(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 105279107 A
(43)申请公布日 2016.01.27

(21)申请号 201510779609.8

(22)申请日 2015.11.13

(71)申请人 北京华虹集成电路设计有限责任公司
地址 100080 北京市海淀区中关村东路66号甲1号楼12层1501-1510

(72)发明人 于永庆

(74)专利代理机构 北京汇思诚业知识产权代理有限公司 11444
代理人 王刚 龚敏

(51)Int.Cl.
G06F 12/14(2006.01)

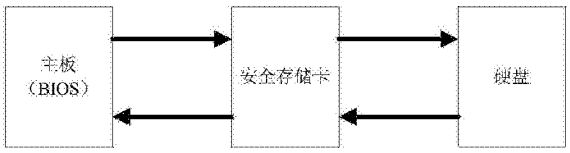
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种防止从盘启动的方法及系统

(57)摘要

本发明提供一种防止从盘启动的方法及系统。所述系统包括主板、硬盘和安全存储卡，所述安全存储卡连接于所述主板和所述硬盘之间，所述安全存储卡包括SATA DEVICE接口、SATA HOST接口、加解密模块。本发明所述方法为通过安全存储卡截获计算机主盘发送的数据流，并对该数据流进行分析和获取当前的启动状态是主盘启动或是从盘启动，当检测到从盘启动时，切断主盘数据通路，从而有效保护主盘数据不被拷出。本发明适用于政府、军工及金融等涉密行业，只有对硬盘加密并且真正从数据通路上防止从盘启动，才能打造真实可信的安全办公环境。



CN 105279107 A

1.一种防止从盘启动的系统，所述系统包括主板、硬盘，其特征在于，所述系统还包括安全存储卡，所述安全存储卡连接于所述主板和所述硬盘之间，所述安全存储卡包括 SATA DEVICE 接口、SATA HOST 接口、加解密模块，

其中，所述 SATA DEVICE 接口与所述主板连接，

所述 SATA HOST 接口与所述硬盘连接，

所述加解密模块分别与所述 SATA DEVICE 接口、所述 SATA HOST 接口连接，

所述安全存储卡通过与 PCI 或 PCIE 插槽连接进行固定并充电。

2.如权利要求 1 所述的防止从盘启动的系统，其特征在于，在初始化所述安全存储卡的所述 SATA DEVICE 接口和所述 SATA HOST 接口时，建立指令表和 PRD 表。

3.如权利要求 1 所述的防止从盘启动的系统，其特征在于，所述加解密模块设有两个双口 RAM，分别连接所述 SATA DEVICE 接口和所述 SATA HOST 接口。

4.如权利要求 3 所述的防止从盘启动的系统，其特征在于，所述双口 RAM 的大小为 16K。

5.如权利要求 3 所述的防止从盘启动的系统，其特征在于，所述双口 RAM 能够进行 PIPELINE（线性通信模型）的流水操作。

6.如权利要求 1 所述的防止从盘启动的系统，其特征在于，所述加解密模块采用 256 位的 SM1 国密算法对所述硬盘进行全盘扇区级底层加解密。

7.一种采用权利要求 1 所述的系统的防止从盘启动的方法，其特征在于，所述方法包括如下步骤：

加密写入，即所述安全存储卡对从主板获取的数据进行加密处理；

解密读出，即所述安全存储卡对从硬盘获取的数据进行解密处理；

当所述安全存储卡检测到所述主板长时间不发送读取系统引导扇区的指令时，所述安全存储卡自动切断所述主板和所述硬盘之间的数据通路，防止从盘启动。

8.如权利要求 7 所述的防止从盘启动的方法，其特征在于，所述加密写入包括如下步骤：

所述安全存储卡上的所述 SATA DEVICE 接口从所述主板获取数据；

所述加解密模块通过所述 SATA DEVICE 接口接收所述数据，并对获取的所述数据进行加密处理；

所述加解密模块将所述加密处理后的数据，即密文数据，发送给所述安全存储卡上的所述 SATA HOST 接口；

所述 SATA HOST 接口将所述密文数据写入到所述硬盘中。

9.如权利要求 7 所述的防止从盘启动的方法，其特征在于，所述解密读出包括如下步骤：

所述安全存储卡的所述 SATA HOST 接口从所述硬盘获取数据；

所述加解密模块通过所述 SATA HOST 接口接收所述数据，并对获取的所述数据进行解密处理；

所述加解密模块将所述解密后的明文数据发送给所述安全存储卡的所述 SATA DEVICE 接口；

所述 SATA DEVICE 接口将所述明文数据发送给所述主板。

10. 如权利要求 7 所述的防止从盘启动的方法，其特征在于，所述方法还包括当所述安全存储卡被拔出后，所述主板将不能启动系统。

一种防止从盘启动的方法及系统

技术领域

[0001] 本发明涉及计算机安全领域，尤其涉及一种防止从盘启动的系统及方法。

背景技术

[0002] 随着信息技术的普及和发展，几乎各行各业都在应用计算机进行办公。对于涉及敏感信息或秘密的行业，如政府、军工和银行等，在使用信息化带来方便的同时也带来了风险，所以这些行业一般都采用内网办公与外网隔绝，并且安装各种安全可信管理平台。通过管理平台进行端口管控、进程管理和审计跟踪，从而达到事前预防和事后跟踪的目的。

[0003] 上述信息安全只是建立在系统正常工作的情况下，但是采用 Windows PE(Windows Preinstallation Environment，Windows 预安装环境）从盘启动时，该安全将不复存在。计算机主盘中的数据可以随意拷贝，并且可以通过更改或删除配置文件对可信安全管理平台进行破坏。

[0004] 因此为了防止计算机主盘中的数据被拷贝或破坏，就需要防止 Windows PE 从盘启动，或者允许从盘启动，但是断开计算机的主盘。

[0005] 针对上述目的，当前各软件厂商通过在 BIOS 中更改启动顺序，将计算机的主盘作为第一启动选项，并为 BIOS 设定密码从而达到防止从盘启动目的。但是，在该方法中，由于 BIOS 密码容易被破解或者通过软件方法进行破解，也可以通过 CMOS 放电使得 BIOS 密码丢失，恢复原来设置。因此，该方法安全性低不可靠。

[0006] 此外，软件厂商还会通过加密主引导扇区的方法达到防止从盘启动保护主盘的方法。该方法通过对主盘的主引导扇区加密，当主盘启动时解密该主引导扇区；当从盘启动时，由于该主盘引导扇区加密，所以无法加载主盘，从而达到保护计算机主盘的目的。但是由于各主盘生产厂商的不一致，使得该加密主引导扇区的方法兼容性不好，无法应用在定制的计算机上。

发明内容

[0007] 针对上述现有技术的缺陷，本发明提供一种防止从盘启动的系统及方法。通过该方法提供的安全存储卡截获计算机主盘发送的数据流，并对该数据流进行分析和获取当前的启动状态，主盘启动或是从盘启动，当检测到从盘启动时，切断主盘数据通路，从而有效保护主盘数据不被拷出。

[0008] 本发明提供一种防止从盘启动的系统，所述系统包括主板、硬盘，所述系统还包括安全存储卡，所述安全存储卡连接于所述主板和所述硬盘之间，所述安全存储卡包括 SATA DEVICE 接口、SATA HOST 接口、加解密模块，其中，所述 SATA DEVICE 接口与所述主板连接，所述 SATA HOST 接口与所述硬盘连接，所述加解密模块与所述 SATA DEVICE 接口、所述 SATA HOST 接口连接，所述安全存储卡通过与 PCI 或 PCIE 插槽连接进行固定并充电。

[0009] 上述方案中优选的是，在初始化所述安全存储卡的所述 SATA DEVICE 接口和所述 SATA HOST 接口时，建立指令表和 PRD 表。

[0010] 上述方案中优选的是，所述加解密模块设有两个双口 RAM，分别连接所述 SATA DEVICE 接口和所述 SATA HOST 接口。

[0011] 上述方案中优选的是，所述双口 RAM 的大小为 16K。

[0012] 上述方案中优选的是，所述双口 RAM 能够进行 PIPELINE（线性通信模型）的流水操作。

[0013] 上述方案中优选的是，所述加解密模块采用 256 位的 SM1 国密算法对所述硬盘进行全盘扇区级底层加解密。

[0014] 本发明还提供一种防止从盘启动的方法，所述方法包括：

[0015] 加密写入，即所述安全存储卡对从主板获取的数据进行加密处理；

[0016] 解密读出，即所述安全存储卡对从硬盘获取的数据进行解密处理；

[0017] 当所述安全存储卡检测到所述主板长时间不发送读取系统引导扇区的指令时，所述安全存储卡自动切断所述主板和所述硬盘之间的数据通路，防止从盘启动。

[0018] 上述方案中优选的是，所述加密写入包括如下步骤：

[0019] 所述安全存储卡上的所述 SATA DEVICE 接口从所述主板获取数据；

[0020] 所述加解密模块通过所述 SATA DEVICE 接口接收所述数据，并对获取的所述数据进行加密处理；

[0021] 所述加解密模块将所述加密处理后的数据，即密文数据，发送给所述安全存储卡上的所述 SATA HOST 接口；

[0022] 所述 SATA HOST 接口将所述密文数据写入到所述硬盘中。

[0023] 上述方案中优选的是，所述解密读出包括如下步骤：

[0024] 所述安全存储卡的所述 SATA HOST 接口从所述硬盘获取数据；

[0025] 所述加解密模块通过所述 SATA HOST 接口接收所述数据，并对获取的所述数据进行解密处理；

[0026] 所述加解密模块将所述解密后的明文数据发送给所述安全存储卡的所述 SATA DEVICE 接口；

[0027] 所述 SATA DEVICE 接口将所述明文数据发送给所述主板。

[0028] 上述方案中优选的是，所述方法还包括当所述安全存储卡被拔出后，所述主板将不能启动系统。

[0029] 本发明采用安全存储卡，通过截获并分析数据流判断当前为主盘启动还是从盘启动。若为从盘启动，则断开数据通路，从而有效保护数据。本发明适用于政府、军工及金融等涉密行业，只有对硬盘加密并且真正从数据通路上防止从盘启动，才能打造真实可信的安全办公环境。

附图说明

[0030] 图 1 为本发明所述的防止从盘启动系统的设计方案框图。

具体实施方式

[0031] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是

本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

[0032] 本发明通过安全存储卡达到防止从盘启动的目的。图 1 为本发明所述的防止从盘启动的设计方案框图。

[0033] 本发明所述的安全存储卡通过 SATA(Serial Advanced Technology Attachment 串行磁盘接口总线，为硬盘接口规范）接口连接于主板和硬盘之间，并利用 PCI(Peripheral Component Interconnect 局部总线标准）或 PCIE(PCI-Express，总线和接口标准）插槽进程固定并取电。防止从盘启动的安全存储卡不但可以完成对硬盘的加解密，而且可以从数据通路上防止从盘启动，具有良好的兼容性，能够兼容所有的主板和硬盘。

[0034] 安全存储卡的工作机理位于操作系统之下，对用户完全透明，通过截获并分析通路中数据流达到对数据加解密和防止从盘启动的目的。

[0035] 本发明所述的安全存储卡能够解决两个问题：一、完成对硬盘的全盘加解密；二、防止从盘启动。只有完成对硬盘的加解密，才能更好的防止从盘启动。因为当人为地将安全存储卡取走后恢复原来数据通路，若硬盘未加密或进行绑定处理，则会重新启动系统，即若硬盘未采用安全存储卡加密或没有与所述安全存储卡进行绑定处理，则会重新开机，成功启动系统。

[0036] 如图 1 所示，本发明所述的安全存储卡连接主板和硬盘之间，用于截获主板发送给硬盘的指令。

[0037] 当作为主盘启动时，BIOS 首先找到硬盘的主引导扇区，然后找到系统引导扇区，最后 BIOS 将控制权交给系统，进而实现主盘启动系统。

[0038] 当作为从盘启动时，BIOS 首先找到硬盘的主引导扇区，然后不再寻找系统引导扇区。

[0039] 根据上述特点，当本发明所述的安全存储卡检测到主板上的 BIOS 长时间不发送读取系统引导扇区的指令时，将会自动切断数据通路，从物理连接上隔绝主板和硬盘，达到防止从盘启动的目的，优选地，当安全存储卡检测到主板上的 BIOS 三十秒不发送读取系统引导扇区的指令时，就可以自动切断数据通路。

[0040] 数据加解密技术利用 256 位高强度的 SM1 国密算法对硬盘进行全盘扇区级底层加解密，是操作系统之下的加解密，对用户的完全透明的。其操作过程如下：

[0041] (1) 加密写入

[0042] 所述安全存储卡上的 SATA DEVICE 接口从主板获取数据，然后通过加解密模块进行加密处理，然后将密文数据发送给所述安全存储卡上的 SATA HOST 接口，最后再由 SATA HOST 接口将密文数据写入到硬盘中。

[0043] (2) 解密读出

[0044] 所述安全存储卡的 SATA HOST 接口从硬盘获取数据，然后通过加解密模块进行解密处理，然后将解密后的明文数据发送给安全存储卡的 SATA DEVICE 接口，最后再由 SATA DEVICE 接口将明文数据发送给主板。

[0045] 所述安全存储卡的 SATA DEVICE 接口和 SATA HOST 接口在初始化时都会预先建立

指令表和PRD表(Physical Region Descriptior物理区域描述符表,里面的内容就是存储的数据的地址和长度)。当SATADEVICE接口从主板上的BIOS接收到指令后,会同时转发给SATA HOST接口。加解密模块设有两个16K的双口RAM,分别连接SATA DEVICE接口和SATA HOST接口。由于根据SATA(Serial Advanced Technology Attachment串行磁盘接口总线)通信协议,传输数据的包的最大长度为8K,所以利用16K的双口RAM可以进行PIPELINE(线性通信模型)的流水操作,从而大大提高加解密性能。

[0046] 以上所述,以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

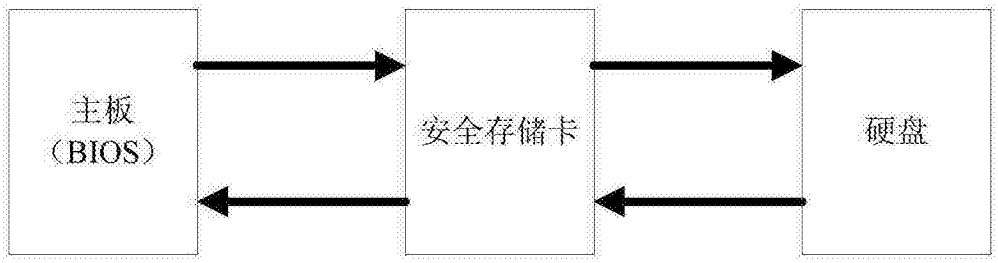


图 1