(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
2007 年8 月2 日 (02.08.2007)

PCT

(10) 国际公布号
WO 2007/085137 A1

(51) 国际专利分类号:
G06F 11/00 (2006.01)

(21) 国际申请号: PCT/CN2006/000477

(22) 国际申请日: 2006 年3 月23 日 (23.03.2006)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200510136600.1
2005 年12 月30 日 (30.12.2005) CN

(71) 申请人 (对除美国外的所有指定国): 联想(北京)有限公司(LENOVO (BEIJING) LIMITED) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。

(72) 发明人; 及

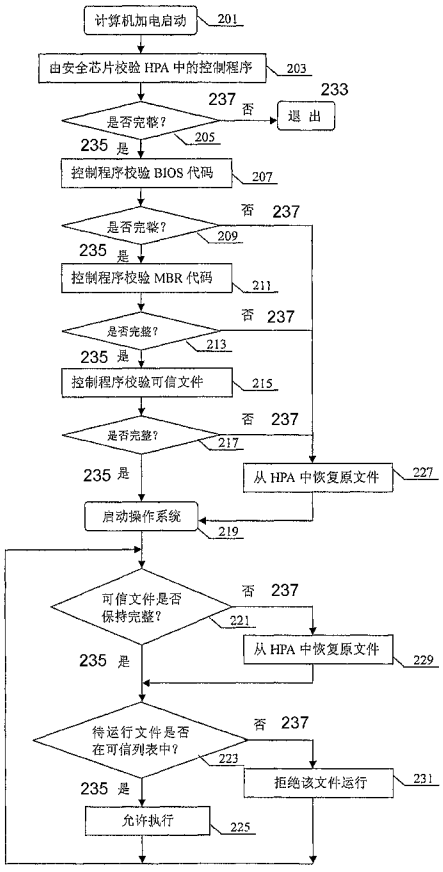
(75) 发明人/申请人 (仅对美国): 李俊(LI, Jun) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。 王凯(WANG, Kai) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。 冯荣峰(FENG, Rongfeng) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。 徐娜(XU, Na) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。

(74) 代理人: 中科专利商标代理有限责任公司(CHINA SCIENCE PATENT & TRADEMARK AGENT LTD.); 中国北京市海淀区王庄路1号清华同方科技大厦B座25层, Beijing 100083 (CN)。

[见续页]

(54) Title: A METHOD FOR AMTI-VIRUS BASED ON A SAFETY CHIP

(54) 发明名称: 基于安全芯片的防病毒方法



201 COMPUTER START UP OF POWER UP
203 CONTROL PROGRAM TN THE HPA IS VERIFIED BY SAFETY CHIP
205 IF IT IS INTEGRATED?
207 CONTROL PROGRAM VERIFY BIOS CODE
209 IF IT TS INTEGRATED?
211 CONTROL PROGRAM VERIFY MBR CODE
213 IF IT IS INTEGRATED?
215 CONTROL PROGRAM VERIFY AUTHENTIC FILE
217 IF IT IS INTEGRATED?
219 START UP THE OS
221 IF AUTHENTIC FTLE RETAINS INTEGRITY?
223 IF TO BE RUNNING FILE IS IN THE AUTHENTIC LISTS?
225 ALLOW PERFORMING
227 ORIGINAL FILE IS RESTORED FROM HPA
229 ORIGINAL FILE IS RESTORED FROM HPA
231 REJECT TO RUN THE FILE
233 EXIT
235 YES
237 NO

(57) Abstract: A method for anti-virus based on a safety chip according to the present invention is provided. The method includes the following steps: a hash value obtained by hashing operation a computer key file and a system control program is stored in a memory of the safety chip, and a backup file of the computer key File is stored in a backup storage area. When power up, the integrity of the system control program is verified by using the hash value of the system control program stored in the memory of the safety chip. If the system control program is integrated, the system control program executes control, and the system control program verifies the integrity of the computer key file using the hash value of the computer key file stored in the memory of the safety chip, If all the computer key file are integrated, then OS is started up; on the contrary, if any of the computer key file is not integrated, then it will be restored using the backup file of the computer key file stored in the backup storage area.

[见续页]

WO 2007/085137 A1

(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, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, 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, LV, 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”。

(57) 摘要：

根据本发明，提出了一种基于安全芯片的防病毒方法，所述方法包括以下步骤：在安全芯片的存储器中存储将计算机关键文件和系统控制程序进行散列运算所获得的哈希值，并且在备份存储区中存储计算机关键文件的备份文件；在机器加电时，利用安全芯片的存储器中所存储的系统控制程序的哈希值来校验系统控制程序的完整性；如果系统控制程序是完整的，则由所述系统控制程序执行控制，所述系统控制程序利用安全芯片的存储器中所存储的计算机关键文件的哈希值，校验计算机关键文件的完整性；如果计算机关键文件均是完整的，则启动操作系统；以及相反，如果计算机关键文件的任一个不完整，则利用备份存储区中存储的计算机关键文件的备份文件来恢复其。

摘　要

根据本发明，提出了一种基于安全芯片的防病毒方法，所述方法包括以下步骤：在安全芯片的存储器中存储将计算机关键文件和系统控制程序进行散列运算所获得的哈希值，并且在备份存储区中存储计算机关键文件的备份文件；在机器加电时，利用安全芯片的存储器中所存储的系统控制程序的哈希值来校验系统控制程序的完整性；如果系统控制程序是完整的，则由所述系统控制程序执行控制，所述系统控制程序利用安全芯片的存储器中所存储的计算机关键文件的哈希值，校验计算机关键文件的完整性；如果计算机关键文件均是完整的，则启动操作系统；以及相反，如果计算机关键文件的任一个不完整，则利用备份存储区中存储的计算机关键文件的备份文件来恢复其。

基于安全芯片的防病毒方法

技术领域

本发明涉及一种基于安全芯片的防病毒方法，通过以安全芯片为信任根，对BIOS代码文件、MBR代码文件、可信文件等计算机关键文件进行安全备份和智能修复，并且在操作系统运行时执行文件监控功能，构建了完整的信任链，从而可以实现操作系统的安全启动，防止恶意程序的运行，达到防御已知和未知病毒的目的。

背景技术

目前存在多种能实现类似目的的解决方案。例如，在现有技术公知的普通防病毒方法中，使用病毒扫描引擎，对内存和磁盘文件进行扫描和监控，根据病毒特征库进行比较，发现病毒则报警和清除。然而，此种方法的缺点是只能发现已知病毒，而且由于运行在操作系统启动以后，不能对操作系统启动前和启动时的过程进行监控。

还存在一种操作系统修复方法，在该方法中，使用硬盘的HPA备份操作系统的核心文件，当核心文件与备份文件校验不一致时提示用户进行修复或备份。该方法的缺点是没有采用TPM安全芯片，安全性不够高。因为硬盘HPA是存在较大可能性被攻击者进行修改操作的，备份文件很可能被篡改而不被发现。

因此，需要一种基于安全芯片的防病毒方法，能够在操作系统启动前和启动时，防止恶意程序的运行，从而实现防御已知和未知病毒的目的。

发明内容

为了克服现有技术中存在的缺陷提出了本发明，本发明的目的是提出一种基于安全芯片的防病毒方法，通过以安全芯片为信任根，对BIOS代码文件、MBR代码文件、可信文件等计算机关键文进行安全备份和智能修复，并且在操作系统运行时执行文件监控功能，构建了完整的信任链，从而可以实现操作系统的安全启动，防止恶意程序的运行，达到防御已知和未知病毒的目的。

为了实现上述目的，根据本发明，提出了一种基于安全芯片的防病毒方法，

所述方法包括以下步骤：在安全芯片的存储器中存储将计算机关键文件和系统控制程序进行散列运算所获得的哈希值，并且在备份存储区中存储计算机关键文件的备份文件；在机器加电时，利用安全芯片的存储器中所存储的系统控制程序的哈希值来校验系统控制程序的完整性；如果系统控制程序是完整的，则由所述系统控制程序执行控制，所述系统控制程序利用安全芯片的存储器中所存储的计算机关键文件的哈希值，校验计算机关键文件的完整性；如果计算机关键文件均是完整的，则启动操作系统；以及相反，如果计算机关键文件的任一个不完整，则利用备份存储区中存储的计算机关键文件的备份文件来恢复其。

优选地，所述计算机关键文件包括：BIOS代码文件、MBR部分的代码文件、可信文件。

优选地，所述系统控制程序利用安全芯片的存储器中所存储的计算机关键文件的哈希值、校验计算机关键文件的完整性的步骤包括：所述系统控制程序分别利用安全芯片的存储器中所存储的BIOS代码文件、MBR部分的代码文件、可信文件的哈希值，依次校验BIOS代码文件、MBR部分的代码文件、可信文件的完整性。

优选地，所述备份存储区为硬盘保护区。

优选地，所述方法还包括步骤：在操作系统启动之后，由系统控制程序利用安全芯片的存储器中所存储的可信文件的哈希值，实时校验可信文件的完整性；如果可信文件完整且待运行文件存在可信列表中时，允许所述待运行文件运行；相反，则禁止所述待运行文件运行。

优选地，所述利用安全芯片的存储器中所存储的系统控制程序的哈希值来校验系统控制程序的完整性的步骤包括：对当前系统控制程序执行与所述散列运算相同的散列运算以获得当前系统控制程序的哈希值；将所述哈希值与安全芯片的存储器中所存储的系统控制程序的哈希值进行比较；如果两者一致，则表示当前系统控制程序是完整的。

优选地，所述利用安全芯片的存储器中所存储的计算机关键文件的哈希值，校验计算机关键文件的备份文件的完整性的步骤包括：对计算机关键文件执行与所述散列运算相同的散列运算以获得当前计算机关键文件的哈希值；将所述哈希值与安全芯片的存储器中所存储的计算机关键文件的相应哈希值进行比较；如果两者分别一致，则表示计算机关键文件是完整的。

优选地，在安全芯片的存储器中存储的散列值是通过两次散列运算所获得的散列值。

优选地，所述两次散列运算所分别采用的两个散列函数是相同的。

优选地，所述两次散列运算所分别采用的两个散列函数是不同的。

优选地，所述可信文件是干净的操作系统核心文件。

优选地，所述安全芯片的存储器受到安全芯片的认证保护。

附图说明

通过参考以下结合附图对所采用的优选实施例的详细描述，本发明的上述目的、优点和特征将变得显而易见，其中：

图1是示出了为了实现根据基于安全芯片的防病毒方法，安全芯片的存储器和HPA存储区的存储内容与BIOS（基本输入输出系统）代码文件、MBR（主引导记录）代码文件、可信文件的关系的示意图；以及

图2是示出了根据本发明的基于安全芯片的防病毒方法的流程图。

具体实施方式

本发明的技术原理在于：以安全芯片为信任根，对系统启动过程中的各环节进行完整性检查，传递信任关系，建立整个计算机系统的可信计算环境，从而达到防病毒的目的。

下面将参考附图来描述根据本发明的优选实施例。

图1是示出了为了实现根据基于安全芯片的防病毒方法，安全芯片的存储器和HPA存储区的存储内容与BIOS代码文件、MBR代码文件、可信文件（计算机关键文件）的关系的示意图。

如图1所示，预先将正确的BIOS代码文件及其哈希值（hash值）存储在硬盘保护区（HPA区域，也被称为硬盘隐藏区），该HPA区域是一般用户无法访问的。另外，将HPA区域用作数据保护区域是本领域所公知的。然后，将该哈希值再进行散列运算得到的哈希值保存在安全芯片的存储器中，也就是，将对BIOS代码文件进行了两次散列运算所得到的哈希值存储在图1所示的安全芯片的存储器中，该安全芯片的存储器受到安全芯片的保护，需要得到安全芯片的拥有者的授权和认证才能访问，这里，安全芯片技术也是本领域所公知的，在此不再详细描述。

同样地，预先将正确的硬盘MBR部分的代码文件及其哈希值存储在硬盘保护区，并将该哈希值再进行散列运算得到的哈希值保存在安全芯片的存储器中。

同样地，预先创建可信文件列表，并将该列表中的可信文件（主要是干净的操作系统核心文件）以及哈希值存储在硬盘保护区，并将所有可信文件的哈希值再进行散列运算得到的哈希值保存在安全芯片的存储器中。

最后，系统控制程序文件及其哈希值也存储在硬盘保护区，并将该哈希值再进行散列运算得到的哈希值保存在安全芯片的存储器中。

总之，在硬盘保护区中存储了BIOS代码文件、MBR部分的代码文件、可信文件和系统控制程序文件经过一次散列运算后所得到哈希值。另外，还存储了BIOS代码文件、MBR部分的代码文件、可信文件的备份文件和系统控制程序文件，用于在它们受到篡改时恢复其。在安全芯片的存储器中存储了BIOS代码文件、MBR部分的代码文件、可信文件和系统控制程序文件经过两次散列运算后所得到哈希值，用于在机器启动之前和启动之后执行校验操作，如以下将详细描述的。

需要注意的是，作为示例，如图1所示，MBR部分的代码文件存储区、可信文件存储区和HPA区域通常处于硬盘中，而BIOS代码文件处于计算机的只读ROM中。另外，以上仅作为示例给出了通过两次散列运算来获得散列值的方式，但是本发明并不局限于此，其可以是任意次数的散列运算。此外，BIOS代码文件、MBR部分的代码文件和可信文件并不必须存储在于HPA区域中，其可以存储在任意形式（例如硬盘、ROM等）的文件备份区中。

图2是示出了根据本发明的基于安全芯片的防病毒方法的流程图。

如图2所示，机器加电启动时（步骤201），由安全芯片校验HPA中的控制程序，即，安全芯片对控制程序进行两次散列运算（步骤203），这里所示的两次散列运算如上所述。然后，将经过两次散列运算所获得的哈希值与存储在安全芯片的存储器中的哈希值进行比较（步骤205），如果不同（步骤205中的否），则停止启动并退出。如果相同（步骤205中的是），则将控制权交给控制程序，由控制程序依次校验BIOS代码文件、MBR（主引导记录）代码文件及可信文件，即，对BIOS代码文件、MBR代码文件及可信文件进行两次散列运算（步骤207、步骤211和步骤215）。然后，将两次散列运算所获得的哈希值与存储在安全芯片中的哈希值进行比较（步骤209、步骤213和步骤217），即检查BIOS代码文件、MBR代码文件及可信文件的完整性。如果不同（步骤209、步骤213和步骤217中的否），则修复被

破坏的BIOS代码文件、MBR代码文件及可信文件（步骤227），即，由HPA中的相应备份文件来恢复被破坏的BIOS代码文件、MBR代码文件及可信文件。这样，可保证在操作系统启动前恢复BIOS/MBR/操作系统正常状态，直接消除病毒影响，有效防范已知和未知病毒，保证操作系统安全启动。

操作系统运行后（步骤219），系统控制程序实时监控可信文件的状态（步骤221），即，将可信文件经过两次散列运算所获得的哈希值与安全芯片的存储器中所存储的相应哈希值进行比较以检查可信文件的完整性。如果发现哈希值与安全芯片中的存储值不一致（步骤221中的否），则根据用户的选择自动进行修复或者更新（步骤229），该修复过程与以上的修复过程类似。相反，如果一致，（步骤221中的是），则检查待运行文件是否在该可信列表中（步骤223）。如果该文件不在该可信列表中（步骤223中的否），则可以根据用户的选择不允许其运行（步骤231），这种做法不依赖于病毒特征库即可达到抵御未知或已知病毒目的，使各种病毒无法在系统运行起来。相反，如果该程序存在于可信列表中（步骤223的是），则允许该程序的执行。

需要注意的是，对于以上提到的两次散列运算，两次散列运算所采用的散列函数可以是相同的也可以是不同的。

根据本发明，采用安全芯片保存系统关键信息，安全性高，保证了HPA的安全性，提供了硬件级完整性度量手段。另外，在本发明中，独立于被保护操作系统，从BIOS开始，依次对硬盘信息及操作系统核心文件等系统启动的关键环节进行完整性度量，比一般的防病毒软件提供了更底层、更彻底的防护。

尽管以上已经结合本发明的优选实施例示出了本发明，但是本领域的技术人员将会理解，在不脱离本发明的精神和范围的情况下，可以对本发明进行各种修改、替换和改变。因此，本发明不应由上述实施例来限定，而应由所附权利要求及其等价物来限定。

权 利 要 求

1、一种基于安全芯片的防病毒方法，所述方法包括以下步骤：

在安全芯片的存储器中存储将计算机关键文件和系统控制程序进行散列运算所获得的哈希值，并且在备份存储区中存储计算机关键文件的备份文件；

在机器加电时，利用安全芯片的存储器中所存储的系统控制程序的哈希值来校验系统控制程序的完整性；

如果系统控制程序是完整的，则由所述系统控制程序执行控制，所述系统控制程序利用安全芯片的存储器中所存储的计算机关键文件的哈希值，校验计算机关键文件的完整性；

如果计算机关键文件均是完整的，则启动操作系统；以及

相反，如果计算机关键文件的任一个不完整，则利用备份存储区中存储的计算机关键文件的备份文件来恢复其。

2、根据权利要求1所述的方法，其特征在于所述计算机关键文件包括：BIOS代码文件、MBR部分的代码文件、可信文件。

3、根据权利要求2所述的方法，其特征在于所述系统控制程序利用安全芯片的存储器中所存储的计算机关键文件的哈希值、校验计算机关键文件的完整性的步骤包括：所述系统控制程序分别利用安全芯片的存储器中所存储的BIOS代码文件、MBR部分的代码文件、可信文件的哈希值，依次校验BIOS代码文件、MBR部分的代码文件、可信文件的完整性。

4、根据权利要求1所述的方法，其特征在于所述备份存储区为硬盘保护区。

5、根据权利要求2所述的方法，其特征在于还包括步骤：在操作系统启动之后，由系统控制程序利用安全芯片的存储器中所存储的可信文件的哈希值，实时校验可信文件的完整性；如果可信文件完整且待运行文件存在可信列表中时，允许所述待运行文件运行；相反，则禁止所述待运行文件运行。

6、根据权利要求1所述的方法，其特征在于所述利用安全芯片的存储器中所存储的系统控制程序的哈希值来校验系统控制程序的完整性的步骤包括：对当前系统控制程序执行与所述散列运算相同的散列运算以获得当前系统控制程序的哈希值；将所述哈希值与安全芯片的存储器中所存储的系统控制程序的哈希值

进行比较；如果两者一致，则表示当前系统控制程序是完整的。

7、根据权利要求1所述的方法，其特征在于所述利用安全芯片的存储器中所存储的计算机关键文件的哈希值，校验计算机关键文件的备份文件的完整性的步骤包括：对计算机关键文件执行与所述散列运算相同的散列运算以获得当前计算机关键文件的哈希值；将所述哈希值与安全芯片的存储器中所存储的计算机关键文件的相应哈希值进行比较；如果两者分别一致，则表示计算机关键文件是完整的。

8、根据权利要求1所述的方法，其特征在于在安全芯片的存储器中存储的散列值是通过两次散列运算所获得的散列值。

9、根据权利要求1所述的方法，其特征在于所述两次散列运算所分别采用的两个散列函数是相同的。

10、根据权利要求1所述的方法，其特征在于所述两次散列运算所分别采用的两个散列函数是不同的。

11、根据权利要求1所述的方法，其特征在于所述可信文件是干净的操作系统核心文件。

12、根据权利要求1所述的方法，其特征在于所述安全芯片的存储器受到安全芯片的认证保护。

图 1

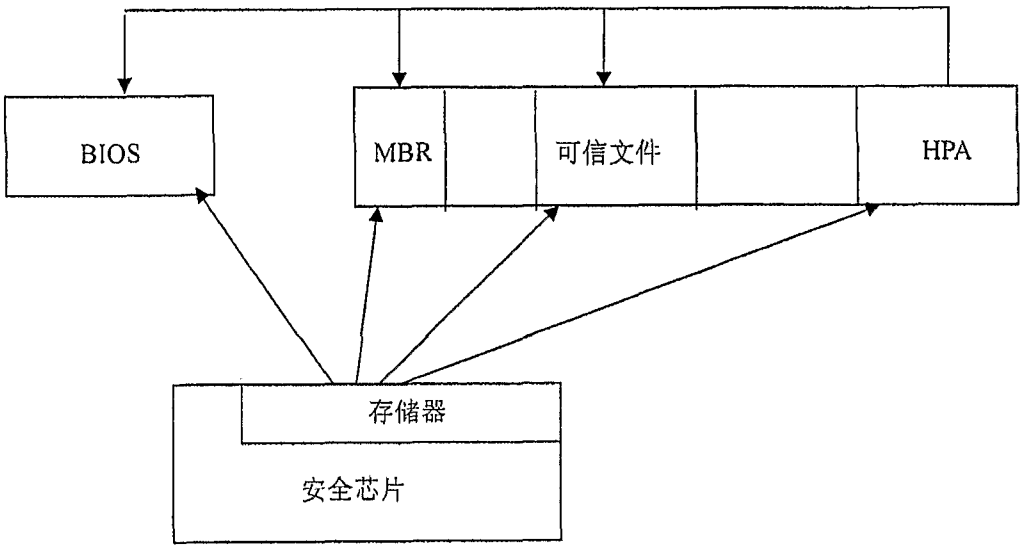
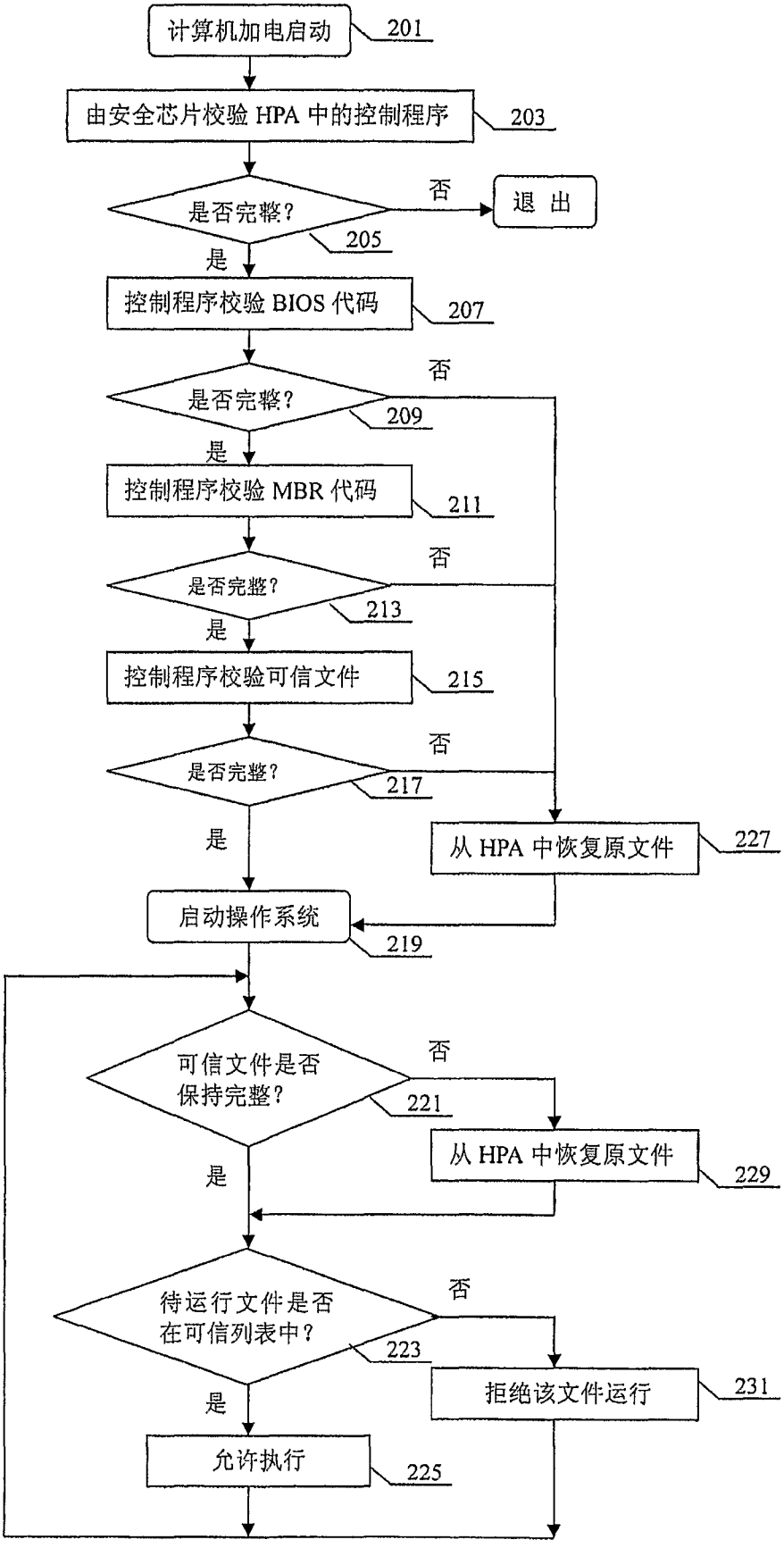


图 2


计算机加电启动
201
由安全芯片校验 HPA 中的控制程序
203
是否完整?
否
退 出
205
是
控制程序校验 BIOS 代码
207
是否完整?
否
209
是
控制程序校验 MBR 代码
211
是否完整?
否
213
是
控制程序校验可信文件
215
是否完整?
否
217
是
从 HPA 中恢复原文件
227
启动操作系统
219
可信文件是否保持完整?
否
221
从 HPA 中恢复原文件
229
是
待运行文件是否在可信列表中?
否
223
拒绝该文件运行
231
是
允许执行
225

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/000477

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/00(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)

G06F11/

G06F12/

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 PATENTPIC PAJ CNPAT

safety,chip,virus,key,code,credible,authentic,system,control,hash,verify,integrity,startup,OS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US5944821A, (COMPAQ COMPUTER CORP), 31.Aug1999(31.08.1999) ,the whole documents	1-12
A	US6021510A, (SYMANTEC CORP), 01.Feb2000(01.02.2000) , the whole documents	1-12
A	US5537540A, (COMPAQ COMPUTER CORP),16.Jul 1996(16.07.1996), the whole documents	1-12
A	EP1181642A1, (HEWLETT-PACKARD CO), 27.Feb 2002(27.02.2002), the whole documents	1-12
A	US5421006A, (COMPAQ COMPUTER CORP) ,30.May 1995(30.05.1995) ,the whole documents	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
08.Aug 2006(08.08.2006)	28 · SEP 2006 (28 · 09 · 2006)
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 A508 Telephone No. 86-10-62084944

Form PCT/ISA /210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2006/000477

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US5944821A	31.Aug 1999(31.08.1999)	none	
US6021510A	01.Feb 2000(01.02.2000)	WO9927450 A1	03.Jun 1999（03.06.1999）
		EP1032877 A1	06.Sep 2000（06.09.2000）
		EP1032877 B1	03.Apr 2002（03.04.2002）
		CA2311658A1	03.Jun 1999(03.06.1999)
		US6094731 A	25.Jul 2000(25.07.2000)
		AT215714T T	15.Apr 2002(15.04.2002)
		DE69804658D D	08.May 2002（08.05.2002）
		DE69804658T T	14.Aug 2002(14.08.2002)
US5537540A	16.Jul 1996(16.07.1996)	none	
EP1181642A1	27.Feb 2002(27.02.2002)	EP1056010 A1	29.Nov 2000（29.11.2000）
		WO0073904 A1	07.Dec 2000（07.12.2000）
US5421006A	30.May 1995(30.05.1995)	none	

国际检索报告

国际申请号
PCT/CN2006/000477

A. 主题的分类

G06F11/00 (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)

G06F11/

G06F12/

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）)数据库:WPI EPODOC PATENTPIC PAJ CNPAT 检索词：安全,芯片,病毒,关键,代码,可信,系统,控制,哈希,散列,校验,完整,启动,操作系统

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	US5944821A,(COMPAQ COMPUTER CORP), 31.8 月 1999(31.08.1999), 全文	1-12
A	US6021510A ,(SYMANTEC CORP) ,01.2 月 2000(01.02.2000), 全文	1-12
A	US5537540A,(COMPAQ COMPUTER CORP),16.7 月 1996(16.07.1996), 全文	1-12
A	EP1181642A1,(HEWLETT-PACKARD CO), 27.2 月 2002(27.02.2002), 全文	1-12
A	US5421006A,(COMPAQ COMPUTER CORP), 30.5 月 1995(30.05.1995), 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
08.8 月 2006(08.08.2006)	28 · 9月 2006 (28 · 09 · 2006)
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 A508 邓[illegible] 电话号码：(86-10)62084944

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2006/000477

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US5944821A	31.8 月 1999(31.08.1999)	无	
US6021510A	01.2 月 2000(01.02.2000)	WO9927450 A1	03.6 月 1999（03.06.1999）
		EP1032877 A1	06.9 月 2000（06.09.2000）
		EP1032877 B1	03.4 月 2002（03.04.2002）
		CA2311658A1	03.6 月 1999(03.06.1999)
		US6094731 A	25.7 月 2000(25.07.2000)
		AT215714T T	15.4 月 2002(15.04.2002)
		DE69804658D D	08.5 月 2002（08.05.2002）
		DE69804658T T	14.8 月 2002(14.08.2002)
US5537540A	16.7 月 1996(16.07.1996)	无	
EP1181642A1	27.2 月 2002(27.02.2002)	EP1056010 A1	29.11 月 2000（29.11.2000）
		WO0073904 A1	07.12 月 2000（07.12.2000）
US5421006A	30.5 月 1995(30.05.1995)	无	