

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(43) 国际公布日
2006 年 3 月 2 日 (02.03.2006)

PCT

(10) 国际公布号
WO 2006/021132 A1

(51) 国际专利分类号⁷: G06F 11/30

(21) 国际申请号: PCT/CN2005/000292

(22) 国际申请日: 2005 年 3 月 10 日 (10.03.2005)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
10/923,921 2004 年 8 月 21 日 (21.08.2004) US
11/053,231 2005 年 2 月 9 日 (09.02.2005) US

(71) 申请人及

(72) 发明人: 方可成(FANG, Ko-Cheng) [CN/CN]; 中国台湾省台北县淡水镇中正路一段130之3号4楼, Taiwan (CN)。

(74) 代理人: 隆天国际知识产权代理有限公司(LUNG TIN INTERNATIONAL INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路5号远大中心B座18层, Beijing 100101 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

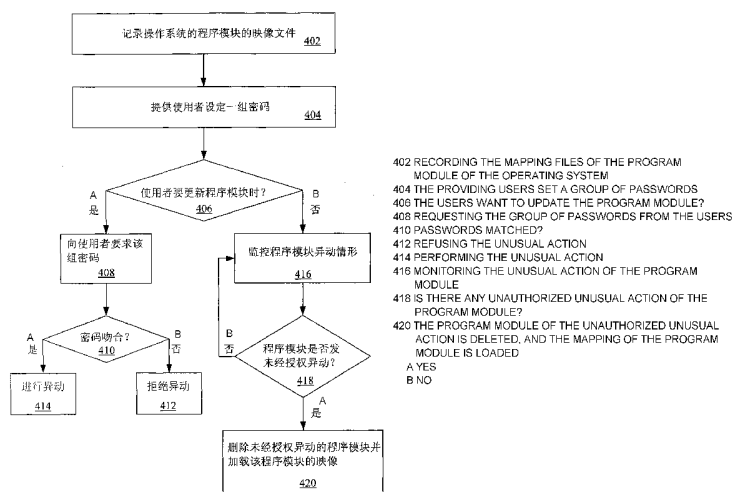
本国际公布:

— 包括国际检索报告。

所引用双字母代码及其它缩写符号, 请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(54) Title: METHOD FOR PROTECTING THE COMPUTER DATA

(54) 发明名称: 计算机数据保护方法



(57) Abstract: The method for protecting the computer data of the invention will request the user to input the correct password so as to change any program module, if the password is not correct, then any action of adding, modifying, deleting, and subtracting the program module will be prevent. Additionally, the program module will be examined periodically to find out that whether the unauthorized unusual action occurs or not. If the unauthorized unusual action occurs, then the program module infected will be deleted, and the program module backedup previously will be loaded, such that the normal operation of the computer can be resumed rapidly. Additionally, also by providing a common password, certain specific functions can have this common password, and through the monitoring of the monitor program, the specific function can be destroyed.

[见续页]



(57) 摘要:

本发明的计算机数据保护方法，会要求使用者输入正确密码借以改变任何程序模块，如密码错误，则阻止任何增修删减程序模块的动作。此外，并定期对程序模块进行检测，以发现是否有未经授权的异动发生。如果有未经授权的异动发生时，则删除受感染的程序模块，并载入原先备份的程序模块，借以迅速恢复计算机的正常运作。此外，亦提供一通用密码，让某些特定功能载有此通用密码，而可通过此监控程序的监控，借以破坏特定功能。

计算机数据保护方法

技术领域

5 本发明涉及一种保护方法，尤其涉及一种计算机数据保护方法。

背景技术

随着计算机的普及与网络技术的进步，计算机已经与今日人们的生活息息相关。例如，人们可使用计算机来记录各式各样的数字数据，甚至人们亦可使用计算机上支付至机器来复制相同的数字数据在一数字记录媒体上。

今日几乎所有的计算机、服务器，甚至个人通讯设备，如手机，都已经连接到网络上。除了因特网，还有企业网络（Intranet）、通信网路（telecommunication network）等。总之，网络已经是生活无法避免重要工具。然而在此同时，网络往往提供给一些非法的侵入者一些破坏或窃取机密数据的机会。对于这些非法的侵入者，通常人们称之为黑客(hacker)。当黑客窃取这些数据后，他可使用复制工具来复制这些数据甚至贩卖这些数据。先今日，有各种保护工具被发展出来用以避免重要数据被窃取，然而，这些新的安全保护工具仍未能为市场所接受。

另一方面，随着计算机的数据量越来越大，同时其与网络之间的互动越来越频繁，使得计算机病毒的问题也越来越严重。一旦计算机病毒发作，轻则造成生活或工作的不便，重则甚至可能造成人命财产的重大损失。

一般而言，常使用防火墙系统和防毒程序来保护计算机数据。防火墙系统用以过滤信息和控制存取，而防毒程序则用来围堵从网络或其黑客处传来的病毒。

25 传统上，防火墙有所谓的硬件防火墙与软件防火墙，而不管是硬件防火墙还是软件防火墙，主要皆是提供系统管理者进行一些安全条件的设定。这些安全条件的例子包括过滤从不认识的地址传来的数据封包，或是将某些传输协议使用的传输端口(port)关闭起来。然而，今日的防火墙所做的工作都只是一味的防堵黑客在第一阶段的入侵。一旦黑客通过了安全条件，则黑客便可肆无忌惮地进行破坏或窃取数据的动作。最常见的黑客使用的方式就是大

量重复试验密码，来破解安全系统。但是今日的防火墙并无法在早期检测黑客的动作，并予以适当的处理。一旦黑客破解安全系统，所有破坏或窃取数据的记录也都会同时被黑客消除。即便对黑客测试密码尝试登入进行记录，也因为黑客尚未进行进一步的动作，而无法采取因应的法律途径。

5 另一方面，防毒程序大部分皆针对各种病毒码分析其样态，并将其样态存成数据库，以便进行病毒扫描检测之用。由于病毒的技术日新月异，从早期必须附加在执行文件到今日甚至可附随在电子邮件中进行散布，使得病毒码的数据库越来越庞大。可想见的是，日后当这个数据库越来越庞大时，每次进行扫毒检测的时间将越来越长，而严重影响计算机正常运作。在这种恶性循环下，即使计算机的硬件与软件功能越来越强大，其效能将因为计算机病毒而无法实质的提升，甚至让使用者对过于复杂的系统望而却步。

此外，使用者亦需随时更新病毒码数据库，否则仍无法通过这些防毒程序来保护其计算机的安全。虽然有若干计算机使用者对计算机安全具有浓厚的兴趣，而愿意随时注意相关信息并更新最新的病毒码数据库，但是有更多的计算机使用者完全对此没兴趣，也根本没有时间耗费在进行这些防毒程序的更新动作。

因此，如何能够找出一种防护计算机安全的方法和系统来避免黑客的攻击并解决计算机病毒的问题，而提供使用者一个安全的计算机使用环境，且能避免非授权者进行计算机数据的复制，便成为一件非常重要的工作。

20

发明内容

因此，本发明的主要目的就是在提供一种数据保护方法，能够在早期检测到黑客的动作，并进而对其进一步的未经授权的動作进行记录，或启动一预定的反制动作。

25 本发明的另一目的在提供一种数据保护方法，避免计算机病毒干扰计算机正常运作。

本发明的再一目的在提供一种数据保护方法，避免非授权数据被复制。

根据本发明，一符合安全条件的使用者经由转接系统连接到内部数据系统。不符合安全条件的未经授权者则被转接到反制系统。反制系统与内部数据系统具有相同的虚拟输出格式，此时未经授权者误以为其已经侵入内部数

30

据系统，而进行进一步的动作。此时反制系统可记录未经授权者的活动并加以追踪，亦可在反制系统的虚拟及伪造数据中加上追踪、木马、病毒、警示程序等。

此外，本发明亦提供一监控程序，首先，针对一操作系统设计一监控程序，也就是防毒程序。该监控程序对操作系统的多个程序模块进行监控，以探知是否有任何系统功能发生异动。此外，系统的初始设定亦包括提供使用者设定一组密码，作为是否有权异动系统文件的依据。

此后，在计算机的操作过程中，如果操作系统的程序模块有任何增修删减的动作时，该监控程序便向使用者要求输入该组密码，如欠缺该组密码，则该监控程序阻止所述程序模块进行任何增修删减的动作。反之，则可容许该异动的进行，并记载该异动情形，以作为日后判断是否有合法异动的依据。

此外，当该监控程序发现所述程序模块未经授权发生异动时，该监控程序删除所述异动程序模块，并加载所述程序模块的备份映像以恢复计算机的正常运作。

另一方面，于可监控程序中亦提供一组通用密码，当使用者使用此组通用密码时，其可再不启动密码授权步骤下，执行某些特定的功能。换言之，当一病毒码具有此通用密码时，此病毒码可通过此监控程序的检测来执行变动任何程序。

为了让本发明的上述和其它目的、特征、优点与实施例能更明显易懂，附图的详细说明如下。

附图说明

图 1 所示为一基本网络结构。

图 2 所示为一被入侵的软件系统的示意图。

图 3 所示为根据本发明的一较佳实施例的外部示意图。

图 4 所示为根据本发明的一较佳实施例的程序操作流程。

图 5 所示为向使用者要求确认密码的画面示意图。

图 6 所示为根据本发明的一较佳实施例的防止黑客浏览储存数据的保护系统概略图。

图 7 所示为根据本发明的一较佳实施例的操作流程图。

其中，附图标记说明如下：

- | | | | |
|----|--------------|--------------|--------|
| 10 | 使用者 | 12 | 黑客 |
| | 101 转接系统 | 102 | 内部数据系统 |
| | 103 反制系统 | 104 | 网络 |
| 5 | 105 使用者要求 | 106 | 电子装置 |
| | 107 使用者 | 200 至 208 步骤 | |
| | 300 驱动程序层 | 302 操作系统层 | |
| | 304 应用程序层 | 306 防毒程序 | |
| | 308 操作系统 | 310 计算机 | |
| 10 | 402 至 420 步骤 | | |

具体实施方式

请参照图 1，此图所示为一基本的网络结构图。当一使用者 10 连接上网络 104 后，使用者 10 储存于计算机上的数据，即有可能因黑客 12 通过网络 104 的入侵，而被毁坏或窃取。例如，若黑客 12 可解码使用者 10 所设定的密码，则其即可经由网络 104 浏览使用者 10 储存于计算机的数据。此外，黑客 12 亦可能制作病毒，并经由网络 104 散布，使用者 10 则在使用网络 104 时，将带有病毒的文件载回。当这些带有病毒的文件被载回使用者 10 的计算机时，便在特定的条件下，例如感染文件被执行或是宏程序被执行时，进一步潜入操作系统的程序模块，伺机发作，执行破坏动作。因此，本发明即是提供一种保护的系统和方法来防止黑客的攻击。

当黑客于网络上散布病毒时，本发明的系统和方法可防止病毒攻击使用者的计算机。

请参照图 2，一般而言，计算机软件系统包括驱动程序层 300、操作系统层 302，与应用程序层 304。这三层各职司不同的工作，但彼此间须紧密合作以完成使用者交付的工作。驱动程序层 300 通常由各硬件厂商研发设计，应用程序层 304 则针对使用者的各种不同应用而开发出来，至于操作系统层 302 则作为应用程序层 304 与驱动程序层 300 之间的重要桥梁，借助对操作系统层 302 进行程序呼叫，应用程序层 304 的设计者便无须处理所有硬件的细节，而专心在设计完成其待处理的工作。

操作系统层 302 通常由许多的程序模块构成，例如当今最常用的个人计算机操作系统为微软操作系统，其由庞大的程序模块构成，这些程序模块被包装到一系列的系统中，当操作系统执行时依照其需求被加载内存以执行相关的工作。

5 然而，当计算机病毒的病毒码被执行时，计算机病毒码会窜改操作系统层 302 的程序模块，以拦截或改变原先程序模块的正常运作。简言之，此时计算机系统即中毒了。

图 3 所示为根据本发明的一较佳实施例的外部示意图，首先，使用者将某操作系统 308 安装到计算机 310 中。在安装完成后，使用者进一步将针对
10 此操作系统 308 设计的防毒程序 306 也安装到计算机 310 中。举例来说，当微软出版 Windows 2000 操作系统，则使用者去购买对应 Windows 2000 操作系统设计的防毒程序。以下将说明此防毒程序 306 如何进行检测以及防毒的工作。

图 4 是此防毒程序 306 的运作流程图。

15 首先，此防毒程序 306 先记录操作系统 302 的程序模块的映像文件(步骤 402)。关于此步骤可预先依据特定的操作系统 302 进行映像文件的备份，而另一种做法则是在操作系统 302 安装后，由此防毒程序 306 动态找寻哪些文件用来储存操作系统 302 的程序模块，例如用附文件名进行搜寻；并且针对这些程序模块将其数据以压缩或不压缩的方式记录其映像文件。此外，为了
20 快速检验是否程序模块遭到修改，亦可额外使用杂凑函数对系统文件进行运算以得出一索引值，届时可通过此索引值的比对，即能快速得知是否程序模块有进行任何的异动。

接着，防毒程序 306 提供使用者设定一组或一组以上的密码(步骤 404)，此密码作为验证使用者权限，以异动上述的程序模块的依据。当数据连上线
25 后，为了避免遭到黑客的盗用，因此在进入数据库前浏览或进行数据更动时，均会要求输入一组设定密码，来确定进入者的身分。但此输入密码程序亦使用程序语言编写，为了避免此程序上线后遭到黑客破解，造成密码保护机制形同虚设，因此，本发明会于输入密码程序上线后，利用一特殊的编码机制，对此程序原始码部分加以编码避免核心的程序代码遭到黑客破解。

30 传统上每一种程序语言在进行组译时，均会使用一特定的编译器，但本

发明借助打破这种特定的使用关系，来对程序进行组译，让黑客于进行反组译，破解原始码时发生错误无形中，进一步提升本发明预防黑客侵入的能力。例如，本发明在编写完设定密码程序和系统程序后，可将设定密码程序的原始码先行重组后，再转换成另一种程序语言，然后以此种程序语言的编译器进行组译。

如此，当黑客欲破解设定密码侵入本发明的系统时，其需先拆解设定密码的程序语言所使用的编译软件为何，进行反组译后，再将原始码重组回原本的状态，才可进行破解。然而，由于本发明的设定密码程序和系统程序虽以同一程序语言进行编写，但设定密码程序的原始码会先行重组再以另一种程序语言的编译器进行组译。如此会让黑客有一错觉，而使用系统程序的编译方法来进行反组译，如此更不可能破解本发明所设密码。

以上为系统设定的基本工作，接着，当使用者要更新任何一个上述的程序模块时(步骤 406)，防毒程序 306 便出现提示窗口，向使用者要求输入密码以作为确认(步骤 408)，如图 5 所示。为了执行此种监控的任务，防毒程序 306 需要有一个常驻部分负责拦截对程序模块进行异动的作业，关于此点的一种做法是让防毒程序 306 去拦截操作系统的文件操作接口，例如在 Windows 操作系统，对文件操作的 API 接口作一个拦截的动作，并检查异动文件是否为记录中存有上述程序模块的系统文件。

如果使用者输入的密码错误时，则防毒程序 306 拒绝该次程序模块的异动(步骤 412)。反之，防毒程序 306 则容许该次程序模块异动的进行(步骤 414)，此外，防毒程序 306 并更新其数据库，将新的程序模块数据存成合法的参考数据。

除了对于可拦截的程序模块的异动进行密码验证的动作，防毒程序 306 亦于每次开机时或定期对于程序模块进行监控(步骤 416)，以探知是否有未经授权之增修删减动作的发生(步骤 418)。假如发现有任何未经授权程序模块发生异动，则判定该程序模块中毒，删除该程序模块，并从数据库将该程序模块的映像重新载回系统，以恢复系统正常的运作。

除此之外，使用者的密码亦可作为一计算机的识别证明号码，易言之，当计算机连上网络后，利用使用者密码可得知哪一台计算机被连上网络。然而，为了避免两台计算机均使用相同的使用者密码作为计算机识别证明号码

(identification number, ID), 可借助事先安排各计算机的识别证明号码来避免上述的情况发生, 因而, 可让每一台计算机均具有一特定的识别证明号码。当每一部计算机均具有各自的特定识别证明号码后, 即可根据此号码确实得知连上网络的计算机。

- 5 此种事先安排各计算机的识别证明号码方法可应用于任一种计算机系统中, 来借以防范黑客的攻击, 例如, 可参阅图 6 所示, 为根据本发明的一较佳实施例的防止黑客浏览储存数据的保护系统概略图。本发明的保护系统具有一转接系统 101、一内部数据系统 102 以及一反制系统 103。其中转接系统 101 分别连接到一外部网络 104、一内部数据系统 102 及反制系统 103。
- 10 而一预先决定的识别证明号码(使用者密码)被安排给各计算机。

图 7 所示为根据本发明的一较佳实施例的操作流程图, 请交互参照图 6 及图 7。在正常的情况下, 使用者 107 使用一电子装置 106, 例如计算机, 将一使用者要求 105, 经由外部网络 104 连接到转接系统 101(步骤 200)。当使用者 107 的使用者要求 105 符合一预定安全条件(步骤 202)时, 转接系统

15 101 将使用者要求 105 转接给内部数据系统 102(步骤 204)继续处理。此转接系统 101 的实施包括 IP 分享器、硬件防火墙、或软件防火墙或其它具通讯协议转送能力的装置, 而此内部数据系统 102 的实施例包括网站服务器、文件服务器等各种能响应使用者要求提供数据的数据提供类型的机器。

然而, 当此使用者要求 105 其无法通过此预定的安全条件(步骤 202)时,

20 亦即判断其为一未经授权的活动时, 转接系统 101 并不直接驳回使用者要求 105, 而是将使用者要求 105 转接给反制系统 103(步骤 206)。反制系统 103 在接收此使用者要求 105 后, 以一预定响应方式, 因应此使用者要求 105, 提供一预定响应内容(步骤 208)。

此时, 此响应内容经过刻意调整, 使得此响应内容与若此内部数据系统

25 102 接收此使用者要求 105 时所提供的响应数据具有一相同格式。

换句话说, 由于反制系统 103 依据使用者要求 105 提供一接口类似于内部数据系统 102 的响应数据, 未经授权的使用者 107 会误以为已经成功侵入此内部数据系统 102。如果此未经授权的使用者 107 继续进一步的数据窃取或是破坏的动作, 反制系统 103 持续记录其不法举动, 并且产生各种响应措施, 例如报警、反检测此使用者 107 的相关数据, 如电子装置 106 的识别证

30

明号码 (ID)，记录此使用者 107 进一步的举动等等。当然，反制系统 103 亦可在该未经授权者 107 尝试登入时即开始记录其行动。

根据本发明，由于每一部计算机均具有特定的识别证明号码 (或使用者密码)，因此一非授权的使用者 107，可借助此识别证明号码来进行追踪。

5 另一方面，即使此非授权的使用者 107 使用公共计算机来连接网络，由于每一台计算机均具特定的识别证明号码，此时公共计算机的管理者，为了避免因非法使用者的违法行为，因此识别证明号码而被追踪到并遭受牵连处罚，会间接迫使其加强监督使用者使用情况。因此，本发明可增进网络的管理安全。

10 另一方面，根据本发明，由于重要的数据，例如机密数据存放于内部数据系统 102，而非反制系统 103，因此本具体实施例能够成功地检测未经授权的使用者 107 的进一步动作，以及进行各种反制动作，而不致于让存有重要数据的内部数据系统 102 遭受危险。借助此种方法，我们提供了解决网络安全的一个重要方式。

15 值得注意的是，上述的反制系统 103 可分别或同时与转接系统 101、内部数据系统 102 耦合在一起。转接系统 101 可分别或同时与反制系统 103、内部数据系统 102 耦合在一起。内部数据系统 102 亦可分别或同时与转接系统 101、反制系统 103 耦合在一起。

此外，转接系统 101 与反制系统 103、内部数据系统 102 及外部网络 104
20 之间的连接包括有线、无线、直接或间接连接的方式。

此外，此外部网络 104 的实施例包括因特网(Internet)、企业内部网络(Intranet)、无线网络(Wireless Network)、通信网路(Telecommunication Network)等等。此使用者要求 105 的类型包括因特网协议封包(IP Package)形式的文件传输协议要求(File Transfer Protocol request, FTP)、超文本传输协议(Hypertext
25 Transfer Protocol request, HTTP)、微软网络芳邻协议 (network neighboring) 及其相似物等。

转接系统 101 的实施例包括硬件及软件形式的防火墙(Firewall)、IP 分享器等等。内部数据系统 102 的实施例包括网站(Web Site)、文件服务器(File Server)、数据库服务器(Database Server)、个人计算机等等。发出使用者要求
30 的电子装置 106 的实施例包括个人计算机、个人数字助理(PDA)、手机、工

作站等等。

至于前述的预定安全条件的实施例则包括当使用者要求具有超过一预定次数的密码错误重试动作，以及发出使用者要求的机器 106 的识别码。此预定安全条件亦得设定使用者要求内容所能够承载的命令或指令内容，例如
5 在网站服务系统的实施例中，系统管理者可设定仅提供部分的命令或指令服务，而非提供全部的 HTTP 命令内容。

至于前述的反制系统 103 的预定响应方式得由一系统管理者进行设定，或是直接设定在反制系统 103 中。此外，此反制系统 103 的预定响应的方式，亦可包括在使用者 107 接收此反制系统 103 的响应内容后，记录此使用者 107
10 继续对此反制系统 103 进行的动作。使用者 107 可能的动作包括窃取或破坏反制系统 103 的数据。如此，便能通过这些动作，对使用者 107 进行相对应的法律行动。此外，此反制系统 103 的响应方式亦可包括追踪使用者 107 的相关数据，例如其所使用机器 106 的地址。

至于反制系统 103 所提供的响应内容可设定为与内部服务器 102 相似的
15 虚拟数据，这些虚拟数据不致泄漏机密，而无安全之虞。甚至，此响应内容中亦可包括反追踪程序，以便追踪此使用者 107 的相关数据。当然，此响应内容亦可包括木马程序。此木马程序能够在使用者 107 所使用的机器执行。

此外，为了确保网络频宽的使用，本发明于另一实施例中，于转接系统 101 外接一管理接口，供系统管理者借助此管理接口来管理联机次数，例如
20 系统管理者可通过此管理接口来设定单位时间内可联机最大次数，对于超过此数目的，则直接退回其要求而不经由反制系统处理。除此之外，本发明对于已经授权者亦提供一监控机制，因为本发明的每一部计算机均具有一特定的识别证明号码，因此，本发明的管理接口，可借助此识别证明号码来分别设定每一部计算机于单位时间内可使用的频宽，一旦超过此设定频宽，即使
25 为已经授权者，亦直接退回其要求而不经由反制系统处理。换言之，本系统可进一步对频宽使用进行管控，对超过一定频宽用量的使用者，直接切断其联机，因此可避免黑客通过大量散发垃圾邮件来瘫痪系统的攻击。

另一方面，本发明亦提供一种防止重制数字记录媒体的方法和系统。根据此方法，一可破坏计算机系统中复制功能的病毒被散布于数字数据中，且
30 布建于数字记录媒体的轨道中。易言之，储存于数字记录媒体中的数字数据

具有可破坏计算机系统中复制功能的病毒。当一使用者欲借助计算机复制此数字记录媒体时，此病毒会被加载至计算机中，进而破坏此计算机系统内的复制功能，造成重制数字记录媒体失败。

然而，根据本发明，当程序模块要被改变时，监控程序会要求使用者输入所设定的使用者密码。假如，所输入的使用者密码错误，此监控程序及禁止任何程序模块的改变。易言之，经由数字记录媒体加载至计算机中的病毒，在此监控程序的运作下，将被禁止执行任何程序模块的删改动作，因此，计算机系统的复制功能仍可正常运作。

因此，为了避免数字记录媒体被重制，一额外的通用密码被设定在每一部计算机系统中。此通用密码的主要功能即是在于让某些计算机特定功能，在监控程序的启动下仍能保持运作，易言之，即是让这些特定功能载有此通用密码，让其可通过监控程序的监控，进而执行此些设定功能。例如，可让此破坏计算机系统复制功能的计算机病毒，载有此通用密码，一旦此病毒经由数字记录媒体加载至计算机中，由于此毒具有此通用密码，因此其可通过监控程序的监控，进而启动病毒运作破坏计算机复制功能，造成计算机无法重制数字记录媒体。

除此之外，亦可借助载有通用密码的病毒，来破坏黑客计算机的浏览功能。例如，可将此载有通用密码的破坏浏览功能病毒散布于图 6 中的反制系统 103。当黑客经由网络非法进入使用者计算机后，并经由本发明的保护系统被引导至反制系统 103，此载有通用密码的病毒会被加载至黑客的计算机系统中，破坏浏览功能。即使黑客的计算机亦装设有本发明的监控程序，但因被加载的病毒具有通用密码，其仍可在监控程序启动的情况下，来破坏黑客计算机的浏览功能。

另一方面，因为每一部计算机均具有其特定的识别证明号码（使用者密码）。因此，对于黑客而言，其需译码每一部计算机的识别证明号码才可广为散布计算机病毒，若仅译码部分计算机，病毒的散布将极为有限。因此，本发明的方法，亦可限制计算机病毒的散布范围。

总而言之，根据本发明的方法，一预先设定的识别证明号码被安排给每一部计算机，利用此识别证明号码，计算机系统即可借助本发明的反制系统追踪侵入的黑客。

当一黑客进入一计算机系统，并键入错误的使用者密码，本发明的转接系统会将此黑客导引至一反制系统让其浏览错误数据，同时追踪此黑客所使用计算机的识别证明号码。因为每一部计算机的识别证明号码均不同，因此很容易得知黑客的位置。

- 5 除此之外，本发明亦提供一监控程序，此监控程序记录操作系统的程序模块的映像数据，并在初始时由使用者设定一组密码。在计算机操作过程中，如有任何程序模块发生异动，此监控程序向使用者要求该组密码以作为验证，如果密码错误，则拒绝对于程序模块进行异动的动作。此外，监控程序并定期对程序模块进行检测，以发现是否有未经授权的异动发生。如果有未经授权的异动发生时，则删除受感染的程序模块，并载入原先备份的程序模块，借以迅速恢复计算机的正常运作。此外，本发明亦提供一通用密码，让某些特定功能载有此通用密码，而可通过此监控程序的监控，借以破坏特定功能。
- 10

- 15 虽然本发明已以一较佳实施例揭示如上，然而其并非用以限定本发明，任何本领域技术人员，在不脱离本发明的精神和范围内，当可作各种的更动与润饰。

权利要求

1、一种保护计算机系统中计算机数据的方法，该方法包括：

针对一操作系统设计一可接受一通用密码的监控程序，其中该监控程序

5 对该操作系统的多个程序模块进行监控；

当该操作系统安装完成时，该监控程序提供使用者设定一组使用者密码

；

当该操作系统的所述程序模块有任何增修删减的动作时，该监控程序向使用者要求输入该组使用者密码；以及

10 如欠缺该组密码，则该监控程序阻止所述程序模块进行任何增修删减的动作。

2、根据权利要求 1 所述的方法，其中该方法还包括安排一特定的识别证明号码给该计算机系统。

3、根据权利要求 2 所述的方法，其中当该计算机系统连接网络时，可
15 借助该识别证明号码而被追踪到。

4、根据权利要求 2 所述的方法，其中该方法还包括针对每一识别证明号码设定一可接受频宽。

5、根据权利要求 1 所述的方法，其中该方法还包括当该监控程序发现所述程序模块未经授权发生异动时，该监控程序删除所述异动程序模块，并
20 加载所述程序模块的备份映像以恢复计算机的正常运作。

6、根据权利要求 1 所述的方法，其中该方法还包括当该监控程序检测到所述程序模块是在具有该通用密码的情况下进行增修删减的动作时，则该增修删减的动作可于该计算机系统中执行。

7、根据权利要求 1 所述的方法，其中该方法还包括散布一具通用密码
25 的破坏复制功能病毒于一数字记录媒体的轨道中。

8、根据权利要求 1 所述的方法，其中该方法还包括散布一具通用密码的破坏浏览功能病毒给一非授权的浏览者。

9、根据权利要求 1 所述的方法，其中该监控程序定期扫描所述程序模块的内容，以检测所述程序模块是否发生未经授权的异动。

30 10、根据权利要求 1 所述的方法，其中该监控程序在每次开机时，于该

操作系统加载前检测所述程序模块是否发生未经授权的异动。

11、根据权利要求 1 所述的方法，其中该监控程序拦截该操作系统的文件操作接口的呼叫，以检测所述程序模块何时发生增修删减的动作。

12、根据权利要求 1 所述的方法，其中该监测程序检查所述程序模块的
5 文件长度以判断是否发生增修删减的动作。

13、根据权利要求 1 所述的方法，其中该监测程序检查所述程序模块的文件异动时间，并对照前次经授权更改的异动时间以判断是否发生增修删减的动作。

14、根据权利要求 1 所述的方法，其中该监测程序对所述程序模块通过
10 一杂凑函数计算一索引，以作为是否异动的判断。

15、根据权利要求 1 所述的方法，其中该监控程序针对不同的该操作系统预先设计。

16、根据权利要求 1 所述的方法，其中该设定密码与该操作系统系采用不同的程序语言编译器进行编译。

15 17、一种计算机数据的保护方法，至少包括下列步骤：

记录操作系统的多个程序模块的映像文件，其中该操作系统接受一通用密码；

提供使用者设定一组密码；

20 监控所述程序模块的异动情形，当所述异动在非使用该通用密码时发生；

当所述程序模块发生异动时，向使用者要求输入该组密码；

如欠缺该组密码，阻止所述程序模块发生异动；以及

当检测所述程序模块发生未经授权的异动，删除未经授权异动的所述程序模块，并以合法的所述程序模块的映像文件取代之，以恢复系统正常运作。

25 18、根据权利要求 17 所述的保护方法，还包含定期扫描所述程序模块的内容，以检测所述程序模块是否发生未经授权的异动。

19、根据权利要求 17 所述的保护方法，还包含每次开机时，于该操作系统加载前检测所述程序模块是否发生未经授权的异动。

30 20、根据权利要求 17 所述的保护方法，还包含拦截该操作系统的文件操作接口的呼叫，以检测所述程序模块何时发生增修删减的动作。

21、根据权利要求 17 所述的保护方法，还包含检查所述程序模块的文件长度以判断是否发生增修删减的动作。

22、根据权利要求 17 所述的保护方法，还包含检查所述程序模块的文件异动时间，并对照前次经授权更改的异动时间以判断是否发生增修删减的动作。

23、根据权利要求 17 所述的保护方法，还包含通过一杂凑函数对所述程序模块计算对应的索引，以作为是否异动的判断。

24、根据权利要求 17 所述的保护方法，还包含提供一数据库，以对应不同的操作系统。

25、根据权利要求 17 所述的保护方法，其中该方法还包括散布一具通用密码的破坏复制功能病毒于一数字记录媒体的轨道中。

26、根据权利要求 25 所述的保护方法，其中当该数字记录媒体数据被加载至一计算机系统中，该计算机的复制功能会被破坏。

27、根据权利要求 17 所述的保护方法，其中该方法还包括散布一具通用密码的破坏浏览功能病毒给一非授权的浏览者。

28、根据权利要求 17 所述的保护方法，其中该设定密码与该操作系统采用不同的程序语言编译器进行编译。

29、一种保护计算机系统中计算机数据的方法，该方法包括：

针对一操作系统设计一监控程序，其中该监控程序对该操作系统的多个程序模块进行监控；

当该操作系统安装完成时，该监控程序提供使用者设定一组使用者密码；

当该操作系统的所述程序模块有任何增修删减的动作时，该监控程序向使用者要求输入该组使用者密码；以及

如欠缺该组使用者密码，则该监控程序阻止所述程序模块进行任何增修删减的动作。

30、如申请专利范围第 29 项所述之方法，其中该方法还包括安排一特定的识别证明号码给该计算机系统。

31、根据权利要求 30 所述的方法，其中当该计算机系统连接网络时，借助该识别证明号码而被追踪到。

32、根据权利要求 30 所述的方法，其中该方法还包括针对每一识别证明号码设定一可接受频宽。

33、根据权利要求 29 所述的方法，其中该方法还包括设定一组通用密码，当该监控程序发现所述程序模块是在具有该通用密码的情况下进行增修删减的动作时，则该增修删减的动作可于该计算机系统中执行。

34、根据权利要求 33 所述的方法，其中该方法还包括散布一具通用密码的破坏复制功能病毒于一数字记录媒体的轨道中。

35、根据权利要求 33 所述的方法，其中该方法还包括散布一具通用密码的破坏浏览功能病毒给一非授权的浏览者。

36、根据权利要求 29 所述的方法，其中该方法还包括当该监控程序发现所述程序模块未经授权发生异动时，该监控程序删除所述异动程序模块，并加载所述程序模块的备份映像以恢复计算机的正常运作。

37、根据权利要求 29 所述的方法，其中该监控程序定期扫描所述程序模块的内容，以检测所述程序模块是否发生未经授权的异动。

38、根据权利要求 29 所述的方法，其中该监控程序在每次开机时，于该操作系统加载前检测所述程序模块是否发生未经授权的异动。

39、根据权利要求 29 所述的方法，其中该监控程序拦截该操作系统的文件操作接口的呼叫，以检测所述程序模块何时发生增修删减的动作。

40、根据权利要求 29 所述的方法，其中该监测程序检查所述程序模块的文件长度以判断是否发生增修删减的动作。

41、根据权利要求 29 所述的方法，其中该监测程序检查所述程序模块的文件异动时间，并对照前次经授权更改的异动时间以判断是否发生增修删减的动作。

42、根据权利要求 29 所述的方法，其中该监测程序对所述程序模块通过一杂凑函数计算一索引，以作为是否异动的判断。

43、根据权利要求 29 所述的方法，其中该监控程序针对不同的该操作系统预先设计。

44、根据权利要求 29 所述的方法，其中该设定密码与该操作系统系采用不同的程序语言编译器进行编译。

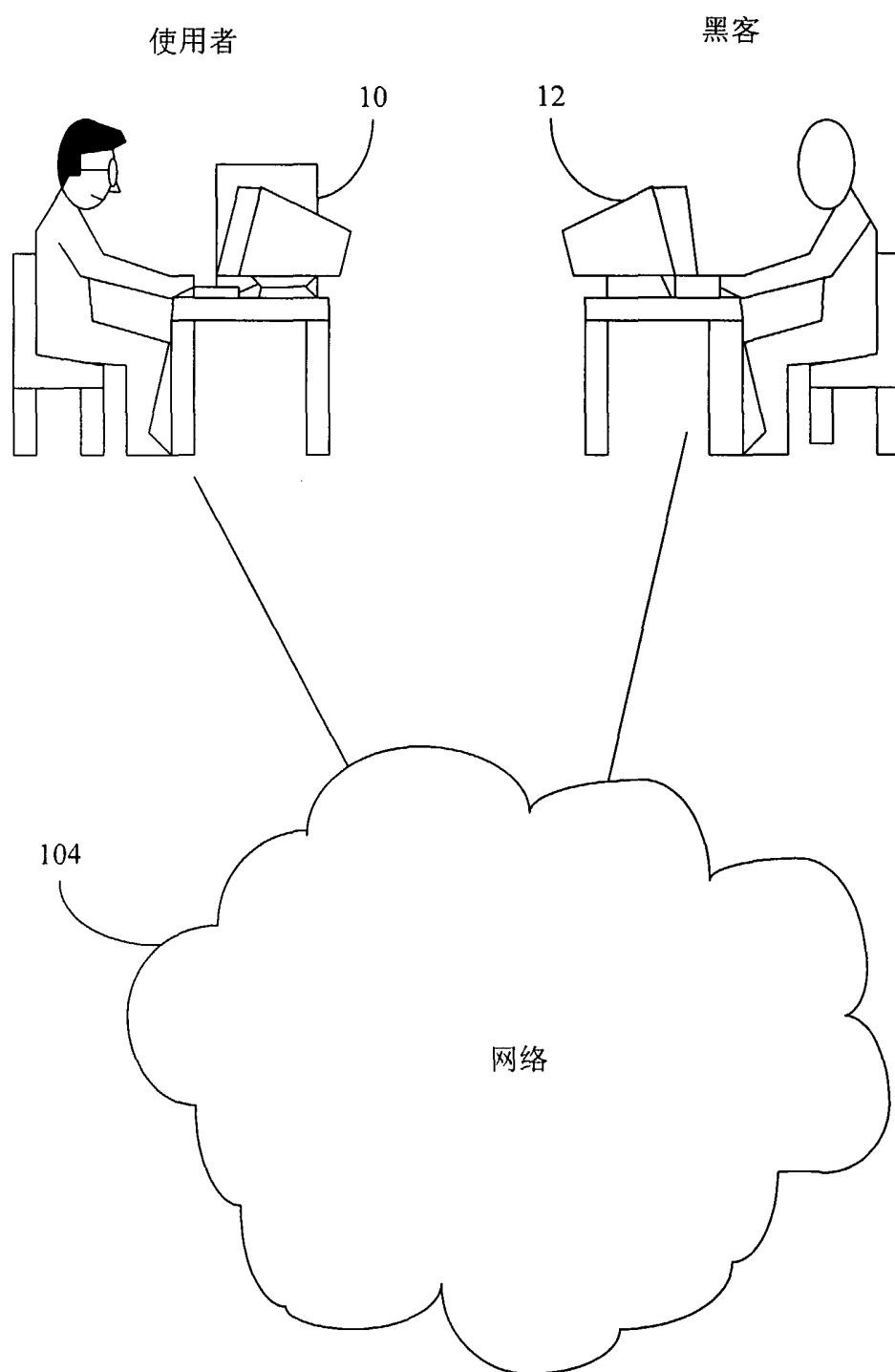


图1

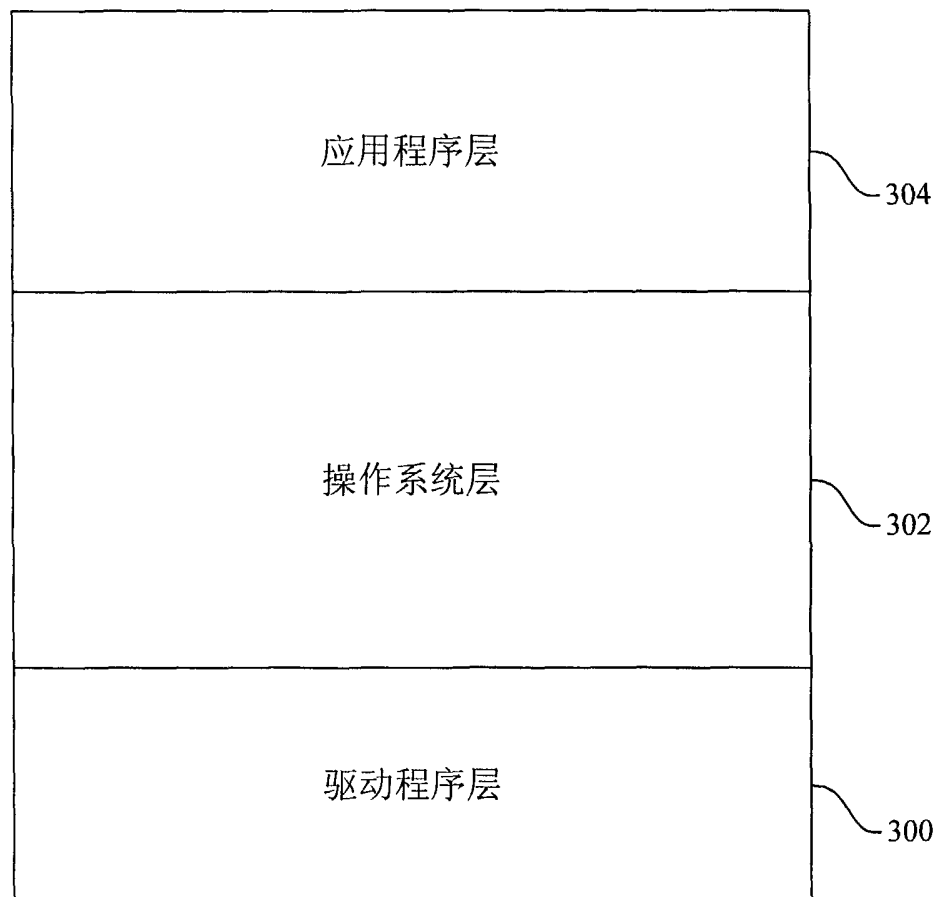


图2

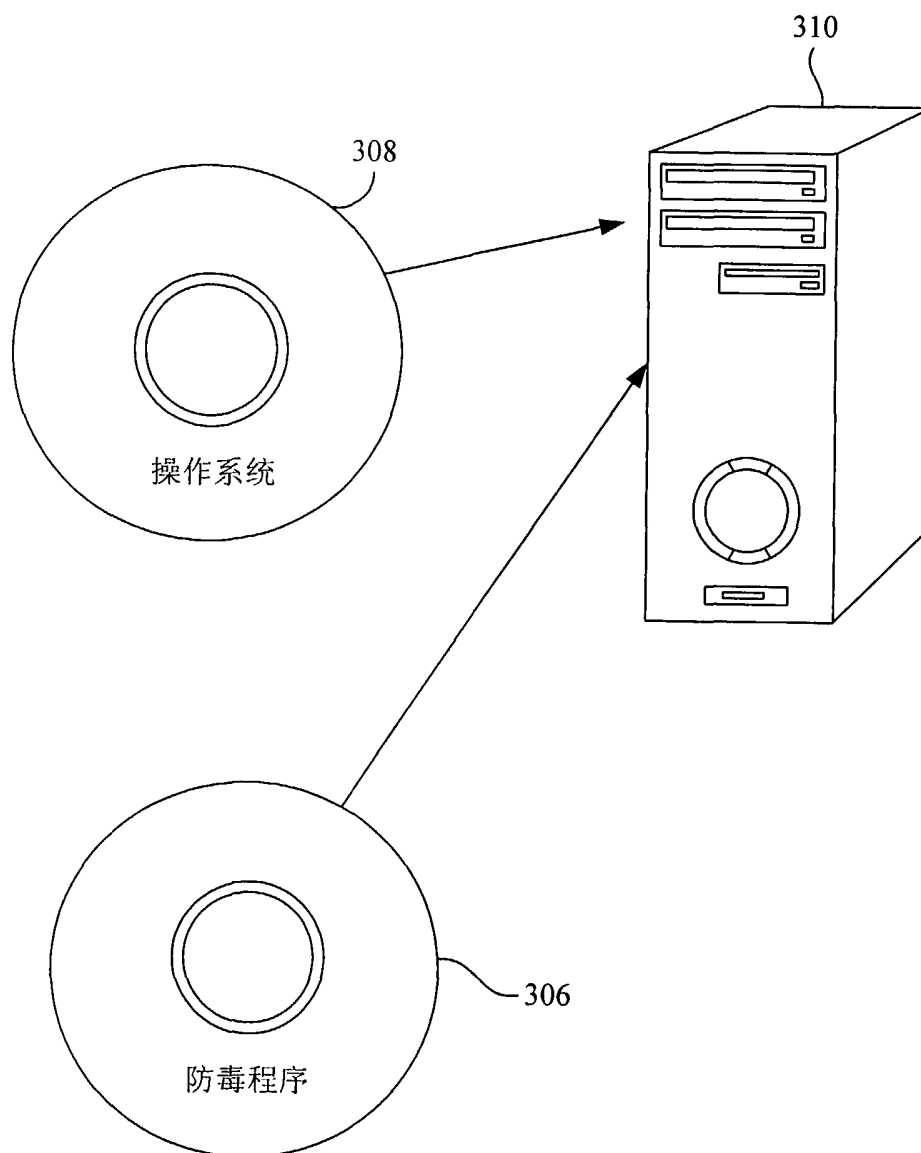


图3

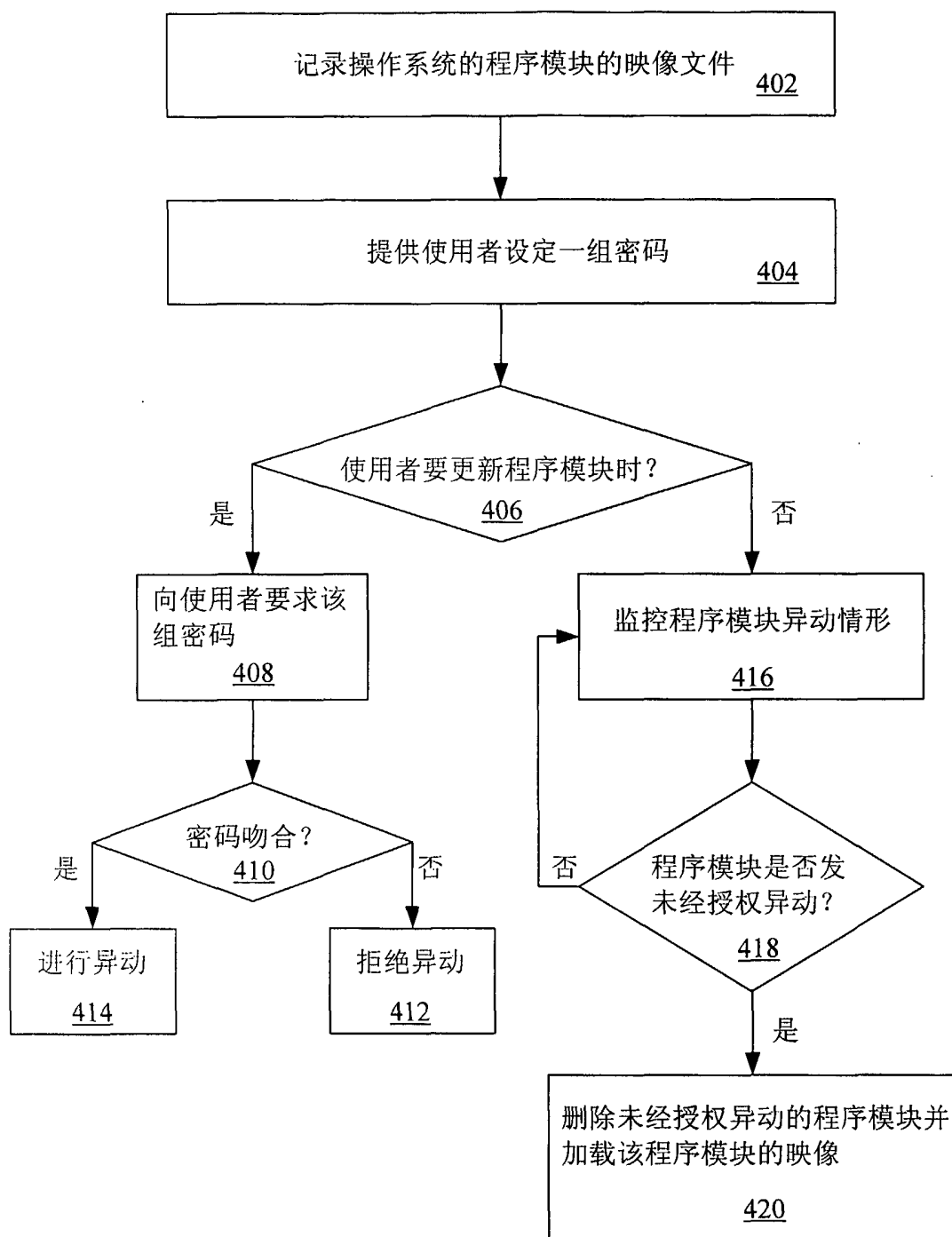


图4

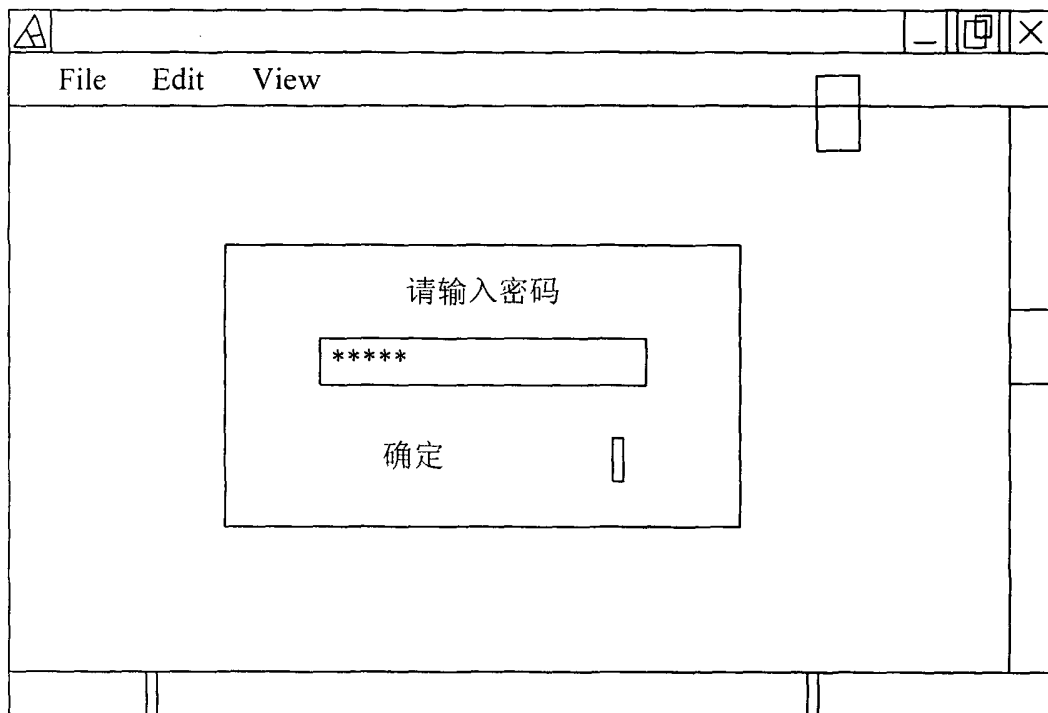


图5

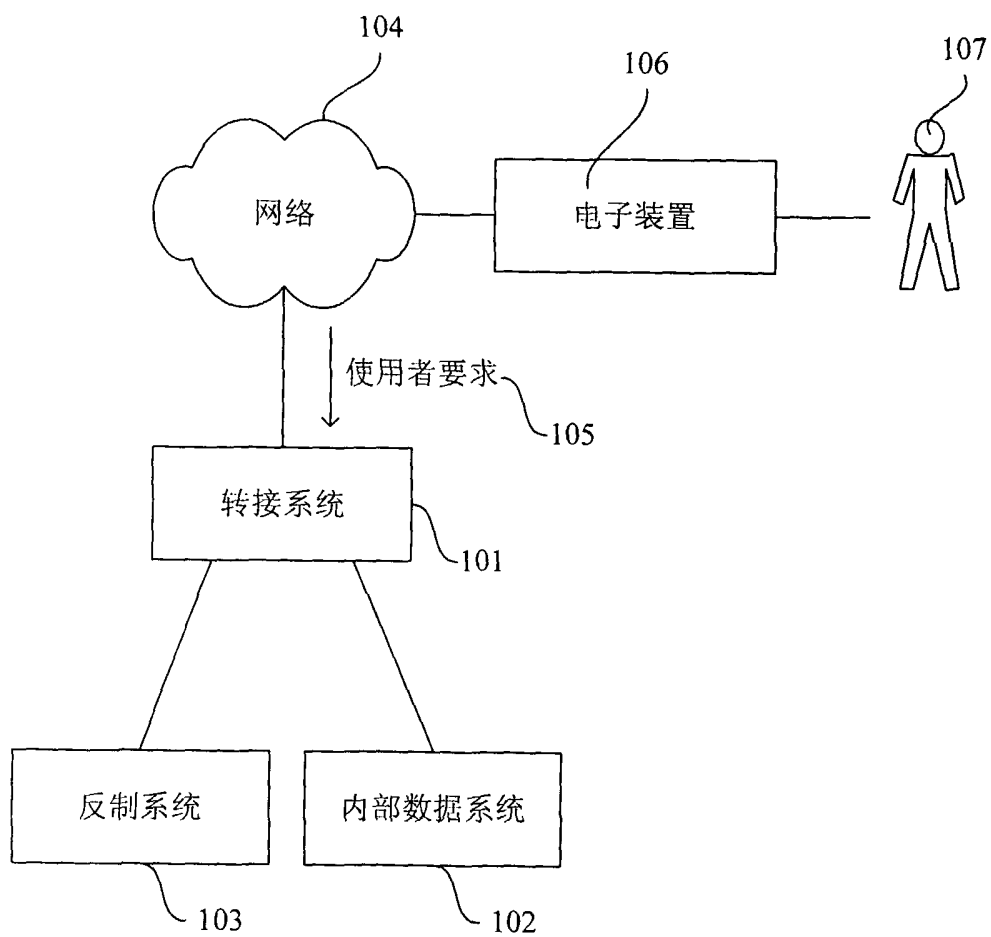


图6

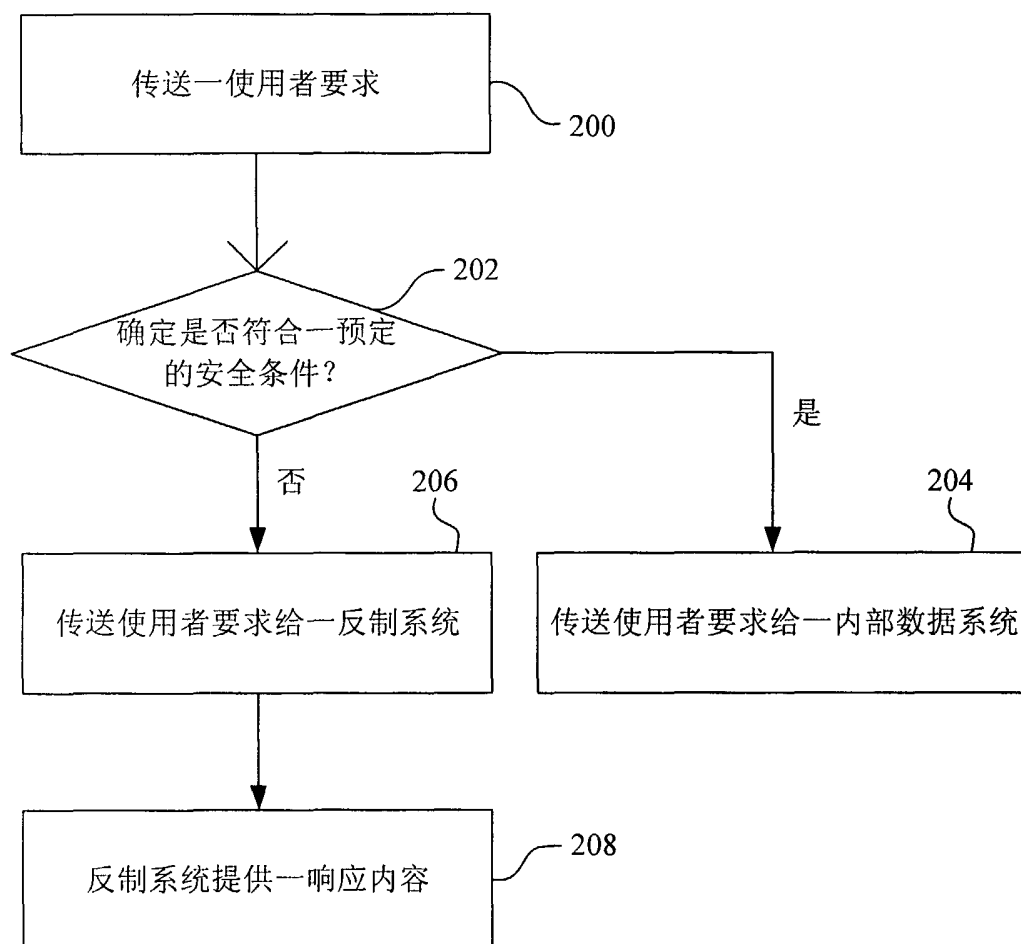


图7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2005/000292

A. CLASSIFICATION OF SUBJECT MATTER

(IPC7): G06F11/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

(IPC7): G06F11/30、12/14 、11/00 H04L12/28、12/24、12/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRS、WPI、EPODOC、PAJ (computer、data、security、monitor+、password、cipher、virus)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO0192981A2 (Mayer,Yaron et.al) , 06.Dec 2001 (06.12.2001) , the whole	1-44
A	CN1475913A (BEIJING GETAI BIOLOGICAL SCI & TECHNOLOG) , 18.Feb 2004 (18.02.2004) , the whole	1-44
A	CN1394041A (HUAWEI TECH CO LTD) , 29.Jan 2003 (29.01.2003) , the whole	1-44

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.*** Special categories of cited documents:**

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&”document member of the same patent family

Date of the actual completion of the international search

29.May 2005 (29.05.2005)

Date of mailing of the international search report

16 · JUN 2005 (16 · 06 · 2005)

Name and mailing address of the ISA/CN

The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer

Hong Yan

Telephone No. (86-10)62084937

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2005/000292

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1394041A	29.Jan 2003 (29.01.2003)	None	
CN1475913A	18.Feb 2004 (18.02.2004)	None	
WO0192981A2	06.Dec 2001 (06.12.2001)	CA2424352A	06.Dec 2001 (06.12.2001)
		AU6263201A	11.Dec 2001 (11.12.2001)
		GB2380303A	02.Apr 2003 (02.04.2003)
		EP1305688A	02.May 2003 (02.05.2003)
		CN1444742T	24.Sep 2003 (24.09.2003)
		JP2003535414T	25.Nov 2003 (25.11.2003)
		US2004034794A	19.Feb 2004 (19.02.2004)

国际检索报告

国际申请号

PCT/CN2005/000292

A. 主题的分类

(IPC7): G06F11/30

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

(IPC7): G06F11/30、12/14 、11/00 H04L12/28、12/24、12/26

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CPRS、 WPI、 EPODOC、 PAJ (computer、 data、 security、 monitor+、 password、 cipher、 virus)

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	WO0192981A2 (Mayer,Yaron 等), 06.12 月 2001 (06.12.2001), 全文	1-44
A	CN1475913A (北京格泰生物科技有限公司), 18.2 月 2004 (18.02.2004), 全文	1-44
A	CN1394041A (华为技术有限公司), 29.1 月 2003 (29.01.2003), 全文	1-44

☐ 其余文件在 C 栏的续页中列出。

☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

29.5 月 2005 (29.05.2005)

国际检索报告邮寄日期

16 · 6 月 2005 (16 · 06 · 2005)

中华人民共和国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

洪岩

电话号码: (86-10)62084937

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2005/000292

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1394041A	29.1 月 2003 (29.01.2003)	无	
CN1475913A	18.2 月 2004 (18.02.2004)	无	
WO0192981A2	06.12 月 2001 (06.12.2001)	CA2424352A	06.12 月 2001 (06.12.2001)
		AU6263201A	11.12 月 2001 (11.12.2001)
		GB2380303A	02.4 月 2003 (02.04.2003)
		EP1305688A	02.5 月 2003 (02.05.2003)
		CN1444742T	24.9 月 2003 (24.09.2003)
		JP2003535414T	25.11 月 2003 (25.11.2003)
		US2004034794A	19.2 月 2004 (19.02.2004)