(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1535411 B
(45)授权公告日 2010.04.28

(21)申请号 02814972.6

(22)申请日 2002.07.25

(30)优先权数据
09/912,931 2001.07.25 US

(85)PCT申请进入国家阶段日
2004.01.29

(86)PCT申请的申请数据
PCT/US2002/023907 2002.07.25

(87)PCT申请的公布数据
WO2003/010643 EN 2003.02.06

(73)专利权人 古书股份有限公司
地址 美国宾夕法尼亚州

(72)发明人 R·H·希巴蒂尤

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陆嘉

(51)Int.Cl.
G06F 1/00(2006.01)
G06F 3/06(2006.01)

(56)对比文件
EP 0965903 A1,1999.12.22, 说明书第013-024段.
US 6173282 B1,2001.01.09, 摘要,附图1-6,权利要求1-3.

审查员 张坦

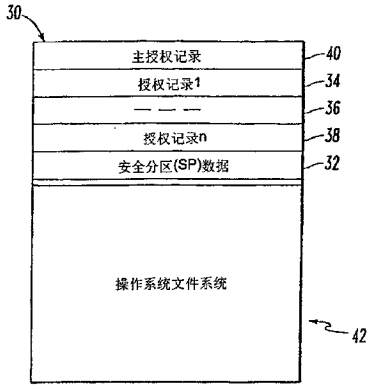
权利要求书 3 页 说明书 10 页 附图 5 页

(54)发明名称

用于在使用附属的存储设备的计算机系统中提升安全性的方法和系统

(57)摘要

本方法和系统使用专门的隔离技术,用于提高计算机系统中的安全性。在这些方法和系统的一个实施例中,一个简单的文件系统被隐藏在计算机系统的存储中,并且由在存储设备上运行的处理器和简单的不可写的代码管理。强加密设计允许本计算机安全方法和系统保护在存储设备上的数据。在一个方法实施例中,为计算机系统提供与至少一个存储设备运行关联的操作系统,在其中存储设备包括用于处理存储在存储设备上的数据和指令的固件和处理器。这个方法包括在存储设备的至少一部分中创建至少一个安全分区,并且限制操作系统对存储设备的至少一部分的访问。这个方法还包括在存储设备中创建至少一个安全分区。这个方法还包括在存储设备中提供至少一个授权记录和与这个授权记录关联的数据。还提供按照在此所述的方法实施例构成的系统和计算机可读介质实施例。



CN 1535411 B

1. 一种磁盘驱动器数据存储设备，包括：

一包含数据存储磁盘的数据存储介质；

一定义在所述数据存储磁盘上的安全区域，所述安全区域包含至少一个授权记录以及至少一个与每一个记录相关的相关数据组，其中每一个记录包含多个字段，包括一包含管理至相关数据组的访问的访问权限的第一字段；以及

位于所述磁盘驱动器数据存储设备中的一控制器和一固件，该控制器和固件用于基于所述至少一个授权记录控制对所述相关数据组的访问。

2. 如权利要求 1 所述的磁盘驱动器数据存储设备，其特征在于，所述控制器用于保护整个数据存储介质的安全。

3. 如权利要求 1 所述的磁盘驱动器数据存储设备，其特征在于，所述控制器阻止附加计算机系统的一文件系统对所述相关数据组的访问。

4. 如权利要求 1 所述的磁盘驱动器数据存储设备，其特征在于，所述至少一个授权记录包含：

一安全分区名称，识别所述安全区域；

一口令，用于访问所述安全区域；以及

访问权限，基于所述口令定义对所述相关数据组的访问的许可。

5. 如权利要求 1 所述的磁盘驱动器数据存储设备，其特征在于，还包含：

保存在所述安全区域内的一加密密钥；以及

嵌入在所述固件中的加密操作，所述加密操作用于使用所述加密密钥加密所述相关数据组。

6. 如权利要求 1 所述的磁盘驱动器数据存储设备，其特征在于，所述至少一个授权记录包含：

一主授权记录，用于确定对所述安全区域中的其他记录的访问，所述主授权记录包含一主口令、以及对相关数据组的访问的许可。

7. 如权利要求 6 所述的磁盘驱动器数据存储设备，其特征在于，所述主授权记录管理所述安全区域中的其他记录的创建和删除。

8. 如权利要求 6 所述的磁盘驱动器数据存储设备，其特征在于，单一的授权在一附加计算机系统的一操作系统中译成组授权。

9. 如权利要求 1 所述的磁盘驱动器数据存储设备，其特征在于，所述控制器对于隐藏信息仅仅允许对所述安全区域的写访问，所述控制器用于禁止对用于隐藏一机密的信息和安全区域的读访问。

10. 如权利要求 9 所述的磁盘驱动器数据存储设备，其特征在于，所述机密包含一加密密钥。

11. 一种用于保护磁盘驱动器数据存储设备中的数据的方法，包含：

在形成在磁盘驱动器数据存储设备的至少一个数据存储磁盘上的一个或多个安全区域中保存一个或多个授权记录以及至少一个与每一个记录相关的相关数据组，其中每一个记录包含多个字段，包括一包含管理至相关数据组的访问的访问权限的第一字段；以及

使用一位于所述磁盘驱动器数据存储设备中的控制器和固件基于所述至少一个授权记录通过一附加计算机系统的一操作系统控制对所述相关数据组的访问。

12. 如权利要求 11 所述的方法，其特征在于，所述至少一个授权记录包含：

一安全分区名称，识别所述安全区域；

一口令，用于访问所述安全区域；以及

访问权限，基于所述口令定义对所述相关数据组的访问的许可。

13. 如权利要求 11 所述的方法，其特征在于，在所述保存步骤之前，所述方法还包含：

对所述数据存储磁盘进行分区以形成所述安全区域。

14. 如权利要求 13 所述的方法，其特征在于，所述分区步骤发生在所述数据存储磁盘的低级格式化部分。

15. 如权利要求 11 所述的方法，其特征在于，所述控制步骤进一步包含：

控制对于保存在安全区域中的至少一个相关数据组的访问。

16. 如权利要求 11 所述的方法，其特征在于，所述控制步骤包含：

隐藏所述至少一个授权记录的被选择的字段以使所述被选择的字段对于所述磁盘驱动器数据存储设备以外的处理不可访问。

17. 如权利要求 11 所述的方法，其特征在于，所述记录包含一公共－私有密钥对和一对称密钥，所述方法还包含：

使用所述公共－私有密钥对中的公共密钥加密所述对称密钥；以及

将所述公共－私有密钥中的私有密钥隐藏，所述私有密钥用于解码所述对称密钥。

18. 一种磁盘驱动器数据存储设备，包含：

一数据存储磁盘；

一定义在所述数据存储磁盘上的安全区域，所述安全区域包含至少一个授权记录以及至少一个与每一个记录相关的相关数据组，其中每一个记录包含管理至相关数据组的访问的访问权限；以及

位于所述磁盘驱动器数据存储设备中的一控制器和一固件，该控制器和固件用于基于所述至少一个授权记录控制对保存在所述安全区域中的至少一个相关数据组的访问。

19. 如权利要求 18 所述的磁盘驱动器数据存储设备，其特征在于，所述至少一个授权记录包含：

一安全分区名称，识别所述安全区域；

一口令，用于访问所述安全区域；以及

访问权限，基于所述口令定义对所述相关数据组的访问的许可。

20. 如权利要求 18 所述的磁盘驱动器数据存储设备，其特征在于，还包含：

保存在所述安全区域内的一加密密钥；以及

嵌入在所述固件中的加密操作，所述加密操作用于使用所述加密密钥加密所述相关数据组。

21. 如权利要求 18 所述的磁盘驱动器数据存储设备，其特征在于，所述至少一个授权记录包含：

一主授权记录，用于确定对所述安全区域中的其他记录的访问，所述主授权记录包含一主口令、以及对相关数据组的访问的许可。

22. 如权利要求 21 所述的磁盘驱动器数据存储设备，其特征在于，单一的授权在一附加计算机系统的一操作系统中译成域授权。

23. 如权利要求 18 所述的磁盘驱动器数据存储设备，其特征在于，所述至少一个授权记录包含：

多个字段，所述字段包含用于确定对所述相关数据组的访问的信息，其中所述多个字段中的一个或多个对于所述磁盘驱动器数据存储设备之外的任何处理是隐藏的。

用于在使用附属的存储设备的计算机系统中提升安全性的方法和系统

技术领域

[0001] 本发明主要涉及用于保护计算机系统的方法和系统。更具体地说，本发明涉及用于保护在计算机系统中的信息的方法和设备，在其中计算机系统可能连接至网络化环境。

背景技术

[0002] 随着因特网的出现和普遍使用，已经发现常规的计算机安全系统是不完善的。因特网的一个缺点是它允许许多方法潜入常规计算机系统外围防御系统。例如，破坏性的病毒程序可通过防火墙并进入计算机系统中被感染。这会危及数据和计算机程序的安全，并且因此派生出诸如数字权限管理的能力。

[0003] 在计算机系统外围防御的不足产生将安全防御系统放在本地计算机系统中的需求。这样一个本地化的计算机系统安全的常规实例是病毒检测软件。不过，病毒检测软件，会受许多利用 (exploit) 的影响，包括但不限于，“哄骗 (spoofing)”或“包装 (wrappering)”策略。因此，可使病毒检测软件在它不是真正在运行的时候，显得正在运行。

[0004] 可能关于常规的计算机安全系统的最基本的问题是它们的操作对于操作系统环境的环境是共同的。而且，例如，用于许多计算机系统的操作系统环境对于因特网环境，或对于另外的网络通信介质，也是共同的。因为这个共同的环境，对计算机系统的攻击的许多方法是有效的，只要通过将计算机代码从因特网移到计算机操作系统。

[0005] 一些常规的计算机保护方法可包括专用安全硬件或安装在计算机系统的 BIOS（基本输入输出系统）中的固件。这些方法可建立第二道防线 (line ofdefense)，内部对于计算机系统的操作，而外部对于复杂的和易于出错的操作系统环境。不过，这些方法常常未能认识到，用为计算机系统提供大量的数据和代码存储的附属的存储设备中非可写固件，可实现更好的防御线。

[0006] 其它常规的计算机安全系统可包括一个连接到 SCSI（小型机系统接口）总线的安全设备，保护在总线上的设备。这种类型的安全系统认识到，当不在一个对于操作系统是普通的环境中运行时，存储设备更安全。不过，这个系统的 SCSI 总线使所有在总线上的设备受到存取，包括存储设备在内，并因此要求直接的操作系统介入。将安全措施 (security measure) 放在附属的存储固件和数据存储中，是对这个技术的改进。然后可将相同的解决方案应用于 SCSI 环境和其它环境诸如 ATA(AT 嵌入式接口）存储设备环境中。

[0007] 另外一个计算机安全系统认识到在控制器级别而不是基于共享的私有密钥保护存储设备的好处。共享的私有密钥是众所周知的，提供比公用私有密钥加密的安全和隐藏元素 (element) 较低的安全性，因为认证密钥是共享的而不是单一设备所私有的。这种类型的系统还贯注于计算机操作系统的文件管理系统的修改，并因此遭受上面对于 SCSI 安全性所说明的操作系统依赖性的同样问题。改进的计算机安全系统可维持操作系统文件管理完整，同时通过一个专用的至附属存储设备的安全接口保持安全性上的独立控制。

[0008] 在另一种类型的计算机安全系统中，安全外围由自包含的软件组成，自包含软件

只输出一个用于外部访问的简单存储接口并在处理命令之前检验每个命令的完整性。相反，大多数文件服务器和客户机执行大量易受攻击的服务。由于这个自保护的存储设备是一个单一功能的设备，所以使它安全的任务就变得更容易。不过，这个系统的目标是依靠先前的安全存储机制，提供自动的恢复至一个已知的良好状态。这种类型的系统还要求操作系统修改。它结合了复杂性，并因此接近操作系统的安全系统的弱点，并且有可能例如引入特洛伊木马（病毒）进入到系统中的机会。而且，这种类型的系统没有认识到，通过使用用于隐藏和保护公用私有密钥的操作的存储设备所提供的改进的安全性。

[0009] 由ATA主保护区域(ATA Host Protected Area)安全协议为计算机系统提供的安全性，可在计算机系统的启动阶段期间由关于准备一存储设备而使用的方法提供。在这个方法中，可向操作系统声明存储设备具有比实际上为由操作系统使用所准备的存储设备小的存储空间。特殊的BIOS固件或其它特殊的代码可具有对未声明的存储空间部分的专有访问。作为一个附加的安全措施，ATA主保护区域可要求通通过码(passcode)访问这个附加数量的存储空间。ATA主保护区域最初被设计为以增强操作系统和应用崩溃恢复效率的形式提供安全保证。一个已知的良好版本的系统或应用软件，可贮藏在操作系统寻址的能力之外的一个位置中。实际上，这对于或者运行于主设备固件中或者运行于操作系统环境中的计算机程序，限制对存储设备的一部分的访问。

[0010] 关于ATA主保护区域协议的一个问题是，还有可能截取与包含重要信息的存储设备的通信。可暴露存储设备的隐藏的ATA主保护区域分区，例如，通过将同一磁盘驱动器放入另一个不保留主机保护空间的计算机中。如果使用通过码，则经过动力循环(power cycle)不保留通过码。ATA主保护区域，实际上是一个可接受的位置，用于保护本地备份代码和数据防止类似病毒的感染，但一般不是隐藏数据的最佳位置。而且，ATA主保护区域所要求的唯一认证是“先到先服务，胜者得全部”类型的设备认证。应用于安全数据存储的扇区的公用私有密钥技术提供对这种类型的安全性的改进。

[0011] 因此，在本领域中，需要处理上述缺点的计算机安全方法和系统。在存储设备环境中，需要提供阻止未经授权的访问和使用计算机程序与数据的方法和系统步骤(approach)。需要这样的方法和系统，允许存储设备的扇区存储不可用于在计算机系统中的文件系统或操作系统读写操作的数据，除了在受控制和密码保护的条件下。这样的受控制条件应该包括在计算机系统的操作系统外部执行受保护的数据集的设备认证和用户认证。还需要这样的方法和系统，提供具有对访问、存储和检索数据的控制的固件和存储设备。这些控制应该不能够被任何可用于计算机系统的过程所写，并且应该被局限在附属的存储设备中。

发明内容

[0012] 本方法和系统使用简单但有效的方法提升计算机系统中的安全性。在这些方法和系统的一个实施例中，在计算机系统中隐藏着一个简单的文件系统，并由在存储设备上运行的一个处理器与非可写的代码管理。这个简单的设计为本计算机安全方法和系统提供用于保护在存储设备上的数据的工具。

[0013] 在一个方法实施例中，为一计算机系统提供一个与至少一个存储设备有效关联的操作系统，在其中这个存储设备包括用于处理存储在这个存储设备上的数据的固件和处理

器。这个方法包括在这个存储设备中的至少一部分中创建至少一个安全分区，以及限制操作系统对这个存储设备的至少一部分的访问。这个方法还包括在这个存储设备中创建至少一个安全分区。这个方法还包括在这个存储设备中提供至少一个授权记录和与这个授权记录关联的数据。

[0014] 在一个实施例中，提出一种磁盘驱动器数据存储设备，包括：一包含数据存储磁盘的数据存储介质；一定义在所述数据存储磁盘上的安全区域，所述安全区域包含至少一个授权记录以及至少一个与每一个记录相关的相关数据组，其中每一个记录包含多个字段，包括一包含管理至相关数据组的访问的访问权限的第一字段；以及位于所述磁盘驱动器数据存储设备中的一控制器和一固件，该控制器和固件用于基于所述至少一个授权记录控制对所述相关数据组的访问。

[0015] 在一个实施例中，提出一种用于保护磁盘驱动器数据存储设备中的数据的方法，包含：在形成在磁盘驱动器数据存储设备的至少一个数据存储磁盘上的一个或多个安全区域中保存一个或多个授权记录以及至少一个与每一个记录相关的相关数据组，其中每一个记录包含多个字段，包括一包含管理至相关数据组的访问的访问权限的第一字段；以及使用一位于所述磁盘驱动器数据存储设备中的控制器和固件基于所述至少一个授权记录通过一附加计算机系统的一操作系统控制对所述相关数据组的访问。

[0016] 在一个实施例中，提出一种磁盘驱动器数据存储设备，包含：一数据存储磁盘；一定义在所述数据存储磁盘上的安全区域，所述安全区域包含至少一个授权记录以及至少一个与每一个记录相关的相关数据组，其中每一个记录包含管理至相关数据组的访问的访问权限；以及位于所述磁盘驱动器数据存储设备中的一控制器和一固件，该控制器和固件用于基于所述至少一个授权记录控制对保存在所述安全区域中的至少一个相关数据组的访问。

[0017] 还提供按照在此讨论的方法实施例构成的系统和计算机可读介质实施例。

附图说明

[0018] 图 1 是一示意图，示出按照提升计算机安全性的方法和系统配置的系统；

[0019] 图 2 是一示意图，示出图 1 的存储设备的细节；

[0020] 图 3 是一示意图，示出在一按照提升计算机安全性的方法和系统的计算机系统的存储设备和操作系统文件系统之间的交互；

[0021] 图 4 是一示意图，示出在图 3 中所示的授权记录和安全分区数据的细节；

[0022] 图 5 是一图表，示出按照本计算机安全方法和系统提供的授权记录的部分；

[0023] 图 6 是一图表，示出按照本计算机安全方法和系统提供的分区首部；

[0024] 图 7 是一图表，示出按照本计算机安全方法和系统提供的基本存储设备程序；以及

[0025] 图 8 是一图表，示出可按照本计算机安全方法和系统产生的错误码。

具体实施方式

[0026] 如在此使用的，“计算机系统”包括，但不限于，台式计算机系统、膝上型计算机系统、网络化计算机系统、无线系统诸如蜂窝式电话和 PDA、包括自包含的网络摄像机

(self-contained web-cam) 的数字摄像机，和 / 或这些系统和设备的任何合理的组合。

[0027] 如在此使用的，术语“存储设备 (storage device)”和“磁盘驱动器 (diskdrive)”或“磁盘 (disk)”是可互换的，除另有说明外，并包括任何在按照在此所述的计算机安全方法和系统的计算机系统中用于存储数据的设备。虽然使用术语“磁盘”，但是存储设备不需要必须结合物理的“磁盘”，但最好结合一个位置，用于具有固件的控制器所管理的存储器。

[0028] 可意识到在这里的某些实施例中使用的术语“分区”，表示一个连续的 512 字节数据块的分组，如由存储设备的低级格式化分配的。

[0029] 特殊的安全分区和支持这些安全分区的结构与过程包括在本计算机安全方法和系统内。本系统和方法的一个主要目标是提供一个实质上不依赖于操作系统的计算机安全系统。

[0030] 现在参考图 1，示出与在下文中所述的方法和系统一致的与网络连接的设备的结构。网络 2，可以是因特网或其它网络通信介质，通过无线或有线的（未示出）连接 4 连接至用户的计算机系统 6。在计算机系统 6 的内部是操作系统 10，它至少部分地依赖于从存储设备 12 得到的软件和数据。

[0031] 现在参考图 1 和 2，在图 1 中示出存储设备 12 的一个更详细的示意图。存储设备 12 包含固件 14，它从存储设备 12 的数据存储部分 16 读写数据。可意识到存储设备固件 14 的至少一部分可由在操作系统 10 中执行的软件重写。存储设备固件 14 的这个可写的部分被认为是可写固件（“WF”）。相反，通过使用一组常规的硬件方法中的一或多个写存储设备固件 14 的至少一部分，这组常规的硬件方法阻止操作系统 10 写这个固件。不能写的存储设备固件 14 的这个部分可被认为是不可写固件（“NWF”）。在一个实施例中，存储设备 12 还可包括一独立的中央处理单元 18（“CPU”）用于控制固件 14 访问和否则操纵存储设备 12 的数据存储部分 16 中的数据。可产生一个要求，即除连同 NWF 或 WF 的执行之外，没有数据可被传输至或从存储设备 12 的数据存储部分 16。

[0032] 为了说明，NWF 和 WF 固件的一些实例结合 ATA 和 SCSI 磁盘控制器协议得到。这些协议的至少部分涉及操作系统与计算机系统的数据存储组件之间的连接。ATA 协议，例如，允许由用户定制命令，诸如控制器命令。在一个实施例中，本计算机安全方法和系统为 ATA/ATAPI-5ANSI（美国国家标准协会）规范提供一个附加标准，NCITS 340-2000。不过，可意识到，可由在此专注于 SCSI 规范和其它合适的允许例如专卖的 (vender-specific) 或标准驱动的扩展的磁盘控制器规范的方法和系统也可理解在此所述的方法和系统可一个新的磁盘控制器规范的组成部分。

[0033] 数据存储，如在此应用的，可与常规的磁盘控制器协议诸如 ATA 或 SCSI 一起提供。可用于 ATA 的一种类型的安全协议，具体地说，对于本领域熟练技术人员，被称为 ATA 主保护区域。标出的存储 (mapped-out storage)，如在此应用的，是由在 NWF 和 WF 中的表标出的表示坏扇区的存储空间。理解可由磁盘控制器为存储设备标出可写存储之外的其它数据。

[0034] 现在参考图 3，本计算机安全方法和系统可增加现有的 ATA 和 SCSI 协议，例如，用简单和有效增强的安全协议。方法和系统包括具有安全分区（“SP”）数据 32 的存储设备和至少一个授权记录，诸如与安全分区数据 32 关联的授权记录 34。这些安全分区数据 34 和授权记录 34、36、38 是包含在存储设备 30 的安全分区中的。本方法和系统在存储设备 30

的低级格式化上提供一个相对简单的文件系统。添加到存储设备 30 的数据的增长从上至下进行，如在图 3 中所示，因此存储设备 30 内容的查询可容易地显示剩余多少数据存储空间用于使用。

[0035] 涉及授权记录 34、36、38 的操作是由存储设备 30 的固件管理的。在一个实施例中，所有的授权记录 34、36、38 可由一个单一主授权记录 40 管理。如所示的，不允许操作系统（“OS”）文件系统 42 访问包含在存储设备 30 内的安全分区数据。安全分区数据 32 的独立于 OS 文件系统 42，提供本安全方法和系统的一个重要的好处：在计算机系统上创建一个位置，在这个位置中有效地隐藏信息诸如一个秘密。

[0036] 现在参考图 4，按照图 3 的授权记录 34、36、38 呈现的授权记录 52 的示意图。授权记录 52 可包括与相应于授权记录 52 的 SP 数据 54 关联的数据、计算机程序和其它类似的信息和功能。授权记录 52 和 SP 数据 54（元素 56 至 84）的内容涉及想要隐藏的信息和 / 或提升在计算机系统中安全数据处理的功能。可存储在 SP 数据 54 的信息类型和由授权记录 52 结合 SP 数据 54 执行的安全处理功能的类型，如在元素 56 至 84 中所示，在下面作为实例呈现。

[0037] 可见，对于如在此所述的封闭的、不可扩展的存储和授权系统存在许多优点。存储设备可为在磁盘上的某些数据定义一个能容易地检查和审计的用于授权和认证的结构。如果在一个封闭的系统中没有提供授权和认证功能，那么计算机系统通常易于受到攻击和渗入。可意识到 63 个用户可定义的授权记录和一个主记录很可能满足本计算机安全方法和系统的大多数实际应用。因为这些方法和系统是存储设备专用安全防御线，所以可将一个单一的授权译成在操作系统环境中的一组授权或一个完整的域授权。因为用户在需要时可创建和删除授权，在理解一个主授权记录可管理这些用户修改的情况下，本方法和系统为计算机系统提供适当的防御线。

[0038] 实例

[0039] 下面的实例是想要说明本计算机安全方法和系统实施例的可能的实现。可意识到这样的实例主要想要为了说明。在此所述的方法和系统实施例的方面中没有特殊的方面想要限制本发明的范围。例如，可意识到，对于由本计算机安全方法和系统执行的安全分区命令的术语的特殊选择是为了说明，不是想要限制本发明的范围。

[0040] 图 5 至 8 简述用于本计算机安全方法和系统的数据内容和结构、基本程序和错误码的图示。

[0041] 图 5 示出跟随在与授权记录关联的数据之后的单一授权记录的字段。授权记录定义一个授权（例如，用户、组、域或其它代理 (agent)）和一个数据集，授权记录为这个数据集管理访问保护。

[0042] 图 6 示出用于包含主授权记录及其数据的分区的首部，其数据包括所有其它用于存储设备的授权记录。这个首部为计算机系统提供用于有效使用安全分区、授权记录及其关联的 SP 数据的信息。

[0043] 图 7 示出与本计算机安全方法和系统关联的基本存储设备程序。这些基本程序包括用于建立新的授权记录、删除数据和 / 或修改先前的授权记录的方法。还示出用于使用建立在一或多个用户应用中的安全特性的程序。

[0044] 图 8 示出可在图 7 中各种程序的应用得到的示例错误码。

[0045] 在应用于本计算机安全方法和系统时，读写数据至一受保护的数据分区可使用常规的读/写机制和协议。在一方面，如果试图读或写一个安全分区，使用一个安全分区打开调用可打开安全分区，诸如 SPOpen 命令。一旦打开，安全分区保持打开直到被关闭（诸如通过使用 SPClose 命令）或者直到一个预定的时间间隔期满。SPOpen 命令可用多种方式限制读写访问，这些方式对于存储设备所需的安全功能是重要的。在另一个实施例中，专用的 SP、定长和面向记录的读写操作被允许不保留打开窗口的机会，即全局 SPOpen 命令可允许的机会。

[0046] 在一些实施例中，SPOpen 和 SPClose 命令是不可用的，因为安全和效率考虑以及通过可用的 APProtRead 和 SPProtWrite 命令执行读写操作。使用 SSProtRead 和 SSProtWrite 命令可执行一个内部的隐藏的 SPOpen 功能，等价于没有向用户交互暴露安全数据的动作。

[0047] 在某些实施例中，本计算机安全方法和系统可使用，例如，ANSIX.509 证书，它能使用陷门加密算法(trap-door cryptographic algorithm)，诸如众所周知的用于认证的 RSA 算法。每个授权记录可包含一个用于认证源自感兴趣的安全分区的数据的公用私有密钥对。提供一个第二公用私有密钥对以确保数据只能被送至特定的安全分区而不会被送至其它用于存储的位置。这些密钥对与 X.509 证书入 (Cert-In)（即只将数据传输至想要的分区）和 X.509 证书出 (Cert-Out)（数据被签署并因此被认证只来自想要的分区）关联。可用实际上与 SSL 和其它等价安全流协议相似的方式，使用对称的密钥加密数据。在这个实施例中，公用私有密钥主要被用于与证书关联的散列，尽管私有密钥可解码一个指向一个授权的通过码。

[0048] 本方法和系统可要求上面提到的加密运算被嵌入在存储设备的固件或物理存储中。密码被认证具有在设备的 NWF 中的根保证 (root assurance)。如此，对读或写受 SP 保护的数据的访问不易受到攻击，除物理地修改存储设备之外。SP 系统还在数据分区中提供加密的数据。加密使用对称密钥。如果关闭加密，那么在存储设备中的数据是纯文本，即使在将数据传输至或从它的存储位置时可能没有使用对称密钥。如果开启加密，那么在存储设备中的数据被加密，即使在将数据传输至或从它的存储位置时可能没有使用对称加密。

[0049] 如果 SP 数据被加密且授权源是外部的，则可提供一个方法和系统以加密在存储设备上的加密数据，因此只有一个外部代理能加密数据。SP DataEncrypt 命令加密 SP 数据，因此可获得一个密钥并由一个外部源应用它。

[0050] 在这个实施例中，不存在容易取得的方法，用于根据可用于存储设备的信息解密来自存储设备的数据。这个方法和系统包括安全地传输公用密钥和对称密钥。当需要对称密钥用于加密或解密数据时，提供私有密钥以解密对称密钥。这个公用密钥/对称密钥/私有密钥方案是用于提供文件加密的常规方法。本计算机安全方法和系统，通过提供只包含在存储设备中的安全方法和系统而不是作为操作系统或文件系统的部分，改进这个常规的方法。

[0051] 控制在一个安全分区中读写数据的授权记录的另一个特点是可隐藏授权记录的某些字段。“隐藏 (hidden)”一般指在这些字段中的值不能由任何外部过程读取，也就是说，既不能通过一个对固件的调用也不能通过存储设备的内容的直接检查读这些值。存在一组已知的硬件技术，通过它们可以保护存储：例如，标出这样的存储的地址空间，除了对

于 NWF。可结合授权记录的通过码字段应用的另一个技术是只存储码的散列。这种技术是有可能的，因为不要求读纯文本通过码。此外，另一种技术是通过用一个授权的公用密钥加密密钥以隐藏一个对称密钥，这样只有隐藏的私有密钥能够解码它。

[0052] 在实施本计算机安全方法和系统时，可在外部授权源与内部授权源之间作出区别。如果安全分区是内部授权源，那么由存储设备的 NWF 和 WF 内部地产生公用私有密钥对和对称密钥。如果安全分区是外部授权源，那么可由一个传输的安全方法（如由 SPCSet 命令定义的，例如）将公用私有密钥对和对称密钥传输至存储设备。这意味着当可以写（诸如通过 SPCSet 或通过内部密钥发生器）某个数据诸如私有密钥时，任何外部过程没有读数据，因为它们被定义为隐藏的。这是重要的，即同样的“写但不读 (Write but Not Read)”能力可以是在任何为“写但不（外部）读”分区的安全分区中的所提供的数据。因此，一个在存储设备外部的用户应用能够使用存储设备作为一个可信赖的地方以隐藏信息和执行具有相对高程度的安全和秘密的加密操作。

[0053] 本计算机安全方法和系统的一个实施例提供宣布 SP 数据是一次写入的 (write-once)。这个实施例的一个说明性使用是在 PKI（公用密钥结构 (publickey infrastructure)）中，在其中在为一个特定的授权验证公用密钥时存在一个问题。本方法和系统的安全分区可动态地验证公用密钥的来源。这克服在 PKI 中被称为密钥撤回 (key revocation) 的一个基本问题。有可能通过本方法和系统具有一个安全的方法，该方法动态地保持当前具有相对高级别的保证的公用密钥。一次写入实施例的另一个应用被应用于对于一个系统或磁盘锁定软件以及建立在没有授权情况下不能被拒绝或被访问的日志。在这个实施例中，例如，可使用存储设备读可能包含信用卡购买信息的日志。

[0054] 本计算机安全实施例一般使用与每个授权记录及关联的数据集关联的固定量的空间。此外，一个主授权记录可包含用于所有其它安全分区的授权记录。例如，每个授权记录可使用六个数据块 (3072 字节）区域的 2633 字节，并可存在 64 个可能的授权记录，在包含用于所有安全分区的授权记录的安全分区中总计 196,608 字节。在这个说明性系统中，可只存在 63 个用户可定义的安全分区。在这个实施例中没有外部的授权被允许访问，除了如由私有 / 公用 / 对称密钥的外部源定义的。这意味着只有一个定义在存储设备上的授权记录可以是被允许读写任何其它授权记录和 / 或数据集的授权。可意识到，在公共可读的和一般出厂设定的授权记录首部中产生允许扩展或减少这个封闭系统的授权至多于或少于 64 个总计授权记录。

[0055] 在本计算机安全系统的实施例中，该系统保持具有用于主授权记录的固定空间使用的有限数量的授权记录，可调节与具有一个使能 SP 的 (SP-enabled) 存储设备关联的性能负担。一般而言，任何在存储设备上读或写操作检查以确定由安全分区保护的低级存储地址（例如，柱面、头、扇区、数据块等等）。

[0056] 在另一个实施例中，将安全分区区域模拟得象 ATA 主保护区域区域。包含主授权记录和其它授权记录的分区具有一个已知的、固定的大小，并使用隐藏的存储，甚至对于 ATA 主保护区域调用也是隐藏的。任何在主授权记录之下的分区可使用 ATA 主保护区域空间的顶部部分。由于在 ATA 主保护区域空间中的读写操作一般是罕见的，所以可有效地增加一个对受 SP 保护的区域的检查的功能。

[0057] 在本方法和系统的另一方面，SPAuthHeader 调用返回一个受保护的磁盘地址区域

的列表。通过指定存储设备的一个固定区域为驻留 SP 数据的区域，可完成检查允许的写操作的功能。SPAuthHeader 调用返回值综合并存储在扩展的授权分区首部中。对于这个调用报告受 SP 保护的存储设备的邻近区域是有用的。如此，可警告用户软件不要在没有适当的 SPOpen 调用的情况下试图寻址于那些区域。SPAuthHeader 调用可不报告用户不访问的磁盘地址。

[0058] 可意识到用户定义的 SP 数据分区可消耗存储设备的全部存储容量，如果 NWF 和 WF 允许这样的消耗。这是将读写主授权记录只限制于预定的用户的一个原因。本系统可提供对这些预定的用户的认证，并最小化具有对授权记录管理员级控制的用户的数量。

[0059] SPAuthHeader 调用的一个重要功能是返回用于与主授权记录通信的公用密钥。这个功能是重要的，因为主授权记录要求公用密钥对访问主授权记录所需的通过码加密。出厂分发的存储设备可具有一个通过码结构，因此试图初始化主授权记录记录的软件必须知道通过码。通过码也是结构化的，因此它不能被“闻出 (sniffed)”或否则在运送中被检查，因为用主授权记录的公用密钥对通过码加密的。

[0060] 已知发布用于加密通过码的公用密钥可利用易受重放攻击 (replay attack) 的公用密钥。要阻止这样的攻击，本安全方法和系统的一个实施例在授权记录和授权首部中包括 SPNonce (包含一个“现时 (nonce)”) 和 SPAuthNonce 字段。现时可以是一个在长度上最大至 256 字节的随机数，其目的是一次性使用。在一个实施例中，用公用密钥加密现时作为通过码的一部分。这确保通过码的发送者知道通过码。现时构成授权记录的一部分，因此可将现时传递至 NWF 和 WF。这允许使用现时，通过存储和隐藏在用户授权记录中的通过码，获得对远程存储设备的授权。

[0061] 为了产生密钥和现时，在 NWF 和 WF 中可提供一个随机数发生器。某些存储设备，诸如硬盘，提供测量可作为一个用于随机数源培养的随机的机械或电子误差的机会。本计算机安全方法和系统可使用这个连续的随机数，例如，与安全的存储对存储传输一起创建一次一密乱数本 (one-time pad)。一次一密乱数本是众所周知的加密 - 解密技术。

[0062] 可意识到，由于授权记录可具有 SP 数据，SP 数据具有起始时间、结束时间和 / 或在预定时间删除或传送 SP 数据的指令，那么需要一个可靠的源用于时钟时间。通过具有在存储设备内部的可通过安全授权的传输与一个外部时钟同步的时钟获得好处。这需要一个附加的调用，这个调用具有被撇开的授权记录或者需要使用主授权记录。通过减少时间量，现时被认为是有效的，然后可限制在被传输的时钟时间中的误差。

[0063] 安全分区的普通使用是存储在其它设备上的其它安全分区的公用密钥。在这个实施例中，可实现存储设备的安全网络，因为允许对在其它设备上的其它授权记录访问的通过码本身在存储设备内部被加密。例如，有可能创建一或多个主记录 (master registry)，主记录可安全地管理在多个其它存储设备上的安全分区。

[0064] 可意识到，本计算机安全实施例必须处理调用认证 (call authentication) 以保护在操作系统中的代码和数据。调用认证具有两种一般的情况。在一种情况下，需要认证一个被调用的计算机程序，例如，是正确的计算机程序。在另一种情况下，需要认证调用这个计算机程序的程序或例程是正确程序或例程。

[0065] 调用认证提供在运行于操作系统中的代码与存储设备授权之间的安全通信的基础。对于操作系统的一般情况是具有一组装入程序 (loader) / 连接程序 (linker)。这些是

操作系统程序，它们从存储读代码；指派符号的、虚拟的和物理的地下；初始化值；将代码装入执行存储器；以及还可初始化代码执行。

[0066] 常规的习惯是将代码认证（code authentication）放在装入程序／连接程序中。不过，一旦合法的程序被认证、装入和连接，侵入的代码可在执行期间修改合法的代码。如果被连接和装入的代码能从存储设备读数据并将那个数据解释为程序代码，则可容易地引入侵入的代码。许多程序具有以此方式偶然地引入侵入的代码的能力。不过，甚至在没有这个能力的情况下，存在诸如常规的缓冲溢出利用（buffer-overflow exploit）这样的方案，缓冲溢出利用可用侵入的代码代替已知为可信的代码。

[0067] 代码认证在装入程序／连接程序级别仍然有用。如果所有读起代码作用的数据是经过认证的读，那么可实现代码认证的许多好处。如果通过良好的编程习惯消除缓冲溢出和相似的利用，那么代码认证可以是有效的技术。这是众所周知的，不过，在一个开放的操作系统环境中运行的代码常常未能符合良好的安全习惯。

[0068] 本计算机安全方法和系统可提供用于代码认证的组件。在一个实施例中，可由一或多个连接程序／装入程序使用一或多个授权记录存储作为数据的公用密钥和检查为认证而装入的代码。装入程序／连接程序因此肯定是公用密钥、散列值和可信的代码。装入程序／连接程序代码可被存储在一个授权记录的非可写空间中以确保其基本代码不受影响。

[0069] 只有当所有的调用代码认证被做成适当的经过认证的代码时，才可处理调用认证问题。保留一种可能性，可引入引起调用一个不正确的代码段的侵入的代码。在一个通过消息传递或相似的面向对象的方法定义通信的操作系统中，由名称或句柄进行调用。在一个“一次写入不删除（write-once-no-delete”模式中可使用授权记录记录代码段之间的经过认证的调用。如果所有代码段是经过认证的，那么一般将它们编码成适当的边界检查标准（bound-checkingstandard）。在这种情况下，调用路径（call-path）被认证并且不太可能具有安全缺口。

[0070] 用于提供调用认证的另一个方法涉及众所周知的包装代码段（wrapperingcode segments）原理。在这个方法中，在另一个已经由代码编译器或装入程序／连接程序引入的代码段的存储空间中执行一个代码段。这样的一个实例是在常规编译器中的调试功能。另一个实例是在解释的字节代码系统（intrepretedbyte code system）中。假定直接来自受保护的磁盘授权空间的包装的代码是可用的，那么它可通过代码模块提供完全经过认证的调用的动作。这个方法确认在代码之外的调用是对原来经过认证的符号的、虚拟的或物理的地址。例如，如果一个代码集（code set）不应该打开一个至因特网的端口，那么如果尝试这样一个端口打开则包装程序（wrapper）提供一个警报。记录在这个包装程序内所允许的调用的数据，最好存储在一个安全的不可写的授权记录中。

[0071] 在本计算机安全方法和系统中调用认证的一般解决方案使用存储设备存储认证数据以完成认证计算；以及存储特殊的代码段，由这个代码段可在操作系统环境中建立信任的根。一般而言，关键的连接程序／装入程序和代码解释器足以建立在操作系统环境对特定的代码操作的信任。这是对建议周期性地改变文件系统或保护整个操作系统环境的其它方法，在通常不能完全地保护那个环境时的改进。本计算机安全实施例提供关键的工具，可使用这些工具保护在操作系统环境中的代码执行并因此为调用认证问题提供一个可伸缩的（scaleable）解决方案。

[0072] 益处 / 优点

[0073] 在此所述的方法和系统为提升计算机系统安全提供相当大的改进和优点，包括下列益处：

[0074] ●为使用本地或远程用于程序和数据的存储设备的计算机系统提供内部的安全性。存储设备可以是存在于一个单一的计算机系统中的一或多个存储设备。可由总线或网络连接计算机系统。

[0075] ●保护计算机系统不受源自网络的攻击，特别是在计算机系统依赖于存储设备的情况下。

[0076] ●保护数据和计算机程序在计算机设备和 / 或系统中不被未经授权的使用和复制。

[0077] ●允许存储设备保护和隐藏私有密钥，并还以隐藏但经过认证的方式签署和检查消息。

[0078] ●升级在依赖于电子或电光数据和计算机程序的局域或广域企业中的现有的计算机安全系统。

[0079] ●通过宽带和 / 或窄带非交换的和 / 或交换的网络将数据和计算机程序传输至存储设备，因此在计算机系统中可提供数据和 / 或计算机程序的安全和准确功能的指示。

[0080] ●为公用密钥结构传输、存储和管理公用密钥；以及为加密用途传输、存储和管理私有密钥。

[0081] ●在局域和广域两者的许多存储设备上管理多媒体音频和视频内容的完整性和权限。

[0082] ●在不妨碍正常使用中存储设备性能的情况下，提供存储安全性。

[0083] ●改进对 ANSI ATA-4 和 ATA-5 主保护区域的使用。

[0084] ●对于一组网络化计算机系统提供保证操作系统的操作和完整性；在计算机系统中的应用系统；对于一组网络化计算机系统的应用系统；在计算机系统中的备份和恢复系统；以及，对于一组网络化计算机系统的备份和恢复系统。

[0085] ●允许在一组存储设备和 / 或计算机系统之间和 / 或之中创建和使用一次一密乱数本。

[0086] 虽然在此已经为了说明本发明而不是为了限制本发明描述了本发明的特定实施例，但是本领域熟练技术人员可意识到，可在本发明的原理和范围之内，在不脱离如在所附权利要求书中描述的本发明的情况下，可产生细节、材料和部件的布置的众多的变化。

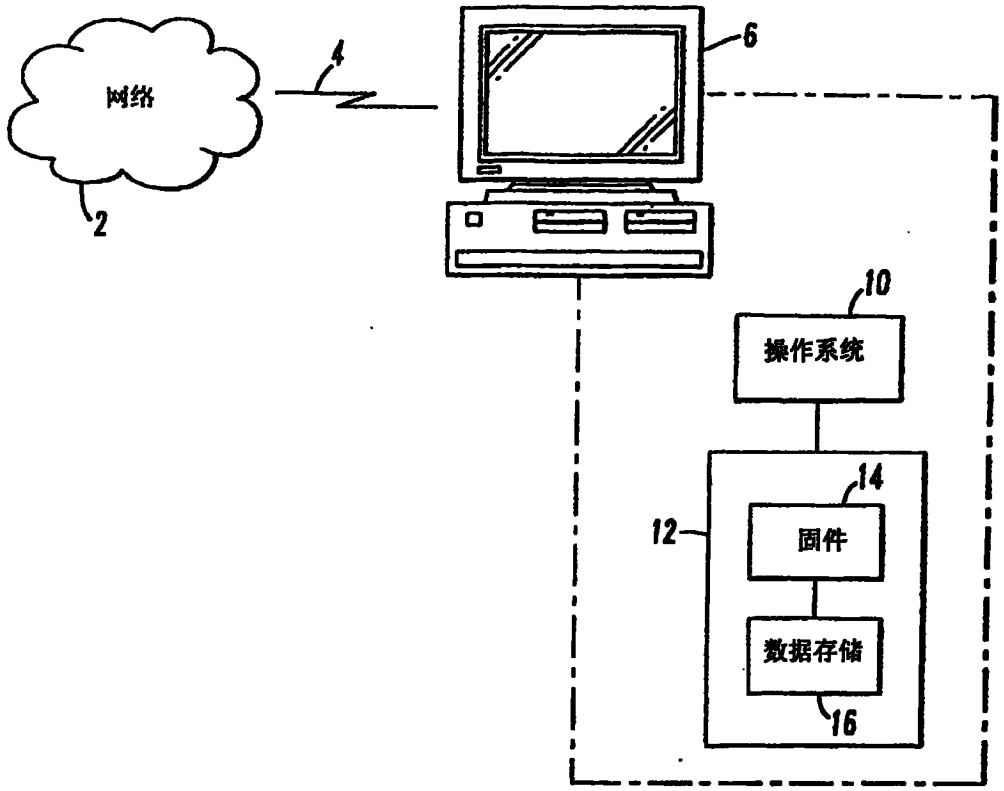


图 1

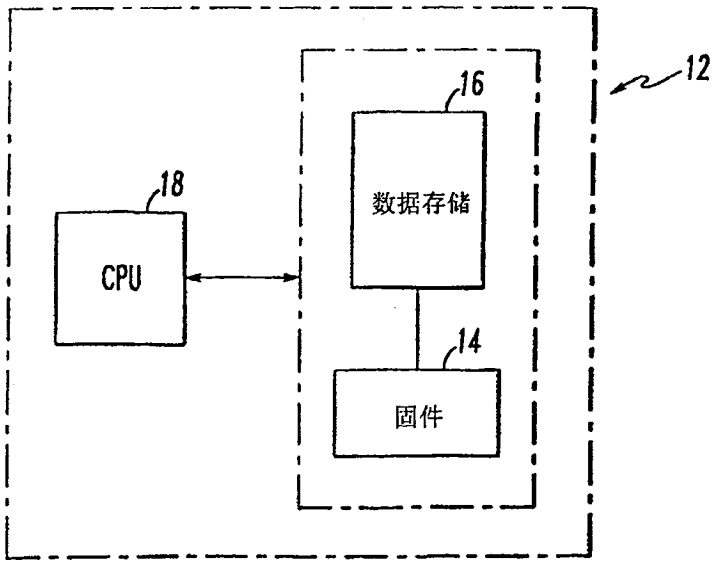


图 2

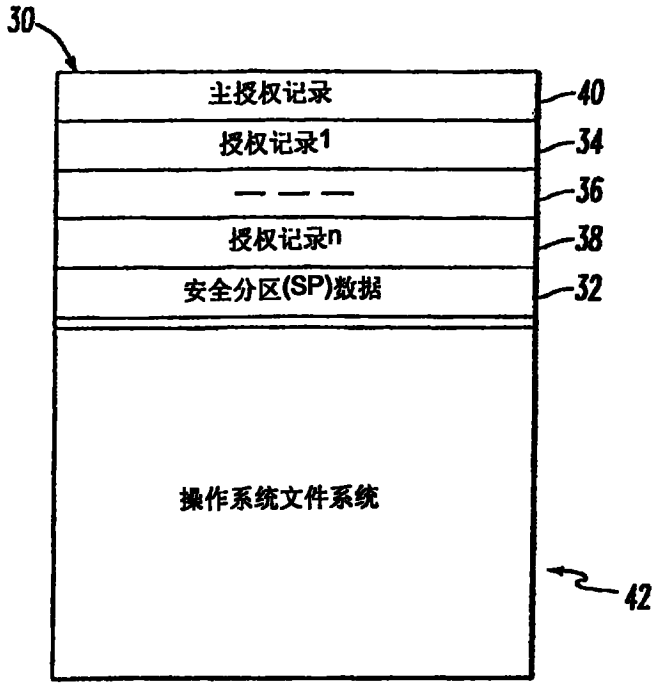

30
主授权记录
授权记录1
— — —
授权记录n
安全分区(SP)数据
操作系统文件系统
40
34
36
38
32
42

图 3

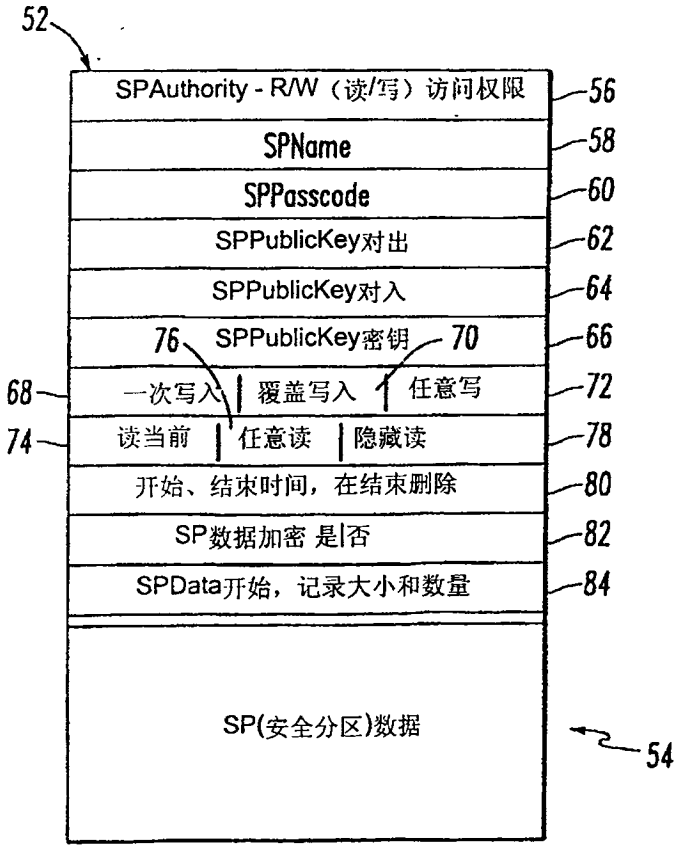

52
SPAuthority - R/W（读/写）访问权限
SPName
SPPasscode
SPPublicKey对出
SPPublicKey对入
SPPublicKey密钥
76
70
一次写入
覆盖写入
任意写
68
读当前
任意读
隐藏读
74
开始、结束时间，在结束删除
SP数据加密 是|否
SPData开始，记录大小和数量
SP(安全分区)数据
56
58
60
62
64
66
72
78
80
82
84
54

图 4

字段	N	位长度	字节长度	注	授权源（见AuthSet调用） 位长度	外部的	根
SPName	1	256	32	第一字节Null（空）	InFrom 设定值	InFrom 设定值	InFrom 设定值
SPPasscode	1	128	16		InFrom CSel, 隐藏	InFrom CSel, 隐藏	InFrom CSel, 隐藏
SPublicKey-Out	1	4096	512		OutFrom 设定值	InFrom CSel, OutFrom 设定值	OutFrom 设定值
SPPrivateKey-Out	1	4096	512		隐藏	InFrom 设定值 隐藏	隐藏
SPPublicKey-In	1	4096	512		OutFrom 设定值	InFrom CSel	OutFrom 设定值
SPPivateKey-In	1	4096	512		隐藏	InFrom CSel, 隐藏	隐藏
SPSymKey	1	1024	128		隐藏	InFrom CSel, 隐藏	隐藏
SPNonce	1	2048	256	避免重放攻击	In | Out from 设定值	In | Out from设定值	In | Out from 设定值
SPAuthSource (Internal | External | Special)	1	2	0.25		不可用	不可用	
SPDataWriteMode (WriteOnce | WriteOver | WriteAny)	1	2	0.25		InFrom 设定值	InFrom 设定值	WriteAny
SPDataReadMode (ReadCur | ReadAny | Hidden)	1	2	0.25		InFrom 设定值	InFrom 设定值	ReadAny
SPDataEncrypt (Yes | No)	1	1	0.125		InFrom 设定值	InFrom 设定值	InFrom 设定值
SPStartTime	1	128	16		InFrom 设定值	InFrom 设定值	InFrom 设定值
SPEndTime	1	128	16		InFrom 设定值	InFrom 设定值	InFrom 设定值
SPEraseAtExpiration (YES | NO)	1	1	0.125		InFrom 设定值	InFrom 设定值	InFrom 设定值
SPNumberofRecords	1	64	8		InFrom 设定值	InFrom 设定值	InFrom 设定值
SPRecordSize	1	64	8		InFrom 设定值	InFrom 设定值	min 3270
SPCurrentRecord	1	64	8		InFrom 设定值	InFrom 设定值	-1
SPDataStart (an abdomulle disk address)	1	768	96		隐藏	隐藏	隐藏
SPAuthority SPName (reader, writer, admin, encrypted passcode, cellN, certOut)*	64	32	256	第一个字节编码要求	InFrom Sel	InFrom Sel	(1,1,1,1,1,1,..)
在一个授权记录中的总字节上舍入		21,096	2,889 3,072		6磁盘存储块		
SPDate (用于这个的磁盘地址通常与授权记录是不连续的)		SPRecSize *NumRecs	对于根数据 其它授权 193,536是 将具有其它 3,072*63 大小				

图 5

字段	位	字节	实例	注解
SPMagic	32	4	xf27f	
SPOffset	32	4	1844	首部字节可按多于一个磁盘起止存储限制项增加
SPVersion	32	4	1.01	文本
SPCryptoSuite	128	16	RSA+RAJD++	文本 在较佳实施例中固定的
SPVendor	128	16	Foobar Corp.	文本
SPNumAuths	32	4	64	
SPAuthSize	32	4	6	在512字节数据块中
SPRootPublicKeyIn	4096	512		来自根授权记录
SPRootNonce	2048	256		在要求时合成的
SPStorageLimits	8192	1024	8	开始/结束绝对磁盘位置 从授权记录合成的

注：授权分区首部一般是可写的

图 6

错误	代码注解
SPSuccess	0
SPBad CertificateIN	1 证书入失败
SPBad CertificateOut	2 证书出失败
SPBad Name	3 未找到名称
SPBad Passcode	4 通过码失败
SPNo PublicKey-Out	5 用于外部授权
SPNo PublicKey-IN	6 用于外部授权
SPNo PrivateKey-Out	7 用于外部授权
SPNo PrivateKey-IN	8 用于外部授权
SPNoAuthority	9 你不能做这个
SPPartition Full	10 SP分区满并且没有开启覆盖写
SPNo Space for Partition	11 你不能创建这个分区，没有连续的空间
SPNo Security Support	12 SP安全在这个设备上关闭-首部失败
SPRead Failure	13 特殊SP读失败
SPWrite Failure	14 特殊SP写失败

图 8

调用	变元				注解
读和写授权记录的调用					
SPAuthHeader SPSet	AuthHeader 名称	通过码 证书入 证书出	AuthRecord	观看|修改|添加|删除	返回首部. 为一个授权设置值	要求 管理员特权
SPCSet	名称	通过码 证书入 证书出	AuthRecord	观看|修改|添加|删除	安全设置用于授权、使用公用密钥的值	要求 管理员特权
允许读和写授权记录的调用						
SPOpen	名称	通过码 证书入 证书出	AuthRecord	以微秒计的持续时间	在SPpartition上打开，用于经过授权的读和写 Closes on SPpartition for authorized read and write	
SPClose	名称	通过码 证书入 证书出	AuthRecord			
CALLS THAT UTILIZE SP'S ABILITY TO HIDE SECRETS AND HIDE BASIC CRYPTOGRAPHY						
SPSignThis	名称	通过码 证书入 证书出	DataToSign	PrivateKeyLocation	SignedData 返回的	
SPCheckThis SPProtHead	名称 名称	通过码 证书入 证书出 通过码 证书入 证书出	DataToCheck Data(Returned)	PrivateKeyLocation MyPublicKey	检查（返回的）位置	
SPProtWrite	名称	通过码 证书入 证书出	Data	MyPublicKey 位置	位置	SPSuccess (返回的)
SPHashThis	名称	通过码 证书入 证书出	DataToHash	散列（返回的）	存储的位置	

注：上面的位置有可能复杂，在其中它们可以指定这个授权具有读或写的权限的其它授权记录，因此位置可以是名称记录编号，一般而言。

图 7