



(12) 发明专利申请

(10) 申请公布号 CN 102763113 A

(43) 申请公布日 2012. 10. 31

(21) 申请号 201180009539. 8

(74) 专利代理机构 北京市中咨律师事务所

(22) 申请日 2011. 02. 14

11247

(30) 优先权数据

61/305, 023 2010. 02. 16 US

(51) Int. Cl.

G06F 21/00 (2006. 01)

(85) PCT申请进入国家阶段日

2012. 08. 15

(86) PCT申请的申请数据

PCT/FI2011/050134 2011. 02. 14

(87) PCT申请的公布数据

W02011/101538 EN 2011. 08. 25

(71) 申请人 诺基亚公司

地址 芬兰埃斯波

(72) 发明人 J-E · 埃克贝里 N · 阿索坎

K · 科斯台宁

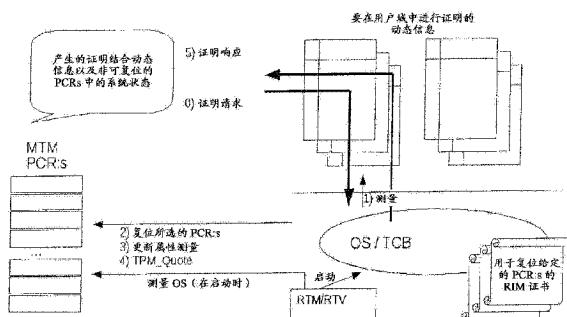
权利要求书 3 页 说明书 9 页 附图 3 页

(54) 发明名称

对移动可信模块中的平台配置寄存器进行复位的方法和设备

(57) 摘要

根据本发明的示例性实施例，至少具有方法、设备和计算机指令的可执行程序以执行以下操作：建立和初始化一组平台配置寄存器，其中平台配置寄存器的第一子集被定义为非可复位的，平台配置寄存器的第二子集被定义为可复位的，在一个或多个非可复位的平台配置寄存器中存储初始启动系统状态信息，动态地复位(2)由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值，以及利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应(5)对证明请求(0)进行响应。



1. 一种方法，包括：

建立和初始化一组平台配置寄存器，其中平台配置寄存器的第一子集被定义为非可复位的，并且平台配置寄存器的第二子集被定义为可复位的；

在一个或多个非可复位的平台配置寄存器中存储初始启动系统状态信息；

动态地复位由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值；

利用包括来自被复位的所述平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应。

2. 根据权利要求 1 所述的方法，其中使用平台配置寄存器属性：

```
typedef struct tdMTM_PCR_ATTRIBUTES {BOOL pcrReset;}
```

MTM_PCR_ATTRIBUTES

将平台配置寄存器定义为可复位的。

3. 根据权利要求 1 所述的方法，其中响应于 MTM_resetPCR 命令而复位平台配置寄存器。

4. 根据权利要求 3 所述的方法，其中所述复位包括参考完整性度量证书更新值。

5. 根据权利要求 3 所述的方法，进一步包括利用下列定义增加核实密钥结构：

```
TPM_VERIFICATION_KEY_USAGE_RESET_PCR 0x0008,
```

其中利用所述定义的所述增加使用命令 MTM_resetPCR 控制对用于复位 PCR:s 的核实密钥的使用。

6. 一种设备，包括：

至少一个数据处理器；和

包括计算机指令的至少一个程序的至少一个存储器，其中所述至少一个存储器和计算机指令的至少一个程序被配置为使用所述至少一个数据处理器使设备至少：

建立和初始化一组平台配置寄存器，其中平台配置寄存器的第一子集被定义为非可复位的，平台配置寄存器的第二子集被定义为可复位的；

在一个或多个非可复位的平台配置寄存器中存储初始启动系统状态信息；

动态地复位由参考完整性度量识别的平台配置寄存器的值以反映由所述参考完整性度量提供的测量值；

利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应。

7. 根据权利要求 6 所述的设备，其中使用平台配置寄存器属性：

```
typedef struct tdMTM_PCR_ATTRIBUTES {BOOL pcrReset;}
```

MTM_PCR_ATTRIBUTES

将平台配置寄存器定义为可复位的。

8. 根据权利要求 6 所述的设备，其中响应于 MTM_resetPCR 命令而复位平台配置寄存器。

9. 根据权利要求 8 所述的设备，其中所述复位包括参考完整性度量证书更新值。

10. 根据权利要求 8 所述的设备，进一步包括至少一个存储器，其中至少一个存储器包括计算机指令的至少一个程序，所述至少一个程序被配置为使用至少一个数据处理器使所

述设备利用下列定义增加核实密钥结构：

TPM_VERIFICATION_KEY_USAGE_RESET_PCR 0x0008,

其中利用所述定义的所述增加使用命令 MTM_resetPCR 控制对用于复位平台配置寄存器的核实密钥的使用。

11. 根据权利要求 6 所述的设备，其中所述设备包括设置在移动平台中的移动可信模块。

12. 一种设备，包括：

用于建立和初始化一组平台配置寄存器的装置，其中平台配置寄存器的第一子集被定义为非可复位的，平台配置寄存器的第二子集被定义为可复位的；

用于在一个或多个非可复位的平台配置寄存器中存储初始启动系统状态信息的装置；

用于动态地复位由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值的装置；以及

用于利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应的装置。

13. 根据权利要求 12 所述的设备，其中所述设备包括设置在移动平台中的移动可信模块。

14. 根据权利要求 12 所述的设备，其中用于所述建立、所述存储、所述动态地复位、所述扩展和所述触发的装置包括至少一个存储器，其中至少一个存储器包括由至少一个数据处理器执行的计算机指令的至少一个程序，并且其中用于所述响应的装置包括发射机。

15. 包括计算机指令的至少一个程序的至少一个非暂态存储器，计算机指令的至少一个程序由至少一个数据处理器执行以执行包括下列步骤的操作：

建立和初始化一组平台配置寄存器，其中平台配置寄存器的第一子集被定义为非可复位的，平台配置寄存器的第二子集被定义为可复位的；

在一个或多个非可复位的平台配置寄存器中存储初始启动系统状态信息；

动态地复位由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值；

利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应。

16. 根据权利要求 15 所述的包括计算机指令的至少一个程序的至少一个非暂态存储器，其中使用平台配置寄存器属性：

```
typedef struct tdMTM_PCR_ATTRIBUTES {BOOL pcrReset;}
```

```
MTM_PCR_ATTRIBUTES
```

将平台配置寄存器定义为可复位的。

17. 根据权利要求 15 所述的包括计算机指令的至少一个程序的至少一个非暂态存储器，其中响应于 MTM_resetPCR 命令而复位所述平台配置寄存器。

18. 根据权利要求 17 所述的包括计算机指令的至少一个程序的至少一个非暂态存储器，其中所述复位包括参考完整性度量证书更新值。

19. 根据权利要求 17 所述的包括计算机指令的至少一个程序的至少一个非暂态存储

器,进一步包括利用下列定义增加核实密钥结构:

TPM_VERIFICATION_KEY_USAGE_RESET_PCR 0x0008,

其中利用所述定义的所述增加使用命令 MTM_resetPCR 控制对用于复位平台配置寄存器的核实密钥的使用。

对移动可信模块中的平台配置寄存器进行复位的方法和设备

技术领域

[0001] 本发明的示例性的和非限制性的实施例一般涉及对例如无线通信系统中的移动可信模块的可信计算、安全和使用。

背景技术

[0002] 该节意在提供在权利要求中涉及的本发明的背景或上下文。这里的描述可包括可执行的概念，但是不是之前已设想或执行的必要的概念。因此，除非在这里进行其它说明，在该节中所描述的不是本申请中的说明书和权利要求的现有技术，并且不因为被包括在该部分而承认其是现有技术。

[0003] 在说明书和 / 或附图中出现的下列缩写定义如下：

ASIC 专用集成电路

DRTM 信任动态测量根

HW 硬件

IMA 完整性度量架构

I/O 输入 / 输出

IV 初始化矢量

MRTM 移动远程所有者可信模块

MTM 移动可信模块

OS 操作系统

PCR 平台配置寄存器

RIM 参考完整性度量

RTM 测量可信根(root-of-trust for measurement)

SW 软件

TCB 可信计算基

TCG 可信计算集

TPM 可信平台模块

TrEE 可信执行环境

[0004] 关于 MTM 可参考“移动可信模块(MTM) - 介绍”，Jan-Erik Ekberg, Markku **Kylämpää**, 诺基亚研究中心, NRC-TR-2007-105, 2007 年 11 月 14 日。

[0005] TPM 规范(可信计算组。可信平台模块(TPM)主规范。版本 1.2 修订版 103, 2007 年 7 月 9 日, http://www.trustedcomputinggroup.org/resources/tpm_main_specification)之前介绍了“动态信任根”，意在支持操作系统下的可信管理程序。管理程序基本上是提供虚拟机环境的系统程序。该专用特征的主要功能是外部的，依赖于芯片的触发器对 TPM PCR 的子集进行复位，将代码(驻留在临时的安全存储位置)发送(launch)到这些 PCR 的一个中。因此，即使在该事件被触发时该机器已经运行了一段时间，相对于由度量代码(假设为

管理程序)进行的计算具有“新的开始”。

[0006] 在过去几年间,研究团体已经发现 DRTM 技术具有与虚拟化和管理程序无关的许多进一步的使用。在这一点上可参照例如 Jonathan M. McCune, Bryan J. Parno, Adrian Perrig, Michael K. Reiter 和 Hiroshi Isozaki,“Flicker :An Execution Infrastructure for TCB Minimization”, Eurosys>08 :第三届 ACM SIGOPS/EuroSys 欧洲计算机系统会议 2008 论文集,第 215-328 页,纽约,美国,2008。ACM。代码片段可被安全地测量(以及其输入和输出)和独立地执行的概念可被看作为给该系统可信执行环境(TrEE)的方面。即使没有初始化,可在用于凭证计算的单一 OS、安全存储器、可信 I/O 和典型地使用虚拟化、外部智能卡和诸如 ARM TrustZone 的处理器安全环境实现的其它安全特征中使用虚拟层 DRTM。

[0007] 作为概念,DRTM 将隔离与硬件支撑的(PCR)复位功能结合。隔离由 HW 而不是在 SW 中进行的事实对实现的安全级别具有重要的贡献,尽管在概念上隔离可由其它(either)装置实现。因此,在这里会集中在状态 /PCR 复位。

[0008] DRTM 的间歇性(所谓的“过山车使用”)对与操作系统状态和 / 或状态历史无关或有非常弱的关系的服务是非常有用的。例如,假设设备用户需要认证网络或服务,或需要授权购买。服务提供商以及甚至是设备用户可能没有动机将这样的处理与设备状态进行绑定,然而至少用户有动机保护用于认证或授权的凭证(以及因此任何相关的计算,例如密钥(secret key)参与)。DRTM 为此目的提供非常适当的机制。然而,例如,将 OS 机制与这样的凭证使用进行绑定是不必要的,并最可能增加这种处理的复杂度。

[0009] 从 DRTM 获益的另一类服务涉及典型地设计为不是不变的而是根据用户需要随意被运行和停止的计算机应用。如果这样的应用定义系统容量或值得关注的特征,通过 OS 将 TPM 事件 /PCR 更新增加到应用运行 / 终止上,在能够(原理上)进行解析以确定系统当前(应用)状态的完整的 TPM 证明的帮助下产生事件潜在的无限长的日志,能够将传统的 TPM 方法具体化。在假设 OS 已经被安全启动或在可信启动中正确地测量,并用作测量点(所谓测量可信根(RTM)的一部分)时,会发现 PCR 不能被复位的需求(对于将指示给定配置中的应用状态的那些 PCR)是不必要的。DRTM 已经提供了用于在 TPM 域中提供 PCR 复位的一个(公认的过程消除)方案。

发明内容

[0010] 在本发明的一个示例性方面,提供了一种方法,包括:建立和初始化一组平台配置寄存器,其中平台配置寄存器的第一子集被定义为非可复位的,平台配置寄存器的第二子集被定义为可复位的,在一个或多个非可复位平台配置寄存器中存储初始启动系统状态信息,动态地复位由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值,以及利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应。

[0011] 在本发明的示例性方面中,提供了一种设备,包括:至少一个数据处理器;和包括计算机指令的至少一个程序的至少一个存储器,其中至少一个存储器和计算机指令的至少一个程序被配置为使用至少一个数据处理器使设备至少:建立和初始化一组平台配置寄存器,其中平台配置寄存器的第一子集被定义为非可复位的,平台配置寄存器的第二子集被定义为可复位的,在一个或多个非可复位平台配置寄存器中存储初始启动系统状态信息,

动态地复位由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值,以及利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应。

[0012] 在本发明的另一示例性方面,提供了一种设备,包括:用于建立和初始化一组平台配置寄存器的装置,其中平台配置寄存器的第一子集被定义为非可复位的,平台配置寄存器的第二子集被定义为可复位的,用于在一个或多个非可复位平台配置寄存器中存储初始启动系统状态信息的装置,用于动态地复位由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值的装置,用于利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应的装置。

[0013] 在本发明的再一示例性方面,提供了包括计算机指令的至少一个程序的至少一个非暂态存储器,计算机指令的至少一个程序由至少一个数据处理器执行以执行包括下列内容的操作:建立和初始化一组平台配置寄存器,其中平台配置寄存器的第一子集被定义为非可复位的,平台配置寄存器的第二子集被定义为可复位的,在一个或多个非可复位平台配置寄存器中存储初始启动系统状态信息,动态地复位由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值,以及利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应。

附图说明

[0014] 在结合附图阅读时,本发明的实施例的上述和其它方面在下面的详细描述中会更明显,其中:

[0015] 图 1 描述了可实现本发明的示例性实施例的通用用例架构。

[0016] 图 2 是示出了移动平台和接入点的简化框图,其中移动平台包括根据本发明的示例性实施例操作的 MTM。

[0017] 图 3 是根据本发明的示例性实施例图示了方法的操作和计算机程序指令的执行结果的逻辑流程图。

具体实施方式

[0018] 因此可能希望提供用于在 TCG MTM 中对 PCR 进行复位的用例(真实世界用例)的技术,并进一步将该属性结合到规范中。本发明的示例性实施例包括这些技术。

[0019] 应当明确的是,一些 PCR 复位特征可以与 DRTM 利用 TPM 发现其“非预期用途”同样的方式有益于移动设备和 MTM。关于 MTM 可以参考例如可信计算组移动可信模块(MTM)规范,版本 1.0 修订版 6,2008 年 6 月 26 日,和可信计算组,TCG 移动参考体系结构规范,版本 1.0 修订版 1,2007 年 6 月 12 日。

[0020] 可以争论的是,相似的概念可基于“抛弃型(throwaway)”MTM 得出。虽然在原理上这是可行的,但是相对于远程证明该方法是不足的,其中远程证明是任何 TPM/MTM 活动、至少那些与网络或通信服务相关的活动的基础。作为非限制性的示例,考虑将应用测量为自己的、短暂的 MTM 的情况,其中 MTM 很有可能被固定(rooted)在系统 MRTM 处(在可信的

情况下(in a trust sense))。现在, MTM 自己可以如所需要的一样“新”,它们各自状态的证明对远程证明人是无痛的。但是,由于这些 MTM (以及它们全部现有的实例)可能也必须测量为用于绑定信任的系统 MRTM,无限测量链(和相应的证明困难)的问题简单地在系统中移动到另一地点,并且仍需要可复位性特征。

[0021] MTM 不是由 HW/SW 特征定义,而是由各种信任根定义。对于复位 PCR 的问题,在不损失一般性的情况下,可假设由 RTM 处理。由于在许多情况下,大部分简单的“执行前测量”原理必须增加发生的 MTM 事件更新特征(例如,当应用终止时,或当一些其它内部或外部条件满足时),因此需要一些附加的功能和逻辑。然而,这与在启动过程中如何预期使用 TPM/MTM 相兼容。例如,在现在的 BIOS 测量中呈现了当功能被成功运行时向结束增加事件的活动。

[0022] 在一个简单的例示中,对 PCR 复位的能力以一个 MTM 的粒度(granularity)来执行。在这种情况下,假设该特定 MTM (其上下文)在上层(upper-level)MTM 中进行测量,并且在 PCR 被复位时该测量不会改变。然而,为了证明的目的,对于本地检查员或可能的远程证明人,在该特定 MTM 中 PCR 可复位的特征需要成为可视的。

[0023] 根据本发明示例性实施例的一个方面,最有希望的机制使用可用的 TPM v1.2 命令 TMP_RESET_PCR 作为起点。如果由固定的 PCR 属性、源自匹配位置(所需的位置是另一固定的 PCR 属性)的命令允许,该命令对可复位的 PCR 的选择进行复位。下面的增加和修改选项可认为在 MTM 的范围内,确认位置看起来至少已引起第一规范回的问题的事实(稍后分析)。

1). 在 MTM 中的 verifiedPCR 列表可利用 MTM_setVerifiedPCRS 进行更新的情况下,可以讨论的是同样可复位的 PCR:s 集合比 TPM:s 更为动态,其中实际上的可复位 PCR 列表目前通常由 DRTM 机制控制(PCR 18-24)。一个选择是增加诸如 MTM_setResettablePCR 的命令。

2. 尽管可以讨论 verified_PCR 的列表在远程证明中不是必须需要的(由于 PCR 表示独立于任何本地接入控制的状态),同样不能是所述复位 PCR:s 的列表 - 该信息是相当必要或至少希望成为远程证明的一部分。在 TPM 中,该信息根据 PCR 的初始 / 复位基值进行传送(convey)。该概念可容易地转换到 MTM,在 TPM 的精神中,可将非可复位的 PCR 在启动时设置为 0x000…000,在复位时将可复位的 PCR 初始化为 0xFFFF…FFF。这给证明人转达足够的信息以确定 PCR 是否已经复位。

3. 从证明人的角度,知道哪个 PCR 是可复位的没有多大区别,相反重点在于知道哪个 PCR 已经复位。然而,对于平台所有者,复位的 PCR 一直是删除历史的方式,至少使提供选择以能够定义非可复位的 PCR 可取的自变量(argument)。在这一点上,一种选择是不定义具体的 resettablePCR 矢量,而是说在 MTM_incrementBootstrapCounter (作为采用对 PCR 进行复位的 RIM 证书作为自变量的命令) 的精神下完成对 PCR 进行复位的机制。该逻辑贯彻验证密钥的能力 - 使 RIM 证书可用于对指定 PCR 进行复位的权利(条件是给定的系统状态),可由验证密钥结构中的性能比特控制。可选地, RIM 证书中的扩展值可用于立即扩展复位 PCR,以留下对 PCR 进行复位的 RIM 证书的持久轨迹(也就是,间接地指示在复位时哪个状态是活动的)。

4. 以规范(版本 1,第 6 稿)中的下列评论为依据考虑对任何 MTM PCR 进行复位的选项 : “然而,在包括核实的 PCR 时一定不要使用位置。PCR 可以是核实的 PCR (在 MTM_

PERMANENT_DATA-verifiedPCR 中具有其索引比特集合) 或者 PCR 可具有位置修正符集合。PCR 当然还能够没有位置比特集合, 不是核实时的 PCR。然而, PCR 一定不是核实时的 PCR 并且具有位置修正符集合。具体地, TPM_PCR_Reset 命令一定不为核实时的 PCR 工作。核实时的扩展允许人们确凿地从核实时的 PCR 检测是否已经将事件记录到相同或另一核实时的 PCR 中。允许用于核实时的 PCR 的 TPM_PCR_Reset 会禁止这些。”

[0024] 根据本发明的示例性实施例, 为了提供一致的设置, 当前用于在 MTM 中结合 PCR 复位的优选(但是非限制性的) 技术概括如下:

1. 启动后全部 MTM PCR 的初始值是 0x000…000 (如当前规定的)。
2. 启动后任何 PCR 复位由值 0xFFFF…FFF 初始化(服从 TPM v. 1.2 的策略)。
3. 按照 TPM 的 PCR 属性, 将多个低指数 PCR(例如, 最初的 4 或 8)定义为不可复位。这仅为了方便起见和增加安全性, 可以假设这些 PCR 通常意在用于捕获系统启动状态(无论“系统”是什么)。所有进一步的 PCR 被原理上定义为可复位的。可将用于此的一个公式用于定义 PCR 属性, 例如, 为

```
typedef struct tdMTM_PCR_ATTRIBUTES {BOOL pcrReset;}  
MTM_PCR_ATTRIBUTES.
```

4. 由于可复位的 PCR 还可从由 RIM 证书提供的完整保护(在启动之间)获益, 因此除去不允许 verified_PCR 列表上的 PCR 可复位的禁令。

5. 使用新命令对 PCR 进行复位, 为了方便起见将其称为 MTM_resetPCR。该命令的格式可以依照 MTM_incrementBootstrapCounter, 因为它们的语法是类似的。RIM 证书以正常的方式, 利用表示要复位的 PCR 的 measurementPcrIndex 以及包括扩展至 PCR 复位的值到值 0xFFFF…FFF 的 measurementValue 进行操作。

6. 验证密钥结构利用定义进行增加:

```
TPM_VERIFICATION_KEY_USAGE_PCR 0x0008
```

使用新命令 MTM_resetPCR 控制对用于复位 PCR:s 的验证密钥的使用。

[0025] 根据示例性实施例的一个方面, 通过尽可能从现有的 TPM 规范进行重新使用, 但同时使 MTM 的现有特征(RIM 证书)的使用最大化, 并处理不是 MTM 规范的已建立部分的位置的问题, 该方法以服从大部分标准的方式提供所需要的功能。该方法不以严格的方式固定可复位的 PCR:s, 而是将其留给 MTM 所有者(设备合作者)以决定策略, 通过该策略允许核实密钥(及其 RIM 证书)对 PCR 空间的部分进行复位。通常, 在制造商端处仍可达到刚度, 如果在一些情况下希望这样。

[0026] 现在参照图 1 以解释一个非限制性的用例。

[0027] 考虑操作系统(OS)需要远程方证明(集合的)哪个应用在运行的情况。可以假设根据 MTM 的原理, OS 自己是安全启动的, 并已达到其具有一个或多个 MRTM:s 活动的状态, 并且在有或者没有 RIM 证书的情况下, 系统状态以 PCR 更新的形式登录到其中。从该点起, 系统需要记录根据用户活动或其它事件在时间上发起或终止的应用。实现这种跟踪的传统方法是增建诸如 IMA 的架构, 但是这些积累要同认证比较的大量数据(测量日志), 或者在 IMA 的情况下它们不会跟踪系统的动态状态。相反, 它们仅确保完整性, 也就是, 仅测量第一应用使用。

[0028] 假设根据示例性实施例使用上述的 PCR 复位工具, 该示例的使用情况可更好地由

MTM 支持。例如,建立 MTM 阵列,与基 MRTM 绑定,例如通过测量它们各自的状态信息连同一些识别值为基 MRTM。现在任何证明是两个 TPM_QUOTE 命令的结合,一个来自证明 OS 状态、并绑定到更多动态的应用证明 MTM 的基 MRTM,第二个来自于相关的应用证明 MRTM。

[0029] 每个应用证明 MRTM 由 OS 使用以跟踪少数特定应用,可能通过一些属性或应用类型进行聚类划分。一个非常直接的方法是在开始和应用终止时将涉及应用的事件记录到专用的、可复位的 PCR 中,优选地作为这些各自动作的不同事件。因此,通过检查所讨论的 PCR,以及记录到其中的事件,证明人可容易地检查在证明时这种类型的一个或几个应用示例是否是活动的。等效地,通过在空闲时对其进行检测,可信操作系统后台程序可将信息内容大小赋值(bind)到 PCR 中。当应用发生和终止彼此相抵时,相应的 PCR 可安全地复位。然而,即使在发生和终止彼此不相抵的情况下,后台程序仍可以复位 PCR,并将区别再次加入到讨论中的 PCR 中。

[0030] 在图 1 中各种编号的操作如下。初始由 RTM/RTV 在启动时间测量 OS,并将结果存储在(非可复位的)MTM PCR:s 中。然后假设动态信息的呈现在用户域中进行证明。在(0)处有证明请求。在(1)处由 OS/TCB 进行测量。假设存在用于复位特定的 PCR:s 的 RIM 证书。在(2)处所选择的 PCR:s 被复位,在(3)处对在(1)得到的属性测量进行更新。TPM_Quote 命令在(4)处执行,在(5)处返回证明响应。产生的证明结合动态信息以及非可复位的 PCR:s 中的系统状态。复位操作可选地包括 RIM 证书更新值。

[0031] 应注意的是,示例性实施例不会与例如 IMA 相抵触,并且实际上可与 IMA 并行操作。在这种方式下可获得系统的动态状态的“快照”,而 IMA 通过列举已至少发生过一次的全部应用,提供应用完整性所需的证据和在一些程度上系统完整性的声明。

[0032] 当启动由传统的 MTM 控制并且然后动态(dynamism)由更好地适用于该任务的任何专有的或其它规定的机制解决时,可能会出现 MTM 或 TPM 是否应当完全用于更多动态的证明活动的问题。乍看这似乎是可行的方法,但是应当考虑下面使用根据本发明的示例性实施例的过程的讨论。

A. 整体架构通过利用 TCG 概念定形。由于仅有一种查看需要被包括的数据(PCR)的方式,这使得证明活动更加直接(straight-forward)。

B. MTM 提供可用作配置(例如以定义事件格式)的工具的 RIM 证书。RIM 证书通过设计是被完整保护的,从而不受制于修改威胁,即使它们作为数据典型地不被信任测量保护。

C. 在移动平台中,MTM(作为状态存储)相比于 OS 存储器通常得到更好的保护。因此如果利用 MTM 来完成,则证明声明更可靠。

D. 动态不适合于仅 OS 概念。例如,TPM/MTM 的典型用例是限制访问 RSA 密钥(密钥使用)。这里,将密钥定义为在特定系统状态中可访问,但是当已经达到该状态时,在实际的密钥使用后,PCR 状态能够被篡改(garble)以确保密钥不能被使用,直到再次达到该状态,传统地在下一次重新启动中(传统的 PCR 不能被复位)。然而,对于一些密钥和它们的使用,这显然太受限制,可能需要在 TPM/MTM 的正常运行时间期间末尾重新使用密钥。显然地,对 PCR 复位的能力对支持这些和相似用例是有益的。如果 MTM 总是(ever)包括用于专用算法和其它代码的可信执行环境(TrEE:s),论点(argument)会变得更强大。

[0033] 图 2 示出了通过链路 11 与无线网络 1 的接入点(AP)21 位于无线通信中的移动平台(MP)10。网络 1 可包括网络控制元件(NCE)14,其中网络控制元件(NCE)14 可包括移动

管理实体(MME) / 网关(GW)功能，并可提供与诸如电话网络和 / 或数据通信网络(例如，互联网)的进一步网络的连通性。MP 10 包括诸如计算机或数据处理器(DP)10A 的控制器，体现为存储计算机指令(PROG)10C 的程序的存储器(MEM)10B 的计算机可读存储器介质，和用于通过一个或多个天线与 AP 12 进行双向无线通信的合适的射频(RF)收发器 10D。AP 12 也包括诸如计算机或数据处理器(DP)12A 的控制器，体现为存储计算机指令(PROG)12C 的程序的存储器(MEM)12B 的计算机可读存储器介质，和用于通过一个或多个天线与 MP 10 进行通信的合适的 RF 收发器 12D。AP 12 通过数据 / 控制路径 13 与 NCE 14 镶合。

[0034] 为了描述本发明的示例性实施例，可假设 MP 10 还包括在 HW、SW 或作为 HW 和 SE (和固件)组合中实现的 MTM 10E。程序 10C 可执行 OS，以及例如 MTM 10E 的全部或一些功能。假设 MTM 10E 根据本发明的示例性实施例操作，从而能够使至少一些 MTM PCR 可复位。可将 MTMPCR 实现为存储器 10B 中的存储位置，或 HW 寄存器，或存储器位置和 HW 寄存器的结合。

[0035] 通常，MP 10 的各种实施例可以包括但不限于，蜂窝电话，具有无线通信能力的个人数字助理(PDA)，具有无线通信能力的便携式计算机，诸如具有无线通信能力的数字照相机的图像捕获设备，具有无线通信能力的游戏设备，具有无线通信能力的音乐存储和回放应用，允许无线互联网接入和浏览的互联网应用，以及并入这些功能的组合的便携式单元或终端。计算机可读 MEM 10B 和 12B 可以是适用于本地技术环境的任何类型，并可使用任何合适的数据存储技术实现，例如基于半导体的存储设备，闪存，磁存储器设备和系统，光存储器设备和系统，固定存储器和可移动存储器。DP 10A 和 12A 可以是适用于本地技术环境的任何类型，并且作为非限制性的实施例，可包括通用计算机，专用计算机，微处理器，数字信号处理器(DSP)和基于多核处理器架构的处理器中的一个或多个。在图 2 中示出的 MP 10 和 AP 12 的全部或部分功能可在每一个或多个各自的 ASIC 中实现。

[0036] 基于上述内容，应显而易见的是，本发明的示例性实施例提供了方法、装置和计算机程序以增强与移动可信模块有关的数据处理系统的操作。示例性实施例提供 RIM 证书和验证密钥的增加，从而以细粒度和动态方式控制 PCR 复位。PCR 的复位可由平台制造商来控制。

[0037] 图 3 是根据本发明示例性实施例图示了方法的操作和计算机程序指令的执行结果的逻辑流程图。根据这些示例性实施例，方法在移动可信模块(MTM)中执行，在块 3A 处，建立和初始化一组平台配置寄存器(PCR)的步骤，其中平台配置寄存器的第一子集被定义为非可复位的，平台配置寄存器的第二子集被定义为可复位的。在块 3B 处，具有在一个或多个非可复位平台配置寄存器中存储初始启动系统状态信息的步骤。在块 3C 处，具有动态地服务由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值的步骤。在块 3D 处，具有利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应的步骤。

[0038] 对于图 3 所述的方法，其中平台配置寄存器被定义为在使用下面的平台配置寄存器属性可复位：

```
typedef struct tdMTM_PCR_ATTRIBUTES {BOOL perReset;}  
MTM_PCR_ATTRIBUTES.
```

[0039] 前述两个段落的方法，其中复位平台配置寄存器是对 MTM_resetPCR 命令作出的

响应。

[0040] 前述段落的方法,进一步包括利用下列定义增加核实密钥结构:

TPM_VERIFICATION_KEY_USAGE_RESET_PCR 0x0008

以使用命令 MTM_resetPCR 控制用于复位 PCR:s 的核实密钥的使用。

[0041] 图 3 所示的各块可视为方法步骤,和 / 或由计算机程序代码的操作引起的操作,和 / 或构建以执行关联的功能的多个耦合的逻辑电路元件。

[0042] 本发明的示例性实施例还提供了包括处理器和包括计算机程序代码的存储器的设备,其中存储器和计算机程序代码被配置为使用处理器使装置至少执行:建立和初始化一组平台配置寄存器,其中平台配置寄存器的第一子集被定义为非可复位的,平台配置寄存器的第二子集被定义为可复位的;在一个或多个非可复位平台配置寄存器中存储初始启动系统状态信息;复位由参考完整性度量识别的平台配置寄存器的值以反映由参考完整性度量提供的测量值;以及利用包括来自被复位的平台配置寄存器的动态信息和来自非可复位的平台配置寄存器的系统状态信息的证明响应对证明请求进行响应。

[0043] 通常,各示例性实施例可在硬件或专用电路、软件、逻辑或其任何组合中实现。例如,一些方面可在硬件中实现,而其它方面可在固件或可由控制器、微处理器或其它计算设备执行的软件中实现,尽管本发明不局限于此。尽管本发明的示例性实施例的各方面可图示和描述为框图、流程图,或使用一些其它图示表达,但是可以理解的是,这里描述的块、设备、系统、技术或方法,作为非限制性示例,可实现在硬件、软件、固件、专用电路或逻辑、通用硬件或控制器或其它计算设备、或其组合中。

[0044] 应显而易见的是,本发明的示例性实施例的至少一些方面可实践在诸如集成电路芯片和模块的各种组件中,并且本发明的示例性实施例可在实施为集成电路的设备中实现。集成电路,或电路,可包括用于体现可配置以根据本发明的示例性实施例进行操作的数据处理器或多个数据处理器,数字信号处理器或多个处理器,基带电路和射频电路中的至少一个或多个的电路(以及可能的固件)。

[0045] 当结合附图阅读时,根据上述描述,对本发明的前述示例性实施例进行各种修改和调整对本领域技术人员来说将变得显而易见。然而,任何和全部修改仍将落入本发明的非限制性的和示例性实施例的范围内。

[0046] 需要说明的是,术语“连接”、“耦合”或其任何变形表示两个或多个元件之间的任何连接或耦合,直接或间接的,并可包括在“连接”或“耦合”在一起的两个元件之间一个或多个中间元件的存在。元件之间的耦合或连接可以是物理的,逻辑的,或其组合。如这里所使用的,作为几个非限制性的和非穷尽的示例,通过使用一个或多个电线、电缆和 / 或印刷电连接,以及通过使用电磁能,例如具有射频区域、微波区域和光(可见和不可见)区域中的波长的电磁能,可认为两个元件是“连接”或“耦合”在一起的。

[0047] 此外,用于所描述的参数的各名称不意在任何方面进行限制,这些参数可由任何合适的名称识别。此外,使用这些各参数的公式和表达可不同于这些明确的表达。此外,分配给不同命令(例如, MTM_resetPCR 等)的各名称不意在任何方法进行限制,这些各种命令可由任何合适的名称来标识。

[0048] 此外,在没有相应使用其它特征的情况下,本发明的各种非限制性的和示例性的实施例的一些特征也可用于获益。同样,前述描述应当仅被认为是对本发明的原理、教导和

示例性实施例的解释，并不对其进行限制。

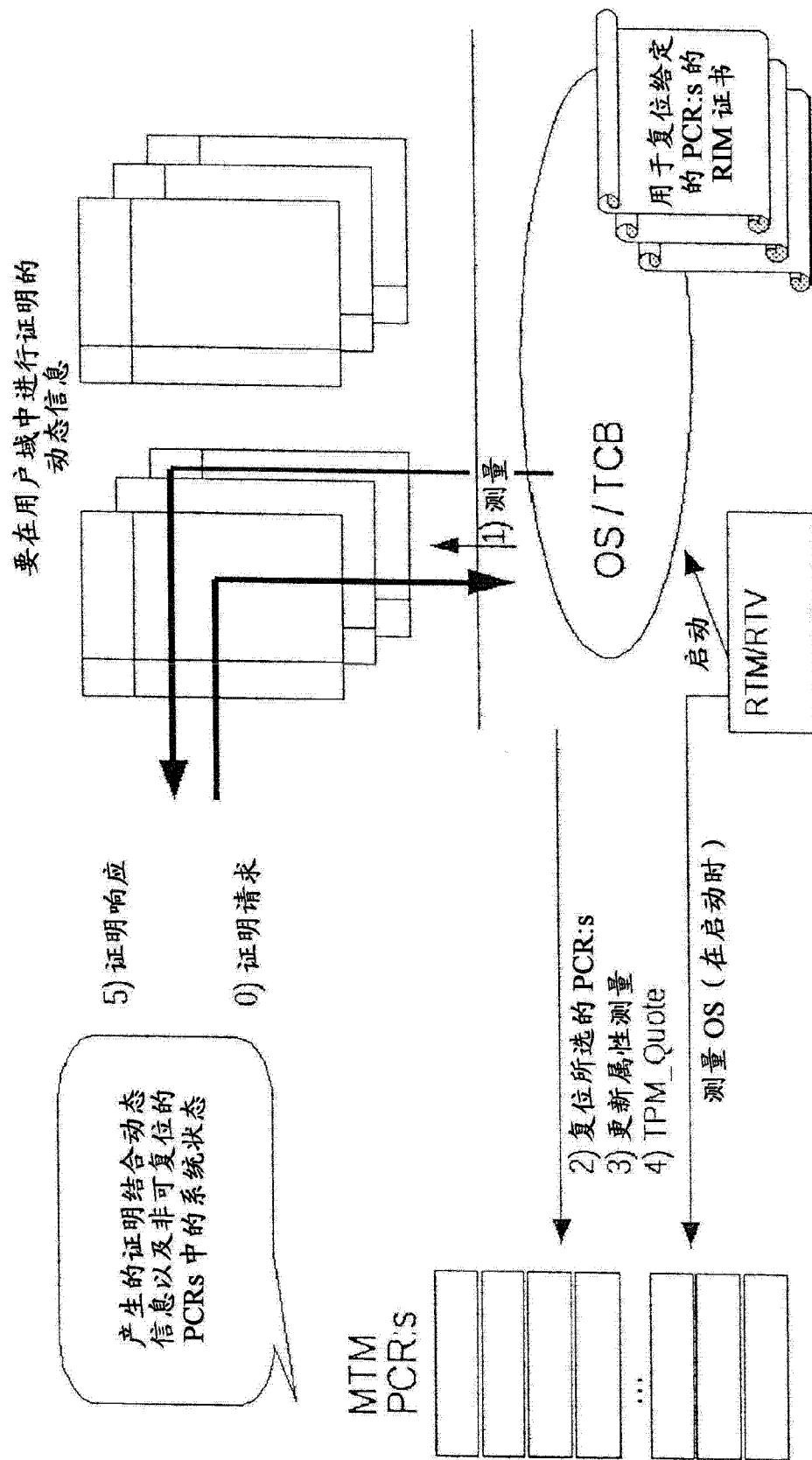


图 1

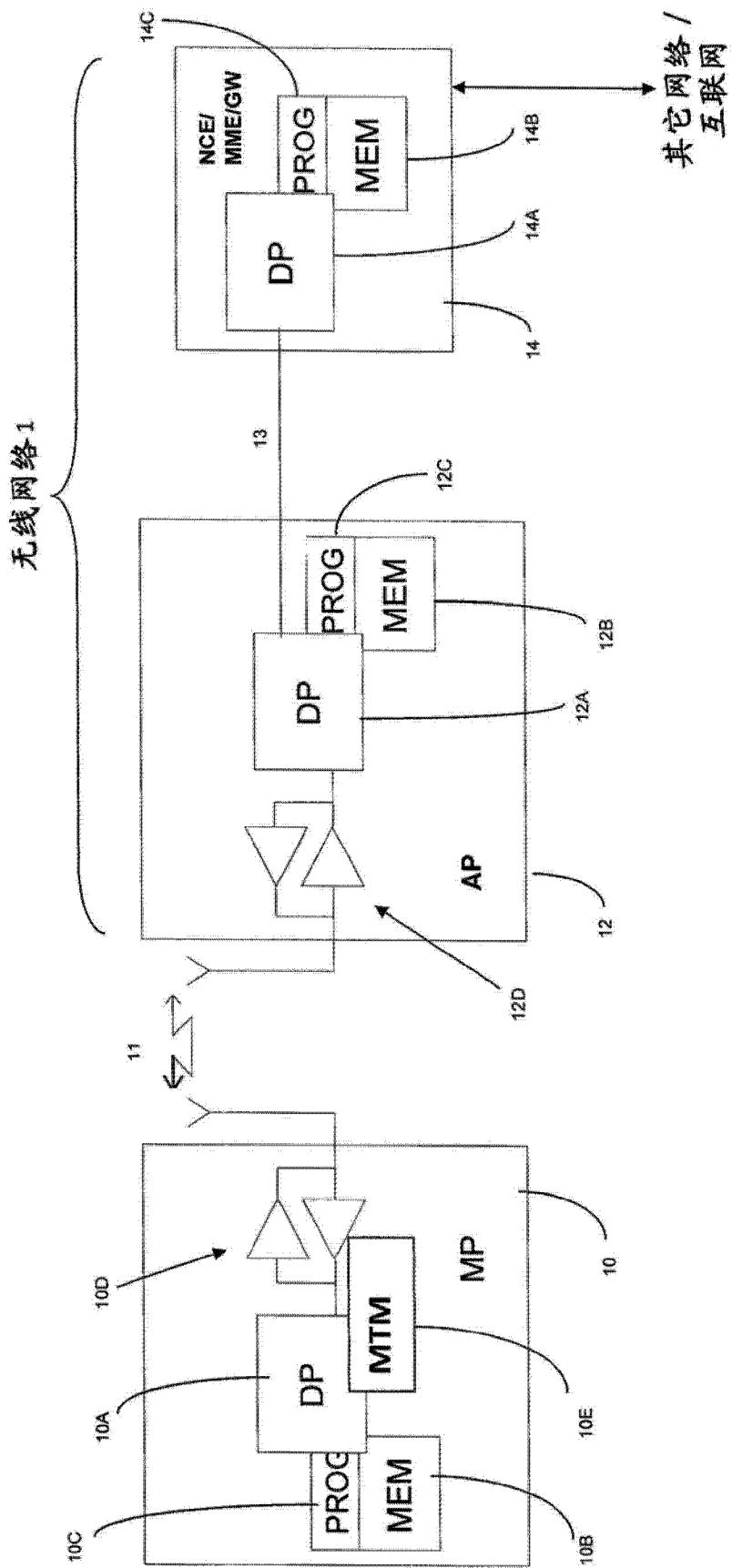


图 2

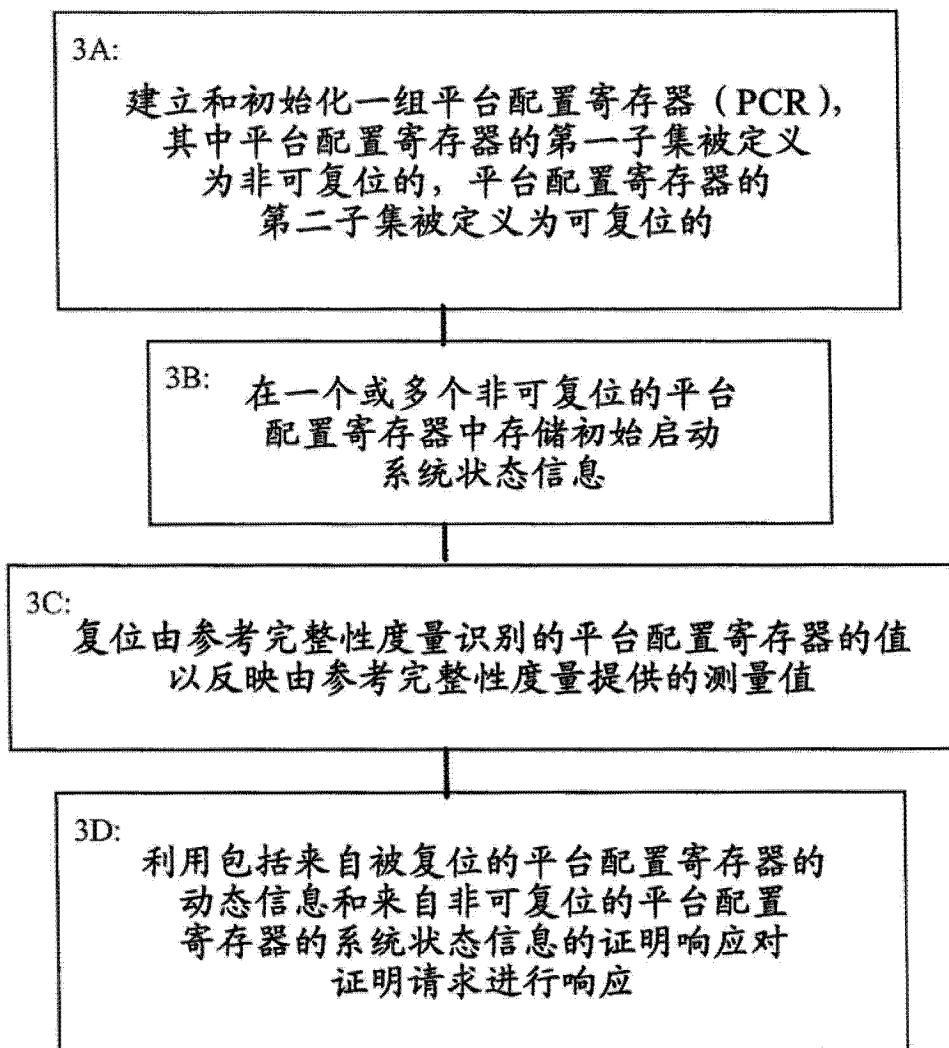


图 3