(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 104268461 B
(45)授权公告日 2018.03.06

(21)申请号 201410471558.8

(22)申请日 2014.09.16

(65)同一申请的已公布的文献号
申请公布号 CN 104268461 A

(43)申请公布日 2015.01.07

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 周冲 付天福

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 冯艳莲

(51)Int.Cl.
G06F 21/50(2013.01)
G06F 21/30(2013.01)

(56)对比文件

CN 103124973 A,2013.05.29,说明书第2页第13、14段,第13页第23段至第6页第68段,说明书附图4、6.

CN 103124973 A,2013.05.29,说明书第2页第13、14段,第13页第23段至第6页第68段,说明书附图4、6.

CN 103488937 A,2014.01.01,全文.

CN 101038556 A,2007.09.19,全文.

CN 101458743 A,2009.06.17,全文.

CN 1991779 A,2007.07.04,全文.

CN 103973680 A,2014.08.06,全文.

石志国等.基于PCR检测机制的时间自校检平台访问控制算法.《计算机研究与发展》.2008,第43卷(第z2期),第114-121页.

审查员 陈雅

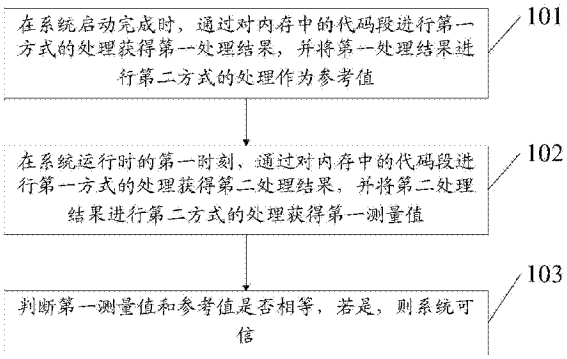
权利要求书2页 说明书11页 附图2页

(54)发明名称

一种可信度量方法及装置

(57)摘要

本申请提供一种可信度量方法及装置,该方法包括:在系统启动完成时,通过对内存中的代码段进行第一方式的处理获得第一处理结果,并将所述第一处理结果进行第二方式的处理作为参考值;在所述系统运行时的第一时刻,通过对所述内存中的代码段进行所述第一方式的处理获得第二处理结果,并将所述第二处理结果进行所述第二方式的处理获得第一测量值;判断所述第一测量值和所述参考值是否相等,若是,则所述系统可信;其中,所述内存中的代码段是指在所述系统的一次启动以及运行过程中,不因所述系统的正常运行而改变的代码段。



CN 104268461 B

1.一种可信度量方法,其特征在于,包括:

在系统启动完成时,通过对内存中的代码段进行第一方式的处理获得第一处理结果,并将所述第一处理结果进行第二方式的处理作为参考值;

在所述系统运行时的第一时刻,通过对所述内存中的代码段进行所述第一方式的处理获得第二处理结果,并将所述第二处理结果进行所述第二方式的处理获得第一测量值;

判断所述第一测量值和所述参考值是否相等,若是,则所述系统可信;

其中,所述内存中的代码段是指在所述系统的一次启动以及运行过程中,不因所述系统的正常运行而改变的代码段。

2.如权利要求1所述的方法,其特征在于,通过对内存中的代码段进行第一方式的处理获得第一处理结果,并将所述第一处理结果进行第二方式的处理作为参考值,包括:

通过对所述内存中的代码段进行哈希计算,获得所述第一处理结果;

通过对所述第一处理结果和预设的第一值进行所述哈希计算,获得所述参考值;

通过对所述内存中的代码段进行所述第一方式的处理获得第二处理结果,并将所述第二处理结果进行所述第二方式的处理得到第一测量值,包括:

通过对所述内存中的代码段进行所述哈希计算,获得所述第二处理结果;

通过对所述第二处理结果和所述第一值进行所述哈希计算,获得所述第一测量值。

3.如权利要求2所述的方法,其特征在于,所述第一值为所述系统复位后平台配置寄存器PCR的初始值或随机生成的值。

4.如权利要求1-3任一项所述的方法,其特征在于,在确定所述第一测量值和所述参考值相等之后,所述方法还包括:

将所述第二处理结果进行所述第二方式的处理,作为第一预期值;

在所述系统运行时的第二时刻,通过对所述内存中的代码段进行所述第一方式的处理,获得第三处理结果;

并将所述第三处理结果进行所述第二方式的处理获得第二测量值;其中,所述第二时刻在所述第一时刻之后;

判断所述第二测量值和所述第一预期值是否相等,若是,则所述系统可信。

5.如权利要求4所述的方法,其特征在于,将所述第二处理结果进行所述第二方式的处理,作为第一预期值,包括:

通过对所述第二处理结果和所述参考值进行哈希计算,获得所述第一预期值;

将所述第三处理结果进行所述第二方式的处理获得所述第二测量值,包括:

通过对所述第三处理结果和所述第一测量值进行所述哈希计算,获得所述第二测量值。

6.如权利要求5所述的方法,其特征在于,在确定所述第二测量值和所述第一预期值相等之后,所述方法还包括:

通过对所述第三处理结果和所述第一预期值进行所述哈希计算,获得第二预期值。

7.如权利要求1-3任一项所述的方法,其特征在于,在确定所述第一测量值和所述参考值相等之后,所述方法还包括:

将所述第二处理结果进行所述第二方式的处理,作为第一预期值;

从所述第一时刻起,在超过一个可信度量间隔的时间段之后,判断最新的参考值是否

与所述第一预期值相同，若相同，则所述系统不可信。

8.一种可信度量的装置，其特征在于，包括：

度量模块，用于在系统启动完成时，通过对内存中的代码段进行第一方式的处理获得第一处理结果；在所述系统运行时的第一时刻，通过对所述内存中的代码段进行所述第一方式的处理获得第二处理结果；

处理模块，用于将所述第一处理结果进行第二方式的处理作为参考值；将所述第二处理结果进行所述第二方式的处理获得第一测量值；并判断所述第一测量值和所述参考值是否相等，若是，则所述系统可信；

其中，所述内存中的代码段是指在所述系统的一次启动以及运行过程中，不因所述系统的正常运行而改变的代码段。

9.如权利要求8所述的装置，其特征在于，所述度量模块具体用于：通过对所述内存中的代码段进行哈希计算，获得所述第一处理结果；通过对所述内存中的代码段进行所述哈希计算，获得所述第二处理结果；

所述处理模块具体用于：通过对所述第一处理结果和预设的第一值进行所述哈希计算，获得所述参考值；通过对所述第二处理结果和所述第一值进行所述哈希计算，获得所述第一测量值。

10.如权利要求9所述的装置，其特征在于，所述第一值为所述系统复位后平台配置寄存器PCR的初始值或随机生成的值。

11.如权利要求8-10任一项所述的装置，其特征在于，所述处理模块具体还用于：在确定所述第一测量值和所述参考值相等之后，将所述第二处理结果进行所述第二方式的处理，作为第一预期值；

所述度量模块还用于在所述系统运行时的第二时刻，通过对所述内存中的代码段进行所述第一方式的处理，获得第三处理结果；

所述处理模块还用于：将所述第三处理结果进行所述第二方式的处理获得第二测量值；其中，所述第二时刻在所述第一时刻之后；判断所述第二测量值和所述第一预期值是否相等，若是，则所述系统可信。

12.如权利要求11所述的装置，其特征在于，所述处理模块具体用于：通过对所述第二处理结果和所述参考值进行哈希计算，获得所述第一预期值；通过对所述第三处理结果和所述第一测量值进行所述哈希计算，获得所述第二测量值。

13.如权利要求12所述的装置，其特征在于，所述处理模块还用于：在确定所述第二测量值和所述第一预期值相等之后，通过对所述第三处理结果和所述第一预期值进行所述哈希计算，获得第二预期值。

14.如权利要求8-10任一项所述的装置，其特征在于，所述处理模块还用于：在确定所述第一测量值和所述参考值相等之后，将所述第二处理结果进行所述第二方式的处理，作为第一预期值；从所述第一时刻起，在超过一个可信度量间隔的时间段之后，判断最新的参考值是否与所述第一预期值相同，若相同，则所述系统不可信。

一种可信度量方法及装置

技术领域

[0001] 本申请涉及安全技术领域，尤其涉及一种可信度量方法及装置。

背景技术

[0002] 为了解决计算机结构上的不安全、从基础上提高计算机的可信性，业界组织了可信计算平台联盟(英文:Trusted Computing Platform Alliance;简称:TCPA)。TCPA定义了具有安全存储和加密功能的可信平台模块(英文:Trusted Platform Module;简称:TPM)。2003年3月，TCPA改组为可信计算组织(英文:Trusted Computing Group;简称:TCG)。

[0003] TCG对“可信”的定义是:一个实体在实现给定目标时，如果该实体的行为总是和预期的相同，则该实体是可信的。

[0004] 可信计算的主要手段是进行身份确认，使用加密进行存储保护及使用完整性度量进行完整性保护。基本思想是在计算机系统中首先建立一个信任根，再建立一条信任链，一级测量认证一级，一级信任一级，把信任关系扩大到整个计算机系统，从而确保计算机系统的可信。具体来说，TPM芯片首先度量当前底层固件的完整性，如正确则完成正常的系统初始化。然后由底层固件度量基本输入输出系统(英文:Basic Input Output System;简称:BIOS)的完整性，如正确，则由BIOS继续度量操作系统的完整性，如正确则正常运行操作系统，否则停止运行。然后操作系统度量应用和新的操作系统组件。当操作系统启动后，由用户决定是否继续信任这个系统平台。这样，一个信任链的建立过程保证了系统平台的可信性。

[0005] 然而，上述可信度量的方法，只能在系统启动过程中执行。但是在系统完成启动后，软件有可能被恶意篡改，如果没有可信度量方法，将无法保证系统可信。

发明内容

[0006] 本申请实施例提供一种可信度量方法及装置，用以解决现有技术中的系统启动后无法进行可信度量的技术问题。

[0007] 本申请第一方面提供了一种可信度量方法，包括:

[0008] 在系统启动完成时，通过对内存中的代码段进行第一方式的处理获得第一处理结果，并将所述第一处理结果进行第二方式的处理作为参考值;

[0009] 在所述系统运行时的第一时刻，通过对所述内存中的代码段进行所述第一方式的处理获得第二处理结果，并将所述第二处理结果进行所述第二方式的处理获得第一测量值;

[0010] 判断所述第一测量值和所述参考值是否相等，若是，则所述系统可信;

[0011] 其中，所述内存中的代码段是指在所述系统的一次启动以及运行过程中，不因所述系统的正常运行而改变的代码段。

[0012] 结合第一方面，在第一方面的第一种可能的实现方式中，通过对内存中的代码段进行第一方式的处理获得第一处理结果，并将所述第一处理结果进行第二方式的处理作为

参考值，包括：

[0013] 通过对所述内存中的代码段进行哈希计算，获得所述第一处理结果；

[0014] 通过对所述第一处理结果和预设的第一值进行所述哈希计算，获得所述参考值；

[0015] 通过对所述内存中的代码段进行所述第一方式的处理获得第二处理结果，并将所述第二处理结果进行所述第二方式的处理得到第一测量值，包括：

[0016] 通过对所述内存中的代码段进行所述哈希计算，获得所述第二处理结果；

[0017] 通过对所述第二处理结果和所述第一值进行所述哈希计算，获得所述第一测量值。

[0018] 结合第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，所述第一值为所述系统复位后平台配置寄存器PCR的初始值或随机生成的值。

[0019] 结合第一方面或第一方面的第一种可能的实现方式或第一方面的第二种可能的实现方式，在第一方面的第三种可能的实现方式中，在确定所述第一测量值和所述参考值相等之后，所述方法还包括：

[0020] 将所述第二处理结果进行所述第二方式的处理，作为第一预期值；

[0021] 在所述系统运行时的第二时刻，通过对所述内存中的代码段进行所述第一方式的处理，获得第三处理结果；

[0022] 并将所述第三处理结果进行所述第二方式的处理获得第二测量值；其中，所述第二时刻在所述第一时刻之后；

[0023] 判断所述第二测量值和所述第一预期值是否相等，若是，则所述系统可信。

[0024] 结合第一方面的第三种可能的实现方式，在第一方面的第四种可能的实现方式中，将所述第二处理结果进行所述第二方式的处理，作为第一预期值，包括：

[0025] 通过对所述第二处理结果和所述参考值进行哈希计算，获得所述第一预期值；

[0026] 将所述第三处理结果进行所述第二方式的处理获得所述第二测量值，包括：

[0027] 通过对所述第三处理结果和所述第一测量值进行所述哈希计算，获得所述第二测量值。

[0028] 结合第一方面的第四种可能的实现方式，在第一方面的第五种可能的实现方式中，在确定所述第二测量值和所述第一预期值相等之后，所述方法还包括：

[0029] 通过对所述第三处理结果和所述第一预期值进行所述哈希计算，获得第二预期值。

[0030] 结合第一方面或第一方面的第一种可能的实现方式或第一方面的第二种可能的实现方式，在第一方面的第六种可能的实现方式中，在确定所述第一测量值和所述参考值相等之后，所述方法还包括：

[0031] 将所述第二处理结果进行所述第二方式的处理，作为第一预期值；

[0032] 从所述第一时刻起，在超过一个可信度量间隔的时间段之后，判断最新的参考值是否与所述第一预期值相同，若相同，则所述系统不可信。

[0033] 本申请第二方面提供一种可信度量的装置，包括：

[0034] 度量模块，用于在系统启动完成时，通过对内存中的代码段进行第一方式的处理获得第一处理结果；在所述系统运行时的第一时刻，通过对所述内存中的代码段进行所述第一方式的处理获得第二处理结果；

[0035] 处理模块，用于将所述第一处理结果进行第二方式的处理作为参考值；将所述第二处理结果进行所述第二方式的处理获得第一测量值；并判断所述第一测量值和所述参考值是否相等，若是，则所述系统可信；

[0036] 其中，所述内存中的代码段是指在所述系统的一次启动以及运行过程中，不因所述系统的正常运行而改变的代码段。

[0037] 结合第二方面，在第二方面的第一种可能的实现方式中，所述度量模块具体用于：通过对所述内存中的代码段进行哈希计算，获得所述第一处理结果；通过对所述内存中的代码段进行所述哈希计算，获得所述第二处理结果；

[0038] 所述处理模块具体用于：通过对所述第一处理结果和预设的第一值进行所述哈希计算，获得所述参考值；通过对所述第二处理结果和所述第一值进行所述哈希计算，获得所述第一测量值。

[0039] 结合第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，所述第一值为所述系统复位后平台配置寄存器PCR的初始值或随机生成的值。

[0040] 结合第二方面或第二方面的第一种可能的实现方式或第二方面的第二种可能的实现方式，在第二方面的第三种可能的实现方式中，所述处理模块具体还用于：在确定所述第一测量值和所述参考值相等之后，将所述第二处理结果进行所述第二方式的处理，作为第一预期值；

[0041] 所述度量模块还用于在所述系统运行时的第二时刻，通过对所述内存中的代码段进行所述第一方式的处理，获得第三处理结果；

[0042] 所述处理模块还用于：将所述第三处理结果进行所述第二方式的处理获得第二测量值；其中，所述第二时刻在所述第一时刻之后；判断所述第二测量值和所述第一预期值是否相等，若是，则所述系统可信。

[0043] 结合第二方面的第三种可能的实现方式，在第二方面的第四种可能的实现方式中，所述处理模块具体用于：通过对所述第二处理结果和所述参考值进行哈希计算，获得所述第一预期值；通过对所述第三处理结果和所述第一测量值进行所述哈希计算，获得第二测量值。

[0044] 结合第二方面的第四种可能的实现方式，在第二方面的第五种可能的实现方式中，所述处理模块还用于：在确定所述第二测量值和所述第一预期值相等之后，通过对所述第三处理结果和所述第一预期值进行所述哈希计算，获得所述第二预期值。

[0045] 结合第二方面或第二方面的第一种可能的实现方式或第二方面的第二种可能的实现方式，在第二方面的第六种可能的实现方式中，所述处理模块还用于：在确定所述第一测量值和所述参考值相等之后，将所述第二处理结果进行所述第二方式的处理，作为第一预期值；从所述第一时刻起，在超过一个可信度量间隔的时间段之后，判断最新的参考值是否与所述第一预期值相同，若相同，则所述系统不可信。

[0046] 本申请第三方面还提供一种计算机系统，包括：

[0047] 处理器，用于在系统启动完成时，通过对内存中的代码段进行第一方式的处理获得第一处理结果；在所述系统运行时的第一时刻，通过对所述内存中的代码段进行第一方式的处理获得第二处理结果；可信平台模块TPM芯片，用于将所述第一处理结果扩展到PCR作为参考值；所述处理器还用于将所述第二处理结果进行所述扩展获得第一测量值；并判

断所述第一测量值和所述参考值是否相等，若是，则所述系统可信；其中，所述内存中的代码段是指在所述系统的一次启动以及运行过程中，不因所述系统的正常运行而改变的代码段。

[0048] 结合第三方面，在第三方面的第一种可能的实现方式中，所述处理器具体用于：通过对所述内存中的代码段进行哈希计算，获得所述第一处理结果；通过对所述内存中的代码段进行所述哈希计算，获得所述第二处理结果；所述TPM芯片具体用于：通过对所述第一处理结果和预设的第一值进行哈希计算，获得所述参考值；所述处理器具体用于通过对所述第二处理结果和所述第一值进行哈希计算，获得所述第一测量值。

[0049] 结合第三方面的第一种可能的实现方式，在第三方面的第二种可能的实现方式中，所述第一值为系统复位后所述PCR的初始值或随机生成的值。

[0050] 结合第三方面或第三方面的第一种可能的实现方式或第三方面的第二种可能的实现方式，在第三方面的第三种可能的实现方式中，所述TPM芯片具体还用于：在确定所述第一测量值和所述参考值相等之后，将所述第二处理结果扩展到所述PCR中，作为第一预期值；

[0051] 所述处理器还用于在所述系统运行时的第二时刻，通过对所述内存中的代码段进行第一方式的处理，获得第三处理结果；将所述第三处理结果进行所述扩展获得第二测量值；判断所述第二测量值和所述第一预期值是否相等，若是，则系统可信。其中，所述第二时刻在所述第一时刻之后。

[0052] 结合第三方面的第三种可能的实现方式，在第三方面的第四种可能的实现方式中，所述TPM芯片具体用于：通过对所述第二处理结果和所述参考值进行哈希计算，获得所述第一预期值；所述处理器还用于通过对所述第三处理结果和所述第一测量值进行哈希计算，获得所述第二测量值。

[0053] 结合第三方面的第四种可能的实现方式，在第三方面的第五种可能的实现方式中，所述TPM芯片还用于：在确定所述第二测量值和所述第一预期值相等之后，通过对所述第三处理结果和所述第一预期值进行哈希计算，获得第二预期值。

[0054] 结合第三方面或第三方面的第一种可能的实现方式或第三方面的第二种可能的实现方式，在第三方面的第六种可能的实现方式中，所述TPM芯片还用于：在确定所述第一测量值和所述参考值相等之后，将所述第二处理结果扩展到所述PCR，作为第一预期值；从所述第一时刻起，在超过一个可信度量间隔的时间段之后，判断最新的参考值是否与所述第一预期值相同，若相同，则所述系统不可信。

[0055] 本申请实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

[0056] 本申请实施例中，在系统启动完成时，通过对内存中的代码段进行第一方式的处理获得第一处理结果，并将第一处理结果扩展到平台配置寄存器PCR作为参考值；在系统运行时的第一时刻，通过对内存中的代码段进行第一方式的处理获得第二处理结果，并将第二处理结果进行扩展获得第一测量值；判断第一测量值和参考值是否相等，若是，则系统可信；其中，所述内存中的代码段是指在所述系统的一次启动以及运行过程中，不因所述系统的正常运行而改变的代码段。因为在系统启动完成时，内存中的代码还没有机会被篡改，所以此时对内存中的代码段进行第一方式的处理，然后将处理结果进行第二方式的处理作为参考值。此时参考值是可信的。然后在系统运行时，可以再对内存中的代码进行第一方式的

处理，并对处理结果进行相同的第二方式的处理作为测量值，然后判断第一测量值和参考值是否相等，如果相等，则说明系统可信。如果在系统运行过程中，内存中的代码未被篡改，那么第一测量值就会等于参考值。如果按照相同处理方式处理得到的第一测量值不等于参考值，因为该代码段不会因为系统的正常运行而改变，所以只能是内存中的代码已经被篡改，所以可以得知此时系统是不可信的。由此可以看出，本申请实施例提供了一种在系统启动后，对系统的可信度量方法，可以度量出系统在运行期间是否可信。

附图说明

[0057] 图1为本申请一实施例中的可信度量方法的流程图；

[0058] 图2为本申请一实施例中的可信度量装置的功能框图；

[0059] 图3为本申请一实施例中的计算机系统的系统框图。

具体实施方式

[0060] 本申请实施例提供一种可信度量方法及装置，用以解决现有技术中的系统启动后无法进行可信度量的技术问题。

[0061] 为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0062] 本申请一实施例提供一种可信度量方法，请参考图1所示，为本申请实施例中可信度量方法的流程图，该方法包括以下内容：

[0063] 步骤101：在系统启动完成时，通过对内存中的代码段进行第一方式的处理获得第一处理结果，并将第一处理结果进行第二方式的处理作为参考值；

[0064] 步骤102：在系统运行时的第一时刻，通过对内存中的代码段进行第一方式的处理获得第二处理结果，并将第二处理结果进行第二方式的处理获得第一测量值；

[0065] 步骤103：判断第一测量值和参考值是否相等，若是，则系统可信。

[0066] 其中，本实施例中的代码段，是指在系统的一次启动以及运行过程中，不因所述系统的正常运行而改变的代码段。所述代码段可以是内存中所有的代码段，例如，在嵌入式系统中，系统启动完成后，所有代码都将驻留在内存，并且不会因为系统的正常运行而改变。所述代码段也可以是内存中的部分代码段，例如在一些非嵌入式系统中，部分代码段是固定的，一些应用的代码段通常在应用运行时才会加载到内存中，当应用关闭之后，该部分代码段又会被从内存中删除掉，所以整个内存中的代码段会随着系统的正常运行而发生改变，所以该种情况下的代码段是指非嵌入式系统中的固定的那部分代码段。

[0067] 可选的，在系统启动过程中可以进行如背景技术中所描述的由TPM芯片执行的可信度量过程。如此可以保证系统在启动完成时是可信的。

[0068] 当系统启动完成时，此时内存中的代码段还没有机会被篡改，此时内存中的代码段是可信的，所以此时就执行步骤101，通过对内存中的代码段进行第一方式的处理获得第二处理结果。其中，第一方式的处理，具体来说，例如是哈希计算。在哈希计算时，两组数据的哈希值仅在相应数据也匹配时才应当匹配。数据的少量更改会在哈希值中产生不可预知

的大量更改。因此，只要内存中的代码段相同，那么哈希计算得到的哈希值一定是相同的。而当内存中的代码段是不相同的，那么经过哈希计算得到的哈希值一定是不相同的。换言之，第一方式的处理得到的处理结果需要在内存中的代码段不同时，一定是不相同的。因此，第一方式的处理除了可以是哈希计算之外，其他满足前述条件的计算方式均可。

[0069] 在本实施例中，第一处理方式以哈希计算为例。那么通过对内存中的代码段进行第一方式的处理获得第一处理结果，包括：通过对内存中的代码段进行哈希计算，获得第一处理结果。第一处理结果例如是一个固定长度的信息摘要。其中，长度和具体采用的哈希算法相关。通过哈希算法处理之后，数据量变小，所以可以节约存储空间。

[0070] 当获得第一处理结果之后，并将第一处理结果进行第二方式的处理作为参考值。第二方式的处理，具体例如是：进行加密处理，或者是按照一定规则进行存储。通过该步骤可以增加数据被破解的难度。

[0071] 其中，一种可能的方式是：为了保证第一处理结果的安全性，在步骤101中，将第一处理结果进行第二方式的处理作为参考值，具体为：将第一处理结果扩展到平台配置寄存器(英文：Platform Configuration Registers；简称：PCR)作为参考值。

[0072] 关于PCR，为了防止PCR中的值被恶意代码随便篡改或伪造，TPM限制对PCR的操作，不能像普通字符设备的寄存器那样通过端口映射来随意进行读写操作。而且PCR位于TPM内部，其内部数据受到TPM的保护。TPM只允许两种操作来修改PCR的值：重置操作(Reset)和扩展操作(Extend)。重置操作发生在机器断电或者系统重新启动之后，PCR的值自动重新清零。

[0073] 系统运行过程中，只能通过扩展操作来改变PCR的内容。扩展操作：PCR[i]＝哈希算法(PCR[i-1]||新度量值)。其中，i为正整数。扩展操作是不可逆的，即先扩展度量值A再扩展度量值B所得到的PCR值跟先扩展B再扩展A的结果是不同的。通过扩展，PCR能够记录一个无限长的度量值序列，这一系列度量值组成的序列反应了系统状态的变迁。这个扩展序列中的某一个度量值被改变了，之后的度量序列都会受到影响。

[0074] 因此，将第一处理结果扩展到PCR作为参考值，即对PCR进行扩展操作。根据前述扩展操作的公式，具体来说，通过对第一处理结果和第一值进行相同的哈希计算，就获得了该参考值。其中，第一处理结果对应公式中的新度量值，第一值对应公式中的PCR[i-1]，参考值对应公式中的PCR[i]。在实际运用中，第一值为系统复位后的PCR的初始值或随机生成的值。通常来讲，系统复位时，对PCR进行前述的重置操作，那么PCR的初始值为0x00。而随机生成的值，被获取或篡改的难度较大，所以更可靠。当然，在实际运用中，如果在启动过程中执行可信度量的话，第一值具体也可以是启动过程中可信度量的最后一个值。

[0075] 在系统启动完成时，执行步骤101，获得参考值。接下来在系统运行过程中的第一时刻，再次对内存中的代码段进行度量，即执行步骤102，通过对内存中的代码段进行前述第一方式的处理获得第二处理结果，并将第二处理结果进行第二方式的处理，例如将第二处理结果进行所述扩展获得第一测量值。其中，再次对内存中的代码段进行度量，采用的是和步骤101相同的方式，这样可以保证度量标准相同。另外，当在步骤101中，为了第一处理结果的安全性，就将第一处理结果扩展到PCR作为参考值，也保证了参考值不容易被篡改。因此，在步骤102中，也要对第二处理结果做相同的扩展操作，只是可以不用扩展到PCR，只是做相同的扩展操作即可，此时获得第一测量值。

[0076] 因此，与步骤101类似的，步骤102具体包括：通过对所述内存中的代码段进行相同的哈希计算，获得第二处理结果；通过对第二处理结果和第一值进行相同的哈希计算，获得第一测量值。

[0077] 接下来执行步骤103，即判断第一测量值和所述参考值是否相等。因为第一测量值和参考值均为对内存中的代码段进行相同的处理，并将处理结果进行相同的扩展操作得到的，只是在不同时机获得的。因此，若第一测量值和所述参考值相同，则表示内存中的代码段是相同的，换言之，在第一时刻，内存中的代码段相比系统刚启动时没有发生变化，也即在第一时刻，内存中的代码段还没有被篡改，所以系统是可信的。如果判断的结果是第一测量值和所述参考值不同，则说明在第一时刻，内存中的代码段已经发生变化，即已经被篡改，说明此时系统不可信。

[0078] 在系统运行过程中，可以重复执行步骤102和步骤103，例如周期性的执行，以对系统是否可信进行实时的监控。

[0079] 需要说明的是，在执行步骤102时，为避免可信度量程序本身，即步骤102的处理方式被篡改，由恶意程序每次都返回和参考值相同的第一测量值，每次步骤103的判断结果都是第一测量值和参考值相等，得出系统可信的结果，但其实内存中的代码已经被篡改的情况，可信度量程序本身可以固化在芯片中，例如固化在中央处理器(英文：Central Processing Unit；简称：CPU)中，此程序不允许进行任何更新操作，永久只读执行，如此可保证可信度量程序本身不被篡改，那么每次获得的第一测量值都是真实的，这样在步骤103中得出的结论才是正确的。在该情况下，可以由CPU的安全引擎周期性的执行步骤102。

[0080] 如果可信度量程序本身没有固化在芯片中时，可以通过以下方式进一步增加可信度量的可靠性。

[0081] 具体来说，在步骤103中，判断第一测量值和所述参考值相等之后，该方法还包括：将第二处理结果进行第二方式的处理，例如将第二处理结果扩展到所述PCR中，作为第一预期值；在系统运行时的第二时刻，通过对内存中的代码段进行第一方式的处理，获得第三处理结果；并将所述第三处理结果进行第二方式的处理获得第二测量值；其中，所述第二时刻在所述第一时刻之后；判断第二测量值和第一预期值是否相等，若是，则系统可信。

[0082] 其中，扩展操作的原理与前述扩展操作的原理相同。将第二处理结果扩展到所述PCR中，作为第一预期值，具体为：通过对第二处理结果和所述参考值进行哈希计算，获得第一预期值。因为第一测量值和参考值相等，则说明内存中的代码未被篡改，那么说明第二处理结果是可信的，所以可以将第二处理结果扩展到PCR，作为第一预期值。而第一预期值即作为下次判断的参考值。换言之，将新的度量结果扩展到PCR作为新的参考值，参考值随着度量次数的增加在逐次变化。如此可以增加黑客获取参考值的难度，提高安全性。

[0083] 在系统运行时的第二时刻，再次度量内存中的代码段，即通过对内存中的代码段进行第一方式的处理，获得第三处理结果，并将第三处理结果进行相同的扩展获得第二测量值。其具体实现方式与步骤102类似，只是在不同时刻执行。在第二时刻的执行过程中，将第三处理结果进行扩展获得第二测量值，具体为：通过对第三处理结果和第一测量值进行哈希计算，获得第二测量值。因为第一测量值和参考值相等，所以在第二时刻的处理过程中，如果内存中的代码段如果没有被篡改的话，获得的第三处理结果就和第二处理结果是相同的，那么对第三处理结果和第二处理结果进行相同的扩展操作之后获得的第二测量值

和第一预期值就是相等的，所以通过判断第二测量值和第一预期值是否相等，就可以确定出在第二时刻的度量结果，即第二时刻，系统是否可信。如果相等，则说明系统可信，如果不相等，则说明系统不可信。

[0084] 因此，该度量方式也可以看作是根据所述参考值和第二处理结果，先计算出一个预期值，然后再度量当前内存中的代码，然后比对度量结果是否符合预期值，如果符合，就说明系统可信，如果不符合，就说明系统不可信。

[0085] 然后，可以继续按照这样的度量方式往下循环，例如：在确定第二测量值和第一预期值相等之后，该方法还包括：通过对第三处理结果和第一预期值进行哈希计算，获得第二预期值。那么第二预期值就作为下次可信度量的参考值。

[0086] 可选的，如果第一测量值和所述参考值不相等，就不会将第二测量结果进行扩展获得第一预期值，那么PCR中的参考值就不会发生变化。类似的，如果第二测量值和第一预期值不相等，也不会将第三处理结果进行扩展获得第二预期值，那么PCR中的参考值就还是第一预期值。或者是系统被攻击，无法执行度量操作，那么PCR中最新的参考值也不会发生变化。因此也可以通过判断PCR中的最新参考值相对前次的参考值是否有变化来确定系统是否可信，如果没有变化，那么系统不可信。如果有变化，可以认为系统可信，但为了提高可靠性，可以在下次度量之后，将度量结果与最新的参考值进行比较，如若相等，则系统可信，若不相等，则不可信。

[0087] 举例来说，例如在步骤103中判断第一测量值和参考值是相等的，那么就将第二处理结果进行第二方式的处理，例如扩展到PCR中，作为第一预期值。那么从第一时刻起，在超过一个可信度量间隔的时间段之后，即第二时刻之后，并在下个度量时刻之前，例如第三时刻之前，判断PCR中最新的参考值是否与第一预期值相同，若相同，则表示在第二时刻的度量中，第二测量值和第一预期值不相等，或者在第二时刻就没有度量，说明系统已被攻击，已经不可信。若不相同，则表示在第二时刻的度量中，第二测量值和第一预期值是相等的，所以才会有第二预期值，即最新的参考值，所以可以说明此时系统是可信的。

[0088] 其中，PCR可以自己判断最新参考值相对前次的参考值是否有变化，然后将判断结果输出，例如告警。也可以是网管等管理设备读取PCR中最新的参考值和前次的参考值，如果发现在超出度量间隔的时间段之后，最新的参考值并未发生变化，则认为系统已经被攻击，此时可以进行告警。

[0089] 可选的，还可以设置硬件狗的功能，具体来说，在发现在超出度量间隔的时间段之后，最新的参考值并未发生变化，就强制重启系统。

[0090] 可选的，本申请实施例中的可信度量方法可以适用于嵌入式系统，也可以适用于其他固定代码段的软件系统，或者在包括动态分配地址的代码段的系统中。当然，也可以运用在非嵌入式系统中。

[0091] 由以上描述可以看出，通过本实施例中的可信度量方法，可以在系统启动之后，对系统进行可信度量，能够实时感知代码的完整性状态，有助于快速发现黑客的恶意代码植入和篡改风险。尤其对于电信级的设备，系统重启通常是数月甚至数年才能进行一次，所以系统启动之后的可信度量意义更重大。

[0092] 基于同一发明构思，本申请实施例还提供一种可信度量装置，请参考图2所示，该装置包括：度量模块201，用于在系统启动完成时，通过对内存中的代码段进行第一方式的

处理获得第一处理结果；在系统运行时的第一时刻，通过对内存中的代码段进行第一方式的处理获得第二处理结果；处理模块202，用于将第一处理结果进行第二方式的处理作为参考值；将第二处理结果进行第二方式的处理获得第一测量值；并判断第一测量值和参考值是否相等，若是，则系统可信。其中，内存中的代码段与前述实施例中的含义相同。

[0093] 可选的，度量模块201具体用于：通过对内存中的代码段进行哈希计算，获得第一处理结果；通过对内存中的代码段进行哈希计算，获得第二处理结果；处理模块202具体用于：通过对第一处理结果和预设的第一值进行哈希计算，获得参考值；通过对第二处理结果和第一值进行哈希计算，获得第一测量值。

[0094] 可选的，第一值为系统复位后PCR的初始值或随机生成的值。

[0095] 可选的，处理模块202具体还用于：在确定第一测量值和参考值相等之后，将第二处理结果进行第二方式的处理，作为第一预期值；

[0096] 度量模块201还用于在系统运行时的第二时刻，通过对内存中的代码段进行第一方式的处理，获得第三处理结果；

[0097] 处理模块202还用于：将第三处理结果进行第二方式的处理获得第二测量值；其中，第二时刻在第一时刻之后；判断第二测量值和第一预期值是否相等，若是，则系统可信。

[0098] 可选的，处理模块202具体用于：通过对第二处理结果和参考值进行哈希计算，获得第一预期值；通过对第三处理结果和第一测量值进行哈希计算，获得第二测量值。

[0099] 可选的，处理模块202还用于：在确定第二测量值和第一预期值相等之后，通过对第三处理结果和第一预期值进行哈希计算，获得第二预期值。

[0100] 可选的，处理模块202还用于：在确定第一测量值和参考值相等之后，将第二处理结果进行第二方式的处理，作为第一预期值；从第一时刻起，在超过一个可信度量间隔的时间段之后，判断最新的参考值是否与第一预期值相同，若相同，则系统不可信。

[0101] 前述图1实施例中的可信度量方法中的各种变化方式和具体实例同样适用于本实施例的可信度量装置，通过前述对可信度量方法的详细描述，本领域技术人员可以清楚的知道本实施例中可信度量装置的实施方法，所以为了说明书的简洁，在此不再详述。

[0102] 基于同一发明构思，本申请实施例还包括一种计算机系统，请参考图3所示，为本申请实施例中的计算机系统的系统框图。如图3所述，该系统包括：处理器301，用于在系统启动完成时，通过对内存中的代码段进行第一方式的处理获得第一处理结果；在系统运行时的第一时刻，通过对内存中的代码段进行第一方式的处理获得第二处理结果；TPM芯片303，用于将第一处理结果扩展到PCR作为参考值；处理器301还用于将第二处理结果进行所述扩展获得第一测量值；并判断第一测量值和参考值是否相等，若是，则系统可信。其中，内存中的代码段与前述实施例中的含义相同。

[0103] 可选的，处理器301具体用于：通过对内存中的代码段进行哈希计算，获得第一处理结果；通过对内存中的代码段进行哈希计算，获得第二处理结果；TPM芯片303具体用于：通过对第一处理结果和预设的第一值进行哈希计算，获得参考值；处理器301具体用于通过对第二处理结果和第一值进行哈希计算，获得第一测量值。

[0104] 可选的，第一值为系统复位后PCR的初始值或随机生成的值。

[0105] 可选的，TPM芯片303具体还用于：在确定第一测量值和参考值相等之后，将第二处理结果扩展到PCR中，作为第一预期值；

[0106] 处理器301还用于在系统运行时的第二时刻，通过对内存中的代码段进行第一方式的处理，获得第三处理结果；将第三处理结果进行所述扩展获得第二测量值；判断第二测量值和第一预期值是否相等，若是，则系统可信。其中，第二时刻在第一时刻之后。

[0107] 可选的，TPM芯片303具体用于：通过对第二处理结果和参考值进行哈希计算，获得第一预期值；处理器301还用于通过对第三处理结果和第一测量值进行哈希计算，获得第二测量值。

[0108] 可选的，TPM芯片303还用于：在确定第二测量值和第一预期值相等之后，通过对第三处理结果和第一预期值进行哈希计算，获得第二预期值。

[0109] 可选的，TPM芯片303还用于：在确定第一测量值和参考值相等之后，将第二处理结果扩展到PCR，作为第一预期值；从第一时刻起，在超过一个可信度量间隔的时间段之后，判断最新的参考值是否与第一预期值相同，若相同，则系统不可信。

[0110] 在以上各实施例中，PCR位于TPM芯片303上。

[0111] 其中，在图3中，总线架构(用总线300来代表)，总线300可以包括任意数量的互联的总线和桥，总线300将包括由处理器301代表的一个或多个处理器和存储器302代表的存储器的各种电路链接在一起。总线300还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口304在总线300和处理器301、TPM芯片303之间提供接口。取决于计算机系统的性质，还可以提供用户接口305，例如小键盘、显示器、扬声器、麦克风、操纵杆。

[0112] 处理器301负责管理总线300和通常的处理，而存储器302可以被用于存储处理器301在执行操作时所使用的数据。

[0113] 前述图1实施例中的可信度量方法中的各种变化方式和具体实例同样适用于本实施例的计算机系统，通过前述对可信度量方法的详细描述，本领域技术人员可以清楚的知道本实施例中计算机系统的实施方法，所以为了说明书的简洁，在此不再详述。

[0114] 申请实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

[0115] 则系统可信；其中，所述内存中的代码段是指在所述系统的一次启动以及运行过程中，不因所述系统的正常运行而改变的代码段。因为在系统启动完成时，内存中的代码还没有机会被篡改，所以此时对内存中的代码段进行第一方式的处理，然后将处理结果进行第二方式的处理作为参考值。此时参考值是可信的。然后在系统运行时，可以再对内存中的代码进行第一方式的处理，并对处理结果进行相同的第二方式的处理作为测量值，然后判断第一测量值和参考值是否相等，如果相等，则说明系统可信。如果在系统运行过程中，内存中的代码未被篡改，那么第一测量值就会等于参考值。如果按照相同处理方式处理得到的第一测量值不等于参考值，因为该代码段不会因为系统的正常运行而改变，所以只能是内存中的代码已经被篡改，所以可以得知此时系统是不可信的。由此可以看出，本申请实施例提供了一种在系统启动后，对系统的可信度量方法，可以度量出系统在运行期间是否可信。

[0116] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器和光学存储器等)上实施的计算机程序产品的形

式。

[0117] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0118] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0119] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0120] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

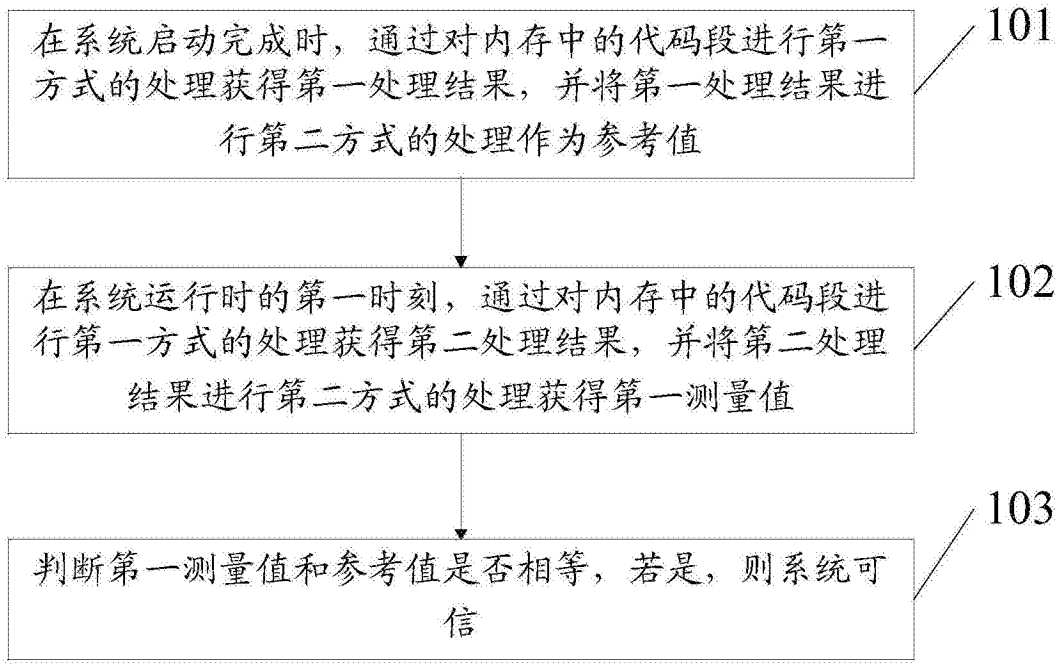

在系统启动完成时，通过对内存中的代码段进行第一方式的处理获得第一处理结果，并将第一处理结果进行第二方式的处理作为参考值
101
在系统运行时的第一时刻，通过对内存中的代码段进行第一方式的处理获得第二处理结果，并将第二处理结果进行第二方式的处理获得第一测量值
102
判断第一测量值和参考值是否相等，若是，则系统可信
103

图1

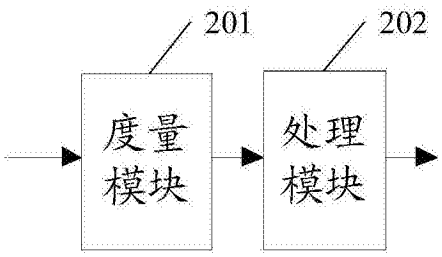

201
202
度量模块
处理模块

图2

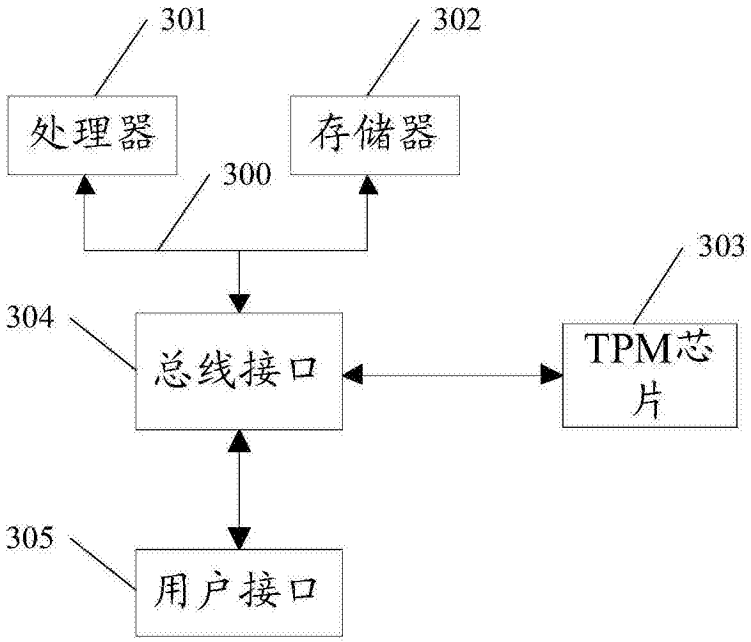


图3