(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102110194 A
(43)申请公布日 2011.06.29

(21)申请号 200910189161.9

(22)申请日 2009.12.24

(71)申请人 黄金富
地址 100032 北京市西城区金融街 27 号投资广场 B 座 19 层

(72)发明人 黄金富

(51)Int.Cl.
G06F 21/00(2006.01)
H04W 4/14(2009.01)
H04W 88/02(2009.01)

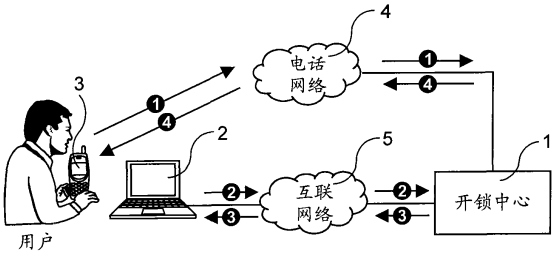
权利要求书 2 页 说明书 4 页 附图 1 页

(54)发明名称

要预先致电开锁中心才能使用计算机的保安系统和方法

(57)摘要

一种要预先致电开锁中心才能使用计算机的保安系统和方法，包括开锁中心(1)、用户计算机(2)和手机(3)，开锁中心(1)设有对应用户计算机(2)及手机(3)的状态标志，状态标志平常是上锁状态，用户通过手机(3)向开锁中心(1)发开锁指令可将其设为开锁状态；计算机(2)设有监控软件(201)，计算机(2)执行受监控操作时，监控软件(201)向开锁中心(1)查询对应的状态标志状态，当状态为开锁时才允许计算机执行该受监控操作。本发明可与防病毒软件服务相结合，将开锁中心(1)整合到防病毒更新服务主机，将监控软件(201)整合到防病毒软件，使防病毒软件除了保护计算机不被病毒感染，还防止计算机被人非法使用。



CN 102110194 A

1. 一种防止计算机被非法使用的保安系统，其特征在于，所述的系统包括有开锁中心(1)、各用户的计算机(2)和手机(3)，其中，开锁中心(1)设有多个状态标志，每一状态标志对应一用户的计算机(2)及手机(3)，各状态标志平常是处于“上锁”状态，用户通过手机(3)向开锁中心(1)发出开锁指令可以设置该手机(3)所对应的状态标志为“开锁”状态；以及，在计算机(2)中设置有包括监控软件(201)，该监控软件(201)用于监控计算机(2)的运作，当发现计算机(2)执行受监控操作时，监控软件(201)暂停该受监控操作，并向开锁中心(1)查询该计算机(2)对应的状态标志的状态，只有在开锁中心(1)回答该状态标志的状态为“开锁”时，监控软件(201)才允许计算机继续执行该受监控操作。

2. 一种防止计算机被非法使用的保安方法，其特征在于，所述的方法包括在开锁中心(1)设置多个状态标志，每一状态标志对应一用户的计算机(2)及手机(3)，各状态标志平常是处于“上锁”状态，用户通过手机(3)向开锁中心(1)发出开锁指令可以设置该手机(3)所对应的状态标志为“开锁”状态；以及，在计算机(2)设置监控软件(201)，该监控软件(201)用于监控计算机(2)的运作，当发现计算机(2)执行受监控操作时，监控软件(201)暂停该受监控操作，并向开锁中心(1)查询该计算机(2)对应的状态标志的状态，只有在开锁中心(1)回答该状态标志的状态为“开锁”时，监控软件(201)才允许计算机继续执行该受监控操作。

3. 如权利要求2所述的防止计算机被非法使用的保安方法，其特征在于，所述的受监控操作包括：登录计算机(2)和/或访问计算机(2)内的受保护数据和/或复制计算机(2)内的受保护数据和/或存储计算机(2)内的受保护数据和/或修改计算机(2)内的受保护数据。

4. 如权利要求2所述的防止计算机被非法使用的保安方法，其特征在于，当开锁中心(1)收到手机(3)发出的开锁指令后，开锁中心(1)将该手机(3)所对应的状态标志设置为“开锁”状态一段指定时间，指定时间过后开锁中心(1)自动将该状态标志设置回复为“上锁”状态。

5. 如权利要求2所述的防止计算机被非法使用的保安方法，其特征在于，当所述的状态标志被计算机(2)查询其状态，开锁中心(1)向计算机(2)回复该状态标志的状态后，自动将该状态标志设置回复为“上锁”状态。

6. 如权利要求2至5任一项所述的防止计算机被非法使用的保安方法，其特征在于，所述方法以用户使用手机(3)致电呼叫开锁中心(1)作为开锁指令。

7. 如权利要求2至5任一项所述的防止计算机被非法使用的保安方法，其特征在于，所述方法采用开锁中心(1)接听用户的手机(3)的来电呼叫后用户在手机(3)所输入的开锁密码作为开锁指令。

8. 如权利要求2至5任一项所述的防止计算机被非法使用的保安方法，其特征在于，所述方法以用户使用手机(3)发送到开锁中心(1)包含有开锁密码的短信或彩信作为开锁指令。

9. 如权利要求2至5任一项所述的防止计算机被非法使用的保安方法，其特征在于，所述方法以用户使用手机(3)发送到开锁中心(1)包含有开锁密码的电邮为开锁指令。

10. 如权利要求2至5任一项所述的防止计算机被非法使用的保安方法，其特征在于，所述的方法还包括如下步骤，是用户使用其计算机(2)执行受监控操作的步骤，具体的步

骤如下：

1. 用户使用计算机 (2) 进行受监控操作前，使用手机 (3) 致电开锁中心 (1)，拨通后就可立即挂线；

开锁中心 (1) 从来电呼叫的电话号码找出对应该手机 (3) 电话号码的状态标志，然后将该状态标志设置为“开锁”状态一段指定时间，并在该段指定时间过后自动将该状态标志设置为“上锁”状态；

2. 用户在该段指定时间期间，使用计算机 (2) 进行受监控操作，计算机 (2) 内的监控软件 (201) 发现计算机 (2) 执行受监控操作，暂停该受监控操作，然后向开锁中心 (1) 查询该计算机 (2) 对应的状态标志的状态；

3. 开锁中心 (1) 找出该计算机 (2) 对应的状态标志的状态，由于计算机 (2) 是在该段指定时间期间查询该状态标志的状态，所以开锁中心 (1) 将该状态标志的状态即“开锁”状态信息回复给计算机 (2)，然后开锁中心 (1) 将该状态标志设置回复为“上锁”状态；

计算机 (2) 收到该“开锁”状态信息后，监控软件 (201) 允许继续执行该受监控操作；

4. 开锁中心 (1) 发短信给用户手机 (3) 通知用户该计算机 (2) 进行了一次受监控操作。

要预先致电开锁中心才能使用计算机的保安系统和方法

【技术领域】

[0001] 本发明涉及计算机保安技术领域，特别是涉及一种要预先致电开锁中心才能使用计算机的保安系统和方法。

【背景技术】

[0002] 随着计算机技术的普及，计算机的应用越来越广泛，计算机已经成为人们生活和工作上的不可缺少的常用设备，计算机的安全性也越来越受到关注，尤其是一些储存有个人私隐或机密信息的计算机，为了保护计算机内信息的安全，通常这些计算机都设置了密码保护，要输入正确的登录密码登入后，才能使用计算机。但是一些不法之徒，通过种种手段盗取计算机用户的登入密码，然后在用户不知情和不在场的情况下，使用盗取回来的登入密码假冒用户登入计算机，进行一些不法行为，例如偷取计算机内的重要信息、破坏计算机内的重要信息、甚至将一些病毒或木马程式安装要计算机内，到用户发现时往往已经给用户造成无可挽回的损失，如何保护计算机不被他人非法使用，是一个有待解决的问题。

【发明内容】

[0003] 本发明的目的，在于提供一种要预先致电开锁中心才能使用计算机的保安系统和方法，以实现防止计算机被非法使用的应用。

[0004] 本发明的目的是这样实现的，采用这样一种防止计算机被非法使用的保安系统，其特征在于，所述的系统包括有开锁中心 (1)、各用户的计算机 (2) 和手机 (3)，其中，开锁中心 (1) 设有多个状态标志，每一状态标志对应一用户的计算机 (2) 及手机 (3)，各状态标志平常是处于“上锁”状态，用户通过手机 (3) 向开锁中心 (1) 发出开锁指令可以设置该手机 (3) 所对应的状态标志为“开锁”状态；以及，在计算机 (2) 中设置有包括监控软件 (201)，该监控软件 (201) 用于监控计算机 (2) 的运作，当发现计算机 (2) 执行受监控操作时，监控软件 (201) 暂停该受监控操作，并向开锁中心 (1) 查询该计算机 (2) 对应的状态标志的状态，只有在开锁中心 (1) 回答该状态标志的状态为“开锁”时，监控软件 (201) 才允许计算机继续执行该受监控操作。

[0005] 以及，还采用这样一种防止计算机被非法使用的保安方法，其特征在于，所述的方法包括在开锁中心 (1) 设置多个状态标志，每一状态标志对应一用户的计算机 (2) 及手机 (3)，各状态标志平常是处于“上锁”状态，用户通过手机 (3) 向开锁中心 (1) 发出开锁指令可以设置该手机 (3) 所对应的状态标志为“开锁”状态；以及，在计算机 (2) 设置监控软件 (201)，该监控软件 (201) 用于监控计算机 (2) 的运作，当发现计算机 (2) 执行受监控操作时，监控软件 (201) 暂停该受监控操作，并向开锁中心 (1) 查询该计算机 (2) 对应的状态标志的状态，只有在开锁中心 (1) 回答该状态标志的状态为“开锁”时，监控软件 (201) 才允许计算机继续执行该受监控操作。

[0006] 在本说明书中，所述的受监控操作包括：登录计算机 (2) 和 / 或访问计算机 (2) 内的受保护数据和 / 或复制计算机 (2) 内的受保护数据和 / 或存储计算机 (2) 内的受保护数

据和 / 或修改计算机 (2) 内的受保护数据。

[0007] 这样就实现了本发明的目的。

[0008] 本发明的防止计算机被非法使用的保安系统和方法，可以保障用户的计算机 (2) 的安全，每次使用计算机 (2) 进行受监控操作前，用户都要预先使用手机 (3) 向开锁中心 (1) 发出有效的开锁指令将该计算机 (2) 对应的状态标志设置为“开锁”状态，才能成功执行该受监控操作，即使用户的登录密码被人偷取了，没有用户的手机 (3) 就无法“开锁”，也就无法使用计算机 (2) 进行受监控操作。

【附图说明】

[0009] 图 1 是本发明的防止计算机被非法使用的保安系统的示意说明图 ；

[0010] 图 2 是本发明的防止计算机被非法使用的保安方法的步骤示意说明图。

[0011] 图中，相同的数字代表相同的系统、装置、部件器件，方法步骤用圆圈的数字和带箭头的直线所标出。附图是示意性的，用以说明本发明的系统和方法的主要特征。

【具体实施方式】

[0012] 下面结合附图，对本发明的系统和方法作进一步详细说明。

[0013] 参阅图 1，图 1 是本发明的防止计算机被非法使用的保安系统的示意说明图，图 1 中示出的系统包括有开锁中心 (1)、各用户的计算机 (2) 和手机 (3)，其中，开锁中心 (1) 设有多个状态标志，每一状态标志对应一用户的计算机 (2) 及手机 (3)，各状态标志平常是处于“上锁”状态，用户通过手机 (3) 向开锁中心 (1) 发出开锁指令可以设置该手机 (3) 所对应的状态标志为“开锁”状态 ；以及，在计算机 (2) 中设置有包括监控软件 (201)，该监控软件 (201) 用于监控计算机 (2) 的运作，当发现计算机 (2) 执行受监控操作时，监控软件 (201) 暂停该受监控操作，并向开锁中心 (1) 查询该计算机 (2) 对应的状态标志的状态，只有在开锁中心 (1) 回答该状态标志的状态为“开锁”时，监控软件 (201) 才允许计算机继续执行该受监控操作。

[0014] 在设置方面，开锁中心 (1) 设有连接电话网络 (4) 的线路及装置和连接互联网络 (5) 的装置，并设有多个用于指示帐户状态的状态标志，每一状态标志分别对应一位用户的计算机 (2) 及他的手机 (3)，用户要在他的计算机 (2) 内设置一监控软件 (201) 和设置电子证书，这电子证书就是用户的计算机 (2) 的身份凭证，也可以采用其他的实施方式来代替电子证书作为用户的计算机 (2) 的身份凭证，用户需要在开锁中心 (1) 登记自己的手机 (3) 电话号码及计算机 (2) 的身份凭证，由开锁中心 (1) 分配一个状态标志给用户，将用户的手机 (3) 电话号码和计算机 (2) 的身份凭证与该状态标志相绑定。此外，用户还要选择设定一个用于开锁的开锁指令，可以采用用户使用手机 (3) 致电呼叫开锁中心 (1) 作为开锁指令或采用开锁中心 (1) 接听用户的手机 (3) 的来电呼叫后用户在手机 (3) 所输入的开锁密码作为开锁指令或用户使用手机 (3) 发送到开锁中心 (1) 包含有开锁密码的短信或彩信作为开锁指令或以用户使用手机 (3) 发送到开锁中心 (1) 包含有开锁密码的电邮为开锁指令等等之类方式，都可以作为开锁指令传送到开锁中心 (1)。以后用户使用计算机 (2) 执行受监控操作前，用户要预先使用手机 (3) 向开锁中心 (1) 发出有效的开锁指令将该计算机 (2) 对应的状态标志设置为“开锁”状态，计算机 (2) 内的监控软件 (201) 才允许执行该

受监控操作。

[0015] 参阅图 2，图 2 是本发明的防止计算机被非法使用的保安方法的步骤示意说明图，图 2 中示出的方法包括在开锁中心 (1) 设置多个状态标志，每一状态标志对应一用户的计算机 (2) 及手机 (3)，各状态标志平常是处于“上锁”状态，用户通过手机 (3) 向开锁中心 (1) 发出开锁指令可以设置该手机 (3) 所对应的状态标志为“开锁”状态；以及，在计算机 (2) 设置监控软件 (201)，该监控软件 (201) 用于监控计算机 (2) 的运作，当发现计算机 (2) 执行受监控操作时，监控软件 (201) 暂停该受监控操作，并通过互联网络 (5) 向开锁中心 (1) 查询该计算机 (2) 对应的状态标志的状态，只有在开锁中心 (1) 回答该状态标志的状态为“开锁”时，监控软件 (201) 才允许计算机继续执行该受监控操作。

[0016] 此外，当开锁中心 (1) 收到手机 (3) 发出的开锁指令后，开锁中心 (1) 将该手机 (3) 所对应的状态标志设置为“开锁”状态一段指定时间 (例如指定时间为 5 分钟)，指定时间过后开锁中心 (1) 自动将该状态标志设置回复为“上锁”状态。这样限制每次开锁的有效时间，可加强本发明的系统和方法的安全性。此外，本发明的进一步改进，是在所述的状态标志被计算机 (2) 查询其状态，开锁中心 (1) 向计算机 (2) 回复该状态标志的状态后，自动将该状态标志设置回复为“上锁”状态，这样可保证每一次开锁操作只能执行一次受监控操作，可进一步提高本发明的系统和方法的安全性。

[0017] 在本说明书中，所述的受监控操作包括：登录计算机 (2) 和 / 或访问计算机 (2) 内的受保护数据和 / 或复制计算机 (2) 内的受保护数据和 / 或存储计算机 (2) 内的受保护数据和 / 或修改计算机 (2) 内的受保护数据。此外，用户还可以将计算机 (2) 内的部分数据设定为受保护数据，当对这些受保护数据进行访问、复制、存储、修改等操作前，用户要预先将该计算机 (2) 对应的状态标志设置为“开锁”状态，才能对这些受保护数据进行访问、复制、存储、修改等操作。

[0018] 继续参阅图 2，图 2 中示出的方法还包括如下步骤，是用户使用其计算机 (2) 执行受监控操作的步骤，具体的步骤如下：

[0019] 1. 用户使用计算机 (2) 进行受监控操作前，使用手机 (3) 致电开锁中心 (1)，拨通后就可立即挂线；

[0020] 开锁中心 (1) 从来电呼叫的电话号码找出对应该手机 (3) 电话号码的状态标志，然后将该状态标志设置为“开锁”状态一段指定时间，并在该段指定时间过后自动将该状态标志设置为“上锁”状态；

[0021] 2. 用户在该段指定时间期间，使用计算机 (2) 进行受监控操作，计算机 (2) 内的监控软件 (201) 发现计算机 (2) 执行受监控操作，暂停该受监控操作，然后向开锁中心 (1) 查询该计算机 (2) 对应的状态标志的状态；

[0022] 3. 开锁中心 (1) 找出该计算机 (2) 对应的状态标志的状态，由于计算机 (2) 是在该段指定时间期间查询该状态标志的状态，所以开锁中心 (1) 将该状态标志的状态即“开锁”状态信息回复给计算机 (2)，然后开锁中心 (1) 将该状态标志设置回复为“上锁”状态；

[0023] 计算机 (2) 收到该“开锁”状态信息后，监控软件 (201) 允许继续执行该受监控操作；

[0024] 4. 开锁中心 (1) 发短信给用户手机 (3) 通知用户该计算机 (2) 进行了一次受监控操作。

[0025] 以上已经详细说明本发明的系统和方法的特征，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化。例如将本发明的系统和方法与计算机防病毒软件服务相结合，将开锁中心 (1) 整合到提供防病毒软件更新服务的服务器主机中，而将监控软件 (201) 整合到防病毒软件中，使防病毒软件除了可保护计算机不被病毒感染，还可提供防止计算机被人非法使用。由于防病毒软件一般都已经具备了监控操作系统和通过网络与服务器连线的功能，只要在防病毒软件作一些修改，并在服务器主机中增设一些电话线路和相关设备，就可以很好地实现本发明的目的。

[0026] 本发明的要预先致电开锁中心才能使用计算机的保安系统和方法，可以保护计算机不被他人非法使用。本发明的实施，对计算机用户十分裨益。

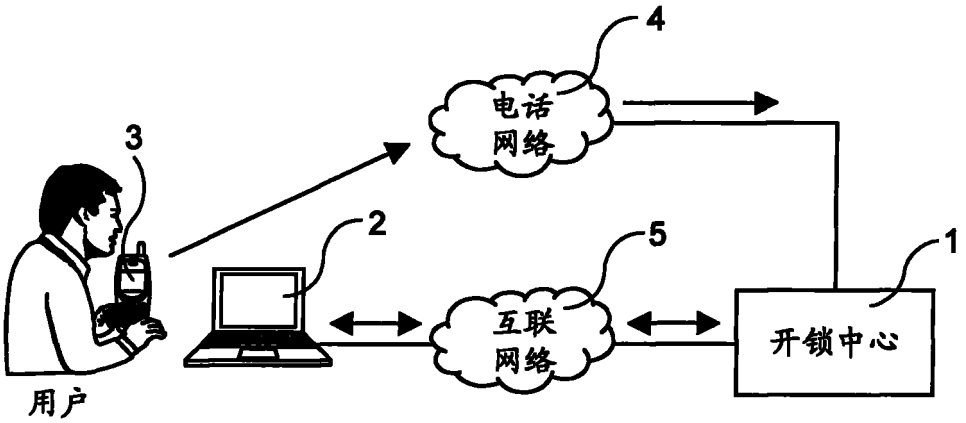


图 1

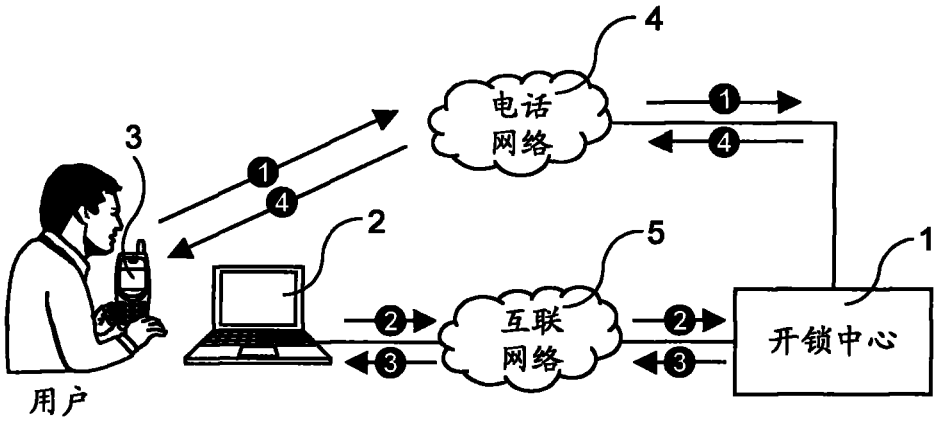


图 2