



(12) 发明专利申请

(10) 申请公布号 CN 102262599 A

(43) 申请公布日 2011.11.30

(21) 申请号 201110257297.6

(22) 申请日 2011.09.02

(71) 申请人 南京博智软件科技有限公司

地址 210000 江苏省南京市雨花台区宁南大道 310 号雨花软件园大 A 楼 A 幢 4 层

(72) 发明人 傅涛 季燕 徐丽娟

(74) 专利代理机构 南京天翼专利代理有限责任公司 32112

代理人 陈建和

(51) Int. Cl.

G06F 12/14 (2006.01)

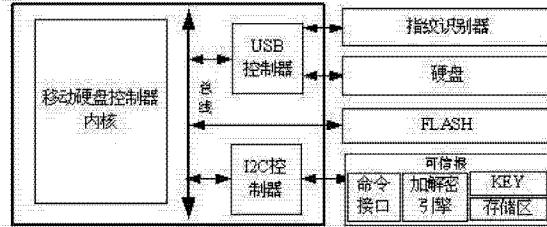
权利要求书 2 页 说明书 4 页 附图 2 页

(54) 发明名称

一种基于可信根的移动硬盘指纹认证方法

(57) 摘要

一种基于可信根的移动硬盘指纹认证方法，由可信根生成用户指纹完整性校验的认证数据块，并将加密的认证数据块放入可信根的存储专区，由此在移动硬盘在上电后，可信根利用认证数据块评估对已存储合法用户指纹的可信度，基于此指纹信息，实现对移动硬盘用户的高可信身份认证；1)当移动硬盘上电后，即由移动硬盘控制器发送初始化可信根命令，2)首先，移动硬盘控制器提示用户通过指纹识别器输入的合法用户的指纹信息；3)由移动硬盘控制器读取控制器内写入的自身移动硬盘设备唯一标识符，将用户输入的指纹信息与标识符组合成数据块；在接收到存储的合法用户指纹信息可信消息后，则开始正常执行移动硬盘其它的初始化工作。



1. 一种基于可信根的移动硬盘指纹认证方法,其特征是由可信根生成用户指纹完整性校验的认证数据块,并将加密的认证数据块放入可信根的存储专区,由此在移动硬盘在上电后,可信根利用认证数据块评估对已存储合法用户指纹的可信度,从而确保合法用户指纹信息没有被修改,基于此指纹信息,即可实现对移动硬盘用户的高可信身份认证;具体步骤如下:

1) 当移动硬盘上电后,即由移动硬盘控制器发送初始化可信根命令,可信根芯片完成初始化后,回复当前设备状态,若为第一次使用,则进入合法用户设置用以身份认证的指纹信息;

可信根及由专用芯片来实现的,包括四个部分:命令接口,用于与移动硬盘控制器之间的信息交互,通过接口来接收移动硬盘控制器发送来的命令与数据,并返回命令执行的结果;加解密引擎,为可信根的实现加/解密操作的算法程序;KEY,是固化在可信根芯片中的加/解密钥,可信根芯片中固化的密钥各不相同;FLASH,为存储认证数据块的可信根专有存储器,不提供外部访问途径;

2) 首先,移动硬盘控制器提示用户通过指纹识别器输入的合法用户的指纹信息;

3) 由移动硬盘控制器读取控制器内写入的自身移动硬盘设备唯一标识符,将用户输入的指纹信息与标识符组合成数据块;然后移动硬盘控制器调用可信根命令接口,发送生成验证数据块命令给可信根;

4) 可信根在接收到生成验证数据块命令后,回复控制器,准备接入控制器发送来的用于生成认证数据的原始数据块;

5) 可信根接收完验证数据块后,调用加密引擎,利用可信根内存储的固化密钥生成认证数据块,并将认证数据块存储到其设定的存储区中,同时设置设备状态寄存器,将其标识为用户指纹已设置状态,然后回复硬盘控制器;

6) 移动硬盘控制器在接收到可信根的回复之后,将用户输入的指纹信息存储至自身的非易失性存储器中,如 FLASH;同时提示用户完成设置过程;

7) 当移动硬盘上电后,即由移动硬盘控制器发送初始化可信根命令,若可信根返回移动硬盘为正常使用状态,则由开始对控制器中存储的合法用户指纹信息的可信度进行评估;

8) 移动硬盘控制器将自身存储的合法用户指纹信息结合移动硬盘设备唯一标识,发送给可信根,由可信根使用自身固化的密钥,调用加密引擎,再次加密生成认证数据块,可信根将新生成的认证数据块与已存储的认证数据块进行对比,若对比一致,则返回当前控制器中存储的合法用户指纹信息可信消息,若不一致,则返回不可信消息;

9) 移动硬盘控制器在接收到存储的合法用户指纹信息可信消息后,则开始正常执行移动硬盘其它的初始化工作;则接收到的消息为不可信,则中止移动硬盘动作。

2. 根据权利要求 1 所述的基于可信根的移动硬盘指纹认证方法,其特征为可信根包括一个专用的芯片,可信根提供:

(1) 生成指纹完整性校验数据块:利用可信根芯片中的加解密引擎与 KEY,实现对唯一设备标识符与合法用户指纹信息摘要的加密,生成用于指纹完整性校验的认证数据块,存储于存储专区;

(2) 已存储指纹信息的可信度评估:利用可信根芯片中包含加解密 KEY 与加解密引擎,

实现对认证信息块的解密,由其中设备唯一标识符及指纹信息摘要来推理评估当前设备中存储的合法用户指纹信息的可信度。

3. 根据权利要求 1 或 2 所述的基于可信根的移动硬盘指纹认证方法,可信根芯片是指符合 TCG 标准的安全芯片,它能有效的保护 PC、硬盘,防止非法用户访问;

其特征在于加解密 KEY 是可信根独有的,外部无法访问与修改;

所述的可信根是用来定义移动硬盘信任链推理的出发点,即能够使移动硬盘系统有理由认为系统中存在的合法用户指纹是完整的,非变更的。

4. 根据权利要求 1、2 或 3 所述的基于可信根的移动硬盘指纹认证方法,其特征是利用可信根芯片中的加密引擎将用户的指纹信息摘要和唯一设置标识符加密后形成认证数据块。

5. 根据权利要求 1、2、3 所述的基于可信根的移动硬盘指纹认证方法,其特征在于加密的认证数据块结构为〈合法用户指纹信息摘要、结束标识、设备唯一标识符〉。

6. 根据权利要求 1、3 所述的基于可信根的移动硬盘指纹认证方法,设备唯一标识符是设备在生产制造时写入的固化数据,一旦设置,外部无法修改。

## 一种基于可信根的移动硬盘指纹认证方法

### 技术领域

[0001] 本发明属于移动硬盘数据安全保障技术领域,涉及了基于可信技术的USB移动硬盘的合法用户身份认证方法,利用硬盘里专有的可信根芯片,以其中包含的key及加解密引擎对用户指纹摘要与设备唯一标识符组成的数据块进行加密,生成用户身份认证数据块,并通过可信根独有的存储专区保存该认证数据块。基于可信根芯片及认证数据块,实现对移动硬盘设备中存储的合法用户指纹信息的可信度进行评估,通过可信根出发的信任链推理实现高可信的移动硬盘用户身份认证,从而保障移动硬盘数据不会被非法使用。

### 背景技术

[0002] 可信计算所指的是一个可信赖的执行环境。可信计算技术通过在计算机中嵌入可信平台模块硬件设备,提供秘密信息硬件保护存储功能;通过在计算机运行过程中各个执行阶段加入完整性测量机制,建立系统的信任链传递机制;通过在操作系统加入底层软件,提供给上层应用程序调用可信计算服务接口;通过构建可信网络协议和设计可信网络设备实现网络中终端的可信。

[0003] 移动硬盘作为常用存储介质,已被广泛用于包括涉密用途的各个方面。将敏感数据以明文形式存储,硬盘内容易于被窃取、非法访问、非法使用等。目前的解决方案一般采用用户身份认证方法来保障移动硬盘的使用安全,如密码、指纹认证等。针对移动硬盘数据易于被非法盗取与使用问题,目前的解决方案一般采用用户身份认证方法来保障移动硬盘的使用安全,如密码、指纹认证等。其中指纹认证方法由于不需要用户记忆密码、认证可靠等优点被广泛采用。但是现有的大部分指纹认证方法只是简单地存储用户指纹信息,然后对比输入的指纹信息来实现认证目标。由于设置时存储的合法用户指纹信息可能会被改写,因此直接使用指纹信息进行认证的可信度不高。

[0004] 认证信息本身是直接存储在移动硬盘的控制器中,同样易被篡改或窃取。因此造成认证的可信度不高,针对这个问题,实现了一种基于可信计算技术根的移动加密硬盘指纹认证方法。本发明基于可信技术,数字内容加/解密,采用专用的可信根芯片作为用户身份认证的信任链推理依据。

[0005] 基于可信根的信任度推理,对已存储的合法用户指纹信息进行信任评估,再采用可信的合法用户指认信息完成用户的身份认证,从而实现高可信度的移动硬盘用户认证目标。由于硬盘控制器芯片中的唯一设备标识符、可信根的加密密钥外部无法访问、存储区一次性写入等特点,保证了可信根的安全,从而保证了用户身份认证的安全性,实现移动硬盘数据不易被非法访问、非法使用的保障目标。

### 发明内容

[0006] 本发明目的是:由于现有移动硬盘所采用用户认证方法,是直接将口令、指纹等认证数据存储在控制器或非易失存储器如FLASH中,这些数据容易被读取或篡改,从而造成认证失败,使得移动硬盘中存储的数据被非法使用。本发明提出一种实现移动硬盘数据不

易被非法访问、非法使用的保障目标。

[0007] 本发明的技术方案如下：

一种基于可信根的移动硬盘指纹认证方法，采用可信根芯片作为用户身份认证信任链推理的可信根，由可信根生成用户指纹完整性校验的认证数据块，并将加密的认证数据块放入可信根的存储专区，由此在移动硬盘在上电后，可信根利用认证数据块评估对已存储合法用户指纹的可信度，从而确保合法用户指纹信息没有被修改，基于此指纹信息，即可实现对移动硬盘用户的高可信身份认证；本方法的具体步骤包括：

1) 当移动硬盘上电后，即由移动硬盘控制器发送初始化可信根命令，可信根芯片完成初始化后，回复当前设备状态，若为第一次使用，则进入合法用户设置用以身份认证的指纹信息；可信根及由专用芯片来实现的，包括四个部分：命令接口，用于与移动硬盘控制器之间的信息交互，通过接口来接收移动硬盘控制器发送来的命令与数据，并返回命令执行的结果；加解密引擎，为可信根的实现加/解密操作的算法程序；KEY，是固化在可信根芯片中的加/解密钥，可信根芯片中固化的密钥各不相同；FLASH，为存储认证数据块的可信根专有存储器，不提供外部访问途径；

2) 首先，移动硬盘控制器提示用户通过指纹识别器输入的合法用户的指纹信息；

3) 由移动硬盘控制器读取控制器内写入的自身移动硬盘设备唯一标识符，将用户输入的指纹信息与标识符组合成数据块；然后移动硬盘控制器调用可信根命令接口，发送生成验证数据块命令给可信根；

4) 可信根在接收到生成验证数据块命令后，回复控制器，准备接入控制器发送来的用于生成认证数据的原始数据块；

5) 可信根接收完验证数据块后，调用加密引擎，利用可信根内存储的固化密钥生成认证数据块，并将认证数据块存储到其设定的存储区中，同时设置设备状态寄存器，将其标识为用户指纹已设置状态，然后回复硬盘控制器；

6) 移动硬盘控制器在接收到可信根的回复之后，将用户输入的指纹信息存储至自身的非易失性存储器中，如 FLASH；同时提示用户完成设置过程；

7) 当移动硬盘上电后，即由移动硬盘控制器发送初始化可信根命令，若可信根返回移动硬盘为正常使用状态，则由开始对控制器中存储的合法用户指纹信息的可信度进行评估；

8) 移动硬盘控制器将自身存储的合法用户指纹信息结合移动硬盘设备唯一标识，发送给可信根，由可信根使用自身固化的密钥，调用加密引擎，再次加密生成认证数据块，可信根将新生成的认证数据块与已存储的认证数据块进行对比，若对比一致，则返回当前控制器中存储的合法用户指纹信息可信消息，若不一致，则返回不可信消息；

9) 移动硬盘控制器在接收到存储的合法用户指纹信息可信消息后，则开始正常执行移动硬盘其它的初始化工作；则接收到的消息为不可信，则中止移动硬盘动作。

[0008] 本发明可信根芯片是指符合 TCG 标准的安全芯片，它能有效的保护 PC、硬盘，防止非法用户访问。其特征在于加解密 KEY 是可信根独有的，外部无法访问与修改。

[0009] 所述的可信根是用来定义移动硬盘信任链推理的出发点，即能够使移动硬盘系统有理由认为系统中存在的合法用户指纹是完整的，非变更的。

[0010] 加密的认证数据块结构为〈合法用户指纹信息摘要、结束标识、设备唯一标识符

>。设备唯一标识符是设备在生产制造时写入的固化数据,一旦设置,外部无法修改。

[0011] 本发明采用专用的可信根芯片作为用户身份认证的安全根,实现了一种基于可信根的移动硬盘指纹认证方法。本发明通过可信根加密合法用户设置的指纹信息摘要与移动硬盘的设备唯一标识,生成用户身份认证的认证数据块,并将加密的认证数据块存放于可信根的存储专区。由此,实现基于可信根的合法用户指纹可信度评估与信任链推理,确保移动硬盘用户认证的安全性。

[0012] 本发明基于可信技术,采用专用的可信根芯片作为用户身份认证的安全根,实现了一种基于可信根的移动硬盘指纹认证方法。该技术通过可信根加密合法用户设置的指纹信息摘要与移动硬盘的设备唯一标识,生成用户身份认证的认证数据块,并将加密的认证数据块存放于可信根的存储专区。如此,基于可信根的信任链推理,对存储在移动硬盘控制中的合法用户指纹信息进行信任评估,再采用可信的合法用户指纹信息完成用户的身份认证,从而实现高可信度的移动硬盘用户身份认证目标。

[0013] 本发明的有益效果如下:

1. 一种基于可信根的移动硬盘指纹认证方法,在移动硬盘上引入专用的可信根芯片,基于 TMP 架构,能够有效的防范非法用户对移动硬盘的身份认证攻击,从而阻止用户非法使用移动硬盘;

2. 利用 < 用户指纹信息摘要,唯一设备标识符 >key 公式进行加密,生成用户指纹完整性校验的认证数据块,存入可信根的存储专区,既提供安全封闭式空间来存储信息,对敏感信息进行保护存储,同时唯一设备标识符和 key 都是只读的,任何用户无法修改,从而达到更好的加密效果;

3. 每次用户在使用硬盘前,必须要进行硬盘控制器芯片中的唯一设备标识符与解密出来的设备标识符进行比对,保证可信根的正确;比对成功再对用户指纹进行比对,从而达到双重加密的效果,安全系数更高,保密效果更好;

4. 在每一次启动硬盘的时候,都会先验证硬盘控制器芯片中的唯一设备标识符,能够及时制止硬盘内容被篡改、非法使用等行为;

5. 本发明中对于可信根中保存的认证数据块及硬盘设备当前状态寄存器采用的是一次性写入存储器,确保了认证数据块及状态寄存器不会被外部改写;

6. 本发明中的认证数据块中加密的是合法用户指纹信息的摘要,有助减少加密运算的时间开销及认证数据块的存储空间开销。

[0014] 附图说明:

图 1 为本发明的系统结构图;

图 2 为本发明工作流程图。

[0015] 具体实施方式:

本发明的实现主要包括以下步骤:

一种基于可信根的移动硬盘指纹认证技术,采用可信计算技术实现的可信根芯片作为用户身份认证推理的可信根,通过可信根来实现对合法用户指纹信息摘要与硬盘控制器芯片中的唯一设备标识符进行加密,生成用户指纹完整性校验的认证数据块,并将加密的认证数据块放入可信根的一次性写入存储专区,从而使得移动硬盘在上电后,利用认证数据块评估对已存储合法用户指纹的可信度,实现高可信的移动硬盘用户身份认证,其实现步

骤为：

步骤1、上电，移动硬盘控制器初始化，读可信根中当前设备状态寄存器，如第一次使用，则进入合法用户指纹信息设置；若不是，发送命令，可信根进行已存储用户指纹信息完整性校验；

移动硬盘控制器由带有 I2C 控制器与 USB 控制器的 ARM 芯片来实现，控制器通过内核实现对移动硬盘、指纹识别器、外接 FLASH 存储器与可信根的控制，完成移动硬盘功能的各项功能；

步骤2：可信根的实现，可信根是本发明用于用户身份认证的重要部分，是通过基于 FLASH 的可编程逻辑阵列（FPGA）芯片来实现的，它主要包括四个功能模块：

1、命令接口，用于与控制器之间的信息交互，可信根 I2C 协议通过接口来接收控制器发送来的命令与数据，并返回命令执行的结果。

[0016] 2、加解密引擎为可信根的实现加 / 解密操作的算法程序；

3、KEY，是固化在可信根芯片中的加 / 解密钥，可信根芯片中固化的密钥各不相同；

4、FLASH 为存储认证数据块的可信根专有存储器，不提供外部访问途径。

[0017] 步骤3：设置合法用户指纹信息：控制器提示用户输入指纹信息，控制器通过指纹识别器接收用户的指纹信息后，将指纹信息与自身的设备唯一标识符发送给可信根；实现存储合法用户指纹信息的 FLASH 存储器，该存储器作为控制器内存一部分，连接在控制器的总线上，可以由控制器直接进行读取。

[0018] 步骤3、可信根调用固化其中的密钥与加密引擎对指纹信息生成摘要后，与设备唯一标识符，组成数据块，生成认证数据块，并存储于一次性写入存储专区，同时写入设置指纹信息成功标识；

步骤4、可信根返回设置成消息，控制器存储设置的指纹信息到自身的 FLASH 数据区，同时提示设置完毕；

步骤5、用户已设置指纹信息的完整性评估，可信根通过专有的储存区读出认证数据块，然后使用自有的密钥，利用可信根中的加解密引擎，对认证数据块 < 用户指纹信息摘要，唯一设备标识符 > key 进行解密，解出存储的用户指纹摘要和唯一设备标识符；

步骤6、校验：将解密出的设备唯一标识符和硬盘控制器中固化的只读唯一设备标识符进行比对，比对成功，则进一步比对硬盘控制器当前存储的用户指纹信息摘要与解密出的用户指纹信息摘要是否一致，如对比结果一致则当前存储的用户指纹信息可信，提示用户输入指纹进入下一步，若不一致，则当前存储的用户指纹信息有问题，硬盘控制器报警；

步骤7、比对用户指纹：针对设置的用户指纹信息可信性评估成功的情况下，通知用户输入指纹；同时将用户输入的指纹和移动硬盘控制器中存储的用户指纹进行比对；

步骤8、如当前用户输入指纹与存储的合法用户指纹信息比对成功，硬盘即启动；比对不成功，硬盘不启动，显示指纹输入错误；

硬盘：存储用户数据的硬盘设备；指纹识别器：用于接收与对比用户输入的指纹信息，具有活体的指纹输入与对比功能；移动硬盘控制器使用 I2C 总线接入可信根，向可信根发送相关命令与数据；指纹识别器与硬盘是通过 USB 控制器接入到移动硬盘控制器。 TCM 产品可打造用户可信根，以 TCM 芯片打造可信链基础。

[0019] 本发明的用户指纹初始化设置与可信度评估及认证算法实现如相关附图所示。

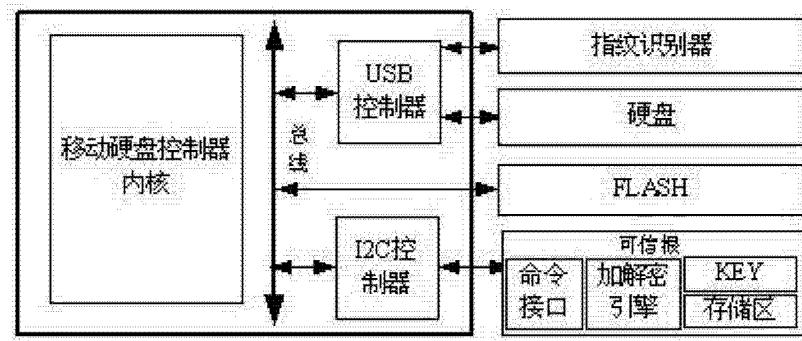


图 1

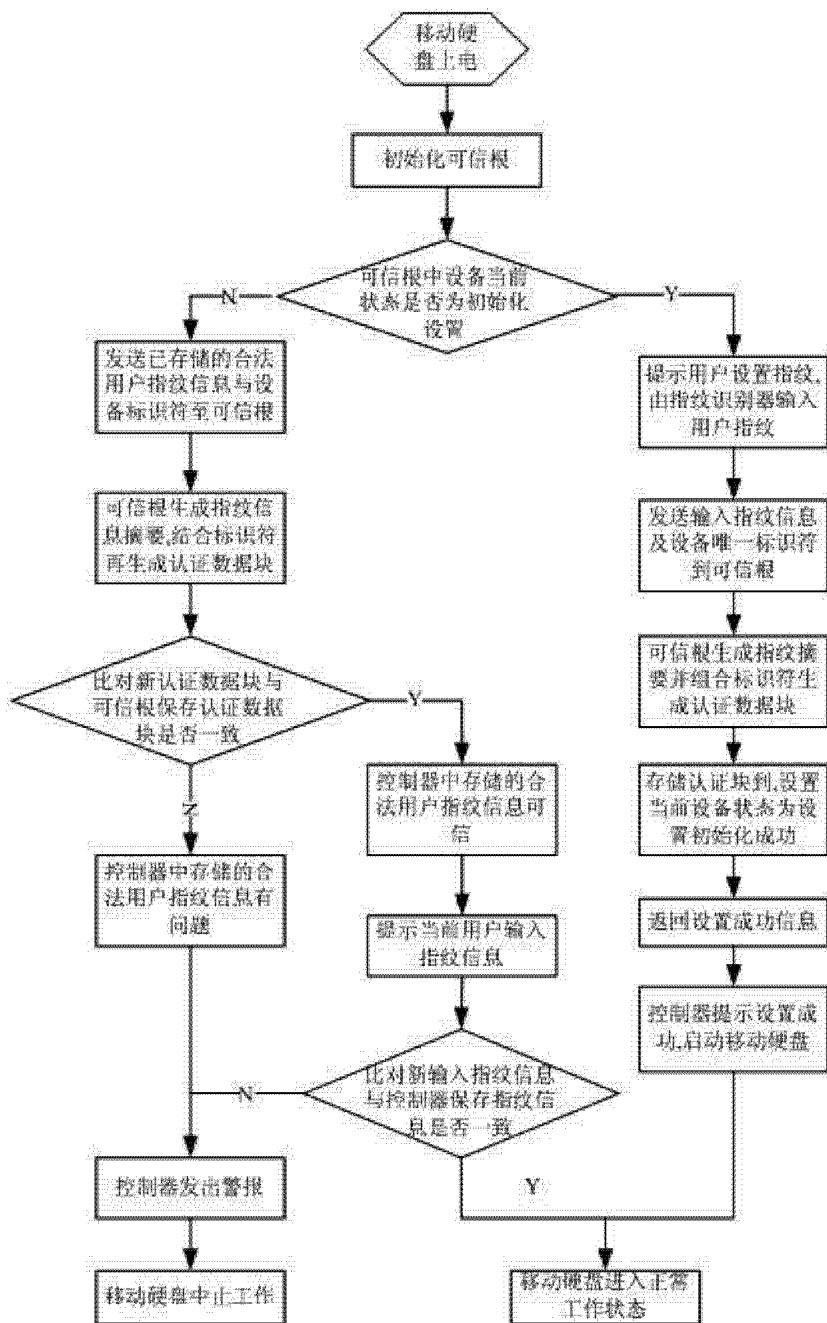


图 2