(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 101894224 B
(45)授权公告日 2015.03.18

(21)申请号 200911000231.8
(22)申请日 2009.12.25
(30)优先权数据
12/319,034 2008.12.30 US
(73)专利权人 英特尔公司
地址 美国加利福尼亚
(72)发明人 P·德万
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英
(51)Int.Cl.
G06F 21/10(2013.01)
H04L 29/06(2006.01)
(56)对比文件
US 2005/0033972 A1,2005.02.10, 说明书第[0002]-[0047]段,附图1和2.
US 2005/0251491 A1,2005.11.10, 全文.
CN 101014922 A,2007.08.08, 全文.
审查员 田民丽

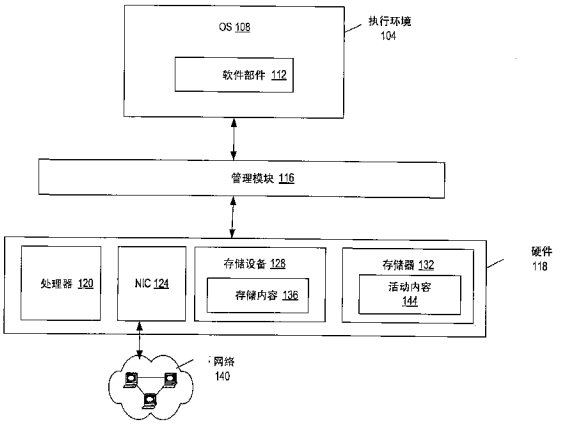
权利要求书2页 说明书13页 附图5页

(54)发明名称

保护客户端平台上的内容

(57)摘要

一种方法、计算机系统和具有指令的计算机可读介质,其提供确保内容免受在接收计算机系统上的恶意软件危害的客户端安全管理层和内容播放器。客户端安全管理层代表部件(例如,运行在计算机系统的处理器上的内容播放器),控制对计算机系统的存储器的保护部分的访问。客户端安全管理层从部件接收加密内容密钥,确认部件的完整性,解密加密内容密钥以提供解密内容密钥,并且响应于确认部件的完整性将解密内容密钥放入存储器的保护部分中。还描述并要求保护了其它实施例。



CN 101894224 B

1. 一种保护客户端平台上的内容的方法，包括：

使用客户端安全管理层，代表部件来控制对计算机系统的存储器的保护部分的访问，以防止由未授权的应用程序来访问所述存储器的保护部分；

从所述部件接收加密的内容密钥；

确认所述部件的完整性；

解密所述加密的内容密钥以提供解密的内容密钥，其中所述解密的内容密钥对应于由所述部件从内容供应者接收的内容；以及

响应于确认所述部件的完整性，将所述解密的内容密钥放在所述存储器的保护部分中，以便所述部件能够解密所述内容并且在所述存储器的保护部分中渲染所述内容。

2. 根据权利要求 1 所述的方法，其中

所述控制对所述存储器的保护部分的访问包括：防止由用于所述计算机系统的操作系统来访问所述存储器的保护部分。

3. 根据权利要求 1 所述的方法，其中

所述部件使用所述解密的内容密钥来解密所述内容。

4. 根据权利要求 1 所述的方法，进一步包括：

从所述部件接收对特定内容的解密请求；以及

在解密所述加密的内容密钥之前，确定针对所述特定内容的内容策略是否允许对所述特定内容进行解密。

5. 根据权利要求 4 所述的方法，其中

在没有连接到提供了所述特定内容的内容服务器的情况下，执行对所述特定内容的内容策略是否允许对所述特定内容进行解密的确定。

6. 根据权利要求 1 所述的方法，其中

所述确认所述部件的完整性包括验证用于所述部件的清单。

7. 根据权利要求 1 所述的方法，其中

所述确认所述部件的完整性包括：确认用于所述部件的代码匹配用于所述部件的代码的标准。

8. 一种保护客户端平台上的内容的方法，包括：

作为部件向客户端安全管理层注册以接收计算机系统的存储器的保护部分的保护；

从内容供应者接收加密的内容和加密的内容密钥；

向所述客户端安全管理层提供所述加密的内容密钥，其中，所述客户端安全管理层确认所述部件的完整性，解密所述加密的内容密钥以提供解密的内容密钥，并且将所述解密的内容密钥放入所述存储器的保护部分中；以及

通过所述部件使用所述解密的内容密钥将所述加密的内容解密，并且将所解密的内容渲染到所述存储器的保护部分中。

9. 根据权利要求 8 所述的方法，进一步包括：

向所述内容供应者提供如下证明：接收的内容被防止受到未授权的拷贝。

10. 根据权利要求 9 所述的方法，其中

所述证明包括用于所述客户端安全管理层的标识信息。

11. 一种保护客户端平台上的内容的装置，包括：

用于使用客户端安全管理层，代表部件控制对计算机系统的存储器的保护部分的访问，以防止由未授权的应用程序来访问所述存储器的保护部分的模块；

用于从所述部件接收加密的内容密钥的模块；

用于确认所述部件的完整性的模块；

用于解密所述加密的内容密钥以提供解密的内容密钥的模块，其中所述解密的内容密钥对应于由所述部件从内容供应者接收的内容；以及

用于响应于确认所述部件的完整性，将所述解密的内容密钥放在所述存储器的保护部分中，以便所述部件能够解密所述内容并且在所述存储器的保护部分中渲染所述内容的模块。

12. 根据权利要求 11 所述的装置，其中

控制对所述存储器的保护部分的访问包括防止由用于所述计算机系统的操作系统来访问所述存储器的保护部分。

13. 根据权利要求 11 所述的装置，其中

所述部件使用所述解密的内容密钥来解密所述内容。

14. 根据权利要求 11 所述的装置，还包括：

用于从所述部件接收对特定内容的解密请求的模块；以及

用于在解密所述加密的内容密钥之前，确定针对所述特定内容的内容策略是否允许对所述特定内容进行解密的模块。

15. 根据权利要求 14 所述的装置，其中

在没有连接到提供所述特定内容的内容服务器的情况下，执行确定针对所述特定内容的内容策略是否允许对所述特定内容进行解密。

16. 根据权利要求 11 所述的装置，其中

确认所述部件的完整性包括验证用于所述部件的清单。

17. 根据权利要求 11 所述的装置，其中

确认所述部件的完整性包括：确认用于所述部件的代码匹配用于所述部件的代码的标准。

18. 一种保护客户端平台上的内容的装置，包括：

用于作为部件向客户端安全管理层注册以接收计算机系统的存储器的保护部分的保护的模块；

用于从内容供应者接收加密的内容和加密的内容密钥的模块；

用于向所述客户端安全管理层提供所述加密的内容密钥的模块，其中，所述客户端安全管理层确认所述部件的完整性，解密所述加密的内容密钥以提供解密的内容密钥，并且将所述解密的内容密钥放入所述存储器的保护部分中；以及

用于通过所述部件使用所述解密的内容密钥将所述加密的内容解密，并且将所解密的内容渲染到所述存储器的保护部分中的模块。

19. 根据权利要求 18 所述的装置，还包括：

用于向所述内容供应者提供如下证明的模块：接收的内容被防止受到未授权的拷贝。

20. 根据权利要求 19 所述的装置，其中

所述证明包括用于所述客户端安全管理层的标识信息。

保护客户端平台上的内容

[0001] 版权声明

[0002] 本文包含的内容是受到版权保护的。当它出现在专利商标局的文件或记录中时，版权所有者不反对任何人复制本专利公开，但是在其它情况下保留对版权的所有权利。

技术领域

[0003] 本公开总体上涉及数字内容的保护。

背景技术

[0004] 数字版权管理是对科技和娱乐业的挑战。通过从互联网非法下载电影和音乐文件，每天会损失数百万美元。到目前为止，实施的解决方案（例如，内容编码方案和高级访问内容系统）对这些数据损失没有提供足够的保护。

[0005] 扩大这些损失是由尝试获得计算机系统的控制和/或窃取数字内容的恶意软件发起的复杂以及进化的攻击。这些攻击可以呈现各种不同的形式，包括从尝试使得软件崩溃到扰乱程序以用于其它目的。运行时间数据的保护（例如，软件程序的代码、配置信息和/或保护在主存储器中以及传送中的内容的密钥）是对科技和娱乐业的特殊的挑战。

附图说明

[0006] 图 1 说明了根据本发明实施例的用于提供对执行环境内的软件部件的保护的平台。

[0007] 图 2 说明了根据本发明实施例的使用并行执行环境的平台。

[0008] 图 3 是示出了根据本发明的一个实施例的用于安全平台的架构的框图。

[0009] 图 4 是内容播放器（例如，图 3 的内容播放器）的操作的方法的流程图，其用于在由图 3 的安全平台架构提供的环境中工作。

[0010] 图 5 是用于与由图 3 的安全平台架构提供的安全环境一起工作的内容服务器的操作的方法的流程图。

[0011] 图 6 是用于提供图 3 的安全平台架构的客户端安全管理层的操作的方法的流程图。

具体实施方式

[0012] 本发明的实施例可以提供一种方法、系统和具有指令的计算机可读存储介质，其用于保护从内容服务器接收的内容并且为接收内容播放器提供保护服务。安全客户端平台向内容服务器提供其完整性的证明。该完整性的证明证明包括：证明证明受保护的“已知的”内容播放器的存在以及对抗设计用于窃取内容的、被称为“内容抓取器 (ripper)”的软件的保护。内容播放器向受到完整性保护的“已知的”内容播放器提供内容密钥。

[0013] 各种实施例可以包括一个或多个元件。元件可以包括安排来执行一些功能的任何结构。按照期望的设计参数或性能约束的给定的组，每个元件可以被实现为硬件、软件或其

任何组合。尽管通过示例在某个拓扑中用有限数量的元件描述了实施例，但是按照期望的给定的实现，在备选拓扑中，实施例可以包括更多或更少的元件。值得注意的是，任何提及的“一个实施例”或“实施例”意味着结合实施例描述的特定特征、结构或特性被包括在至少一个实施例中。在说明书中各种地方中短语“在一个实施例中”的出现并非必然都是指相同的实施例。

[0014] 图 1 说明了根据本发明的实施例的用于保护从内容服务器接收的内容的平台 100。平台 100 可以具有执行环境 104，其可以是执行操作系统 (OS)108 的域。OS 108 可以是用于执行并控制在执行环境 104 内的其它部件 (例如，软件部件 112) 的普通操作的部件，其受到由下面的管理模块 116 提供给选定部件的内部分区 (intra-partition) 存储器访问保护，这将在下文进一步详细讨论。

[0015] 在一些实施例中，部件 112 可以是管理级部件，例如内核部件。在各种实施例中，内核部件可以是服务 (例如，加载程序、调度程序、存储器管理器等)、扩展 / 驱动程序 (例如，用于网卡、通用串行总线 (USB) 接口、磁盘驱动器等) 或服务驱动程序的混合 (例如，用于监视代码的执行的入侵检测器)。可选地，在实施例中，部件 112 可以是应用进程、线程或其它用户空间程序、服务或库。

[0016] 如本文使用的，术语“部件”旨在是指可以使用以获得期望的结果的编程逻辑和关联的数据。术语部件可以与“模块”或“代理”同义并可以是指编程逻辑，其可以体现在硬件或固件中或在软件指令的集合中，可以具有入口和出口点，用例如 C++、Intel 32 位架构 (IA-32) 可执行代码等的编程语言来编写。

[0017] 软件部件可以被编译并且被连接成可执行程序，或被安装在动态链接库中，或可以用解释性语言 (例如，BASIC) 来编写。将理解，软件部件可以从其它部件或从它们自身调用，和 / 或可以响应于检测事件或中断而被调用。可以在机器可存取介质中提供软件指令，当所述指令被访问时可以导致机器进行结合本发明的实施例的部件描述的操作或执行。机器可存取介质可以是固件，例如电可擦除可编程只读存储器 (EEPROM) 或其它可记录 / 不可记录介质，例如只读存储器 (ROM)、随机存取存储器 (RAM)、磁盘存储设备、光盘存储设备等。将进一步理解，硬件部件可以由连接逻辑单元 (例如，门电路和触发器) 组成，和 / 或可以由可编程单元 (例如，可编程门阵列或处理器) 组成。在一些实施例中，本文描述的部件被实现为软件模块，但仍然可以用硬件或固件来表示。此外，虽然可以说明和 / 或描述了仅给定数目的离散软件 / 硬件部件，但是可以在不脱离本发明实施例的精神和范围的情况下，通过额外的部件或更少的部件来表示这种部件。

[0018] 除了执行环境 104 的内部分区选定部件之外，管理模块 116 还可以仲裁对硬件资源 118(例如，一个或多个处理器 120、网络接口控制器 (NIC)124、存储设备 128 和 / 或存储器 132) 的普通部件的访问。

[0019] 处理器 120 可以执行平台 100 的部件的编程指令。处理器 120 可以是单个和 / 或多核心处理器、控制器、专用集成电路 (ASIC) 等。

[0020] 在实施例中，存储设备 128 可以代表非易失性存储设备，其用于存储用于平台 100 上的部件的执行的持久性内容，例如但不限于操作系统、程序文件、配置文件等。在实施例中，存储设备 128 可以包括存储内容 136，其可以代表持久性存储用于部件 112 的源内容。源内容的持久性存储可以包括 :例如，可以具有可执行文件和 / 或代码段的可执行的代码

存储、到其它例程的链接（例如，对动态链接库（DLL）的调用）、数据段等。

[0021] 在各种实施例中，存储设备 128 可以包括集成和 / 或外围存储设备，例如但不限于盘和关联的驱动器（例如，磁的、光的）、通用串行总线（USB）存储设备和关联的端口、闪存存储器、ROM、非易失性半导体器件等。

[0022] 在各种实施例中，存储设备 128 可以是物理上为平台 100 的一部分的存储资源，或可以由平台 100 访问而不必是平台 100 的一部分。例如，可以由平台 100 在网络 140 上经由网络接口控制器 124 来访问存储设备 128。

[0023] 在加载请求（例如，从加载部件或 OS 108 的代理）时，管理模块 116 和 / 或 OS 108 可以将存储内容 136 从存储设备 128 加载到存储器 132 作为活动内容 144 以操作执行环境 104 中的部件 112。

[0024] 在各种实施例中，存储器 132 可以是易失性存储设备，其用于提供用于平台 100 上的部件的操作的活动内容。在各种实施例中，存储器 132 可以包括 RAM、动态 RAM(DRAM)、静态 RAM(SRAM)、同步 DRAM(SDRAM)、双倍数据速率 RAM(DDRRAM)、高速缓存等。

[0025] 在一些实施例中，存储器 132 可以将其中存储的内容组织到多组存储器单元中。可以是固定和 / 或可变大小的这些组织的组可以便于虚拟存储器管理。存储单元的组可以是页、段或其组合。

[0026] 使用分页的虚拟存储器可以便于对具有较小的物理存储器页的大的逻辑 / 线性地址空间进行仿真。所以，执行环境 104 可以提供虚拟的执行环境，其中部件可以工作，然后可以将所述部件映射到存储器 132 的物理页面。由 OS 108 和 / 或管理模块 116 维护的页表可以将由执行环境 104 的部件提供的逻辑 / 线性地址映射到存储器 132 的物理地址。

[0027] 在各种实施例中，可以选择部件 112 或其部分以进行内部分区以将保护服务提供给部件 112。例如，部件 112 可以代表内容播放器，其用于从内容服务器接收内容。管理模块 116 可以识别并隔开部件 112 的部分以由 OS108 或其它部件控制对部件 112 的访问。分区的部分可以包括特定部件的任何部分，直到全部。分区的部分可以物理地或虚拟地与在相同执行环境内的其它部件隔离，以使得如果需要的话，可以由下面的平台监视并限制内部执行环境访问。内部分区可以在不需要部件 112 工作在具有独立的 OS 的完全独立的执行环境的情况下，便于例如部件 112 与 OS 108 的隔离。内部分区还可以在以某种方式（例如，由恶意软件、rootkit、关键运行时间故障等）损害的执行环境 104 内，向部件 112 提供来自其它部件的相似或更高特权级别的保护。本发明的实施例可以提供保护服务同时仍允许在部件 112 与执行环境 104 的其它部件（例如，OS 108）之间许可的交互。由 OS 108 控制对部件 112 的访问可以包括各种级别的访问限制。

[0028] 在各种实施例中，用于保护执行环境内的内容的部件的内部分区可以用于具有多执行环境（例如，工作在允许虚拟化技术（VT）的平台中的虚拟机）的平台。在这种实施例中，管理模块可以包括虚拟机监视器（VMM）或是虚拟机监视器（VMM）的一部分。

[0029] 在可信计算组（TCG）标准化团体中定义了硬件的平台证明和管理程序。由 TCG 定义的证明机制包括提供对“测量的代码”运行在客户端平台上的事实的证明。通过比较当前版本的代码与原始的“金标准（goldstandard）”版本的代码来“测量”代码。来自原始的“金标准”的代码中的任何变化指示了代码被篡改，可能由病毒或其它恶意软件对其进行了改写。

[0030] 在TCG标准下为了平台证明通常测量的代码包括:代码,例如识别并初始化系统硬件部件的BIOS代码以及管理程序代码。管理程序允许多个操作系统运行在主计算机系统上,并且还被称为“虚拟机监视器”。对平台证明的测量通常不会扩展到操作系统或应用程序,因为当今极多版本的操作系统和应用程序是可用的。有如此多可用的版本的操作系统和应用程序,维护每个版本代码的确认原始“金标准”副本以与测量的代码进行比较被认为是难以管理的负担。

[0031] 于2007年8月2日递交的、名称为“Secure Vault Service for SoftwareComponents within an Execution Environment”的专利申请11/229,126被转让给本申请的受让人,并通过引用全文将其并入到本文中。专利申请11/229,126描述了可以用于测量并保护在虚拟机内的操作系统和应用程序部件的安全保险库服务(Secure Vault Service)。由运行在比操作系统高的特权级的虚拟机监视器来提供安全保险库服务。因此,安全保险库服务可以即使在系统中操作系统被损害的情况下保护系统上的数据和程序部件。提供安全保险库服务的虚拟机监视器在本文被称为“客户端安全管理层”。

[0032] 图2说明了根据本发明的实施例的使用虚拟化来为部件提供并行执行环境和保护服务的平台200。在各种实施例中,平台200可以类似于图1的平台100并且基本上可以与图1的平台100互换。此外,下文所述的元件可以类似于如上所描述的相同命名的元件并且基本上可以与如上所描述的相同命名的元件互换,并且反之亦然。

[0033] 在该实施例中,平台200上的管理模块(例如,虚拟机监视器(VMM)204)可以向一个或多个独立运行的执行环境或“虚拟机(VM)”(例如,客户VM 228和辅助VM 232)呈现平台硬件208(例如,一个或多个处理器212、网络接口控制器(NIC)216、存储设备220和/或存储器224)的多个抽象和/或视图。辅助VM 232可以用于执行从客户VM 228独立地或安全地分离的代码,并且可以防止客户VM 228的部件执行可以改变、修改、读取或影响辅助VM 232的部件的操作。虽然平台200示出了两个VM,但是其它实施例可以使用任何数量的VM。

[0034] 在客户VM 228和辅助VM 232中工作的部件中的每一个可以如同它们运行在专用计算机而不是虚拟机上一样工作。也就是说,在客户VM 228和辅助VM 232中工作的部件中的每一个可以期望控制各种事件并且具有对硬件208的完全访问。VMM 204可以管理对硬件208的VM访问。可以以软件(例如,作为独立程序和/或主机操作系统的部件)、硬件、固件和/或其任何组合来实现VMM 204。

[0035] 客户VM 228可以包括OS 236和部件240。在指定的事件发生时,VMM204可以识别并隔开部件240的不同部分以控制OS 236或其它部件对分区部分的访问。一个或多个这些分区部分可以用于代表内容播放器,其用于从内容服务器接收内容。在各种实施例中,指定的事件可以是何时将存储内容244从存储设备220加载到存储器224作为活动内容248或者何时部件240请求保护。然而,在各种实施例中,可以额外/可选地使用其它指定的事件。

[0036] 部件240可以向VMM 204注册,并且更具体地说,向用于保护的VMM204的完整性服务模块(ISM)252注册。在各种实施例中,注册可以在发生注册事件(例如,周期性地将活动内容248加载到存储器224)时发生,和/或以一些其它事件驱动方式发生。在各种实施例中,可以由部件240、VM 228内的另一个部件(例如,OS 236)VMM 204或VM 232的部

件来启动注册。

[0037] 在接收注册时，ISM 252 可以与工作在 VM 232 中的完整性测量模块 (IMM)256 合作来认证并验证部件 240 的完整性。部件 240 的完整性的认证和验证可以有助于防止未授权的修改和 / 或恶意的终止，并且可以确保如由管理员、用户或其它策略所定义的，可以仅向识别的部件提供保护。IMM256 可以工作在 OS 260 的上下文中的 VM 域 232 中或工作在独立的硬件中，所以可以很大程度上独立于 OS 236。通过在 VM 228 的上下文之外运行，IMM 256 可以具有不出现在 OS 236 的上下文中或可能在 OS 236 的上下文中被损害的准确并可靠的存储器测量能力。

[0038] IMM 256 可以向 ISM 252 提供对验证请求的响应，例如通过、失败、有条件的通过 (pass w/qualification)、有条件的失败 (fail w/qualification) 等。在各种实施例中，条件可以反映在通过和失败之间的完整性验证的程度。IMM 256 有效地识别或认证部件及其数据，并且保证其在存储器中具有期望的、正确的形式。

[0039] 在一些实施例中，活动内容 248 可以包括完整性清单，其可以是在部件 240 的完整性的验证中使用的信息的集合。在各种实施例中，完整性清单可以包括一个或多个完整性校验值和 / 或对固定位置的重定位，其覆盖存储内容 244(例如，代码存储和 / 或静态的和 / 或配置设置 / 数据)。IMM 256 可以访问来自活动内容 248 的完整性清单，并且验证部件 240 全部或部分地对应于完整性清单。IMM 256 可以通过验证在完整性清单结构上的加密签名来验证完整性清单自身的可靠性以确保没有改变其正确形式。可以通过例如逐字节分析或通过加密散列分析来完成对映像的比较。

[0040] 在各种实施例中，IMM 256 可以例如通过直接存储器访问 (DMA) 或直接物理存储器访问来在存储器 224 中直接搜索活动内容 248。在各种实施例中，可以例如通过 ISM 252 将部件 240 的线性地址提供给 IMM 256，并且 IMM 256 可以执行虚拟到物理映射以识别活动内容 248 的物理存储单元。在实施例中，VMM 204 可以提供向 IMM 256 提供特殊接口以提供对活动内容 248 的访问。

[0041] 在各种实施例中，可以在当部件 240 正在执行时，周期性地和 / 或以某种其它事件驱动方式进行初始的注册，对活动内容 248 进行完整性测量。在初始的注册请求或对事件处理的请求时的完整性测量可以有助于基于在其被制造或最后加载时的内容的状态来确定活动内容 248 和 / 或存储内容 244 的初始状态。周期性的或事件驱动的完整性测量可以有助于检测不适当地改变活动内容 248 和 / 或存储内容 244 的保护属性的攻击。

[0042] 在 2005 年 6 月 30 日递交的、名称为“Signed Manifest for Run-timeVerification of Software Program Identity and Integrity”的美国专利申请 No. 11/173,851 ;2005 年 12 月 30 日递交的名称为“Identifier Associated withmemory Locations for Managing Memory Accesses”的美国专利申请 No. 11/322,669 以及 2006 年 3 月 30 日递交的名称为“Intra-Partitioning of SoftwareComponents within an Execution Environment”的美国专利申请 No. 11/395,488 中描述了部件的完整性测量的其它细节，所有所述专利申请通过引用其实体并入到本文中。

[0043] 再参考图 2，ISM 252 可以从 IMM 256 接收反映对活动内容 248 的存储器中的完整性和位置的验证的响应。如果验证失败，则 ISM 252 拒绝请求并可以触发警报。如果验证通过，则 ISM 252 可以与存储器管理器 264 合作以对部件 240 的部分进行内部分区以保护

服务。这里，可以在存储器中的保险库或隐藏页周围建立保护，所以可以仅由验证的部件和/或部件自身的全部来访问它们。

[0044] 虽然图2说明了执行环境是虚拟分区，但是其它实施例可以通过其它机制（例如，使用服务处理器、保护执行模式（例如，系统管理模式SMM或安全执行模式SMX）和/或嵌入式微控制器）提供各种执行环境。在各种实施例中，可以经由各种不同类型的分区将辅助环境与主机环境隔开，所述分区包括如上所述的虚拟分区（例如，虚拟化技术(VT)方案中的虚拟机）和/或完全独立的硬件分区（例如，使用活动管理技术(AMT)、“可管理引擎”(ME)、使用隔离平台资源的平台资源层(PRL)、系统管理模式(SMM)和/或其它类似的或相似的技术）。在各种实施例中，VT平台还可以用于实现AMT、ME和PRL技术。

[0045] 参考图1和2如上所描述的平台可以用于保护从内容服务器接收的内容并为接收内容播放器提供保护服务。

[0046] 图3是示出了根据本发明的一个实施例的用于安全平台300的架构的框图。安全平台300将其完整性的证明提供给远程处理系统（例如，内容服务器360）。该完整性的证明包括证明受保护的“已知的”内容播放器330的存在以及对被称为设计用于窃取内容的“内容抓取器”的软件的防护。内容服务器360将加密内容随内容密钥一起提供给受完整性保护的“已知的”内容播放器330。安全平台300包括客户端安全管理层310，其用于保护系统存储器340中的内容和内容密钥。由客户端安全管理层310将内容密钥仅发布给其代码被验证并确认的授权“已知的”内容播放器330。

[0047] 客户端安全管理层310在用于内容播放器的存储器的保护部分342中提供对存储器340内的内容播放器的代码、数据和帧缓冲的保护。例如，为了由内容播放器330来使用，由操作系统内核320分配的保护代码344、保护数据346和保护的帧缓冲存储器348仅可以由内容播放器330访问并与其它应用程序隔离。客户端安全管理层310确保不可以通过截取由内容播放器330放入帧缓冲器的帧、读取存储器340或从持久性存储设备或从网络信道（例如，通信链路350）读取文件来“窃取”内容。防止由未授权的应用程序以及由操作系统访问用于内容播放器的存储器的保护部分342。

[0048] 安全平台300可以使用如上所描述的专利申请11/229,126的客户端安全管理层的功能来测量并保护客户端内容播放器330、包括保护的帧缓冲存储器348的、由客户端内容播放器330使用的存储器340以及存储在存储器340中的数据（例如，保护代码344和保护数据346）。此外，安全平台300使用由客户端安全管理层310提供的平台证明来向内容供应者（例如，内容服务器360）确保动态内容将在客户平台300上受到保护。

[0049] 安全平台300向远程内容服务器360证明：即使内容的授权用户是恶意的或客户端平台300安装了恶意软件，也不可以以未授权的方式来复制由远程服务器提供的内容。可以提供该证明，因为客户端安全管理层310防止了对其中存储了内容的存储器340的未授权访问（使用用于内容播放器的存储器的保护部分342）。响应于所述证明，内容服务器360将用内容密钥加密的内容提供给客户端平台300。由于由客户端安全管理层310在安全平台300中提供的保护，即使授权用户也不能使用内容抓取软件来对内容进行非法拷贝。

[0050] 在一个实施例中，内容播放器330用于在不将用户限定到特定硬件实例的情况下将内容密钥从一个平台转移到另一个平台。例如，如果发生系统故障，则可以使用该迁移功能，以使得已知的并验证的内容播放器330可以重新安装在不同的硬件上。这种迁移除了

内容播放器 330 的所需的认证之外，还需要测量、验证并认证的新硬件平台。在另一个实施例中，安全平台 300 包括另一个授权并保护的应用程序（未示出），其用于允许将内容密钥从一个平台上的授权内容播放器 330 转移到另一个平台上。在下文进一步详细讨论平台的测量和认证。

[0051] 在一个实施例中，安全平台 300 包括平台硬件 302，其是提供了硬件扩展以增强平台的安全能力的 Intel ®可信执行技术 (TXT) 平台。在 BIOS 中允许测量的引导以提供平台证明能力。通过允许测量引导，在以系统重置指令开始的引导处理期间执行的所有指令被测量，并且测量被记录。然后，测量可以与期望的软件和固件的“金标准”副本进行比较以确定指令是否与期望的软件和固件一致。

[0052] 可选地，在一个实施例中，平台硬件 302 包括由用户允许的可信平台模块 (TPM)304。将概括地描述 TPM 的功能，随后是对当其工作在平台 300 内时 TPM 304 的说明。TPM 是硬件部件，通常是微控制器，其驻留在处理系统内并提供用于增强处理系统的安全性的各种设施和服务。可以根据规范（例如，日期为 2003 年 10 月 2 日的可信计算组 (TCG) TPM 规范版本 1.2（下文称为“TPM 规范”），其可以从互联网 www.trustedcomputinggroup.org/home 获得）来实现 TPM。

[0053] TCG 兼容的 TPM 安全地存储密钥、口令和数字证书。TPM 提供可以生成在数字证书中使用的密钥、创建数字签名并且提供加密的核心安全技术。通过使用定义的接口的安全子系统来访问和控制安全操作。像硬盘加密、安全电子邮件和身份 / 访问管理的应用程序受益于由 TPM 提供的安全功能。

[0054] TPM 基于特征（例如，包括处理器和芯片组的平台的硬件部件以及驻留在平台中的软件（例如，固件和操作系统）来证明平台的身份和 / 或完整性。TPM 还可以支持软件进程的审核和记录以及平台引导完整性、文件完整性和软件许可证的验证。TPM 通常被描述为为平台提供信任的根。

[0055] TPM 通过存储关于平台的配置的信息来提供安全功能。然后，该信息可以用于 TPM 的主要功能、平台证明和受保护的存储。平台可以将信息提供给需要的远程实体以允许远程实体确定平台的可信赖性。平台还可以指示 TPM 确保仅在系统处于已知的“好的”配置时才发布密钥或敏感数据。

[0056] 为了存储平台状态，TPM 使用平台配置寄存器 (PCR，例如图 3 的 TPM304 的 PCR 306)，其用于存储以软件的 160 位 SHA1（安全散列算法 1）散列的形式的测量以及对平台的配置信息。这些测量在引导模块处开始。每个引导部件测量下一个部件，将测量记录在 TPM 中，然后运行该部件直到操作系统接管其核心的测量为止。因为向 PCR 的每次写入都将测量增加到寄存器而不是覆盖先前的测量，所以没有实体可以改变由前面的部件所作出的对其代码的测量。因此，得到测量的链，以使得如果链的开始（被称为测量的信任的根）和每个链路都是可信赖的，那么整个链是可信赖的。

[0057] 证明是指允许平台以可信赖的方式将其配置报告给远程方的 TPM 功能和协议的设置。例如，TPM 提供了对用于存储平台状态的 PCR 进行签名的能力。例如，平台可以使用证明身份密钥 (AIK) 来对 PCR 进行签名。这种签名的 PCR 可以被称为引用。

[0058] 为了将由真实 TPM 对引用进行签名的证据提供给远程实体，每个 TPM 具有一组证书。例如，由 TPM 制造商签名的签注证书说明了 TPM 满足 TPM 规范。制造商还将被称为签

注密钥 (EK) 的唯一密钥存储在 TPM 中，并且制造商使用 EK 来对签注证书进行签名。理论上，可以直接使用 EK 来对 PCR 的引用进行签名。然而，因为 EK 是唯一的，所以在一些实现中，使用第三方来代替以提供保密。具体地说，平台使用被称为保密认证机构 (CA) 的第三方来为每个 AIK 创建身份证书。TCG 定义了协议，其允许 TPM 使用 EK 和签注证书向保密 CA 证明 TPM 是真的 TPM。继而，保密 CA 为 TPM 声称其拥有的 AIK 创建身份证书。

[0059] 假定远程实体信任 TPM 的制造商、保密 CA 和用于测量的信任的根，则由附有身份证书的 AIK 签名的引用是平台的当前状态的加密证据。可以用于允许可信平台的远程认证的另一个加密协议是直接匿名证明 (DAA)。

[0060] TPM 提供的另一组服务是密钥及其它数据的安全存储。TPM 可以创建 Rivest-Shamir-Adleman(RSA) 密钥，它将只允许使用一次 (a) 请求者经由机密 SHA1 散列提供授权，以及 (b) 如由 PCR 确定的当前配置指示了“好的”状态。该功能允许平台加密数据，以使得如果机器被损害、从外部介质引导或被篡改，则数据将仍然不可访问。

[0061] 为支持服务（例如，安全存储设备），TPM 为不同的操作创建具有单个目的类型的密钥。类型 EK 的密钥仅对从保密 CA 中解密身份证书是可用的。AIK 用于对其它密钥进行签名并且引用 PCR。存储设备密钥 (SK) 用于保护其它密钥或“密封”数据，其是使用口令或 PCR 绑定来保护数据的数据的专用加密。绑定密钥 (BK) 用于加密任意数据并将数据转换成 TPM 绑定的数据结构。签名密钥 (SigK) 用于对任意数据进行签名。

[0062] 再次参考图 3，在一个实施例中，客户端安全管理层 310 向内容服务器 360 提供平台证明，其证明了接收的内容受到保护。作为响应，内容服务器 360 提供加密内容以及加密了的内容密钥。在一个实施例中，针对客户端安全管理层 310，使用证明身份密钥 (AIK) 的公开部分来加密内容密钥。内容、加密内容密钥和内容策略被发送给客户端内容播放器 330。客户端内容播放器 300 向客户端安全管理层 310 证明其完整性，并且客户端安全管理层 310 将解密内容密钥提供给保护存储器 342 中的授权客户端内容播放器 330。由客户端安全管理层 310 提供的解密内容密钥可以考虑到关于内容播放器 330 的、由客户端安全管理层 310 维护的策略。客户端内容播放器 330 解密内容并且将内容移交给保护的帧缓冲存储器 348，所述存储器 348 在受保护以供内容播放器 330 使用的内容播放器 342 的存储器的保护的部分内。因此，内容抓取器软件不能从持久性存储设备、存储器 340、保护的帧缓冲存储器 348 或网络信道 350 中的任何一个中窃取内容。该机制防止对为了内容保护在图形硬件中允许加密的昂贵硅栅极的需要，并且跨越离散或集成的图形适配器工作。

[0063] 在一个实施例中，平台硬件 302 的 TPM 304 具有用于签名的证明身份密钥 (AIK) 和用于加密的 AIK。这些 AIK 可以存储在 PCR 306 中并可以由保密认证机构或使用直接匿名证明 (DAA) 来认证。TPM 304 还可以获得显示作为客户端安全管理层密钥 316 的、专用于客户端安全管理层 310 的 AIK。客户端安全管理层 310 使用客户端安全管理层密钥 316 来向远程处理系统（例如，内容服务器 360）断言平台 300 的可信赖性。

[0064] 通过了解计算机系统内的不同架构部件具有对资源访问的不同级别，可以进一步了解平台 300 的架构中客户端安全管理层 310 的角色。保护环是在计算机系统的架构内的分层的级别或层级的特权的组中的一个。通常由固件层处提供了不同的处理器模式的一些处理器架构通过硬件来实施特权的使用。环被布置在从最高特权（最可信，通常编号为 0）到最低特权（最不可信，通常具有最高环数）的分层中。在大部分操作系统上，环 0 是具有

最高特权的级并与物理硬件（例如，处理器和存储器）基本上直接交互。Intel 虚拟化技术 (VT-x) 平台扩展了该概念，其包括比环 0 级更可信的“根”特权级。在引导平台时，测量在根特权级处运行的代码。在一个实施例中，如图 3 所示的根特权级是如在 Intel VT-x 平台中定义的根特权级，尽管本发明不限制于此。可以想象，可以使用备选的虚拟化技术来实现客户端安全管理层 310，所述虚拟化技术可以允许在比由传统的操作系统内核代码所使用的环 0 级更可信的特权级处发生一些操作。

[0065] 在图 3 中示出了如在根特权级处工作的客户端安全管理层 310，其具有比工作在环 0 特权级的操作系统内核 320 更高的特权。在引导平台 300 时，测量用于客户端安全管理层 310 的代码。因此，在引导平台 300 以后，TPM304 的 PCR 寄存器 306 具有包括对客户端安全管理层 310 的代码的测量的 SHA-1 散列值。针对客户端安全管理层 310，生成客户端安全管理层密钥 316（如由 TPM 304 产生的 AIK）。

[0066] 在图 3 中，操作系统内核 320 工作在比应用程序（例如，内容播放器 330）高的环 0 特权级，所述播放器 330 工作在环 3 特权级。通过工作在根特权级处（所述根特权级是甚至比环 0 高的特权级），客户端安全管理层 310 能够确保在存储器 340 内的用于内容播放器的存储器的保护部分 342 是不可访问的，即使对操作系统内核 320 来说也是不可访问的。

[0067] 客户端安全管理层 310 包括运行时间存储器保护部件 312 和内容保护管理器 314。运行时间存储器保护部件 312 在用于内容播放器的存储器的保护部分 342 内，对保护代码 344 和保护数据 346 两者以及保护的帧缓冲存储器 348 进行保护。运行时间存储器保护部件 312 可以使用如上所描述的在专利申请 11/229,126 中描述的安全保险库服务功能来在用于内容播放器的存储器的保护部分 342 内对保护代码 344、保护数据 346 以及保护的帧缓冲存储器 348 进行保护。例如，保护代码 344 可以包含数据链接库、可执行代码及与保护部件有关的其它软件（例如，内容播放器 330）。保护数据 346 可以包含例如数据（例如，由内容播放器 330 从内容服务器 360 下载的内容以及用于下载内容的加密与解密密钥）。相似地，保护的帧缓冲存储器 348 由内容播放器 330 来使用以由用户渲染用于显示的内容。通过限制对用于内容播放器的存储器的保护部分 342 的访问，在运行在环 0 特权级的操作系统内核 320 或运行在环 3 特权级的其它应用程序受到损害的情况下，客户端安全管理层 310 的运行时间存储器保护部件 312 提供保护。

[0068] 客户端安全管理层 310 的内容保护管理器 314 使用由平台硬件 302 的 TPM 304 提供的安全特征来证明平台 300 的可信赖性。例如，客户端安全管理层 310 使用客户端安全管理层密钥 316 来向远程处理系统（例如，内容服务器 360）断言平台 300 的可信赖性，所述密钥 316 可以是例如由 TPM304 生成的 AIK。下文进一步详细描述客户端安全管理层 310 的内容保护管理器 314 的操作。

[0069] 图 4 是用于在由图 3 的安全平台架构提供的环境中工作的内容播放器（例如，图 3 的内容播放器 330）的操作的方法的流程图。参考图 4 执行的操作被描述为由图 3 的部件来执行。在启动时，内容播放器 330 转移到“针对存储器和内容保护，向客户端安全管理层注册”的步骤 410。在该步骤，内容播放器 330 调用对客户端安全管理层 310 的超级调用以提供存储器的保护部分 342，以保护其代码和数据，其包括所述代码和数据的动态链接库以及用于渲染内容的帧缓冲存储器 348。对客户端安全管理层 310 的这些超级调用可以调用上面引用的专利申请 11/229,126 中概述的安全保险库服务。一旦客户端安全管理层 310 例

如通过提供用于内容播放器的存储器的保护部分 342 来向内容播放器 330 提供该保护时，不可以由不具有与内容播放器 330 相同的来自客户端安全管理层 310 的访问许可的任何环 0 或环 3 的部件来访问用于内容播放器 330 的保护代码 344、保护数据 346 和保护的帧缓冲器 348。

[0070] 作为向客户端安全管理层 310 的注册处理的一部分，可以创建用于内容播放器 330 的清单以及应用程序标识符。可以根据上面引用的于 2005 年 6 月 30 日递交的、名称为“Signed Manifest for Run-Time Verification ofSoftware Program Identity and Integrity”的专利申请 11/173,851 来创建该清单。清单可以包含可以用于验证内容播放器 330 的完整性并且可以由客户端安全管理层 310 在随后的交互中确认内容播放器 330 的完整性的信息。

[0071] 再次参考图 4，在最初“针对存储器和内容保护，向客户端安全管理层注册”步骤 410 中，向客户端安全管理层 310 注册之后，内容播放器 330 转移到“从客户端安全管理层请求安全信息”步骤 420。在一个实施例中，内容播放器 330 请求的安全信息包括用于客户端安全管理层 310 的 PCR 值。响应于对安全信息的请求，客户端安全管理层 310 提供包含 TPM 中的特定 PCR 寄存器的 PCR 值的签名的团点 (blob)。使用 AIK 签名密钥对团点进行签名。团点还包含客户端安全管理层 310 的 AIK 加密密钥的公开部分以及从保密认证机构接收的证书。在本文描述的实施例中，安全信息被描述为根据基于 AIK 的加密方案来进行管理。本领域的普通技术人员将了解，可选地，还可以使用其它方案（例如，保护用户的保密的直接匿名证明）来管理安全信息。

[0072] 内容播放器 330 从“从客户端安全管理层请求安全信息”步骤 420 转移到“从内容服务器请求内容，提供来自客户端安全管理层的安全信息”步骤 430。内容播放器 330 使用由客户端安全管理层 310 提供的安全信息来向内容服务器 360 证明平台 300 是安全的。内容请求包含用于内容服务器的内容播放器的账户的用户证书、从客户端安全管理层 310 接收的签名的团点以及请求内容的策略参数。例如，策略参数可以指示在用于播放视频的用户的许可证到期之前允许用户播放内容的视频的时间的数量。参考图 5 进一步详细描述了内容服务器 360 对请求内容的处理。

[0073] 内容播放器 330 从“从内容服务器请求内容，提供来自客户端安全管理层的安全信息”步骤 430 转移到“从内容服务器接收内容和加密内容密钥”步骤 440。内容播放器 330 从内容服务器 360 中接收封装的团点，所述团点包括加密内容和加密内容密钥。然后，内容播放器 330 转移到“从客户端安全管理层请求解密密钥”步骤 450。内容播放器 330 将加密内容密钥（下文参考图 5 进一步详细描述）与其自身的应用程序标识符一起传递到客户端安全管理层 310。下文参考图 6 进一步详细讨论了客户端安全管理层 310 对加密内容密钥的处理。

[0074] 响应于“从客户端安全管理层请求解密密钥”步骤 450，内容播放器 330 接收解密密钥，内容播放器 330 使用所述解密密钥可以解密由内容服务器 360 提供的加密内容。内容播放器 330 进入“使用由客户端安全管理层提供的解密密钥来解密内容”步骤 460 并解密由内容服务器 360 提供的内容。内容播放器 330 将加密内容加载到用于内容播放器的存储器的保护部分 342 中并使用解密密钥来解密所述内容。内容播放器 330 进入到“渲染内容”步骤 470，其中，内容播放器 330 使用包括在保护代码 344 中的标准应用程序接口来在

保护帧缓冲器上渲染解密内容。解密内容被直接写入用于内容播放器的存储器的保护部分342内的保护数据346，而不是调用操作系统内核320以渲染内容。

[0075] 图5是用于与本发明的安全平台一起工作的内容服务器的操作的方法的流程图。响应于从内容播放器330接收对内容的请求，内容服务器360验证如“验证来自内容播放器的对内容的请求以及来自客户端安全管理层的安全信息”步骤510中所示的请求。例如，内容服务器360可以针对保密认证机构的根证书，验证签名的团点中提供的客户端安全管理层310的证书。随后，内容服务器360可以比较PCR寄存器的散列值与所述散列值的金标准副本，由此确定客户端安全管理层310的有效性。此外，内容服务器360可以针对用户数据库来认证用于内容播放器330的用户证书并且检查作为请求的一部分的策略参数。例如，可以根据当将在内容请求中提供策略中的值与在服务数据库中存储的用户的策略进行比较时哪个策略更有约束性来提供内容。

[0076] 内容服务器360从“验证来自内容播放器的对内容的请求以及来自客户端安全管理层的安全信息”步骤510转移到“创建包含加密内容和加密内容密钥的封装团点”步骤520。在一个实施例中，内容服务器360用被称作内容密钥(CK)的对称密钥来加密内容，并用客户端安全管理层310的AIK加密密钥来加密CK、内容策略(CP)和应用程序标识符(AI)。例如在该实施例中，按照如下使用用于内容服务器360的服务密钥来创建封装的团点：

[0077] BLOB = Sign service-key(E CK(Content) ‖ E AIK-Encryption(CK ‖ CP ‖ AI))。在该公式中，通过使用签名的服务密钥来创建团点以加密由两个分量组成的串接字符串。第一分量使用内容密钥加密内容，而第二分量加密内容密钥、内容策略和具有证明身份密钥的证明标识符的串接字符串。在“将加密内容和加密内容密钥提供给验证的内容播放器”步骤530中，将封装的团点发送回内容播放器330。

[0078] 图6是用于提供图3的安全平台架构的客户端安全管理层的操作的流程图。如参考图4“针对存储器和内容保护，向客户端安全管理层注册”步骤410所描述的，客户端安全管理层310响应于应用程序的注册请求。响应于这种注册请求，客户端安全管理层310转移到“响应于部件的注册，提供存储器和内容保护”步骤610。可以按照上述参考客户端安全管理层310的运行时间存储器保护部件312来提供存储器保护。如上所述，客户端安全管理层310的运行时间存储器保护部件312保护在用于内容播放器的存储器的保护部分342内的保护代码344、保护数据346和保护的帧缓冲存储器348。运行时间存储器保护部件312可以使用如上所描述的在专利申请11/229,126中描述的安全保险库服务功能来保护用于内容播放器的存储器的保护部分342内的保护代码344、保护数据346和保护的帧缓冲存储器348。

[0079] 尽管关于图6提供的服务被描述为由客户端安全管理层310来执行，但是可以由客户端安全管理层310的内容保护管理器314来提供内容保护。如“从部件接收解密请求”步骤620中所示，客户端安全管理层310可以从部件接收解密请求。响应于这种解密请求，客户端安全管理层310可以转移到“确认部件的完整性”的步骤630。在确认部件的完整性中，客户端安全管理层310可以针对封装团点中由内容服务器360提供的应用程序标识符来验证解密请求中由内容播放器330提供的应用程序标识符。客户端安全管理层310可以进一步执行其它完整性测量以验证内容播放器330的完整性，例如在将解密密钥提供给内

容播放器 330 之前验证用于内容播放器 330 的清单。

[0080] 响应于确认部件的完整性，客户端安全管理层 310 可以解密返回到内容播放器 330 的封装的团点中的内容服务器 360 提供的内容密钥以及其它参数。客户端安全管理层 310 可以针对内容策略来验证解密请求并且还可以将来自封装的团点的策略信息记录到策略数据库（使用未保护的环 3 应用程序）。通过在将解密内容密钥提供给内容播放器 330 之前，针对内容策略来验证解密请求，即使客户端内容播放器 330 不再连接到用于内容服务器 360 的网络时，客户安全管理层 310 可以在传送了内容之后，实施提供内容服务器 360 所需的策略。

[0081] 然后，控制从“确认部件的完整性”步骤 630 转移到“将解密密钥放入用于部件的保护存储器中”步骤 640，其中，客户端安全管理层 310 和 / 或客户端安全管理层 310 的运行时间存储器保护部件 312 将解密密钥放入部件的存储器的保护部分，例如用于内容播放器的存储器保护部分 342。

[0082] 概述的机制在不需要额外的硬件的情况下使用标准特征在平台上提供内容保护。由于本发明通过将保护器放在比保护内容（即，内容播放器）高的特权的级处来使用合理的加密技术，所以由本发明的客户端安全管理层提供的保护服务相比于其它基于模糊的技术提供更严密的防护。概述的机制允许远程内容服务供应者来将内容分发到对攻击者具有高度抵抗力的客户端。该机制是不被入侵的并且不需要修改平台硬件、操作系统或额外的驱动器。

[0083] 可以以硬件、软件或这种实现方式的组合来实现本文公开的机制的实施例。本发明的实施例可以被实现为在可编程系统上执行的计算机程序，所述系统包括至少一个处理器、数据存储系统（包括易失性和非易失性存储器和 / 或存储元件）、至少一个输入设备和至少一个输出设备。

[0084] 可以将程序代码应用到用于执行本文描述的功能并且生成输出信息的输入数据。本发明的实施例还包括机器可访问介质，其包含用于执行本发明的操作的指令或者包含设计数据（例如，HDL，其定义了结构、电路、装置、处理器和 / 或本文描述的系统特征）。这种实施例还可以被称为程序产品。

[0085] 这种机器可访问存储介质可以包括但不限制于由机器或器件制造或形成的颗粒的有形排列，其包括 :例如，硬盘和任何其它类型的盘，其包括软盘、光盘、只读紧致盘存储器 (CD-ROM)、可重写紧致盘 (CD-RW) 和磁光盘、半导体器件（例如，只读存储器 (ROM))、随机存取存储器 (RAM)(例如，动态随机存取存储器 (DRAM)、静态随机存取存储器 (SRAM))、可擦除可编程只读存储器 (EPROM)、闪存、电可擦除可编程只读存储器 (EEPROM)、磁或光卡，或适合于存储电子指令的任何其它类型的介质。

[0086] 可以以已知的方式将输出信息应用到一个或多个输出设备。对该申请的目的来说，处理系统包括具有处理器的任何系统，所述处理器例如是数字信号处理器 (DSP)、微控制器、专用集成电路 (ASIC) 或微处理器。

[0087] 可以以高层的过程或面向对象编程语言来实现程序以与处理系统进行通信。如果需要，还可以以汇编或机器语言来实现程序。实际上，本文描述的机制不被限制在任何特定的编程语言的范围内。在任何情况下，语言可以是编译的或解释的语言。

[0088] 本文呈现的是用于向从内容服务器接收的内容提供安全平台的方法和系统的实

施例。虽然示出了并描述了本发明的特定实施例，但是对本领域的这些技术人员明显的是，在不脱离所附权利要求的范围的情况下，可以进行多种改变、变化和变型。因此，本领域的一个技术人员将认识到，在不脱离本发明的宽广的方面的情况下，可以进行改变和变型。所附权利要求将包括落入本发明的真正范围和精神内的所有这种改变、变化和变型。

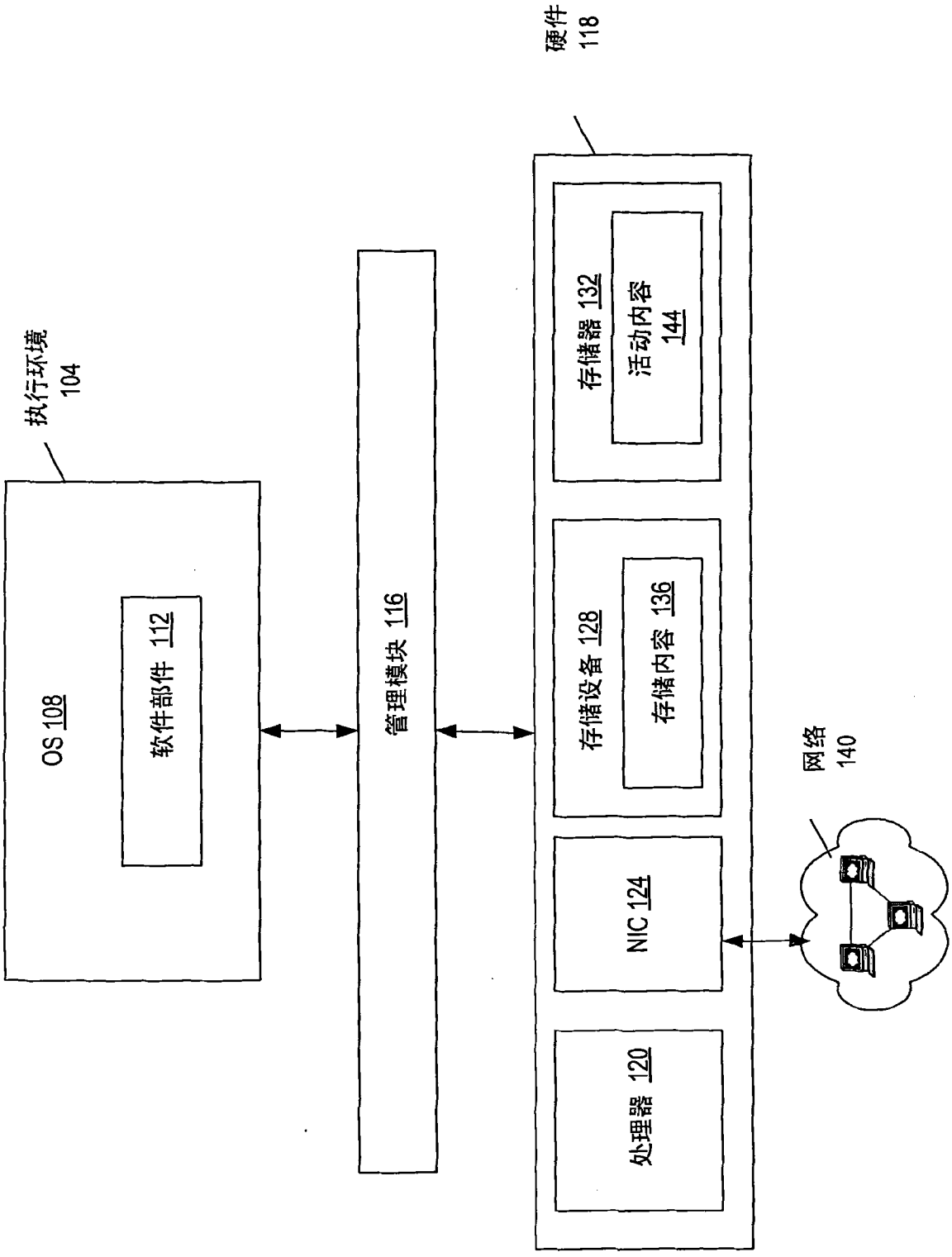

硬件
118
执行环境
104
OS 108
软件部件 112
管理模块 116
存储器 132
活动内容
144
存储设备 128
存储内容 136
NIC 124
处理器 120
网络
140

图 1

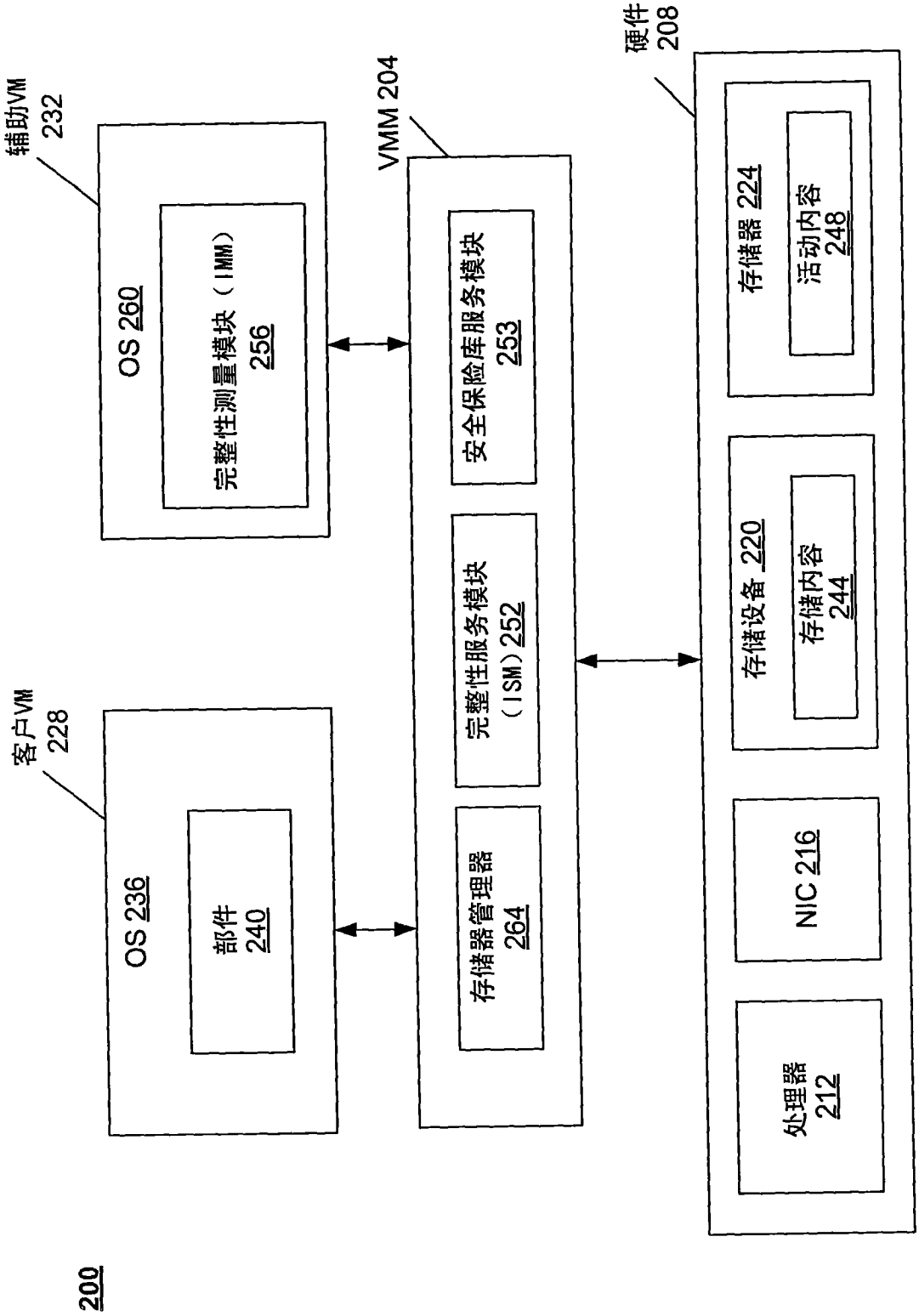

200
辅助VM 232
OS 260
完整性测量模块（IMM）256
客户VM 228
OS 236
部件 240
VMM 204
存储器管理器 264
完整性服务模块（ISM）252
安全保险库服务模块 253
硬件 208
处理器 212
NIC 216
存储设备 220
存储内容 244
存储器 224
活动内容 248

图 2

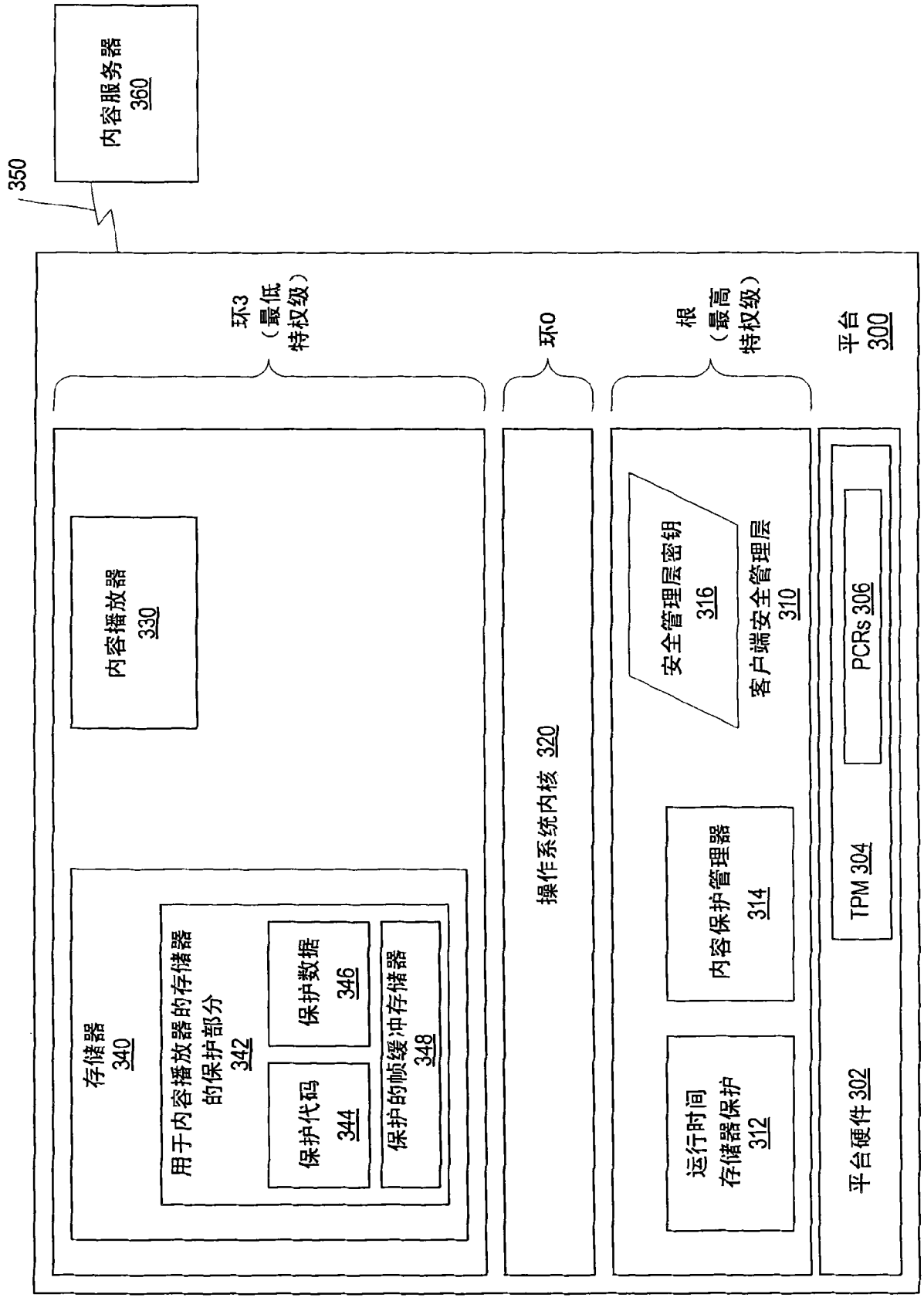

内容服务器
360
350
环3
（最低
特权级）
环0
根
（最高
特权级）
平台
300
内容播放器
330
存储器
340
用于内容播放器的存储器
的保护部分
342
保护代码
344
保护数据
346
保护的帧缓冲存储器
348
操作系统内核 320
安全管理层密钥
316
客户端安全管理层
310
内容保护管理器
314
运行时间
存储器保护
312
平台硬件 302
TPM 304
PCRs 306

图 3

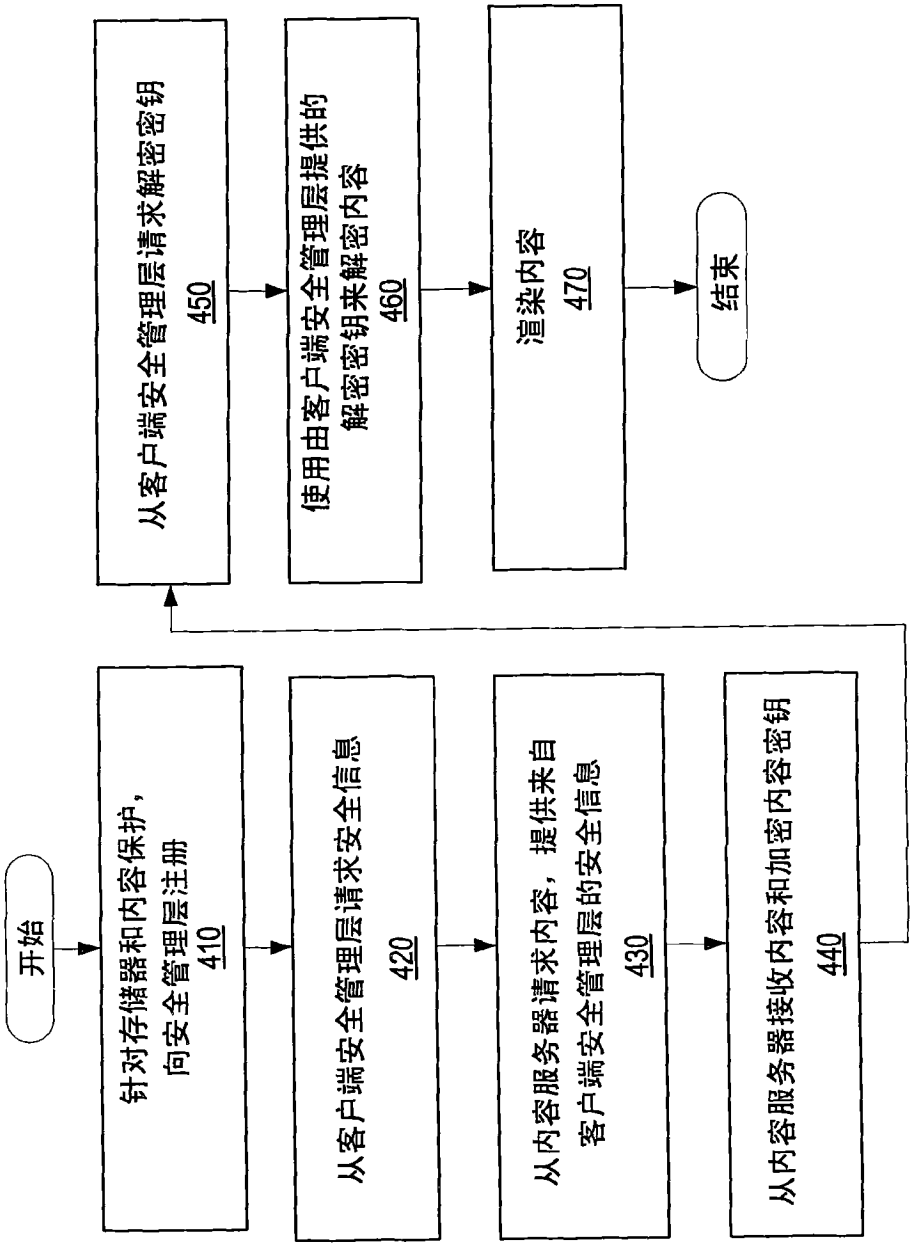

开始
针对存储器和内容保护，向安全管理层注册
410
从客户端安全管理层请求安全信息
420
从内容服务器请求内容，提供来自客户端安全管理层的安全信息
430
从内容服务器接收内容和加密内容密钥
440
从客户端安全管理层请求解密密钥
450
使用由客户端安全管理层提供的解密密钥来解密内容
460
渲染内容
470
结束

图 4

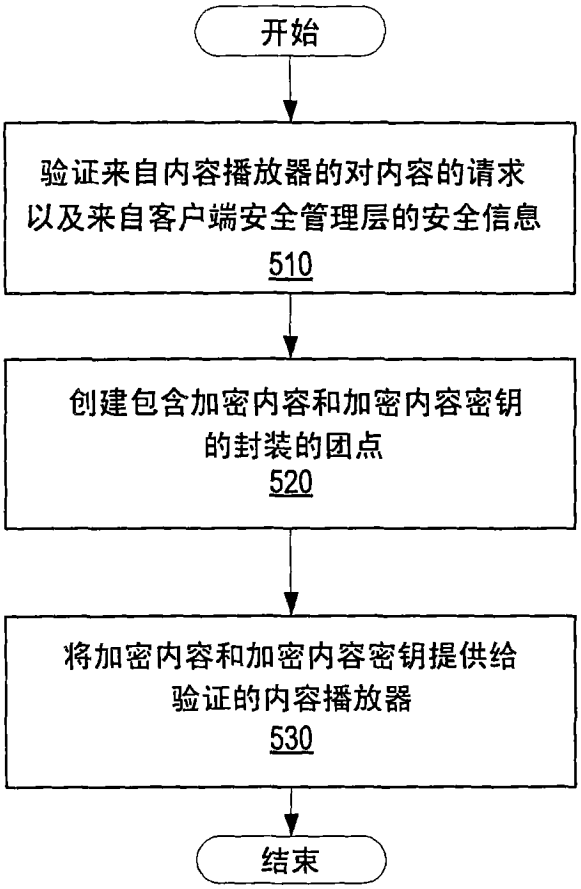

开始
验证来自内容播放器的对内容的请求以及来自客户端安全管理层的安全信息
510
创建包含加密内容和加密内容密钥的封装的团点
520
将加密内容和加密内容密钥提供给验证的内容播放器
530
结束

图 5

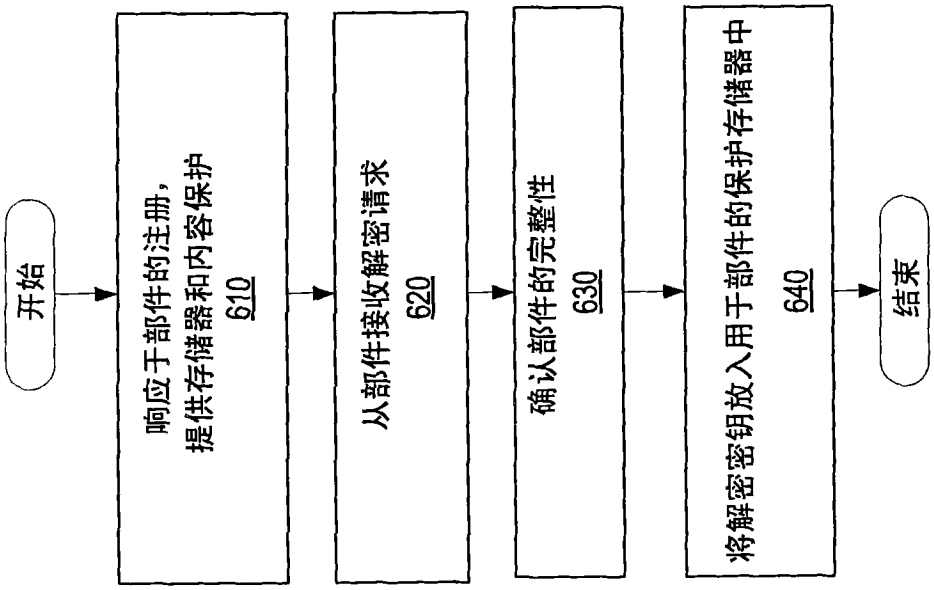

开始
响应于部件的注册，提供存储器和内容保护
610
从部件接收解密请求
620
确认部件的完整性
630
将解密密钥放入用于部件的保护存储器中
640
结束

图 6