统计示出实际的攻击以及自动攻击工具的分布。

[0006] 公开

[0007] 技术问题

[0008] 本公开试图提供软件许可保护方法、系统、和服务器、终端、以及计算机介质可读的介质，其中，特定软件的用户 / 购买者被提供有运行来自服务器的软件所必需的安全程

序的组件，其被提供到通常附接至用户终端的软件狗类型的令牌，在软件执行期间提示用户检查在软件狗类型的令牌中是否存在必需的安全程序（该软件的操作组件），如果存在，则将运行该安全程序的执行指令传送至令牌，并且接收其执行结果以控制软件继续运行。

[0009] 技术方案

[0010] 为了实现上述目标，本公开提供了一种软件许可保护终端，其包括：终端通信器，其与耦接的软件狗类型的令牌协同操作；终端控制器，其用于操作和控制特定的软件，其检查令牌是否具有运行该软件所必需的安全程序，如果有，则向所述令牌传送用于执行所述安全程序的执行指令，并且从令牌接收执行结果以激活特定的软件；以及终端存储器，其用于存储软件。

[0011] 本公开的另一方面提供了一种软件许可保护服务器，其包括：服务器通信器，其与用户终端协同操作；服务器控制器，其用于检查在购买了特定软件后用户终端是否具有软件狗类型的令牌附件，如果有，则对运行软件所必需的安全程序进行编码并将其发送至令牌；以及服务器存储器，其用于存储特定的软件和安全程序中的至少一个的信息。

[0012] 本公开的另一方面提供了一种软件许可保护系统，其包括：用户终端，其用于操作和控制特定的软件，其在存在运行所述特定的软件的安全程序时传送用于执行所述安全程序的执行指令，并且接收执行结果以激活所述软件；以及令牌，其存储安全程序，并且能够以软件狗格式耦接到用户终端，以将安全程序传送至用户终端，并且在接收执行指令时，向所述用户终端传送将所述安全程序装载至可执行存储区的执行结果。

[0013] 本公开的另一方面提供了一种软件许可保护方法，该方法包括：执行特定的软件；在所关联的令牌中检查运行特定软件的安全程序的存在，如果存在所述安全程序，则将用于执行该安全程序的执行指令传送至令牌；以及在接收到执行安全程序的结果时激活软件。

[0014] 本公开的另一方面提供了一种计算机可读介质，其对在计算机上执行上述的软件许可保护方法的各个步骤的计算机程序进行编码。

[0015] 有利效果

[0016] 根据上述的本公开，向特定的软件的用户 / 购买者提供了一种运行从服务器到软件类型的令牌的软件的安全程序所必需的组件，所述令牌被物理隔离并且通常普遍地可连接至用户终端，在执行软件期间提示用户检查是否在软件狗类型的令牌中存在运行软件所必需的安全程序，如果存在，则将运行安全程序的执行指令传送至令牌，并且在接收到执行结果时以受控的方式激活软件。

[0017] 另外，本公开提供了一种被划分并形成为安全程序的在特定的软件的运行中不可或缺的组件，所述安全程序能够存储在保护性令牌中直到它被执行，由此克服了有价值的软件易受反向工程的攻击的缺陷以保护许可，并使客户避免了完全绕开耦合的令牌而通过网络、主机终端等进行通常认证这种困扰而带来的不便。

附图说明

[0018] 图 1 是根据本公开的一个方面的软件许可保护系统的示意性框图；

[0019] 图 2 是根据图 1 的方面的用户终端的示意性框图；

[0020] 图 3 是根据图 1 的方面的软件提供服务器的示意性框图；

[0021] 图 4 是根据图 1 的方面的令牌的示意性框图；

[0022] 图 5 是根据一个方面的安全程序的示意性框图；

[0023] 图 6 是例示了软件提供服务器提供安全程序的方法的流程图；以及

[0024] 图 7 是例示了用于执行与令牌协同操作的用户终端的特定软件的方法的流程图。

[0025] 发明方式

[0026] 此后，将参照附图描述本公开的示例性方面。在以下描述中，即使在不同的附图中示出，同样的元件也将通过同样的标号来指定。此外，在本公开的以下描述中，当可能使得本公开的主题不十分清楚时，将忽略此处并入的对已知功能和配置的详细描述。

[0027] 同时，在对本发明的部件的描述中，会有象第一、第二、A、B、(a) 和 (b) 来使用的措辞。这些仅仅是为了区分一个部件和其它部件，但并不表明或暗示部件的实质、顺序或次序。如果将部件描述为“被连接”、“被耦合”或“被链接”到另一个部件，则这既可以表示部件直接地“被链接”、“被耦合”或“被链接”，也可以理解为通过第三部件间接地“被连接”、“被耦合”或“被链接”。

[0028] 现在参照图 1，图 1 总地示出了在根据本公开的一个方面的软件许可保护系统的示例性框图。

[0029] 软件许可保护系统可以包括用户终端 110、令牌 120 以及软件提供服务器 130。

[0030] 用户终端 110 表示可以响应于用户的键入操作以通过有线以及无线通信网络接收各种网页数据的终端，并且包括个人计算机或 PC、笔记本或膝上型计算机、个人数字助理或 PDA、以及移动通信终端和其它终端，其可以具有：存储器，所述存储器用于存储用于经由有线和无线通信网络与软件提供服务器 130 进行连接的网络浏览器以及计算机程序；以及用于执行程序以进行计算和控制的微处理器。虽然可以使用任何其它形式的终端（只要它们连接到有线或无线通信网络以进行服务器 - 客户端通信），但是通常用户终端 110 可以是 PC，并且旨在包括笔记本计算机、移动通信终端和其它终端、PDA、以及任意其它通信和 / 或计算终端等价物。

[0031] 用户终端 110 适于计算和控制特定的软件，其中，检查以软件狗形式耦接于用户终端 110 的令牌 120 是否存有用于运行软件的必须的安全程序（或称为“软件块”），如果有，则将运行安全程序的执行指令传送给令牌 120，并且在从令牌 120 接收到执行结果时允许以受控的方式运行软件。这里，措辞安全程序 (seculet) 源于安全 (secure) 和小程序 (applet) 的措辞的组合。

[0032] 当在执行特定软件期间需要安全程序时，用户终端 110 向令牌 120 请求安全程序的识别路径信息，并且在接收安全程序的路径信息时执行在令牌 120 中识别安全程序的功能。

[0033] 用户终端 110 执行功能以通过特定程序和令牌 120 的共享密钥利用在特定程序和令牌 120 之间发送和接收已编码或已解码的消息来认证令牌 120，从而确认它们是否具有通常的编码方法。基于识别路径或安全程序的信息，用户终端 110 将输入参数以及执行指令传送至令牌 120，并且在设置输入参数之前将安全程序从令牌 120 装载至可执行存储区域，以对相关代码的执行结果进行接收。

[0034] 令牌 120 可以存储安全程序并以软件狗形式连接到用户终端 110，从而将安全程序传送给终端 110，并且在从用户终端 110 接收执行指令时，向用户终端传送将安全程序装

载至可执行存储区的执行结果。

[0035] 软件提供服务器 130 在硬件上具有与通常的网络服务器相同的结构。然而，在软件方面，软件提供服务器 130 可结合有提供各种功能的程序模块，这些程序模块可以利用 C、C++、Java、Visual Basic、Visual C 或任何其它语言来实现。可以以网络服务器的形式来实现软件提供服务器 130，网络服务器通常表示安装有计算机软件（网络服务器程序）的计算机系统，所述计算机系统通过类似因特网的开放式计算机网络连接有未指定的多个客户端和 / 或其它服务器，以接收来自客户端或其它网络服务器的执行任务的请求，并提供所生成的执行结果。

[0036] 然而，软件提供服务器 130 旨在不仅包括所描述的网络服务器程序，而且扩展至包括在上述网络服务器上运行的一系列应用程序，并且在某些情况下，包括内建数据库。

[0037] 这样的软件提供服务器 130 可利用网络服务器程序实现，取决于操作系统可将多种版本的网络服务器程序提供至典型的服务器硬件，其中，所述操作系统包括 DOS、windows、Linux、UNIX 和 Macintosh，其中，用于 windows 环境的网站和因特网信息服务器 (IIS) 以及用于 UNIX 环境的 CERN、NCSA、APPACH 等都是常规的。同时，软件提供服务器 130 可关联于认证和支付系统进行操作以分发软件。

[0038] 另外，软件提供服务器 130 可在数据库中存储并管理有关于成员应用和软件分发的分类信息，这可以在软件提供服务器 130 的内部或外部实现。

[0039] 具体地，这种数据库即是利用数据库管理程序 (DBMS) 在计算机系统存储空间（硬盘或内存）内实现的通用数据结构，以形成自由地进行数据查询（提取）、删除、编辑、增加等的数据存储区，根据本方面的目的，利用具有用于满足数据库自身功能的适当字段或要素，可以利用例如 Oracle、Infomix、Sybase 和 DB2 的关系型数据库管理系统 (RDBMS) 来实现，利用包括 Gemston、Orion 和 O2 的面向对象数据库管理系统 (OODBMS) 来实现，以及利用类似 Excelon、Tamino 以及 Sekaiju 的 XML 本地数据库来实现。

[0040] 当用户终端 110 购买了特定软件时，软件提供服务器 130 检查软件狗格式的令牌是否存在于用户终端 110 上，并且如果存在令牌 120，则对用于运行特定的软件的安全程序进行编码，并接着将编码的安全程序传送给令牌。

[0041] 软件提供服务器 130 以置换、对换、转动机 (rotor machine)、私钥、公钥中的至少一种方法对安全程序执行编码。

[0042] 在完成软件购买前，软件提供服务器 130 还对已编码的安全程序执行解码，检查并存储已解码的安全程序。

[0043] 现在参照图 2，图 2 示意性示出了根据该方面的用户终端 110 的框图。

[0044] 在该方面中的用户终端 110 可以包括终端通信器 210、终端控制器 220 以及终端存储器 230。

[0045] 在该方面，虽然仅示例性地描述了组成用户终端 110 的终端通信器 210、终端控制器 220 和终端存储器 230，但是本领域技术人员应理解的是，在本方面的必要特征内，可以对用户终端 110 的这些部件进行变化和修改。

[0046] 终端通信器 210 是适于与令牌 120 协同操作的并且对各种数据进行收发的通信装置。

[0047] 在该方面中的终端控制器 220 是用于总体控制用户终端 110 的功能来计算和控制

特定的软件的控制装置，该控制装置检查软件狗格式的令牌 120 是否存有运行特定的软件所必需的安全程序，如果有，则向令牌 120 传送用于执行安全程序的指令，并且从令牌 120 接收执行结果以激活特定的软件。

[0048] 在运行特定软件的过程中需要安全程序时，终端控制器 220 执行如下所述的功能，即向令牌 120 请求安全程序的识别路径信息，当从令牌 120 接收到识别路径信息时，识别为在令牌 120 中存在安全程序。

[0049] 终端控制器 220 通过收发经由特定的软件和令牌 120 之间的共享的密钥编码或解码的消息，来确定特定的软件和令牌 120 共享公共的编码方案，以对令牌 120 进行认证。基于安全程序或识别路径的信息，终端控制器 220 向令牌 120 传送输入参数和执行指令，将安全程序从令牌 120 载入到可执行存储区域，并接着对输入参数进行设置以接收相关代码的执行结果。

[0050] 终端存储器 230 是用于存储对用户终端 110 进行操作所需的各种数据的装置，其功能是存储特定的软件产品。

[0051] 参照图 3，图 3 是根据本方面的软件提供服务器 130 的示意性框图。

[0052] 该方面的软件提供服务器 130 可包括服务器通信器 310、服务器控制器 320 以及服务器存储器 330。

[0053] 在该方面，虽然仅示例性地描述了组成软件提供服务器 130 的服务器通信器 310、服务器控制器 320 和服务器存储器 330，但是本领域技术人员应当理解的是，在本方面的必要特征范围内可以改变和修改软件提供服务器 130 的这些部件。

[0054] 服务器通信器 310 是适合于与用户终端 110 协同操作并且对各种数据进行收发的通信装置。

[0055] 在本方面的服务器控制器 320 是用于总体控制服务器 130 的功能特别是服务器通信器 330 的控制装置，所以当用户终端 110 已经购买了特定软件时，服务器控制器 320 检查在用户终端 110 处是否存在软件狗格式的令牌，如果找到了令牌 120，则对运行软件所必需的安全程序进行编码并将其传送到令牌 120。

[0056] 服务器控制器 320 以置换、对换、转动机、私钥和公钥中的至少一种方法对安全程序执行编码。服务器控制器 320 对已编码的安全程序进行解码，并检查令牌 120 对已解码安全程序进行了编码和存储，从而完成软件购买过程。

[0057] 服务器存储器 330 是用于存储操作服务器 130 所需的各种数据的装置，其功能是存储特定的软件产品和 / 或安全程序。

[0058] 图 4 是根据该方面的令牌 120 的示意性框图。

[0059] 在该方面的令牌 120 可以包括令牌管理器 410 和存储器 420。

[0060] 在该方面，虽然示例性地描述了仅具有令牌管理器 410 和存储器 420 的部件的令牌 120，但本领域技术人员应当理解的是，在本方面的必要特征范围内可以改变和修改令牌 120 的这些部件。

[0061] 该方面的令牌管理器 410 是用于控制令牌 120 的一般功能的控制装置，该控制装置将安全程序传送至用户终端 110，并且在接收执行指令时，将安全程序载入至可执行存储器的执行结果传送至用户终端 110。更明确地，令牌管理器 410 可以是通过执行存储在存储部 420 中的安全程序来进行计算和控制的微处理器。存储器 420 是用于对操作令牌 120 所

需的各种数据进行存储的装置，其功能是存储多个安全程序。

[0062] 图 5 是根据该方面的安全程序的示意性框图。

[0063] 根据该方面的安全程序是运行特定软件所必需的程序，并且可以包括标识部分、代码部分、永久数据部分以及动态数据部分。

[0064] 标识部分可以包括用于确定安全程序标识的字符串、说明、图标、以及唯一的数字数据中的至少一个。标识部分可用作搜索 / 执行选择信息，所述选择信息对于在用户终端 110 使用驻留于令牌 120 内的安全程序是必不可少的。

[0065] 代码部分可以包括在令牌 120 内运行的执行指令。可由机器语言或更高级的程序语言来实现代码部分，并且包括安全程序的执行指令。由于当该执行命令的输入 / 输出复杂度过于简单时，容易复制，因此通过利用永久数据 / 动态数据使其具有适当级别以上的复杂度。

[0066] 永久数据部分可以存储用作参考的永久数据。永久数据部分可以存储在例如 NAND 闪存的大容量存储器中。并且可以在执行代码部分期间参考已存储的永久数据部分。也就是说，在不同的软件产品中所使用的各种参考表成为待参考的对象。

[0067] 动态数据部分存储执行安全程序的历史信息。动态数据部分适合于记录执行代码期间引出的状态信息，并且可以存储在 NAND 闪存中，但是根据情况也可以存储在 EEPROM 或 Nor 等 I/O 速度快的区域。另外，动态数据使得安全程序上下文相关 (context sensitive)，允许基于使用、功能、次数、数据量等实现各种许可方案。

[0068] 图 6 是用于例示软件提供服务器 130 在该方面提供安全程序的方法的流程图。

[0069] 在步骤 S610，用户终端 110 开始访问软件提供服务器 130 以购买特定软件。软件提供服务器 130 接着检查软件狗格式令牌 120 是否存在于用户终端 110。如果令牌 120 存在，则软件提供服务器 130 在步骤 S630 检查服务器 130 和令牌 120 是否交叉认证。

[0070] 当在 S630 确认了服务器 130 和令牌 120 之间的交叉认证时，软件提供服务器 130 在步骤 S640 对运行特定的软件所必需的安全程序进行编码，并将其传送至令牌 120。此时，软件提供服务器 130 可以以置换、对换、转动机、私钥和公钥中的至少一种方法对安全程序进行编码。

[0071] 在步骤 S650，令牌 120 对已编码的安全程序进行解码和存储。软件提供服务器 130 在确认令牌 120 解码并存储了安全程序之后，完成软件的购买处理。

[0072] 虽然图 6 例示了软件提供服务器 130 以编号的顺序执行步骤 S610 到步骤 S650，但这仅仅例示了该方面的技术理念，但是本领域技术人员应当理解的是，在本方面的必要特征的范围内，软件提供服务器 130 可以与图 6 所示的不同的顺序执行这些步骤，或同时执行从步骤 S610 到步骤 S650 中选出的一个或更多个步骤，等等，不将图 6 限制于串行的顺序。

[0073] 图 7 是例示了根据本方面的用于利用与令牌 120 协同操作的用户终端 110 来运行特定的软件的方法的流程图。

[0074] 在步骤 S710，用户终端 110 开始运行特定的软件。在步骤 S720，用户终端 110 接着检查耦合到用户终端 110 的软件狗格式的令牌 120 是否存有运行软件所必需的安全程序。例如，当在运行软件的过程中需要安全程序的识别路径时，用户终端 110 可以向令牌 120 请求安全程序的识别路径的信息，并且在接收来自令牌 120 的识别路径信息时，用户终端 110 可以识别安全程序在令牌 120 处的存在。

[0075] 此外，在用户终端 110 通过收发经由特定软件和令牌 120 之间的共享密钥所编码或解码的消息来确认特定软件和令牌 120 具有公共的编码方案时，用户终端 110 对令牌 120 进行认证。

[0076] 从步骤 S710 开始，在用户终端 110 确认了安全程序的存在时，用户终端 110 在步骤 S730 向令牌 120 传送执行指令以运行安全程序。也就是说用户终端 110 根据安全程序或识别路径信息向令牌 120 传送输入参数和执行指令。

[0077] 在步骤 S740，令牌 120 接着将安全程序载入可执行存储器区域。在步骤 S750，令牌 120 通过设置输入参数来执行相关的代码。接着，在步骤 S760，令牌 120 将执行结果传送至用户终端 110。最后，用户终端 110 从令牌 120 接收执行结果以激活特定的软件。

[0078] 虽然图 7 例示了用户终端 110 和令牌 120 以编号顺序执行步骤 S710 到 S760，这仅仅例示了该方面的技术理念，但是本领域技术人员应当理解的是，在本方面的必要特征的范围内，用户终端 110 和令牌 120 可以以与图 7 所示的不同的顺序执行这些步骤，或同时执行从步骤 S710 到步骤 S760 中选出的一个或更多个步骤等等，不将图 7 限制于串行的顺序。

[0079] 如上所述，在公开的方面中的软件许可保护方法可以通过计算机程序实现并提供在计算机可读记录媒介中。根据本发明实施例的记录有用于体现软件许可保护方法的程序并能够由计算机读取的存储介质，包括能够由计算机系统读取的存储有数据的所有种类的存储装置。这种计算机可读记录媒介的示例包括 ROM、RAM、CD-ROM、磁带、软盘和光学数据存储器，并进一步包括在载波中的实现（例如，因特网传输）。此外，计算机可读记录媒介可以提供在分布式处理系统中，其中，计算机系统是网络化的，以在分布的位置处存储并执行计算机可读代码。此外，本领域程序员可以容易地推导出实现公开的方面的功能性程序、代码以及代码段。

[0080] 在以上描述中，虽然已经将本公开的各个方面的所有部件解释为装配或操作地连接为单元，本公开不旨在将其本身限制于这样的方面。相反，在本公开的客观的范围内，各个部件可以以任意数量选择性地并且操作地进行组合。而且，部件中的每一个可以独自由硬件实现，同时各个部件可以选择性地部分地或者作为整体进行组合，并且可以在具有用于执行硬件等价物的功能的程序模块的计算机程序中实现。本领域技术人员可以容易地推导出组成这种程序的代码或代码段。计算机程序可以存储在计算机可读媒介中，其在运行时可以实现本公开的各个方面。作为计算机可读媒体的备选包括磁记录媒体、光记录媒体以及载波媒体。

[0081] 同时，除非明确地定义为相反的，否则像“包括”、“包含”、“具有”的措辞应当默认被解读为包括性的或开放的而不是排它的或封闭的。除非明确地定义为相反的，否则所有技术的、科学的或其它措辞与本领域技术人员所理解的含义相一致。在字典中找到的通用术语应当在相关技术著作的上下文中不过于理想地或不切实际地进行解读，除非本公开明确地如此定义它们。

[0082] 虽然已经针对说明性的目的描述了本公开的示例性方面，但是本领域技术人员应当理解的是，在不脱离本公开的范围和精神的情况下，可以进行各种修改、增加和替换。因此，不针对限制性目的描述本公开的示例性方面。因此，不通过上述方面来限定本公开的范围，而是通过权利要求及其等价来进行限定。

[0083] 工业适用性

[0084] 如上，根据上述本公开的软件许可保护方法、系统、服务器、终端以及计算机可读记录介质从服务器向特定的软件的用户 / 购买者提供了通过可分离地耦接至用户终端的软件狗格式的令牌来运行软件所必需的安全程序的部件，在执行软件期间提示用户检查运行软件所必需的安全程序是否存在于软件狗形式的令牌中，如果存在，则将运行安全程序的执行指令传送至令牌，并且在接收到执行结果时，以受控的方式激活软件，由此克服了软件易受反向工程攻击的缺陷，使客户避免了在其它方案中通常依靠在线认证的不便。

[0085] 相关申请的交叉参考

[0086] 如果适用，本申请根据 35U.S.C § 119(a) 要求 2008 年 12 月 26 日在韩国提交的第 2008-0134892 号的专利申请的优先权，其全部内容通过引用合并于此。另外，在美国以外的其它国家，以相同的理由，本非临时性申请要求基于该韩国专利申请的优先权，该韩国专利申请全部内容通过引用合并于此。

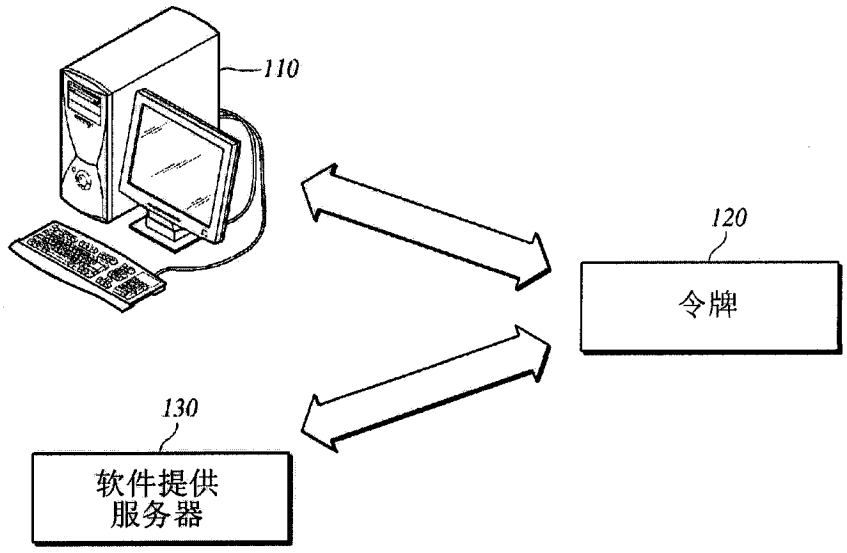


图 1

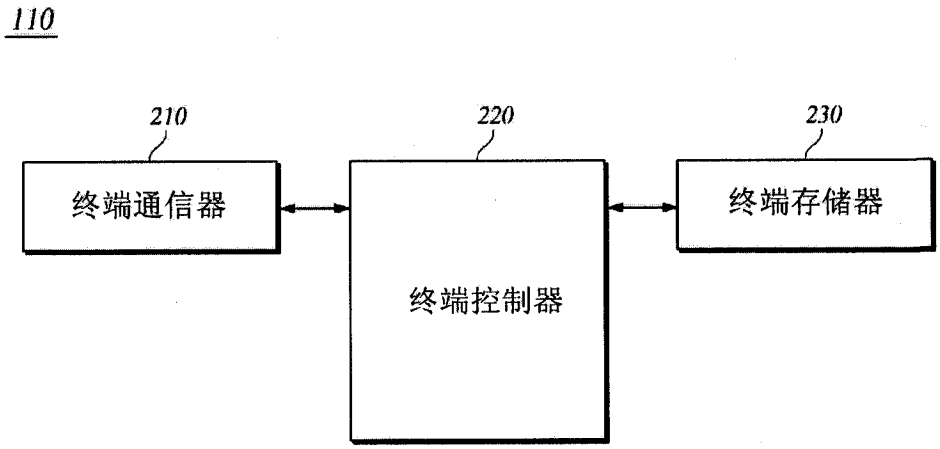


图 2

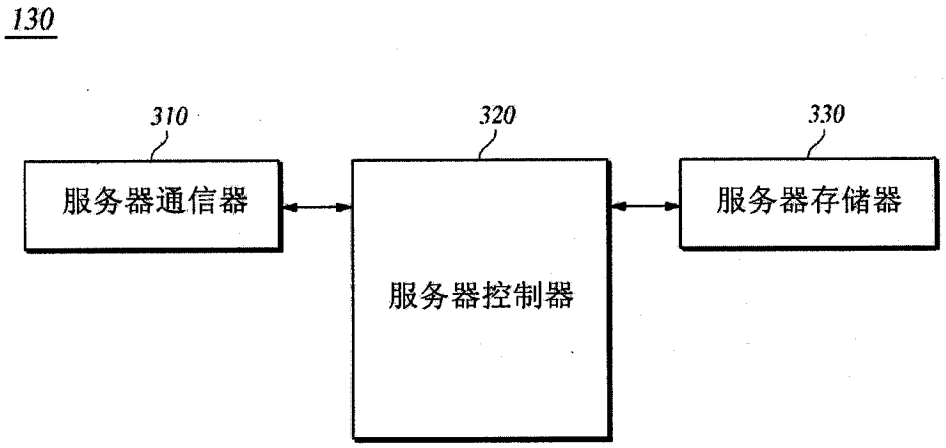

130
310
320
330
服务器通信器
服务器控制器
服务器存储器

图 3

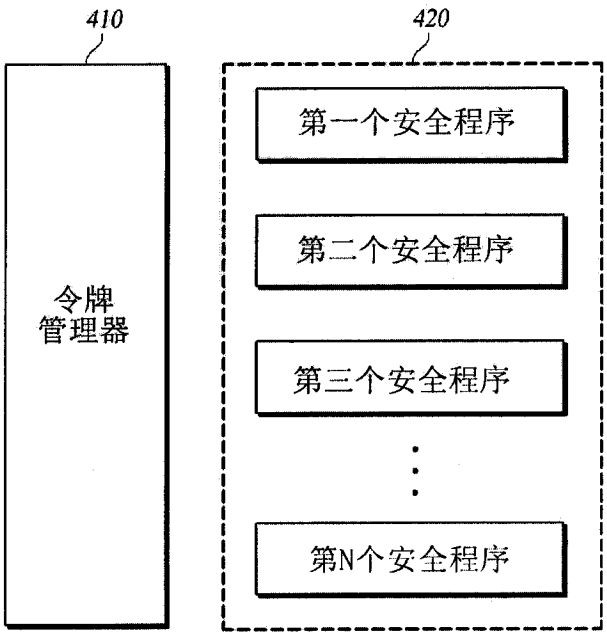

410
420
令牌
管理器
第一个安全程序
第二个安全程序
第三个安全程序
第N个安全程序

图 4

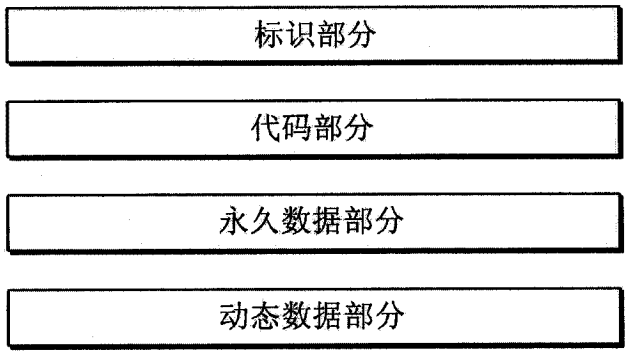

标识部分
代码部分
永久数据部分
动态数据部分

图 5

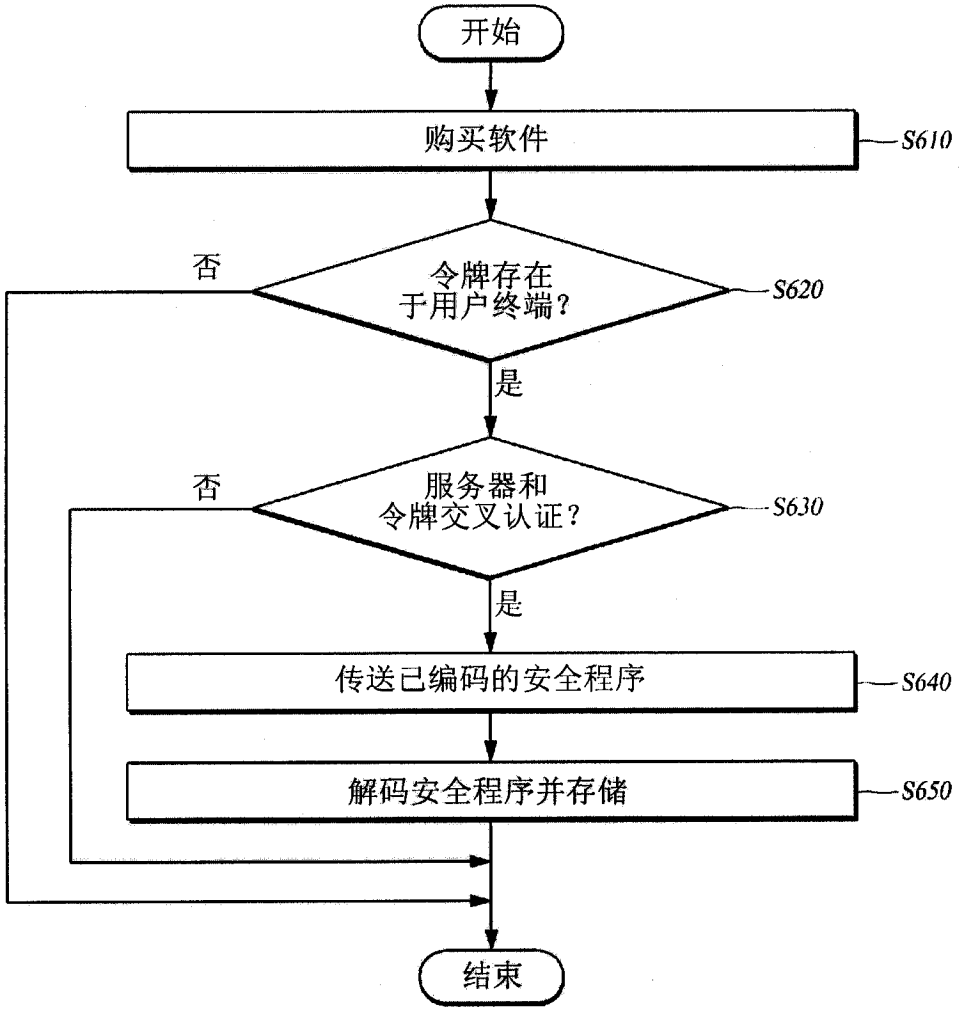

开始
购买软件
S610
令牌存在
于用户终端？
S620
否
是
服务器和
令牌交叉认证？
S630
否
是
传送已编码的安全程序
S640
解码安全程序并存储
S650
结束

图 6

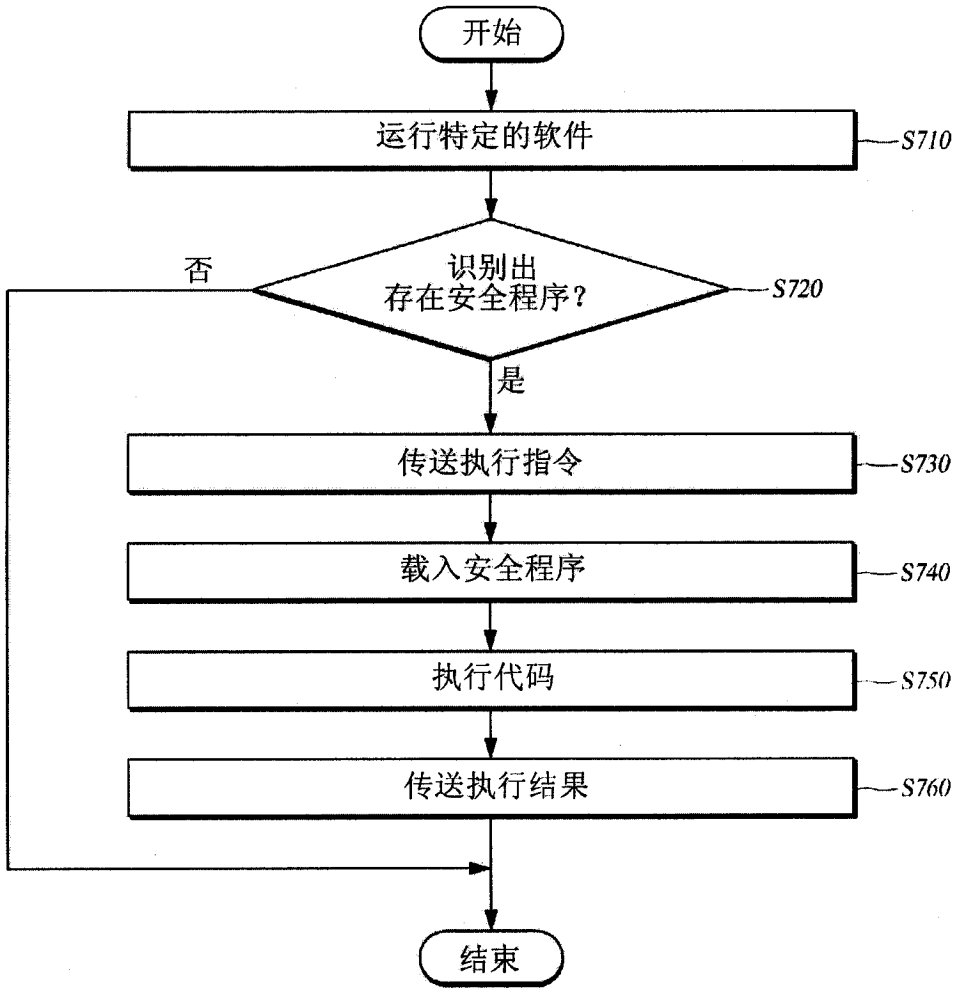

开始
运行特定的软件
S710
识别出
存在安全程序？
S720
否
是
传送执行指令
S730
载入安全程序
S740
执行代码
S750
传送执行结果
S760
结束

图 7