(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106164872 A
(43)申请公布日 2016.11.23

(21)申请号 201580019549.8

(22)申请日 2015.04.14

(30)优先权数据
14/256,681 2014.04.18 US

(85)PCT国际申请进入国家阶段日
2016.10.13

(86)PCT国际申请的申请数据
PCT/US2015/025685 2015.04.14

(87)PCT国际申请的公布数据
WO2015/160759 EN 2015.10.22

(71)申请人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 C·E·阿卡尔
埃里希·詹姆士·普罗恩德克
罗伯特·J·图尔纳
B·B·布伦利

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 宋献涛

(51)Int.Cl.
G06F 11/36(2006.01)

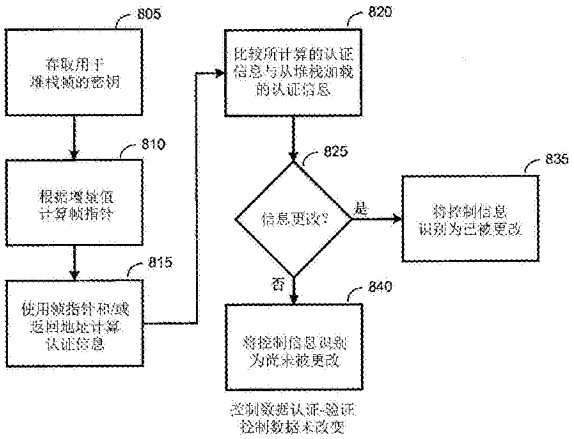
权利要求书3页 说明书12页 附图7页

(54)发明名称

基于硬件的堆栈控制信息保护

(57)摘要

本发明提供用于保护与处理器相关的堆栈的内容的技术。所述技术包含一种方法，所述方法包含：从正通过所述处理器执行的软件程序接收存储指令，所述存储指令包含与子例程相关的控制信息；响应于从所述软件程序接收所述存储指令，更改所述控制信息以产生受保护的控制信息；在所述堆栈上存储所述受保护的控制信息；从所述软件程序接收加载指令；以及响应于从所述软件程序接收所述加载指令，从所述堆栈加载所述受保护的控制信息，更改所述受保护的控制信息以恢复所述控制信息，和将所述控制信息返回到所述软件程序。



CN 106164872 A

1.一种用于保护与处理器相关的堆栈的内容的方法,所述方法包括:

从正通过所述处理器执行的软件程序接收存储指令,所述存储指令包含与子例程相关的控制信息;

响应于从所述软件程序接收所述存储指令,更改所述控制信息以产生受保护的控制信息;

在所述堆栈上存储所述受保护的控制信息;

从所述软件程序接收加载指令;以及

响应于从所述软件程序接收所述加载指令,

从所述堆栈加载所述受保护的控制信息,

更改所述受保护的控制信息以恢复所述控制信息,以及

将所述控制信息返回到所述软件程序。

2.根据权利要求1所述的方法,其中更改所述控制信息以产生所述受保护的控制信息包括:

加密所述控制信息以产生所述受保护的控制信息。

3.根据权利要求2所述的方法,其中所述加密所述控制信息以产生所述受保护的控制信息包括使用基于分块密码的消息认证码算法加密所述控制信息。

4.根据权利要求2所述的方法,其中所述加密所述控制信息以产生所述受保护的控制信息包括使用与当前堆栈帧相关的密钥加密所述控制信息,所述当前堆栈帧与所述子例程相关。

5.根据权利要求2所述的方法,其中更改所述受保护的控制信息以恢复所述控制信息包括:

解密所述受保护的控制信息以恢复所述控制信息。

6.根据权利要求1所述的方法,其中更改所述控制信息以产生所述受保护的控制信息包括:

添加认证标签到所述控制信息以产生所述受保护的控制信息。

7.根据权利要求6所述的方法,其中所述认证标签与当前堆栈帧相关,所述当前堆栈帧与所述子例程相关。

8.根据权利要求6所述的方法,其中更改所述受保护的控制信息以恢复所述控制信息包括从所述受保护的控制信息导出帧指针和返回地址。

9.根据权利要求8所述的方法,其中更改所述受保护的控制信息以恢复所述控制信息包括:

应用消息认证码到所述帧指针和所述返回地址以产生标签值;以及

比较所述标签值与包含于所述受保护的控制信息中的所述认证标签来验证所述控制信息在所述堆栈上时未被更改。

10.一种处理器,其用于保护与所述处理器相关的堆栈的内容,所述处理器包括:

用于从正通过所述处理器执行的软件程序接收存储指令的装置,所述存储指令包含与子例程相关的控制信息;

用于响应于从所述软件程序接收所述存储指令,更改所述控制信息以产生受保护的控制信息的装置;

用于在所述堆栈上存储所述受保护的控制信息的装置；

用于从所述软件程序接收加载指令的装置；以及

响应于从所述软件程序接收所述加载指令，

用于从所述堆栈加载所述受保护的控制信息的装置，

用于更改所述受保护的控制信息以恢复所述控制信息的装置，以及

用于将所述控制信息返回到所述软件程序的装置。

11.根据权利要求10所述的处理器，其中用于更改所述控制信息以产生所述受保护的控制信息的所述装置包括：

用于加密所述控制信息以产生所述受保护的控制信息的装置。

12.根据权利要求11所述的处理器，其中用于加密所述控制信息以产生所述受保护的控制信息的所述装置包括用于使用基于分块密码的消息认证码算法加密所述控制信息的装置。

13.根据权利要求11所述的处理器，其中用于加密所述控制信息以产生所述受保护的控制信息的所述装置包括用于使用与当前堆栈帧相关的密钥加密所述控制信息的装置，所述当前堆栈帧与所述子例程相关。

14.根据权利要求11所述的处理器，其中用于更改所述受保护的控制信息以恢复所述控制信息的所述装置包括：

用于解密所述受保护的控制信息以恢复所述控制信息的装置。

15.根据权利要求10所述的处理器，其中用于更改所述控制信息以产生所述受保护的控制信息的所述装置包括：

用于添加认证标签到所述控制信息以产生所述受保护的控制信息的装置。

16.根据权利要求15所述的处理器，其中所述认证标签与当前堆栈帧相关，所述当前堆栈帧与所述子例程相关。

17.根据权利要求15所述的处理器，其中用于更改所述受保护的控制信息以恢复所述控制信息的所述装置包括用于从所述受保护的控制信息导出帧指针和返回地址的装置。

18.根据权利要求17所述的处理器，其中用于更改所述受保护的控制信息以恢复所述控制信息的所述装置包括：

用于应用消息认证码到所述帧指针和所述返回地址以产生标签值的装置；以及

用于比较所述标签值与包含于所述受保护的控制信息中的所述认证标签来验证所述控制信息在所述堆栈上时未被更改的装置。

19.一种系统，其包括：

存储器；

所述存储器中的堆栈，其用于存储与一或多个子例程相关的数据；以及

耦合到所述存储器的处理器，所述处理器经配置以执行处理器可执行指令，所述处理器可执行指令经配置以使所述处理器进行以下操作：

从正通过所述处理器执行的软件程序接收存储指令，所述存储指令包含与子例程相关的控制信息；

响应于从所述软件程序接收所述存储指令，更改所述控制信息以产生受保护的控制信息；

在所述堆栈上存储所述受保护的控制信息；

从所述软件程序接收加载指令；以及

响应于从所述软件程序接收所述加载指令，所述处理器经配置以

从所述堆栈加载所述受保护的控制信息，

更改所述受保护的控制信息以恢复所述控制信息，以及

将所述控制信息返回到所述软件程序。

20.根据权利要求19所述的系统，其中经配置以更改所述控制信息以产生所述受保护的控制信息的所述处理器进一步经配置以：

加密所述控制信息以产生所述受保护的控制信息。

21.根据权利要求20所述的系统，其中所述处理器经配置以使用基于分块密码的消息认证码算法加密所述控制信息。

22.根据权利要求20所述的系统，其中所述处理器经配置以使用与当前堆栈帧相关的密钥加密所述控制信息，所述当前堆栈帧与所述子例程相关。

23.根据权利要求20所述的系统，其中所述处理器经配置以解密所述受保护的控制信息，从而恢复所述控制信息。

24.根据权利要求19所述的系统，其中经配置以更改所述控制信息以产生所述受保护的控制信息的所述处理器进一步经配置以：

添加认证标签到所述控制信息以产生所述受保护的控制信息。

25.根据权利要求24所述的系统，其中所述认证标签与当前堆栈帧相关，所述当前堆栈帧与所述子例程相关。

26.根据权利要求24所述的系统，其中经配置以更改所述受保护的控制信息以恢复所述控制信息的所述处理器进一步经配置以从所述受保护的控制信息导出帧指针和返回地址。

27.根据权利要求26所述的系统，其中经配置以更改所述受保护的控制信息以恢复所述控制信息的所述处理器进一步经配置以：

应用消息认证码到所述帧指针和所述返回地址以产生标签值；以及

比较所述标签值与包含于所述受保护的控制信息中的所述认证标签来验证所述控制信息在所述堆栈上时未被更改。

基于硬件的堆栈控制信息保护

背景技术

[0001] 软件实施错误，例如遗漏或不正确输入验证，可导致越界缓冲区存取和内存损坏。这些实施错误可导致软件在正常条件下变得不稳定或最终失效。然而，当输入由意图攻击计算机系统的恶意方操控时，攻击者可利用这些内存损坏和溢出错误来改变软件代码的预期行为，并执行由攻击者确定的代码或功能。

[0002] 攻击者通常通过覆写在存储器中的数据结构(例如返回解决、函数指针或虚表指针)取得对执行的控制。在大型和传统的代码库中发现和修理全部可利用的内存损坏错误并不总是可能的。因此，许多计算机系统含有被称作“攻击缓解机制”的一般防御特征，其有效地对抗攻击者用来利用这些错误取得对目标计算机系统的控制和/或破坏目标计算机系统的熟知技术。

[0003] 通常包含于计算机系统中的攻击缓解机制的一些实例包含：数据执行防止(DEP)、堆栈保护(SP)和地址空间布局随机化(ASLR)。在DEP技术中，全部代码区被标记为只读，并且全部可写入区域不可执行。通常，代码区的只读特性和可写入区的不可执行特性通过处理器的内存管理单元(MMU)强制执行。此技术可防止攻击者将其自己的代码放置到数据区中并引导执行流到那一代码。在SP方法中，编译程序实施用于检测堆栈上的缓冲区溢出。由于就在局部数组后的堆栈上经常存在返回地址或所保存的链接寄存器，所以基于堆栈的缓冲区溢出会很容易被利用。攻击者可使局部数组溢出并覆写返回地址/链接寄存器，且重新引导软件的执行流。许多常规堆栈保护实施方案插入保护值到函数序言中的堆栈上，并且在从那个函数返回之前，检查那个值的修改。如果已发生缓冲区溢出，那么保护值连同返回地址将已经被覆写，因为保护值位于缓冲区和返回地址之间的堆栈中。保护值必须是随机和/或不可预测的值，以确保SP方法的安全。在ASLR方法中，应用程序的内存布局可在每次执行时随机化。例如，可随机确定用于代码、静态数据、堆栈和堆的基地址。此方法使得利用难以进行，因为攻击者需要预测他们需要瞄准/操控以进行成功攻击的代码/数据/指针的位置。

发明内容

[0004] 根据本发明的用于保护与处理器相关的堆栈的内容的实例方法包含：从通过处理器执行的软件程序接收存储指令，所述存储指令包含与子例程相关的控制信息；响应于从软件程序接收存储指令，更改控制信息以产生受保护的控制信息；在堆栈上存储受保护的控制信息；从软件程序接收加载指令；以及响应于从软件程序接收加载指令，从堆栈加载受保护的控制信息，更改受保护的控制信息以恢复控制信息，和将控制信息返回到软件程序。

[0005] 这种方法的实施方案可包含以下特征中的一或多者。更改控制信息以产生受保护的控制信息包含加密控制信息以产生受保护的控制信息。加密控制信息以产生受保护的控制信息包含使用基于分块密码的消息认证码算法加密控制信息。加密控制信息以产生受保护的控制信息包含使用与当前堆栈帧相关的密钥加密控制信息，所述当前堆栈帧与子例程相关。更改受保护的控制信息以恢复控制信息包含解密受保护的控制信息以恢复控制信

息。更改控制信息以产生受保护的控制信息包含添加认证标签到控制信息以产生受保护的控制信息。认证标签与当前堆栈帧相关，所述当前堆栈帧与子例程相关。更改受保护的控制信息以恢复控制信息包含从受保护的控制信息导出帧指针和返回地址。更改受保护的控制信息以恢复控制信息包含应用消息认证码到帧指针和返回地址以产生标签值，以及比较标签值与包含于受保护的控制信息中的认证标签来验证控制信息在堆栈上时未被更改。

[0006] 根据本发明的用于保护与处理器相关的堆栈的内容的实例处理器包含用于从正通过处理器执行的软件程序接收存储指令的装置，所述存储指令包含与子例程相关的控制信息，用于更改控制信息以响应于从软件程序接收存储指令产生受保护的控制信息的装置、用于在在堆栈上存储受保护的控制信息的装置、用于从软件程序接收加载指令的装置；以及响应于从软件程序接收加载指令，用于从堆栈加载受保护的控制信息的装置、用于更改受保护的控制信息以恢复控制信息的装置，和用于将控制信息返回到软件程序的装置。

[0007] 这种处理器的实施方案可包含以下特点中的一或多者。用于更改控制信息以产生受保护的控制信息的装置包含用于加密控制信息以产生受保护的控制信息的装置。用于加密控制信息以产生受保护的控制信息的装置包含用于使用基于分块密码的消息认证码算法加密控制信息的装置。用于加密控制信息以产生受保护的控制信息的装置包含用于使用与当前堆栈帧相关的密钥加密控制信息的装置，所述当前堆栈帧与子例程相关。用于更改受保护的控制信息以恢复控制信息的装置包含用于解密受保护的控制信息以恢复控制信息的装置。用于更改控制信息以产生受保护的控制信息的装置包含用于添加认证标签到控制信息以产生受保护的控制信息的装置。认证标签与当前堆栈帧相关，所述当前堆栈帧与子例程相关。用于更改受保护的控制信息以恢复控制信息的装置包含用于从受保护的控制信息导出帧指针和返回地址的装置。用于更改受保护的控制信息以恢复控制信息的装置包含用于应用消息认证码到帧指针和返回地址以产生标签值的装置，以及用于比较标签值与包含于受保护的控制信息中的认证标签来验证控制信息在堆栈上时未被更改的装置。

[0008] 根据本发明的实例系统包含存储器、用于存储与一或多个子例程相关的数据的存储器中的堆栈，以及耦合到存储器的处理器。处理器经配置以执行处理器可执行指令，所述处理器可执行指令经配置以使处理器进行以下操作：从正通过处理器执行的软件程序接收存储指令，所述存储指令包含与子例程相关的控制信息；响应于从软件程序接收存储指令，更改控制信息以产生受保护的控制信息；在堆栈上存储受保护的控制信息；从软件程序接收加载指令；以及响应于从软件程序接收加载指令，处理器经配置以从堆栈加载受保护的控制信息，更改受保护的控制信息以恢复控制信息，和将控制信息返回到软件程序。

[0009] 这种系统的实施方案可包含以下特征中的一或多者。经配置以更改控制信息以产生受保护的控制信息的处理器进一步经配置以加密控制信息以产生受保护的控制信息。处理器经配置以使用基于分块密码的消息认证码算法加密控制信息。处理器经配置以使用与当前堆栈帧相关的密钥加密控制信息，所述当前堆栈帧与子例程相关。处理器经配置以解密受保护的控制信息，从而恢复控制信息。经配置以更改控制信息以产生受保护的控制信息的处理器进一步经配置以添加认证标签到控制信息以产生受保护的控制信息。认证标签与当前堆栈帧相关，所述当前堆栈帧与子例程相关。经配置以更改受保护的控制信息以恢复控制信息的处理器进一步经配置以从受保护的控制信息导出帧指针和返回地址。经配置以更改受保护的控制信息以恢复控制信息的处理器进一步经配置以应用消息认证码到帧

指针和返回地址以产生标签值，以及比较标签值与包含于受保护的控制信息中的认证标签来验证控制信息在堆栈上时未被更改。

附图说明

[0010] 图1是其中可实施本文中所论述的基于硬件的堆栈控制信息保护技术的实例计算机系统的功能框图。

[0011] 图2是来自图1的实例计算机系统的功能框图，示出了可用于实施本文所揭示的基于硬件的堆栈控制信息技术的控制数据认证技术的实施方案。

[0012] 图3是来自图1的实例计算机系统的功能框图，示出了可用于实施本文所揭示的基于硬件的堆栈控制信息技术的控制数据加密技术的实施方案。

[0013] 图4是用于保护与处理器相关的堆栈的内容的过程的流程图，所述处理器可用于实施本文所揭示的基于硬件的堆栈控制技术。

[0014] 图5是用于使用控制数据认证技术更改控制信息以产生受保护的控制信息的过程的流程图。

[0015] 图6是用于在堆栈上存储受保护的控制信息的过程的流程图。

[0016] 图7是用于从堆栈加载受保护的控制信息的过程的流程图。

[0017] 图8是用于确定使用控制数据认证技术所产生的受保护的控制信息在堆栈上时是否已被更改的过程的流程图。

[0018] 图9是用于使用控制数据加密技术更改控制信息以产生受保护的控制信息的过程的流程图。

[0019] 图10是用于在堆栈上存储受保护的控制信息的过程的流程图。

[0020] 图11是用于从堆栈加载受保护的控制信息的过程的流程图。

[0021] 图12是用于确定使用控制数据加密技术所产生的受保护的控制信息在堆栈上时是否已被更改的过程的流程图。

具体实施方式

[0022] 本文所揭示的技术经配置以提供基于硬件的堆栈控制信息保护。所述技术可防止恶意攻击者修改返回地址(或链接寄存器)、帧指针和/或堆栈上的其它控制信息的内容，以取得对计算机系统的控制，或使其上被执行的软件的行为变得不稳定。本文所揭示的技术包含控制数据认证和控制数据加密技术，当控制信息使成功更改堆栈上的控制信息更为困难时，所述技术可用于识别，并且当控制信息已被更改时，所述技术可用于使识别更加容易。

[0023] 实例硬件

[0024] 图1是其中可实施本文中所论述的基于硬件的堆栈控制信息保护技术的实例计算机系统100的功能框图。本文所揭示的基于硬件的堆栈控制信息保护技术可用于防止控制信息(例如，与堆栈115的堆栈帧145相关的返回地址125和帧指针120)被恶意攻击者或通过不良写入的软件代码所更改。图1中所说明的计算机系统可用于实施图4到12中所说明的过程。

[0025] 计算机系统100包含处理器105和存储器110。处理器105可为智能装置，例如，个人

计算机中央处理单元(CPU)(例如由Intel®公司或AMD®制造的那些)、微控制器、专用集成电路(ASIC)等。存储器110是可包含随机存取存储器(RAM)和/或其它类型的存储器的非瞬时性存储装置,处理器105可从所述其它类型的存储器读取数据,并且处理器105可写入数据到所述其它类型的存储器。在一些实施方案中,存储器110的部分可为只读存储器(ROM),所述只读存储器可包含可通过处理器105读取而非更新的软件指令和/或数据。

[0026] 存储器110可存储处理器可读、处理器可执行的软件代码,所述软件代码含有用于控制处理器105执行例如本文所描述的那些的各种函数的指令(尽管所述描述可读取到软件执行函数)。可通过经由网络连接下载、从磁盘上传等将软件加载到存储器260上。另外,软件可能并非可直接执行,例如,要求在执行之前进行编译。

[0027] 存储器110可包含堆栈115。堆栈115是存储器110中的数据结构,所述存储器110可用于存储与通过处理器105执行的一或多个软件程序中的一或多个活跃的子例程相关的数据。在一些实施方案中,通过处理器105执行的每一软件程序和/或线程可与不同的堆栈115相关。堆栈115可由一或多个堆栈帧145构成。堆栈帧145含有用于尚未通过处理器105终止于返回的子例程的状态信息。在堆栈的典型实施方案中,位于堆栈的顶部处的堆栈帧是与当前正通过处理器105执行的子例程相关的堆栈帧。堆栈帧145可含有与子例程相关的信息,例如可能已通过调用子例程的例程传递到那个子例程的任何参数值,以及可用于控制软件程序流和其中程序存取数据的控制信息。例如,控制信息可包含指向回到与堆栈帧145相关的子例程的调用程序的返回地址(RA)125,以及帧指针(FP)120。堆栈帧145还可用于存储与子例程相关的其它信息。

[0028] 返回地址125指向调用与堆栈帧145相关的子例程的指令的地址,并且稍后可由处理器105用于在处理器105完成子例程时返回到调用了所述子例程的调用指令。

[0029] 帧指针120指向在与子例程相关的堆栈帧的开始处的地址,并且在子例程的持续时间内并不改变。处理器105还可经配置以保持参考堆栈115的顶部的堆栈指针(SP)(未图示)。当内容添加到堆栈中时,堆栈指针的值改变,而帧指针120继续指向与堆栈帧相关的数据。帧指针120可用于指向堆栈帧内的固定位置,所述固定位置允许帧指针120用作固定的参照点,所述参照点可用于促进对与子例程相关的自变量和/或局部变量的存取,所述子例程与堆栈帧相关。自变量和/或局部变量的位置可确定为从帧指针120的值的固定偏移。

[0030] 本文所揭示的技术可用于帮助防止返回地址125和/或帧指针120被不良写入代码或通过对攻击计算机系统100的恶意尝试更改。通过将返回地址覆写成不同指令的返回地址,恶意方可尝试将由处理器105执行的程序代码重新引导到不同于调用子例程的指令的指令。恶意代码还可更改可用于指向由攻击者插入到堆栈上的数据的帧指针。攻击者可利用堆栈缓冲区溢出以将数据写入到堆栈数据结构之外的堆栈115,所述堆栈数据结构实际上经分配以存储数据。如果正通过处理器105执行的程序代码并未检查来确保被写入到堆栈的数据实际上经适当地设定大小以用于意图存储所述数据的缓冲区,那么在堆栈115上数据可被损坏,和/或攻击者可利用这种技术来修改帧指针120和/或返回地址125以取得对计算机系统100的控制。本文所揭示的技术可实施在计算机系统100的硬件中,以使得更改控制信息(例如帧指针120和返回地址125)更为困难。一些实施方案还可包含在将控制信息返回到通过处理器105执行的软件程序之前,验证已从堆栈115加载的受保护的控制信息。

[0031] 处理器105提供用于在堆栈115上存储数据的装置(在一个方面,用于在堆栈115上

存储数据的装置是用于将数据推送到堆栈115上的装置)。处理器105还提供用于从堆栈115加载数据的装置(在一个方面,用于从堆栈115加载数据的装置是用于从堆栈115弹出数据的装置)。处理器105还可充当用于从正通过处理器105执行的软件程序接收存储指令和加载指令的装置。存储指令还可包含控制信息。处理器105提供用于更改控制信息以产生受保护的控制信息和用于在堆栈115上存储受保护的控制信息的装置。处理器105还提供用于从堆栈115加载受保护的控制信息和用于更改受保护的控制信息以恢复控制信息的装置。处理器105还可提供用于加密控制信息以产生受保护的控制信息和用于解密受保护的控制信息以恢复控制信息的装置。处理器105还可提供用于添加认证标签到控制信息以产生受保护的控制信息的装置。处理器105还提供用于通过从受保护的控制信息导出帧指针和返回地址来更改受保护的控制信息以恢复控制信息的装置。处理器105还可提供用于应用消息认证码到帧指针和返回地址以产生标签值的装置,以及用于比较标签值与包含于受保护的控制信息中的认证标签来验证控制信息在堆栈上时未被更改的装置。除非另外指定,否则处理器105可提供用于实施图4到12中所说明的过程的各个阶段的装置。图4到12在下文中详细地论述。

[0032] 为清楚起见,图1仅示出了处理器105和存储器110。计算机系统100可包含额外元件,例如网络接口、输入/输出端口和/或输入输出装置、无线接口,和/或此处未示出的其它组件。

[0033] 图2是来自图1的实例计算机系统100的功能框图,示出了可用于实施本文所揭示的基于硬件的堆栈控制信息技术的控制数据认证技术的实施方案。在图2中所说明的控制数据认证技术中,产生呈认证信息140形式的受保护的控制信息并存储在堆栈115上。在图2中所说明的实施方案中,认证信息140已被推送到堆栈上,而不是帧指针120被推送到堆栈上。认证信息140可用于验证受保护的控制信息在堆栈上时尚未被更改。例如,当完成与受保护的控制信息相关的子例程时,处理器105可基于从堆栈115加载的返回地址125来产生新的认证信息。处理器105可使用用于产生被推送到堆栈115上的认证信息140的同一技术来产生新的认证信息。处理器105可比较由从堆栈115弹出的返回地址125所产生的新的认证信息与包含于认证信息140中的认证信息140。如果新的认证信息并不匹配来自堆栈的认证信息140,那么处理器105可执行异常处理例程以暂停正在执行的应用程序的执行,因为返回地址125已被更改或损坏。如果新的认证信息匹配认证信息140,那么返回地址125尚未被更改或损坏,并且处理器105可继续执行由返回地址125所指代的指令。图2中所说明的控制数据认证技术的额外细节在下文中相对于图4到12中所说明的过程进行论述。

[0034] 图3是来自图1的实例计算机系统100的功能框图,示出了可用于实施本文所揭示的基于硬件的堆栈控制信息技术的控制数据加密技术的实施方案。在图3中所说明的控制数据加密技术中,产生呈加密帧数据135形式的受保护的控制信息,并将其推送到堆栈上。在图3中所说明的实施方案中,加密帧数据135已被推送到堆栈上,而不是帧指针120和返回地址125被推送到堆栈上。加密帧数据135可用于验证受保护的控制信息在堆栈上时尚未被更改。例如,当完成与受保护的控制信息相关的子例程时,处理器105可解密加密帧数据135以确定加密帧数据135在堆栈115上时是否被更改。如果新的加密帧数据135在堆栈115上时被更改,那么处理器105可经配置以执行异常处理例程,从而暂停正在执行的应用程序的执行,因为控制信息已被更改或损坏。如果加密帧数据135在堆栈上时未被更改,那么处理器

可从已解密的加密帧数据135中获得帧指针120和返回地址125，并且可继续执行由返回地址125所指代的指令。图3中所说明的控制数据认证技术的额外细节在下文中相对于图4到12中所说明的过程进行论述。

[0035] 实例实施方案

[0036] 图4是用于保护与处理器相关的堆栈的内容的过程的流程图，所述处理器可用于实施本文所揭示的基于硬件的堆栈控制技术。图4中所说明的过程可使用图1中所说明的计算机系统100实施。图1中所说明的实例计算机系统100提供其中可实施图4中所说明的过程的一个计算机系统的一个实例，并且图4中所说明的过程可通过具有与图1中所说明的实例不同的架构的计算机系统的处理器实施。

[0037] 过程可开始于从通过处理器105执行的软件程序接收存储指令(阶段401)。存储指令可包含与子例程相关的控制信息，软件程序想要将所述控制信息存储在堆栈115上。参考图1中所说明的实例计算机系统，处理器105可经配置以响应于接收从软件程序接收到的存储指令，在堆栈115上存储与通过处理器105执行的软件程序的子例程相关的信息。例如，处理器105可经配置以将帧指针120和返回地址125推送到堆栈115上，以作为存储在用于与堆栈帧145相关的子例程的堆栈上的控制信息的部分。在其它实施方案中，控制信息可包含其它信息，作为帧指针120和返回地址125的补充或替代。

[0038] 接着，可更改控制信息以产生受保护的控制信息(阶段405)。处理器105可经配置以使用本文所论述的控制数据认证和/或控制数据加密技术来更改与软件程序相关的控制信息。更改控制信息使攻击者更难通过更改帧指针120、返回地址125和/或堆栈115上的其它控制信息来取得对计算机系统100的控制。在一些实施方案中，处理器105可验证受保护的控制信息在堆栈115上时尚未被更改。在控制数据加密技术中，处理器105经配置以加密控制信息，从而产生受保护的控制信息。用于使用控制数据加密技术产生安全控制信息的实例过程在图9中说明。在控制数据认证技术中，处理器105经配置以产生认证标签，所述认证标签被添加到控制信息中，并可用于验证受保护的控制信息在堆栈115上时尚未被更改。认证标签可使用秘密密钥产生，所述秘密密钥对处理器105已知，但不可用于通过处理器105执行的软件代码。在一些实施方案中，密钥可实施在处理器的硬件中，或可存储在计算机系统100的受信任存储器组件中，使得受信任存储器组件的内容无法被在计算机系统100上执行的软件代码存取或更改。认证标签如何可产生的额外细节在下文中详细地论述。例如，图5中所说明的过程论述可用于产生认证标签的一种技术。认证标签可考虑到帧指针120、返回地址125和/或待保护的其它控制信息。

[0039] 接着，受保护的控制信息可存储在堆栈115上(阶段410)。在一些实施方案中，受保护的控制信息可存储在堆栈115上，而不是控制信息存储在堆栈115上。图3中所说明的实例实施方案提供实施方案的实例，其中加密帧数据135已被推送到堆栈115上，而不是如在图1中示出的实例中的包含帧指针120和返回地址125的未更改的控制信息被推送到堆栈115上。在此实施方案中，在堆栈上不可用未更改的控制信息，这防止恶意代码和/或恶意方的攻击存取未受保护的控制数据。在其它实施方案中，除了控制信息以外，受保护的控制信息的至少一部分可推送到堆栈上，并且可用于确定控制信息在堆栈上时尚未被更改。图2中所说明的实例实施方案提供实施方案的实例，其中认证信息140已被推送到堆栈115上，而不是如在图1中示出的实例中的帧指针120被推送到堆栈115上。除了认证信息140以外，返回

地址125已被推送到堆栈115上。在图2中示出的实例中的认证信息可至少部分地基于与堆栈帧相关的帧指针和返回地址来确定，并且认证信息140可用于确定返回地址和/或堆栈115上的其它信息是否已被更改。

[0040] 加载指令可从通过处理器105执行的软件程序接收(阶段415)。处理器105可经配置以响应于来自软件程序的加载指令，从堆栈115加载控制信息，并且提供控制信息到发布加载指令的软件程序。在一些实施方案中，处理器115可经配置以响应于加载指令，从堆栈115中去除控制信息(和/或受保护的控制信息)以在堆栈115上释放内存。响应于从通过处理器105执行的软件程序接收加载指令，过程可继续到阶段417、420和425。

[0041] 受保护的控制信息可从堆栈加载(阶段417)。响应于完成子例程，与子例程相关的堆栈115的内容可从堆栈115中弹出以在堆栈115上释放内存。此清理过程的部分可包含从堆栈115中弹出受保护的控制信息，并且在一些实施方案中，可包含从堆栈中弹出其它控制信息。

[0042] 过程可继续到更改受保护的控制信息以恢复控制信息(阶段420)。处理器105可经配置以从受保护的控制信息中恢复控制信息。处理器105如何恢复是否已被更改的受保护的控制信息取决于用于产生受保护的控制信息的技术。如果控制数据认证技术用于产生受保护的控制信息，那么基于用于堆栈帧145的控制信息所产生的认证标签可使用用于产生被推送到堆栈上的认证标签的密钥来重新产生，并且可做出所重新产生的密钥是否匹配包含于受保护的控制信息中的密钥的确定，所述受保护的控制信息用于堆栈115上的堆栈帧145。如果所重新产生的认证标签并不匹配包含于受保护的控制信息中的认证标签，那么受保护的控制信息在堆栈115上时已被损坏或更改。图8可用于从受保护的控制信息中恢复控制信息。如果在阶段405中控制数据加密技术用于产生受保护的控制信息，那么包括被推送到用于堆栈帧145的堆栈上的受保护的控制信息的加密帧数据135可使用与在阶段405中用于加密数据的加密技术相关的合适密钥进行解密。如果加密帧数据135未使用与用于加密控制数据的密钥相关的解密密钥来适当地解密，那么受保护的控制信息在堆栈115上时已被损坏或更改。图12示出了用于恢复使用控制数据加密技术所产生的受保护的控制信息的实例过程。

[0043] 接着，控制信息可被返回到软件程序(阶段425)。接着，处理器105可返回控制信息到发布加载指令到处理器105的软件程序。在一些实施方案中，处理器105可经配置以确定受保护的控制数据是否被更改，以及引发异常，所述异常可暂停软件程序的处理和/或执行可防止恶意或不良实施的代码利用已更改或损坏的控制数据的其它动作。例如，在使用控制数据认证和认证标签并不匹配的情况下，处理器105可暂停软件程序的执行或执行其它处理任务。在另一个实例中，在使用控制数据加密的情况下，处理器105可经配置以确定与帧指针120和/或返回地址125相关的地址是否落在地址的有效范围内。如果地址落在地址可允许的范围之外，这可指示地址信息在堆栈115上时被更改或损坏，那么处理器105可经配置以暂停软件程序的执行或执行其它处理任务。

[0044] 图5是用于使用控制数据认证技术更改控制信息以产生受保护的控制信息的过程的流程图。图5中所说明的过程可用于实施图4中所说明的过程的阶段405。控制数据认证技术可用于至少部分地基于待保护的控制信息产生认证标签，并且认证标签可用于确定控制信息在堆栈115上时是否已被更改。除非另外指示，否则图5中所说明的过程可通过处理器

105实施。

[0045] 可存取与堆栈帧相关的密钥(阶段505)。在一些实施方案中,相同密钥可用于产生用于堆栈帧中的每一个堆栈帧的认证标签。在其它实施方案中,不同密钥可选自多个密钥,以使得每一堆栈帧与多个密钥中的一个密钥相关。在一些实施方案中,每一堆栈帧可与不同密钥相关,并且那一密钥可用于产生用于那一堆栈帧的认证信息。在一些实施方案中,堆栈115上的每一堆栈帧与将用于产生认证信息的独特密钥相关,所述认证信息可用于验证与堆栈帧145相关的控制信息(例如帧指针120和/或返回地址125)在堆栈115上时尚未被更改。在一些实施方案中,处理器105可经配置以在堆栈帧产生于堆栈115上时,产生用于每一堆栈帧的密钥,并且存储密钥在受保护的存储器中,所述存储器可由处理器105存取,但不可由在计算机系统100上执行的软件代码存取。在一些实施方案中,一或多个密钥可存储在处理器可存取的计算机系统100的受信任存储器组件中,并且处理器105可经配置以从存储在受信任存储器组件中的一或多个相关密钥中选择密钥,所述密钥用于产生与堆栈帧相关的认证信息。用于产生用于堆栈115上的堆栈帧的认证信息的密钥应保持秘密,以防止恶意用户能够更改控制信息,并且以基于更改的控制信息,产生新的认证信息。当与那一密钥相关的堆栈帧从堆栈115中弹出时,可再使用所述密钥。

[0046] 过程还可包含计算用于帧指针120的增量值(阶段510)。帧指针120可编码为表示相对于堆栈115上的堆栈指针的地址的偏移的增量值。增量值可足够小于帧指针120,使得存储器中原先分配用于存储帧指针120的空间可用于存储堆栈帧145的增量值和认证信息。

[0047] 过程还可包含计算用于与堆栈帧相关的控制信息的认证信息(阶段515)。基于返回地址125、帧指针120、帧指针的增量值和/或待监测以用于在堆栈115上时未授权的更改的其它控制信息,可计算认证信息。在一些实施方案中,认证标签包括消息认证码(MAC)标签,所述消息认证码(MAC)标签使用MAC算法和在阶段505中存取的密钥来计算。MAC标签可使用相同密钥产生和验证。MAC算法可基于加密散列函数、分块密码算法、全域散列或其它类型的技术。处理器105可经配置以跟踪用于认证堆栈115上的堆栈帧的密钥,其中堆栈帧中的至少一些堆栈帧使用不同密钥认证。在其它实施方案中,其它类型的技术可用于通过应用过程到控制信息来产生认证信息,所述过程可用于验证受保护的控制信息的数据完整性和真实性。

[0048] 图6是用于在堆栈上存储使用控制数据认证技术所产生的受保护的控制信息的过程的流程图。图6中所说明的过程可用于实施图4中所说明的过程的阶段410,其中图5中所说明的过程用于实施图4中所说明的过程的阶段405。除非另外指示,否则图6中所说明的过程可通过处理器105实施。

[0049] 可在堆栈115上存储增量值和认证信息(阶段605)。处理器105可经配置以推送增量值和认证信息到堆栈115上,而不是推送帧指针120,因为增量值来源于帧指针120,并且稍后可用于计算帧指针120的值。增量值和认证信息的大小可允许增量值和认证标签刚好放入到与帧指针120相同数量的堆栈115上的存储器中。在一些实施方案中,认证信息包括基于待保护的受保护的控制信息所计算的MAC标签,所述受保护的控制信息可包含帧指针120、与帧指针相关的增量值、返回地址125和/或其它控制信息。

[0050] 返回地址125还可存储在堆栈115上(阶段610)。返回地址125尚未被更改,并且可被推送到堆栈115上。如果返回地址125在堆栈115上时改变,那么在阶段605中包含于被推

送到堆栈上的受保护的控制信息中的认证标签将不匹配基于在控制信息从堆栈115中弹出时更改的返回地址所产生的认证标签，所述堆栈115将发信号通知处理器105控制信息在堆栈115上时已被更改以及应该执行异常处理程序。

[0051] 图7是用于从堆栈115中获取使用控制数据认证技术所产生的受保护的控制信息的过程的流程图。图7中所说明的过程可用于实施图4中所说明的过程的阶段417。除非另外指示，否则图7中所说明的过程可通过处理器105实施。图7中所说明的过程可用于获取在图6中所说明的过程中存储在堆栈115上的信息。

[0052] 过程可包含从堆栈115加载返回地址125(阶段705)。增量值和认证信息还可从堆栈加载(阶段710)。如上文相对于图6中所说明的过程所论述，返回地址125可被推送到堆栈115上，而不需更改返回地址125。如果返回地址125在堆栈115上时已被更改，那么包含于被推送到堆栈上的受保护的控制信息内的认证标签将不匹配由已从堆栈中弹出的控制信息所产生的认证标签。

[0053] 图8是用于确定使用控制数据认证技术所产生的受保护的控制信息在堆栈上时是否已被更改的过程的流程图。图8中所说明的过程可用于实施图4中所说明的过程的阶段425的至少部分，其中处理器105经任选配置以在返回控制信息到已请求控制信息的软件程序之前，验证控制信息在堆栈115上时尚未被更改。图8中所说明的过程可用于验证使用图5中所说明的过程产生的受保护的控制信息在堆栈115上时尚未被更改。图8中所说明的过程可通过处理器105实施。

[0054] 可存取与堆栈帧相关的密钥(阶段805)。与堆栈帧相关的密钥可存储在受保护的存储器中，所述受保护的存储器可由处理器105而非通过处理器105执行的未授权的程序代码存取，以防止恶意方获得对用于产生认证信息的密钥的存取权，所述认证信息用于确保控制信息在堆栈115上时尚未被更改。如上文所论述，密钥可与消息认证码(MAC)相关。通过基于在控制信息从堆栈115加载/弹出时从堆栈115获得的控制信息计算认证标签，与堆栈帧相关的密钥可用于认证受保护的控制信息的内容。在控制信息在堆栈115上时已被更改的情况下，所计算的认证标签将不匹配在图6中所说明的过程的阶段605中存储在/被推送到堆栈115上的认证标签。

[0055] 与堆栈帧相关的帧指针120可根据从堆栈115弹出的增量值计算(阶段810)。帧指针120可编码为表示相对于堆栈指针的堆栈115上的地址的增量值。在堆栈115上存储增量值而不是帧指针可在堆栈115上释放空间，所述空间可用于存储用于堆栈帧的认证信息。通过添加增量值的偏移到由堆栈指针表示的地址，帧指针120可根据增量值计算。

[0056] 可使用帧指针120、返回地址125和/或其它控制信息，使用与堆栈帧145相关的密钥计算认证信息(阶段815)。认证信息应该使用用于计算存储在/被推送到堆栈115上的认证信息的同一技术来计算。例如，如果特定的MAC算法用于根据帧指针120、返回地址125和/或其它控制信息来产生MAC标签，那么相同的MAC算法应该适用于用于产生包含于认证信息中的MAC标签的相同控制信息元件，所述认证信息存储在/被推送到堆栈115上。

[0057] 使用帧指针120、返回地址125和/或其它控制信息和使用与堆栈帧相关的密钥所计算的认证信息可与包含于受保护的控制信息内的认证信息比较，所述受保护的控制信息作为受保护的控制信息的部分存储在堆栈115上(阶段820)。例如，如果认证信息包括MAC标签，那么包含于受保护的控制信息中的MAC标签可与使用帧指针120、返回地址125和/或从

堆栈115弹出的其它控制信息所计算的MAC标签比较。可作出所计算的认证标签是否匹配从堆栈115获得的认证标签的确定(阶段825)。如果所计算的认证标签并不匹配从堆栈115获得的认证标签，那么受保护的控制信息可被识别为从受保护的控制信息被推送到堆栈115上已被更改(阶段835)。否则的话，如果所计算的认证标签的确匹配从堆栈115获得的认证标签，那么受保护的控制信息可被识别为从受保护的控制信息被推送到堆栈115上尚未被更改(阶段840)。

[0058] 图9是用于使用控制数据加密技术更改控制信息以产生受保护的控制信息的过程的流程图。图9中所说明的过程可用于实施图4中所说明的过程的阶段405。控制数据加密技术可用于加密在堆栈115上时待保护的控制信息。除非另外指示，否则图9中所说明的过程可通过图1中所说明的处理器105实施。

[0059] 可存取与堆栈帧145相关的密钥(阶段905)。与堆栈帧相关的加密密钥可存储在受保护的存储器中，所述受保护的存储器可由处理器105存取，而不可由通过处理器105执行的未授权的程序代码存取，以防止攻击者获得对密钥的存取权，所述密钥用于加密和解密受保护的控制数据以确保受保护的控制信息在堆栈115上时被更改。与堆栈帧相关的加密密钥可用于在控制信息从堆栈115中弹出时，解密受保护的控制信息的内容。在控制信息在堆栈115上时已被更改的情况下，解密密钥将产生无效结果。在一些实施方案中，用于加密受保护的控制数据的加密密钥可为用于解密受保护的控制数据的同一密钥。在其它实施方案中，加密密钥和解密密钥可为不同的密钥。在一些实施方案中，相同的加密密钥可用于加密用于多个堆栈帧的数据，并且每一堆栈帧可不与不同密钥相关。在一些实施方案中，处理器105可存取加密密钥和解密密钥池，并且处理器105可从可用的加密密钥池选择用于产生用于特定的堆栈帧的受保护的控制信息的加密密钥。

[0060] 与堆栈帧相关的控制信息可使用与堆栈帧相关的密钥加密以产生受保护的控制信息(阶段910)。控制信息可包含返回地址125和/或帧指针120。在其它实施方案中，控制信息可包含额外信息。加密控制信息可防止当受保护的控制信息在堆栈115上时对控制信息作出未授权的更改。

[0061] 图10是用于在堆栈上存储使用控制数据加密技术所产生的受保护的控制信息的过程的流程图。图10中所说明的过程可用于实施图4中所说明的过程的阶段410。受保护的控制信息包括加密帧数据135，并且可包含额外控制信息或其它信息。

[0062] 加密控制信息可存储在/被推送到堆栈115上(阶段1005)。加密控制信息(在本文中也被称作加密帧数据135)可与特定的堆栈帧145相关。处理器105可经配置以推送在图9中所说明的过程的阶段910中加密的受保护的控制信息到堆栈115上。加密帧数据135可被推送到堆栈115上，为处理器105执行另一子例程做准备，并且用于当前正执行的子例程的信息被推送到用于当前正执行的子例程的堆栈上。以加密形式推送控制信息到堆栈上可防止攻击者通过更改堆栈115的内容来更改控制信息。攻击者将需要知道用于加密受保护的控制信息的密钥，以能够成功地修改返回地址或包含于受保护的控制信息中的其它信息。

[0063] 返回地址125还可任选地存储在/被推送到堆栈上(阶段1010)。在一些实施方案中，除了受保护的控制信息以外，返回地址125还可被推送到堆栈上。在此类实施方案中，返回地址可用于分支预测和/或利用返回地址的其它技术。返回地址125可通过解密受保护的控制信息来验证，从而验证返回地址在堆栈115上时未被更改。

[0064] 图11是用于从堆栈115中获取使用控制数据加密技术所产生的受保护的控制信息的过程的流程图。图11中所说明的过程可用于实施图4中所说明的过程的阶段415。当完成与堆栈帧145相关的子例程时，图11中所说明的过程可通过处理器105执行。处理器105可经配置以从堆栈115中去除从堆栈115加载的信息以在存储器110中释放空间。

[0065] 如果返回地址被推送到堆栈115上，那么返回地址可从堆栈115加载(阶段1105)。如果在图10中所说明的过程的阶段1010中，返回地址被推送到堆栈上，那么处理器105可经配置以从堆栈115中弹出返回地址。在一些实施方案中，返回地址未被推送到堆栈上，并且过程可继续到阶段1110，其中受保护的控制信息从堆栈中弹出。

[0066] 加密受保护的控制信息可从堆栈115加载(阶段1110)。处理器105可从堆栈115中弹出受保护的控制信息。例如，当完成与相堆栈帧145关的子例程时，处理器105可从堆栈115中弹出受保护的控制信息，这作为堆栈帧145的清理的部分。接着，受保护的控制信息可进行解密和验证。如果受保护的控制信息在堆栈115上时尚未被更改，那么处理器105可继续执行由返回地址指示的子例程。否则的话，在受保护的控制信息在堆栈115上时已被更改的情况下，处理器105可执行异常处理程序。

[0067] 图12是用于确定使用控制数据加密技术所产生的受保护的控制信息在堆栈115上时是否已被更改的过程的流程图。图12中所说明的过程可用于实施图4中所说明的过程的阶段425的至少部分，其中处理器105经任选配置以在返回控制信息到已请求控制信息的软件程序之前，验证控制信息在堆栈115上时尚未被更改。

[0068] 可存取与堆栈帧相关的密钥(阶段1205)。与堆栈帧相关的密钥可存储在受保护的存储器中，所述受保护的存储器可由处理器105存取，而不可由通过处理器105执行的未授权的程序代码存取，以防止恶意方获得对密钥的存取权，所述密钥用于加密加密帧数据135以确保受保护的控制信息在堆栈115上时被更改。与堆栈帧相关的密钥可用于在控制信息从堆栈115中弹出时，解密受保护的控制信息的内容。在一些实施方案中，用于加密加密帧数据135的密钥可为与可用于解密受保护的控制信息的密钥相同的密钥。在其它实施方案中，用于加密和解密受保护的控制信息的密钥是不同的密钥。处理器105可经配置以跟踪已利用加密密钥加密的堆栈帧，其中多个加密密钥可用，并且以选择用于解密加密帧数据135的合适的解密密钥。

[0069] 加密的受保护的控制信息可使用密钥解密以恢复控制信息(阶段1210)，并且可作出加密控制信息在堆栈115上时是否被更改或损坏的确定(阶段1215)。处理器105可经配置以使用在阶段1205中获得的密钥解密加密帧数据135。处理器105可经配置以通过比较由解密加密帧数据135恢复的控制信息中的地址与地址的有效范围来确定加密帧数据135是否已被更改。如果通过解密加密帧数据135恢复的控制信息中的帧指针120和/或返回地址125落在此范围之外，那么加密帧数据135在堆栈115上时可能已被更改或损坏。

[0070] 如果数据已被更改或损坏，那么受保护的控制信息可被识别为已被更改(阶段1220)。否则的话，受保护的控制信息可被识别为尚未被更改(阶段1225)。响应于数据已被更改的指示，处理器105可经配置以引发异常，所述异常可暂停软件程序的处理和/或执行可防止恶意或不良实施的代码利用已被更改或损坏的控制数据的其它动作。响应于数据尚未被更改的指示，处理器105可经配置以返回控制数据到已发布加载命令到处理器105的软件程序(见图4中所说明的过程的阶段405)。

[0071] 取决于应用，本文所述的方法可由各种装置实施。例如，这些方法可在硬件、固件、软件或其任何组合中实施。对于硬件实施方案，处理单元可在一或多个专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理装置(DSPD)、可编程逻辑装置(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器、电子装置、经设计以执行本文中所描述的功能的其它电子单元或其组合内实现。

[0072] 对于固件和/或软件实施方案，可使用执行本文中所描述的功能的模块(例如，程序、函数等等)实施方法。在实施本文中所描述的方法的过程中，可使用任何有形地体现指令的机器可读媒体。例如，软件代码可存储在存储器中，并且由处理器单元执行。存储器可实施于处理器单元内或处理器单元外部。如本文中所使用，术语“存储器”是指任何类型的长期、短期、易失性、非易失性或其它存储器，且并不限于任何特定类型的存储器或特定数目的存储器或特定类型的媒体。有形媒体包含机器可读媒体的一或多个物理物品，例如随机存取存储器、磁性存储装置、光学存储媒体等等。

[0073] 如果在固件和/或软件中实施，那么可将功能作为一或多个指令或代码存储在计算机可读媒体上。实例包含编码有数据结构的计算机可读媒体和编码有计算机程序的计算机可读媒体。计算机可读媒体包含物理计算机存储媒体。存储媒体可为可由计算机存取的任何可用媒体。借助于实例而非限制，此类计算机可读媒体可包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储器，磁盘存储器或其它磁性存储装置，或任何其它可用于存储呈指令或数据结构形式的所要程序代码且可由计算机接入的媒体；如本文中所使用，磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)，软性磁盘和蓝光光盘，其中磁盘通常以磁性方式再现数据，而光盘用激光以光学方式再现数据。上述的组合应包含于计算机可读媒体的范围内。此类媒体还提供可为机器可读的非暂时性媒体的实例，且其中计算机为可从此类非暂时性媒体读取的机器的实例。

[0074] 在不脱离本发明或权利要求的精神或范畴的情况下，本文中所论述的一般原理可应用于其它实施方案。

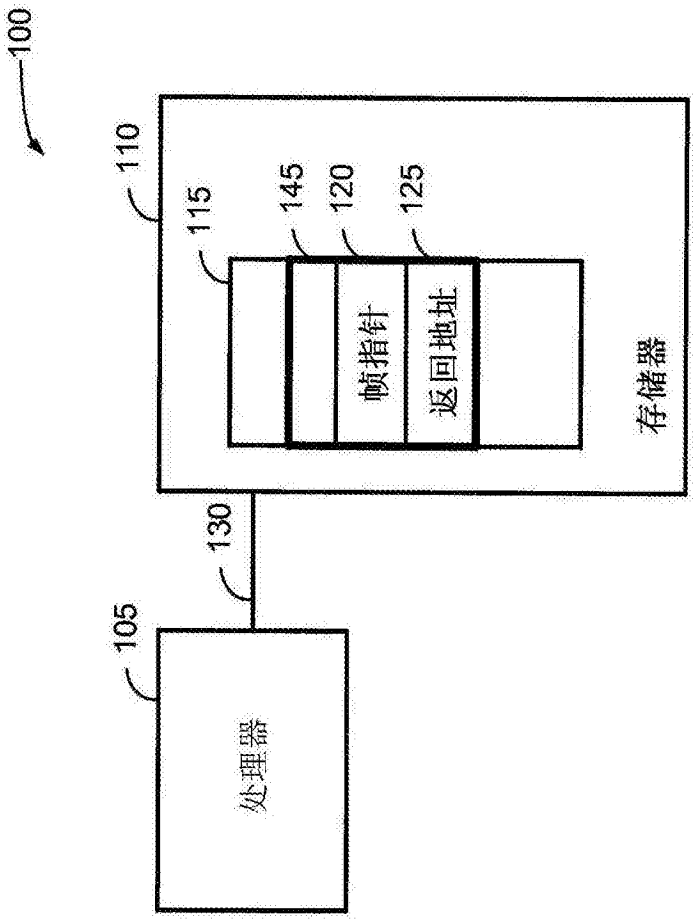


图1

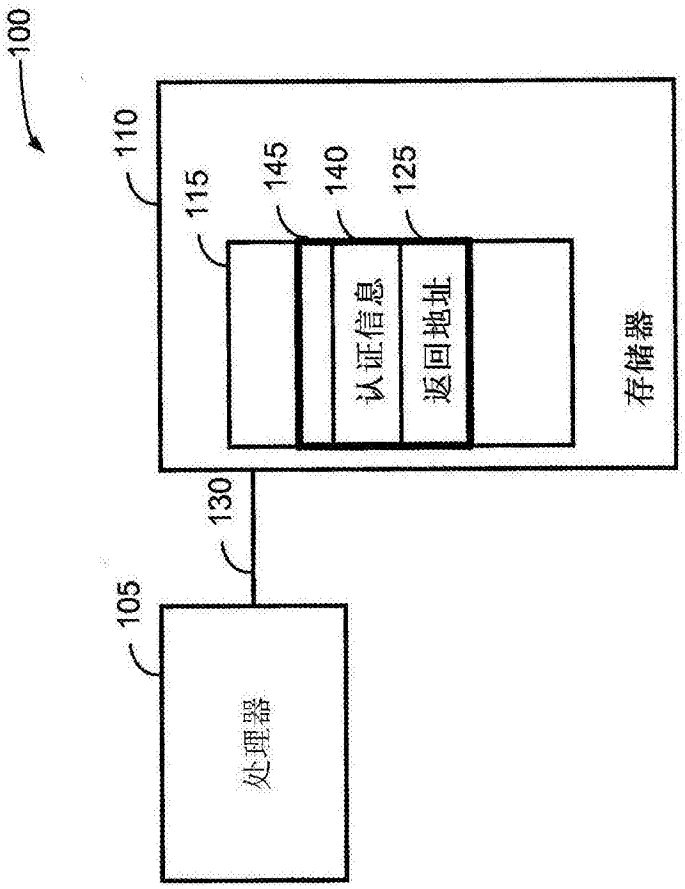


图2

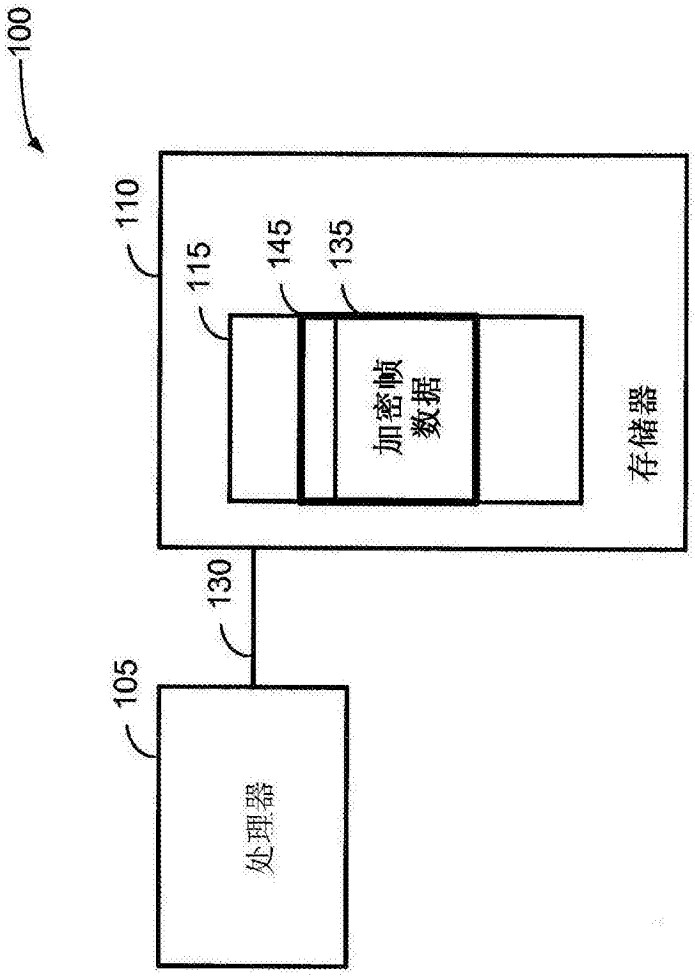


图3

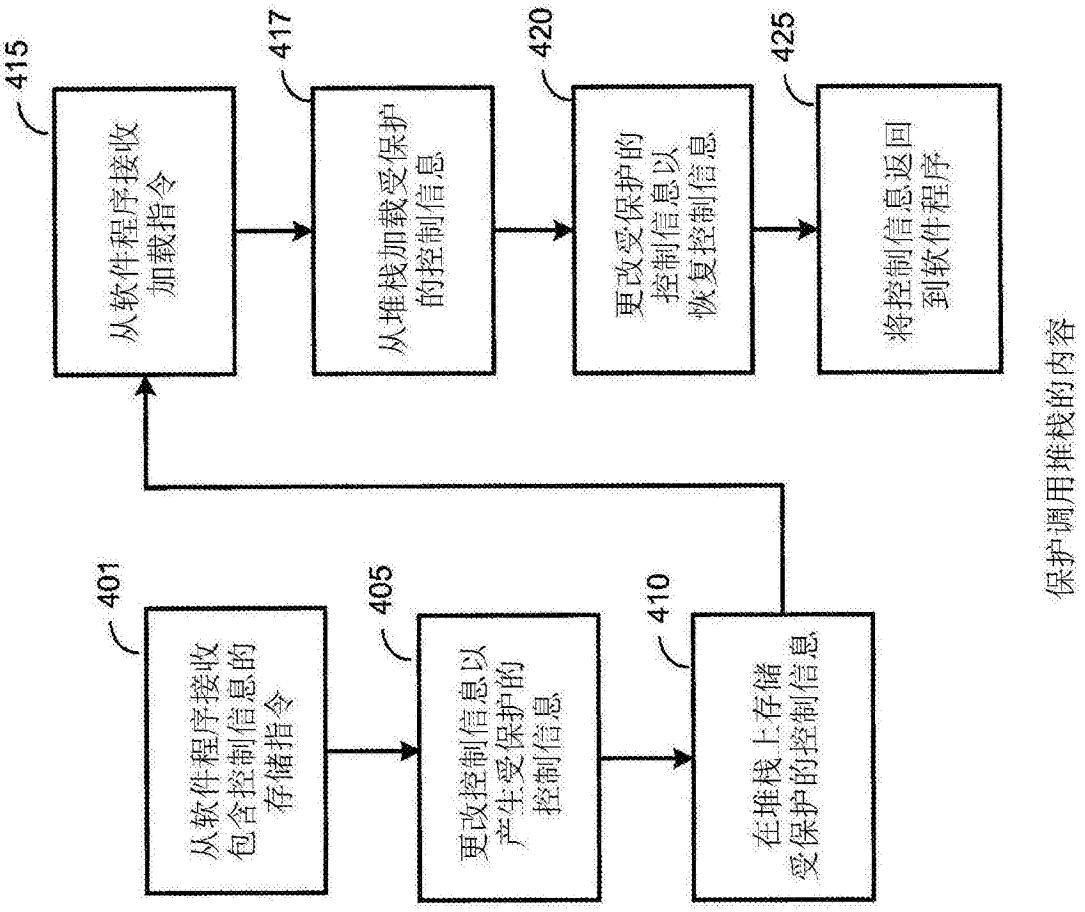

415
从软件程序接收
加载指令
417
从堆栈加载受保护
的控制信息
420
更改受保护的
控制信息以
恢复控制信息
425
将控制信息返回
到软件程序
保护调用堆栈的内容
401
从软件程序接收
包含控制信息的
存储指令
405
更改控制信息以
产生受保护的
控制信息
410
在堆栈上存储
受保护的控制信息

图4

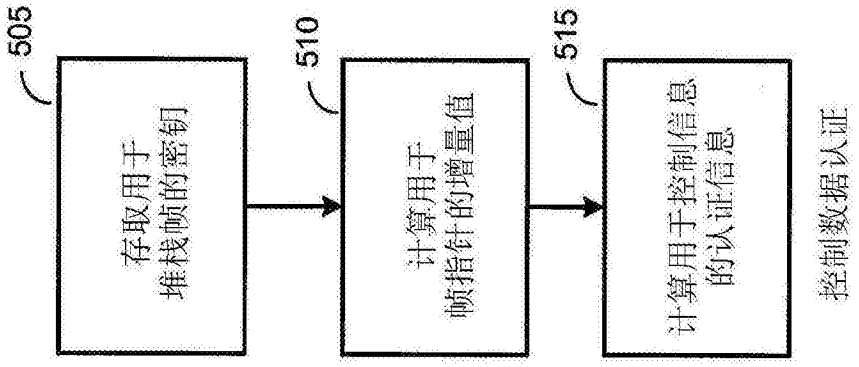

505
存取用于
堆栈帧的密钥
510
计算用于
帧指针的增量值
515
计算用于控制信息
的认证信息
控制数据认证

图5

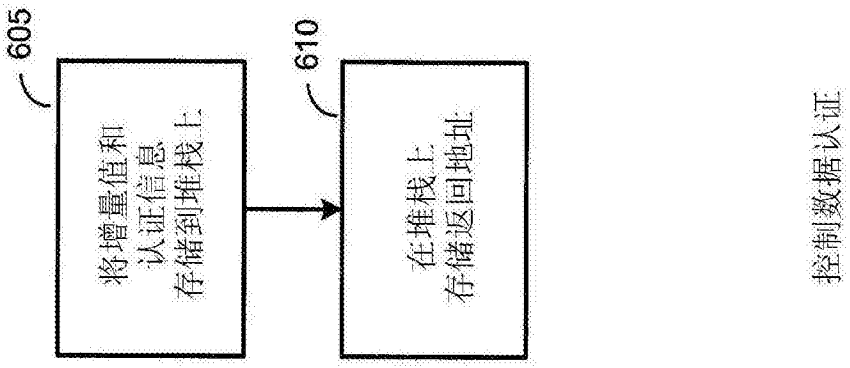

605
将增量值和
认证信息
存储到堆栈上
610
在堆栈上
存储返回地址
控制数据认证

图6

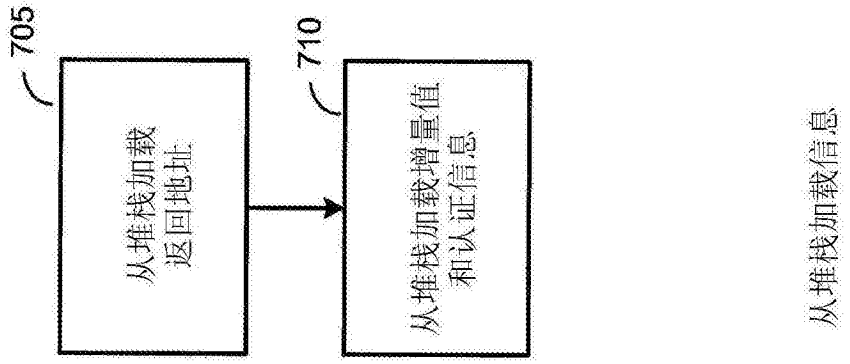

705
从堆栈加载
返回地址
710
从堆栈加载增量值
和认证信息
从堆栈加载信息

图7

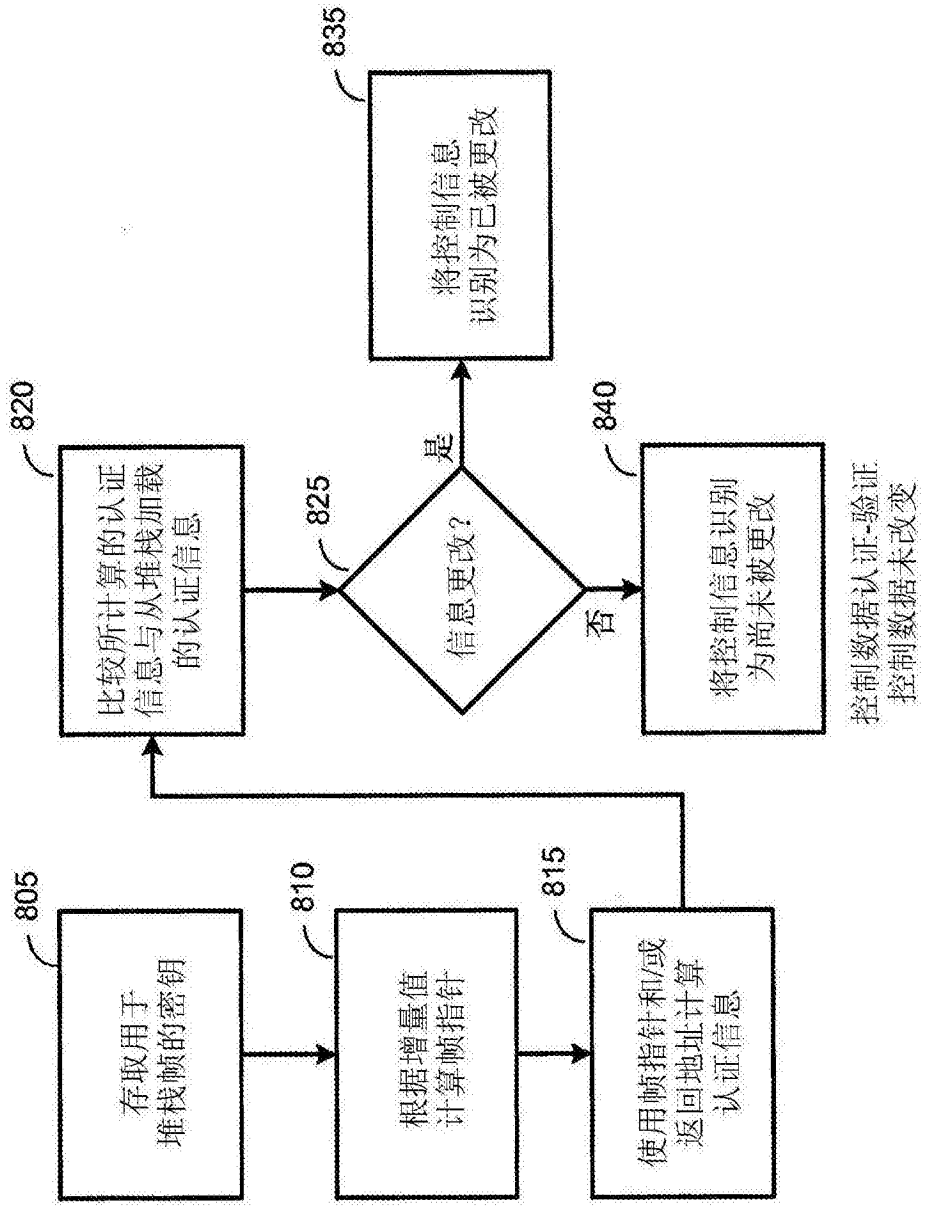

805
存取用于
堆栈帧的密钥
810
根据增量值
计算帧指针
815
使用帧指针和/或
返回地址计算
认证信息
820
比较所计算的认证
信息与从堆栈加载
的认证信息
825
信息更改?
是
否
835
将控制信息
识别为已被更改
840
将控制信息识别
为尚未被更改
控制数据认证-验证
控制数据未改变

图8

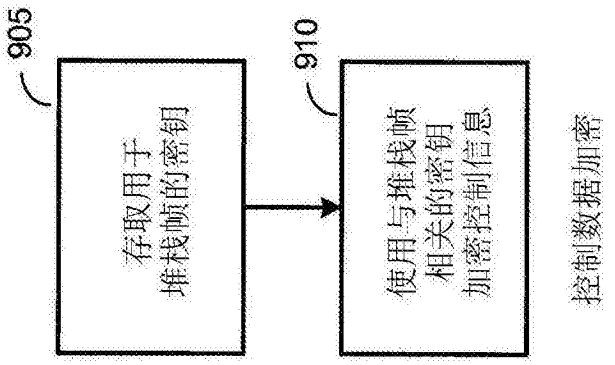

905
存取用于
堆栈帧的密钥
910
使用与堆栈帧
相关的密钥
加密控制信息
控制数据加密

图9

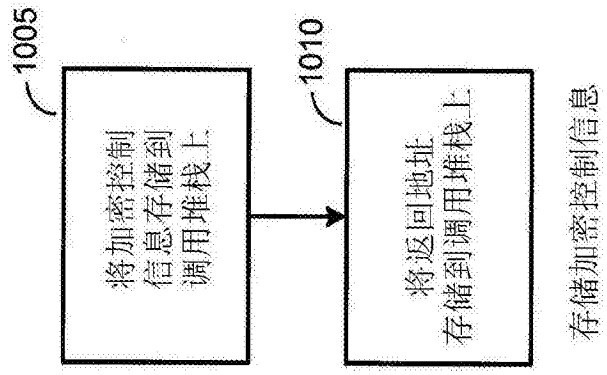

1005
将加密控制
信息存储到
调用堆栈上
1010
将返回地址
存储到调用堆栈上
存储加密控制信息

图10

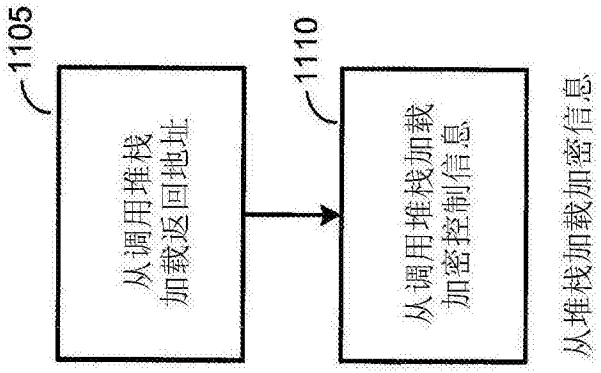

1105
从调用堆栈
加载返回地址
1110
从调用堆栈加载
加密控制信息
从堆栈加载加密信息

图11

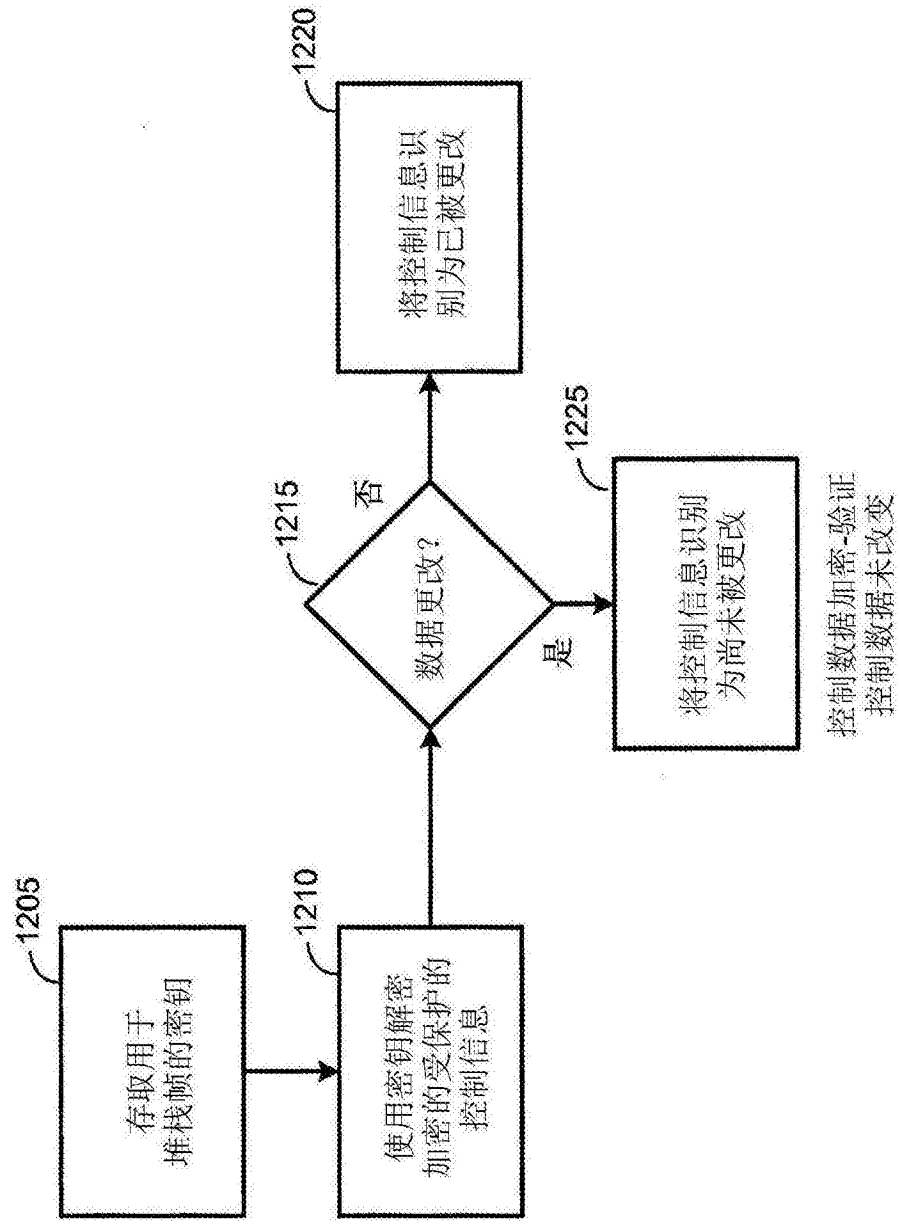

1205
存取用于
堆栈帧的密钥
1210
使用密钥解密
加密的受保护的
控制信息
1215
数据更改?
否
是
1220
将控制信息识
别为已被更改
1225
将控制信息识别
为尚未被更改
控制数据加密-验证
控制数据未改变

图12