(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
2009 年2 月12 日 (12.02.2009)

PCT

(10) 国际公布号
WO 2009/018716 A1

(51) 国际专利分类号:
G06F 21/24 (2006.01)

(21) 国际申请号: PCT/CN2008/001358

(22) 国际申请日: 2008 年7 月23 日 (23.07.2008)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200710120031.0
2007 年8 月7 日 (07.08.2007) CN

(71) 申请人及
(72) 发明人: 江雨(JIANG, Yu) [CN/CN]; 中国北京市海淀区清河中街69号力度家园4号楼2单元1102, Beijing 100085 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (BEIJING TONGDAXINHENG INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: A SECURITY DISPOSING METHOD AND DEVICE FOR INPUT DATA

(54) 发明名称: 一种输入数据的安全处理方法及装置

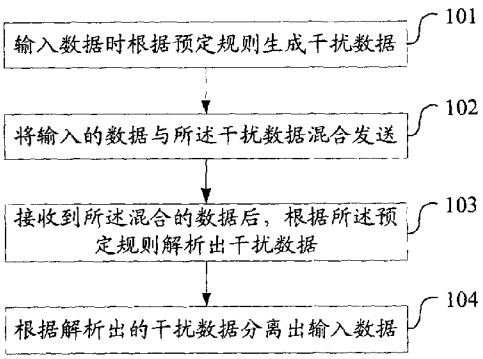

图 1 / Fig 1

101 GENERATING THE INTERFERENCE DATA ACCRODING TO THE PREDEFINED RULE WHEN INPUTTING DATA
102 MIXING THE INPUT DATA WITH THE INTERFERENCE DATA AND SENDING THE MIXED DATA
103 PARSING OUT THE INTERFERENCE DATA ACCRODING TO THE PREDEFINED RULE AFTER RECEIVING THE MIXED DATA
104 SEPARATING THE INPUT DATA ACCRODING TO THE INTERFERENCE DATA

(57) Abstract: A security disposing method and device for the input data involves generating an interference data according to a predefined rule when inputting the data, and mixing the input data with the interference data and sending the mixed data, and parsing out the interference data according to the predefined rule after receiving the mixed data, and separating the input data according to the parsed interference data.

(57) 摘要:

一种输入数据的安全处理方法及装置，包括：输入数据时根据预定规则生成干扰数据；将输入的数据与干扰数据混合发送；接收到混合的数据后，根据所述预定规则解析出干扰数据；根据解析出的干扰数据分离出输入数据。

WO 2009/018716 A1

(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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, 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。

一种输入数据的安全处理方法及装置

技术领域

本发明涉及信息安全，特别涉及一种输入数据的安全处理方法及装置。

背景技术

目前，在不同的操作系统中都提供了获取用户的输入数据信息的接口或者机制，例如在微软 windows 操作系统中所提供的 Hook（钩子）就是一个非常重要的接口，它可以截获并处理送给其他应用程序的消息。据此，现在的黑客可以轻松的使用各种不同 API（Application Program Interface，应用编程接口，）层面的钩子接口程序，从而实现对键盘等数据输入设备输入的数据进行截获，达到盗窃用户的密码等重要数据信息的目的。这些技术的出现都对目前的信息安全构成了极大的威胁。

现有技术中，对于钩子的防御程序，采用了禁止部分钩子的被调用环节的方案；或者使该防御程序本身就成为一个超强的钩子程序，从而在其他钩子生效之前提前获取用户的键盘输入。

但发明人在发明过程中注意到：现有技术中的这些防御方案效果都不够好，因为至少黑客可以通过获取更高的系统权限来保障黑客程序的执行优先顺序来达到目的，或者使用更底层的操作系统调用函数，提前获取用户输入来达到目的。

面对黑客对输入数据信息越来越猖獗的盗取，非常需要更好的技术方案来保护用户输入的数据信息。

发明内容

本发明实施例提供了一种输入数据的安全处理方法及装置，用以解决现有技术中在输入数据环节上存在的信息盗取问题。

本发明实施例提供了一种输入数据的安全处理方法，包括如下步骤：

输入数据时根据预定规则生成干扰数据;

将输入的数据与所述干扰数据混合发送;

接收到所述混合的数据后，根据所述预定规则解析出干扰数据;

根据解析出的干扰数据分离出输入数据。

本发明实施例还提供了一种输入数据的安全处理装置，应用于包括数据输入设备、数据接收设备的数据处理系统，包括干扰模块、发送模块、分离模块，其中:

干扰模块，用于在通过数据输入设备输入数据时根据预定规则生成干扰数据;

发送模块，用于将通过数据输入设备输入的数据与所述干扰数据混合发送;

分离模块，用于根据所述预定规则从数据接收设备接收到的所述混合的数据中解析出干扰数据，并根据解析出的干扰数据分离出输入数据。

本发明实施例有益效果如下:

在本发明实施例中，通过在输入数据时根据预定规则生成干扰数据，并将输入的数据与所述干扰数据混合发送，从而使得想非法获取数据信息的人无法在大量杂乱无章的信息中，分辨出哪些是用户输入的信息; 即: 接收用户输入数据的操作系统，其获取到的是所有的干扰信息和用户通过数据输入设备输入的数据的总集合。由此可知，客户端上没有任何操作系统、程序知道用户实际的键盘输入。虽然用户的键盘输入信息在传输信息中以明文形式存在，但是由于大量干扰信息的掩盖，非法获取数据信息的人无法有效获取该信息，从而实现用户数据输入的隐形。

在输入数据部分进行了上述处理后，当能合法接收该输入数据的设备接收到这些混合的数据后，再根据预定规则解析出干扰数据; 通过解析出的干扰数据分离出输入数据，这样就保障了输入数据的安全还原，从而使得在数据输入时阻碍了非法者的获取，同时也能够安全的获得所输入的数据信息。

附图说明

图 1 为本发明实施例中所述输入数据的安全处理方法实施流程示意图;

图 2 为本发明实施例中所述输入数据与干扰数据的混合发送示意图;

图 3 为本发明实施例中所述输入数据的安全处理装置结构示意图;

图 4 为本发明实施例中所述对输入数据进行安全处理的环境示意图;

图 5 为本发明实施例中所述对输入数据进行安全处理的实施流程示意图;

图6为本发明实施例中所述对输入数据进行安全处理的另一实施流程示意图。

具体实施方式

下面结合附图对本发明的具体实施方式进行说明。

图 1 为输入数据的安全处理方法实施流程示意图，如图所示，可以包括如下步骤:

步骤 101、输入数据时根据预定规则生成干扰数据;

步骤 102、将输入的数据与所述干扰数据混合发送;

步骤 103、接收到所述混合的数据后，根据所述预定规则解析出干扰数据;

步骤 104、根据解析出的干扰数据分离出输入数据。

进行数据输入的输入设备都安装有执行数据处理的操作系统，比如 windows 操作系统，数据输入设备最为常见的如 PC（Personal Computer，个人电脑）等。将输入的数据与所述干扰数据混合发送是将输入的数据与干扰数据混合后发送至操作系统，然后由操作系统进行处理，本步骤中，具体的，通常实施中，假设用户通过 PC 的键盘进行具体的数据输入，操作系统中通过窗口来进行数据的各项处理。接收用户输入的窗口所获取到的是所有的干扰数据信息和用户键盘输入的数据总集合。即，到目前为止，客户端 PC 包括接收窗口在内，没有任何程序知道用户实际的键盘输入。由钩子的原理可知，虽然用户的键盘输入信息在传输信息中以明文形式存在，但是由于大量干扰

信息的掩盖，黑客是无法有效获取该输入数据的信息的，从而实现了用户键盘输入数据的“隐形”。

图 2 为输入数据与干扰数据的混合发送示意图，如图所示，具体的输入数据时根据预定规则生成干扰数据；将输入的数据与所述干扰数据混合发送，可以按以下方式实施；

步骤 201、将输入的数据传输至操作系统；

步骤 202、输入数据时根据预定规则生成干扰数据，并传输至操作系统；

步骤 203、操作系统将输入的数据与干扰数据发送。

由此可见，通过该方法的实施后，操作系统得到的是混合后的数据，即使此时数据被非法获取，其获得的也是混合后的数据，并不能从中获取到用户所输入的数据信息。

为了更有效地将输入信息隐藏在干扰信息中，干扰数据输入操作系统的速度可以大于输入数据输入操作系统的速度，比如以远高于普通用户键盘输入速率的速率输入操作系统。

为进一步的提高安全性，可以进一步的包括如下步骤：

输入数据时获取输入设备的硬件信息和/或输入时间；

根据所述输入设备的硬件信息和/或输入时间按预定规则生成干扰数据；

将输入的数据与所述干扰数据混合发送；

输入数据结束时，将所述输入设备的硬件信息和/或输入时间发送；

接收到所述混合的数据、以及所述输入设备的硬件信息和/或输入时间后，根据所述输入设备的硬件信息和/或输入时间按所述预定规则解析出干扰数据。

本步骤中，并不仅局限于硬件信息以及时间信息，其目的在于，通过选择随机的、不可预测的量，结合预定的规则生成干扰数据，就可以更进一步的达到安全效果，如时间信息，由于用户输入数据的时间是没有规律的，是用该量来生成干扰数据信息，即便是获取到生成干扰数据的规则，由于该变量的随机性也不能够破译出干扰的数据。

当在合法接收方预知到干扰数据的生成规则、以及结合规则生成干扰数据的变量（如输入时间）后，根据解析出的干扰数据分离出输入数据则是容易实现的，比如可以将解析出干扰数据与混合的数据对比；再将与干扰数据相同的数据去除后分离出输入数据即可。

本发明实施例还提供了一种输入数据的安全处理装置，下面结合附图对安全处理装置的具体实施方式进行说明。

图 3 为输入数据的安全处理装置结构示意图，安全处理装置应用于包括数据输入设备、数据接收设备的数据处理系统，如图所示，装置中包括干扰模块、发送模块、分离模块，其中：

干扰模块，用于在通过数据输入设备输入数据时根据预定规则生成干扰数据；

发送模块，用于将通过数据输入设备输入的数据与所述干扰数据混合发送；

分离模块，用于根据所述预定规则从数据接收设备接收到的所述混合的数据中解析出干扰数据，并根据解析出的干扰数据分离出输入数据。

实施中，数据输入设备安装有执行数据处理的操作系统，发送模块进一步用于将所述通过数据输入设备输入的数据与所述干扰数据混合后发送至所述操作系统。

数据输入设备安装有执行数据处理的操作系统，发送模块可以包括数据传输单元、干扰数据传输单元，其中：

数据传输单元，用于将通过数据输入设备输入的数据传输至操作系统；

干扰数据传输单元、用于将根据预定规则生成的干扰数据传输至操作系统；

操作系统，用于将输入的数据与所述干扰数据发送。

实施中，干扰数据传输单元将干扰数据输入操作系统的速度可以大于所述数据传输单元将输入数据输入操作系统的速度。

安全处理装置中还可以进一步包括获取模块，用于在通过数据输入设备

输入数据时获取数据输入设备的硬件信息和/或输入时间;

干扰模块可以进一步用于根据所述输入设备的硬件信息和/或输入时间按预定规则生成干扰数据;

发送模块可以进一步用于在输入数据结束时，将所述输入设备的硬件信息和/或输入时间发送;

分离模块可以进一步用于在接收到所述混合的数据、以及所述输入设备的硬件信息和/或输入时间后，根据所述输入设备的硬件信息和/或输入时间按所述预定规则解析出干扰数据。

分离模块中可以包括解析单元、对比单元、分离单元，其中:

解析单元，用于根据所述预定规则从数据接收设备接收到的所述混合的数据中解析出干扰数据;

对比单元，用于将解析出干扰数据与所述混合的数据对比;

分离单元，用于根据对比单元对比出的与所述干扰数据相同的数据去除后分离出输入数据。

下面再举一实例来进一步阐述本发明的实施。

图 4 为对输入数据进行安全处理的环境示意图，如图所示，该环境中，数据的输入设备可以视为包含一用户具体输入数据的键盘、一用于数据处理的客户端，客户端上安装了操作系统，数据的各种处理流程由操作系统完成，为便于理解，操作系统具体的各种数据操作通过窗口来描述。但是易知，数据输入设备还可以有很多形式，如手写键盘与服务器等，并不仅限于本例所示。数据的接收设备可以是因特网上的一服务器，该服务器指用户输入数据所需到达的设备，但并不仅限于服务器，逻辑上，它还可以是客户端上另一需要得到用户输入数据的设备、或实体、或系统等，这是本领域人员易知的。

由上述可知，本发明实施例是涉及如何将客户的输入数据安全的传递到需要接收该数据信息的一端，比如服务器，而不被黑客在客户端通过钩子函数截获的方法。因此，本例中，所描述的流程大致为：用户通过键盘输入数据，数据传输至操作系统，操作系统经过处理后发送至该数据的所需到达的

接收端服务器。

下面对每一环节展开对本发明进行说明。

图 5 为对输入数据进行安全处理的实施流程示意图，如图所示，实施流程可以如下:

步骤 501、客户端下载掩护键盘输入控件或者其他形式的程序;

产生干扰数据的实现方式是多样的，本例中以程序的实施方式进行说明;可以通过 WEB 控件或者其他任何途径来分发本程序，使其能在客户端运行。

步骤 502、启动程序，随机决定采用的算法和种子，动态产生干扰数据信息，并将干扰数据信息发送到操作系统中;

本步骤可以分为以下几个步骤来执行:

1、获取本机硬件信息，和/或获取本机时间信息，以此作为最基本的种子，按照预制规则的算法，运算出结果;

2、按照运算结果，确定本次干扰算法及干扰算法的种子;

3、执行干扰算法，将产生的干扰信息，以一个远高于普通用户键盘输入速率的速率输入操作系统底层;

4、干扰信息根据算法随着时间变化，并不断的发送，直到客户提交或者因其他意外的中止，比如超时。

步骤 503、操作系统接收客户输入的窗口同时捕获干扰信息和用户输入的信息;

本步骤中，接收用户输入的窗口获取的是所有的干扰信息和用户键盘输入的总集合。到目前为止，客户端包括接收窗口在内，没有任何程序知道用户实际的键盘输入。虽然用户的键盘输入信息在传输信息中以明文形式存在，但是由于大量干扰信息的掩盖，黑客无法有效获取该信息，从而实现了用户键盘输入的隐形。

步骤 504、客户提交输入结束，干扰线程或者进程停止工作，并将产生干扰信息所使用的算法代号及种子传递给接收用户输入信息的窗口;

本步骤中，可以分为以下几个步骤来执行:

1、用户使用特殊的键盘输入，比如回车键或者鼠标点击触动，可以中止本控件的运行，并且发起提交输入信息的操作;

2、控件将最早收集的客户端硬件信息与时间信息，以一个事先约定的格式，发送到接收用户输入信息的窗口。

步骤 505、接收信息的窗口将接收到的干扰信息和用户输入信息的混合数据，以及本次干扰所用的算法代号及种子打包，发送到需要接收用户输入信息的服务器;

本步骤中，接收用户输入信息的窗口，将所有接收到的数据打包，发送到需要接收用户键盘信息的地方即可，比如服务器。

步骤 506、服务器解除干扰，根据硬件信息及时间，计算出干扰信息，从而得出客户输入的实际输入信息，比如银行密码。

本步骤的目的是在一个安全环境下解除干扰数据信息，具体可以分为以下几个步骤来执行:

1、通过传递来的数据中的硬件信息和时间，检查其安全性，防御比如重放攻击等方式的攻击;

2、通过硬件信息和时间，按照预制规则的算法，计算出结果;

3、按照计算结果，判断客户端本次采用的算法和种子;

4、计算出干扰信息;

5、将接收到的信息与计算出的干扰信息对比，相同的删除，剩下的部分就是用户实际的输入。

图 6 为对输入数据进行安全处理的另一实施流程示意图，如图所示，可以包括如下步骤:

步骤 601、触发干扰数据生成程序;

步骤 602、获取硬件信息和/或时间信息;

步骤 603、按预定规则确定算法和种子;

步骤 604、产生干扰数据信息;

步骤 605、发送干扰数据信息到操作系统，转入步骤 607;

步骤 606、用户输入数据信息;

步骤 607、操作系统接收干扰数据信息和用户输入数据信息;

步骤 608、接收窗口接收全部数据信息;

步骤 609、打包全部数据信息并发送，其中含有步骤 602 中的硬件信息和/或时间信息;

步骤 610、将数据信息解包;

步骤 611、确定客户端使用的算法和种子;

步骤 612、计算干扰数据信息;

步骤 613、排除干扰信息;

步骤 614、获得客户输入数据信息。

由图上标识的黑客钩子程序执行的流程位置可以看出，通过该方法可以有效的干扰黑客获取客户键盘输入，从而达到保护客户输入信息的目的。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种输入数据的安全处理方法，其特征在于，包括如下步骤：

输入数据时根据预定规则生成干扰数据；

将输入的数据与所述干扰数据混合发送；

接收到所述混合的数据后，根据所述预定规则解析出干扰数据；

根据解析出的干扰数据分离出输入数据。

2、如权利要求 1 所述的安全处理方法，其特征在于，进行数据输入的输入设备安装有执行数据处理的操作系统，所述将输入的数据与所述干扰数据混合发送具体为：将输入的数据与所述干扰数据混合后发送至操作系统。

3、如权利要求 1 所述的安全处理方法，其特征在于，进行数据输入的输入设备安装有执行数据处理的操作系统，所述输入数据时根据预定规则生成干扰数据；将输入的数据与所述干扰数据混合发送，包括如下步骤；

将输入的数据传输至操作系统；

输入数据时根据预定规则生成干扰数据，并传输至操作系统；

操作系统将输入的数据与所述干扰数据发送。

4、如权利要求 3 所述的安全处理方法，其特征在于，所述干扰数据输入操作系统的速度大于输入数据输入操作系统的速度。

5、如权利要求 1 至 4 任一所述的安全处理方法，其特征在于，进一步包括如下步骤：

输入数据时获取输入设备的硬件信息和/或输入时间；

根据所述输入设备的硬件信息和/或输入时间按预定规则生成干扰数据；

将输入的数据与所述干扰数据混合发送；

输入数据结束时，将所述输入设备的硬件信息和/或输入时间发送；

接收到所述混合的数据、以及所述输入设备的硬件信息和/或输入时间后，根据所述输入设备的硬件信息和/或输入时间按所述预定规则解析出干扰数据。

6、如权利要求 1 所述的安全处理方法，其特征在于，所述根据解析出的干扰数据分离出输入数据，包括如下步骤:

将解析出干扰数据与所述混合的数据对比;

将与所述干扰数据相同的数据去除后分离出输入数据。

7、一种输入数据的安全处理装置，应用于包括数据输入设备、数据接收设备的数据处理系统，其特征在于，包括干扰模块、发送模块、分离模块，其中:

干扰模块，用于在通过数据输入设备输入数据时根据预定规则生成干扰数据;

发送模块，用于将通过数据输入设备输入的数据与所述干扰数据混合发送;

分离模块，用于根据所述预定规则从数据接收设备接收到的所述混合的数据中解析出干扰数据，并根据解析出的干扰数据分离出输入数据。

8、如权利要求 7 所述的安全处理装置，其特征在于，所述数据输入设备安装有执行数据处理的操作系统;

所述发送模块进一步用于将所述通过数据输入设备输入的数据与所述干扰数据混合后发送至所述操作系统。

9、如权利要求 7 所述的安全处理装置，其特征在于，所述数据输入设备安装有执行数据处理的操作系统; 所述发送模块包括数据传输单元、干扰数据传输单元，其中:

数据传输单元，用于将通过数据输入设备输入的数据传输至操作系统;

干扰数据传输单元、用于将根据预定规则生成的干扰数据传输至操作系统;

操作系统，用于将输入的数据与所述干扰数据发送。

10、如权利要求 9 所述的安全处理装置，其特征在于，所述干扰数据传输单元将干扰数据输入操作系统的速度大于所述数据传输单元将输入数据输入操作系统的速度。

11、如权利要求 7 至 10 任一所述的安全处理装置，其特征在于，进一步包括获取模块，用于在通过数据输入设备输入数据时获取数据输入设备的硬件信息和/或输入时间；

所述干扰模块进一步用于根据所述输入设备的硬件信息和/或输入时间按预定规则生成干扰数据；

所述发送模块进一步用于在输入数据结束时，将所述输入设备的硬件信息和/或输入时间发送；

所述分离模块进一步用于在接收到所述混合的数据、以及所述输入设备的硬件信息和/或输入时间后，根据所述输入设备的硬件信息和/或输入时间按所述预定规则解析出干扰数据。

12、如权利要求 7 所述的安全处理装置，其特征在于，所述分离模块包括解析单元、对比单元、分离单元，其中：

解析单元，用于根据所述预定规则从数据接收设备接收到的所述混合的数据中解析出干扰数据；

对比单元，用于将解析出干扰数据与所述混合的数据对比；

分离单元，用于根据对比单元对比出的与所述干扰数据相同的数据去除后分离出输入数据。

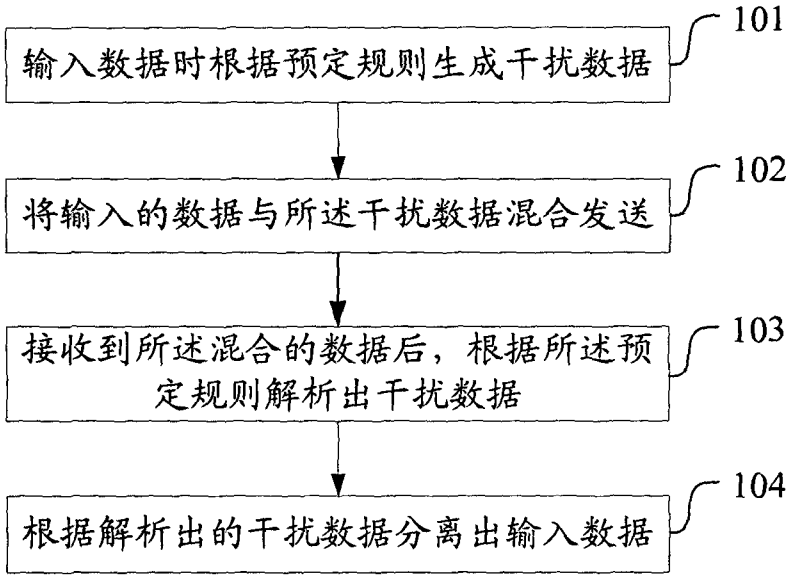
输入数据时根据预定规则生成干扰数据
101
将输入的数据与所述干扰数据混合发送
102
接收到所述混合的数据后，根据所述预定规则解析出干扰数据
103
根据解析出的干扰数据分离出输入数据
104

图 1

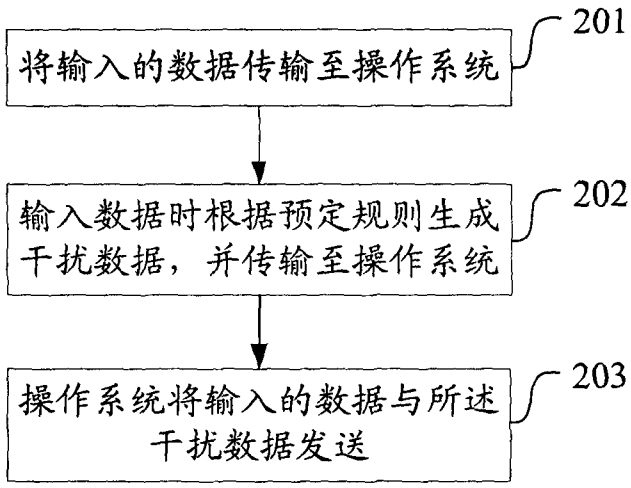
将输入的数据传输至操作系统
201
输入数据时根据预定规则生成干扰数据，并传输至操作系统
202
操作系统将输入的数据与所述干扰数据发送
203

图 2

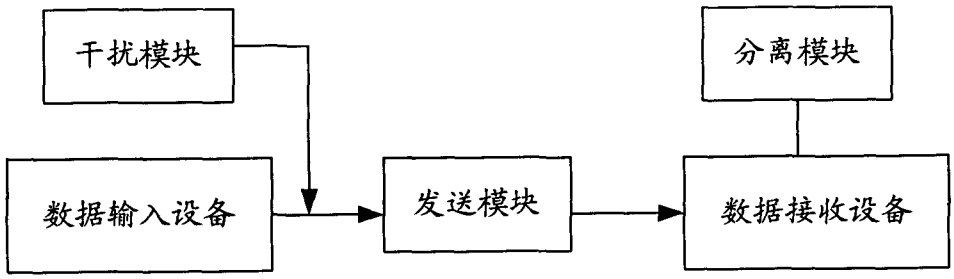

图 3

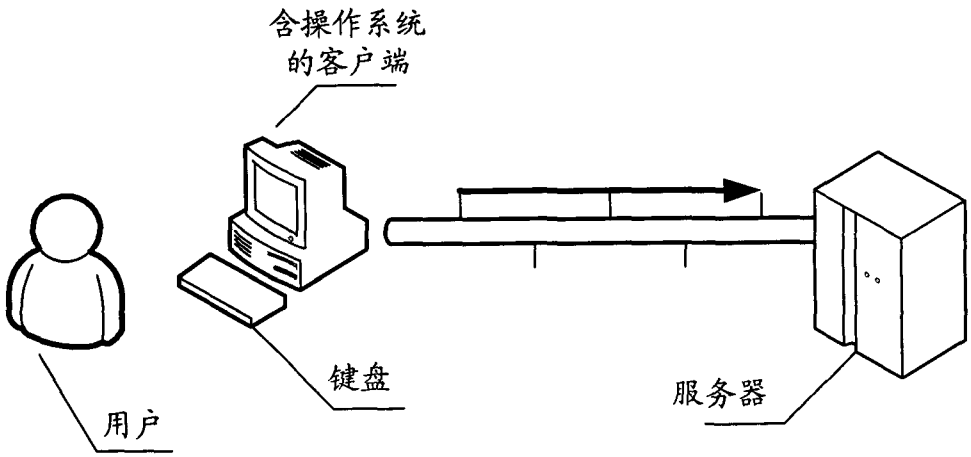

图 4

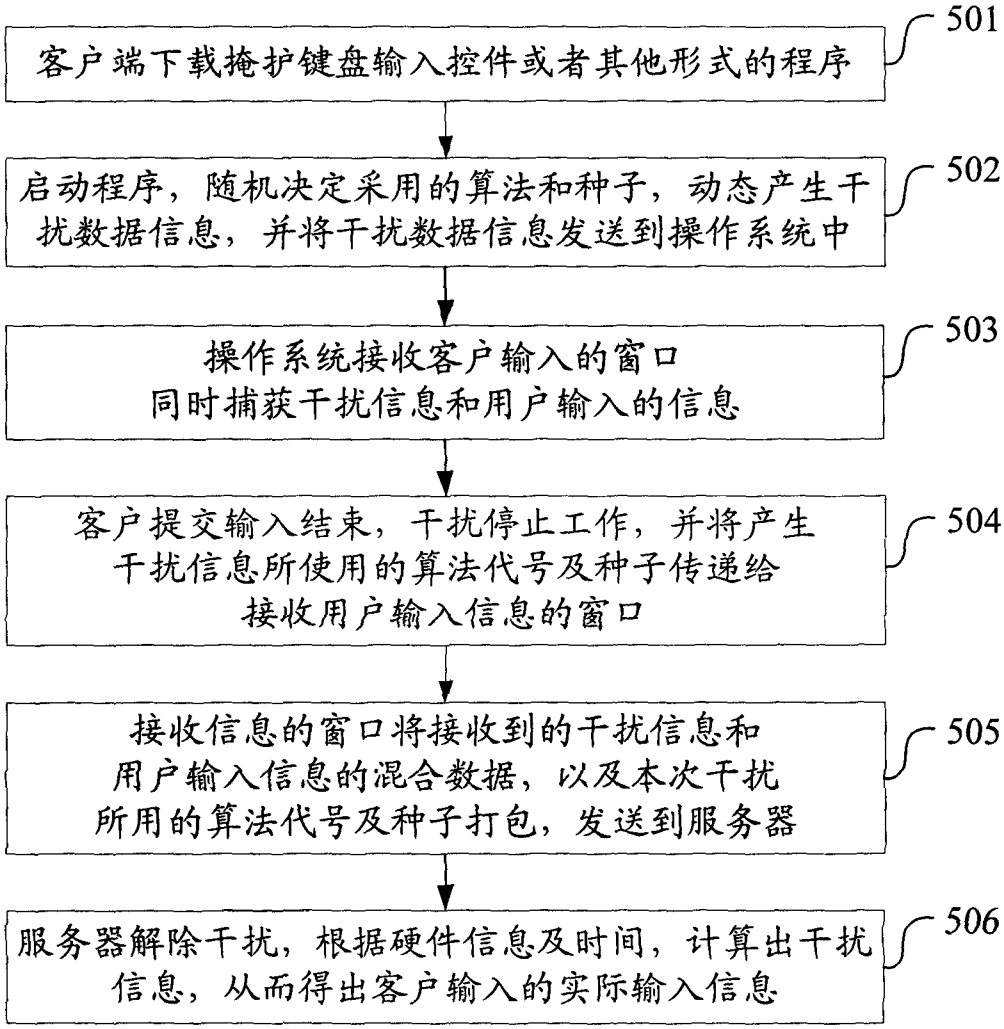
客户端下载掩护键盘输入控件或者其他形式的程序
501
启动程序，随机决定采用的算法和种子，动态产生干扰数据信息，并将干扰数据信息发送到操作系统中
502
操作系统接收客户输入的窗口
同时捕获干扰信息和用户输入的信息
503
客户提交输入结束，干扰停止工作，并将产生干扰信息所使用的算法代号及种子传递给接收用户输入信息的窗口
504
接收信息的窗口将接收到的干扰信息和用户输入信息的混合数据，以及本次干扰所用的算法代号及种子打包，发送到服务器
505
服务器解除干扰，根据硬件信息及时间，计算出干扰信息，从而得出客户输入的实际输入信息
506

图 5

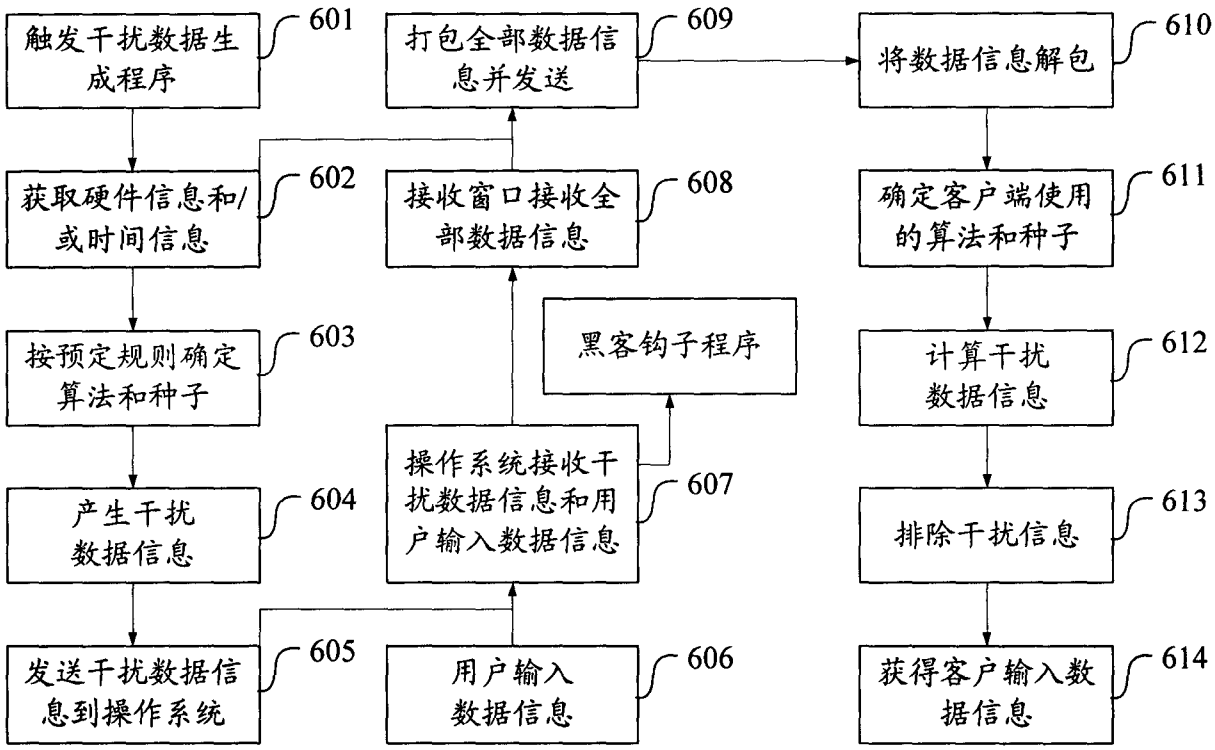
触发干扰数据生成程序
601
获取硬件信息和/或时间信息
602
按预定规则确定算法和种子
603
产生干扰数据信息
604
发送干扰数据信息到操作系统
605
用户输入数据信息
606
操作系统接收干扰数据信息和用户输入数据信息
607
接收窗口接收全部数据信息
608
黑客钩子程序
打包全部数据信息并发送
609
将数据信息解包
610
确定客户端使用的算法和种子
611
计算干扰数据信息
612
排除干扰信息
613
获得客户输入数据信息
614

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2008/001358

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/24 (2006.01) i

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)

IPC: G06F; G09C; H04L

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)

WPI;EPODOC;PAJ;CNKI;IEE;CRRS

information, data, cipher+, encrypt+, secur+,mix+,fill+,hid+,random list,disturb+,hash,sign+,authenticat+,watermark

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	CN101101625 A (YU JIANG) 9 January 2008 (09.01.2008) see the whole document	1-12
X	CN1937008 A (FUJITSU LTD, HIROTA O) 28 March 2007 (28.03.2007) see description page 13-page 19, page 64-page 74, figures 1,2,31	1-12
A	CN101008972 A (BEIJING FEITIAN CHENXIN TECHNOLOGICAL CO LTD) 1 August 2007 (01.08.2007) see the whole document	1-12
A	US20060112270 A (Chet Erez,San Jose) 25 May 2006 (25.05.2006) see the whole document	1-12

☐ 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	Date of mailing of the international search report
21 October 2008(21.10.2008)	**06 Nov. 2008 (06.11.2008)**
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 LI, Le Telephone No. (86-10)62411827

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2008/001358

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101101625A	09.01.2008	none	
CN1937008A	28.03.2007	EP1768299A2	28.03.2007
		JP2007116659A	10.05.2007
		US2008044011A1	21.02.2008
CN101008972A	01.08.2007	none	
US20060112270A	25.05.2006	none	

国际检索报告

国际申请号
PCT/CN2008/001358

A. 主题的分类

G06F 21/24 (2006.01) i

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)

IPC： G06F; G09C; H04L

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）)

WPI;EPODOC;PAJ;CNKI;IEE;CRRS

信息,数据,密码,密文,加密,安全,混合,填充,隐藏,随机数,随机序列,干扰,哈希,杂凑,签名,认证,水印;information, data, cipher+, encrypt+, secur+,mix+,fill+,hid+,random list,disturb+,hash,sign+,authenticat+,watermark

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
P，X	CN101101625 A (江雨) 9.1 月 2008 (09.01.2008) 全文	1-12
X	CN1937008 A (富士通株式会社，広田修) 28.3 月 2007 (28.03.2007) 说明书第 13 页至第 19 页，第 64 页至第 74 页，图 1，2，31	1-12
A	CN101008972 A (北京飞天诚信科技有限公司) 1.8 月 2007 (01.08.2007) 全文	1-12
A	US20060112270 A (Chet Erez，San Jose) 25.5 月 2006 (25.05.2006) 全文	1-12

☐ 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	国际检索报告邮寄日期
21.10 月 2008(21.10.2008)	**06.11 月 2008 (06.11.2008)**
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 李乐 电话号码：(86-10) **62411827**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2008/001358

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101101625A	09.01.2008	无	
CN1937008A	28.03.2007	EP1768299A2	28.03.2007
		JP2007116659A	10.05.2007
		US2008044011A1	21.02.2008
CN101008972A	01.08.2007	无	
US20060112270A	25.05.2006	无	