(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 112115477 A
(43)申请公布日 2020.12.22

(21)申请号 202010824141.0

(22)申请日 2020.08.17

(71)申请人 南方科技大学
地址 518055 广东省深圳市南山区西丽学苑大道1088号

(72)发明人 张锋巍 周雷

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 黄广龙

(51)Int.Cl.
G06F 21/57(2013.01)

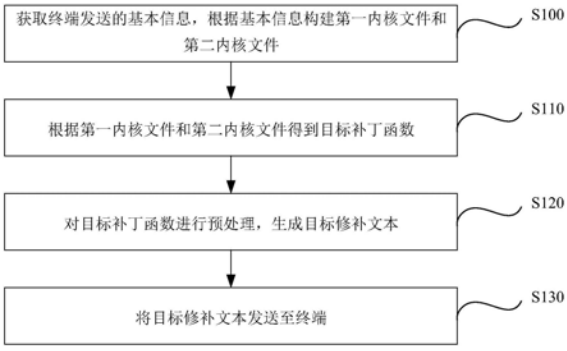
权利要求书2页 说明书10页 附图3页

(54)发明名称

内核修复方法、装置、电子设备及存储介质

(57)摘要

本发明公开了一种内核修复方法、装置、电子设备及存储介质，用于服务器和终端，其中，用于服务器的内核修复方法包括：获取终端发送的基本信息，根据所述基本信息构建第一内核文件和第二内核文件；根据所述第一内核文件和所述第二内核文件提取得到目标补丁函数；对所述目标补丁函数进行预处理，生成目标修补文本；将所述目标修补文本发送至终端。通过上述内核修复方法，能够增强内核修补的可靠性、有效性，提高实时修补性能。



CN 112115477 A

1.内核修复方法,用于服务器,其特征在于,包括:

获取终端发送的基本信息,根据所述基本信息构建第一内核文件和第二内核文件;

根据所述第一内核文件和所述第二内核文件提取得到目标补丁函数;

对所述目标补丁函数进行预处理,生成目标修补文本;

将所述目标修补文本发送至终端。

2.根据权利要求1所述的方法,其特征在于,所述根据所述第一内核文件和所述第二内核文件提取得到目标补丁函数,包括:

基于所述第一内核文件创建第一函数调用图和第二函数调用图;

基于所述第二内核文件创建第三函数调用图和第四函数调用图;

将所述第一函数调用图和所述第二函数调用图进行比对,得到第一比对结果,将所述第三函数调用图和所述第四函数调用图进行比对,得到第二比对结果;

根据所述第一比对结果和所述第二比对结果提取得到目标补丁函数。

3.根据权利要求1所述的方法,其特征在于,所述对所述目标补丁函数进行预处理,生成目标修补文本,包括:

获取对称密钥;

根据所述对称密钥加密所述目标补丁函数,得到目标修补文本。

4.内核修复方法,用于终端,其特征在于,包括:

获取操作系统的基本信息,将所述基本信息发送至服务器;

获取所述服务器发送的目标修补文本,对所述目标修补文本进行处理得到目标补丁;

根据所述目标补丁进行内核修复。

5.根据权利要求4所述的方法,其特征在于,所述根据所述目标修补文本处理得到目标补丁,包括:

验证所述目标修补文本的完整性,得到第一验证结果;

对所述目标修补文本中的分支指令进行简化处理,得到简化处理结果;

补充所述目标修补文本的标识信息,得到补充结果;

根据所述第一验证结果、所述简化处理结果和所述补充结果进行加密处理,得到目标补丁。

6.根据权利要求4所述的方法,其特征在于,所述根据所述目标补丁进行内核修复,包括:

验证所述目标补丁的完整性,得到第二验证结果;

根据所述第二验证结果将所述目标补丁进行写出,并获取修补指令;

根据所述修补指令进行内核修复。

7.内核修复装置,其特征在于,包括:

获取模块,用于获取终端发送的基本信息,根据所述基本信息构建第一内核文件和第二内核文件;

提取模块,用于根据所述第一内核文件和所述第二内核文件提取得到目标补丁函数;

第一处理模块,用于对所述目标补丁函数进行预处理,生成目标修补文本;

第一发送模块,用于将所述目标修补文本发送至终端。

8.内核修复装置,其特征在于,包括:

第二发送模块，用于获取操作系统的基本信息，将所述基本信息发送至服务器；

第二处理模块，用于获取所述服务器发送的目标修补文本，对所述目标修补文本进行处理得到目标补丁；

修复模块，用于根据所述目标补丁进行内核修复。

9.电子设备，其特征在于，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现：

如权利要求1至3中任一项所述的内核修复方法；

或者，

如权利要求4至6任一项所述的内核修复方法。

10.计算机可读存储介质，其特征在于，存储有计算机可执行指令，所述计算机可执行指令用于：

执行权利要求1至3中任一项所述的内核修复方法；

或者，

执行权利要求4至6任一项所述的内核修复方法。

内核修复方法、装置、电子设备及存储介质

技术领域

[0001] 本发明涉及计算机技术领域，尤其是涉及一种内核修复方法、装置、电子设备及存储介质。

背景技术

[0002] 随着信息领域的发展，软件服务日益复杂和异构化，导致补丁的应用越来越频繁。目前的Kpatch、kGraft等实时补丁机制，真正实现了修复指定内核函数且不中断软件执行。其主要思路是通过跟踪目标函数，截获执行指令和在内存中替换补丁函数。

[0003] 为了保证系统和软件执行状态的一致性，现有的实时补丁修复程序需要保存和恢复当前系统执行状态，此操作引入大量的存储和计算开销。现有的实时补丁修复技术都是基于正常的内核功能进行修复，如果内核处于受损或者被攻击状态，所有的实时补丁方案将存在被破坏的风险；而且已有方案实时补丁修复方案需要内核权限来实现跟踪、截获系统内核指令，其自身代码复杂存在的自身漏洞将引入更多内核安全问题。

发明内容

[0004] 本发明旨在至少解决现有技术中存在的技术问题之一。为此，本发明实施例提出一种内核修复方法，能够增强内核修补的可靠性、有效性，提高实时修补性能。

[0005] 本发明实施例还提出另一种内核修复方法。

[0006] 本发明实施例还提出另一种内核修复方法。

[0007] 本发明实施例还提出一种内核修复装置。

[0008] 本发明实施例还提出另一种内核修复装置。

[0009] 本发明实施例还提出一种电子设备。

[0010] 本发明实施例还提出一种计算机可读存储介质。

[0011] 根据本发明的第一方面实施例的内核修复方法，用于服务器，包括：

[0012] 获取终端发送的基本信息，根据所述基本信息构建第一内核文件和第二内核文件；

[0013] 根据所述第一内核文件和所述第二内核文件提取得到目标补丁函数；

[0014] 对所述目标补丁函数进行预处理，生成目标修补文本；

[0015] 将所述目标修补文本发送至终端。

[0016] 根据本发明第一方面实施例的内核修复方法，至少具有如下有益效果：首先，根据终端发送的基本信息可以构建得到第一内核文件和第二内核文件，其次，根据第一内核文件和第二内核文件提取得到目标补丁函数；再次，可以对目标补丁函数进行预处理，生成目标修补文本；最后，将所述目标修补文本发送至终端，可以增强内核修补的可靠性、有效性，提高实时修补性能。

[0017] 根据本发明的一些实施例，根据所述第一内核文件和所述第二内核文件提取得到目标补丁函数，包括：基于所述第一内核文件创建第一函数调用图和第二函数调用图；基于

所述第二内核文件创建第三函数调用图和第四函数调用图;将所述第一函数调用图和所述第二函数调用图进行比对,得到第一比对结果,将所述第三函数调用图和所述第四函数调用图进行比对,得到第二比对结果;根据所述第一比对结果和所述第二比对结果提取得到目标补丁函数。

[0018] 根据本发明的一些实施例,所述对所述目标补丁函数进行预处理,生成目标修补文本,包括:获取对称密钥;根据所述对称密钥加密所述目标补丁函数,得到目标修补文本。

[0019] 根据本发明的第二方面实施例的内核修复方法,用于终端,包括:

[0020] 获取操作系统的基本信息,将所述基本信息发送至服务器;

[0021] 获取所述服务器发送的目标修补文本,对所述目标修补文本进行处理得到目标补丁;

[0022] 根据所述目标补丁进行内核修复。

[0023] 根据本发明第二方面实施例的内核修复方法,至少具有如下有益效果:首先,获取操作系统的基本信息,将基本信息发送至服务器;其次,获取服务器发送的目标修补文本,对目标修补文本进行处理得到目标补丁;最后,根据目标补丁进行内核修复,可以支持受损内核进行实时补丁修复,减少存储开销,还可以保证操作系统和软件执行状态的一致性。

[0024] 根据本发明的一些实施例,所述根据所述目标修补文本处理得到目标补丁,包括:验证所述目标修补文本的完整性,得到第一验证结果;对所述目标修补文本中的分支指令进行简化处理,得到简化处理结果;补充所述目标修补文本的标识信息,得到补充结果;根据所述第一验证结果、所述简化处理结果和所述补充结果进行加密处理,得到目标补丁。

[0025] 根据本发明的一些实施例,所述根据所述目标补丁进行内核修复,包括:验证所述目标补丁的完整性,得到第二验证结果;根据所述第二验证结果将所述目标补丁进行写出,并获取修补指令;根据所述修补指令进行内核修复。

[0026] 根据本发明第三方面实施例的内核修复方法,用于服务器和终端,包括:

[0027] 服务器执行本发明第一方面实施例的内核修复方法,终端执行本发明第二方面实施例的内核修复方法。

[0028] 根据本发明第三方面实施例的内核修复方法,至少具有如下有益效果:通过服务器执行本发明第一方面实施例的内核修复方法,通过终端执行本发明第二方面实施例的内核修复方法,可以提高实时修补性能,减少存储开销,保护补丁隐私。

[0029] 根据本发明第四方面实施例的内核修复装置,包括:

[0030] 获取模块,用于获取终端发送的基本信息,根据所述基本信息构建第一内核文件和第二内核文件;

[0031] 提取模块,用于根据所述第一内核文件和所述第二内核文件提取得到目标补丁函数;

[0032] 第一处理模块,用于对所述目标补丁函数进行预处理,生成目标修补文本;

[0033] 第一发送模块,用于将所述目标修补文本发送至终端。

[0034] 根据本发明第四方面实施例的内核修复装置,至少具有如下有益效果:通过执行本发明第一方面实施例的内核修复方法,可以增强内核修补的可靠性、有效性,提高实时修补性能。

[0035] 根据本发明第五方面实施例的内核修复装置,包括:

[0036] 第二发送模块，用于获取操作系统的基本信息，将所述基本信息发送至服务器；

[0037] 第二处理模块，用于获取所述服务器发送的目标修补文本，对所述目标修补文本进行处理得到目标补丁；

[0038] 修复模块，用于根据所述目标补丁进行内核修复。

[0039] 根据本发明第五方面实施例的内核修复装置，至少具有如下有益效果：通过执行本发明第二方面实施例的内核修复方法，可以支持受损内核进行实时补丁修复，减少存储开销，还可以保证操作系统和软件执行状态的一致性。

[0040] 根据本发明第六方面实施例的电子设备，包括：至少一个处理器，以及，与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器执行所述指令时实现第一方面实施例和/或本发明第二方面实施例和/或本发明第三方面实施例所述的内核修复方法。

[0041] 根据本发明第六方面实施例的内核修复电子设备，至少具有如下有益效果：通过执行本发明第一方面实施例和/或本发明第二方面实施例和/或本发明第三方面实施例的内核修复方法，可以提高实时修补性能，减少存储开销，保护补丁隐私。

[0042] 根据本发明第七方面实施例的计算机可读存储介质，所述存储介质存储有计算机可执行指令，所述计算机可执行指令用于使计算机执行第一方面实施例和/或本发明第二方面实施例和/或本发明第三方面实施例所述的内核修复方法。

[0043] 根据本发明第七方面实施例的计算机可读存储介质，至少具有如下有益效果：通过执行本发明第一方面实施例和/或本发明第二方面实施例和/或本发明第三方面实施例的内核修复方法，可以提高实时修补性能，减少存储开销，保护补丁隐私。

[0044] 本发明的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0045] 本发明的上述和/或附加的方面和优点从结合下面附图对实施例的描述中将变得明显和容易理解，其中：

[0046] 图1为本发明一实施例的内核修复方法的流程示意图；

[0047] 图2为本发明另一实施例的内核修复方法的流程示意图；

[0048] 图3为本发明一实施例的内核修复装置的结构示意图；

[0049] 图4为本发明另一实施例的内核修复装置的结构示意图；

[0050] 图5为本发明实施例的电子设备的功能模块图。

[0051] 附图标记：

[0052] 获取模块300、提取模块310、第一处理模块320、第一发送模块330、第二发送模块400、第二处理模块410、修复模块420、处理器500、存储器510、数据传输模块520、摄像头530、显示屏540。

具体实施方式

[0053] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附

图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。

[0054] 本发明的描述中，除非另有明确的限定，设置、安装、连接等词语应做广义理解，所属技术领域技术人员可以结合技术方案的具体内容合理确定上述词语在本发明中的具体含义。

[0055] 参照图1，根据本发明第一方面实施例的内核修复方法，包括：

[0056] 步骤S100，获取终端发送的基本信息，根据基本信息构建第一内核文件和第二内核文件。

[0057] 其中，基本信息可以是终端的有关操作系统的信息；第一内核文件可以是基于基本信息构建得到的修复前原始代码文件；第二内核文件可以是基于基本信息构建得到的修复后代码文件。可选的，服务器可以是远程补丁服务器，基本信息可以包括操作系统的内核版本、配置等足以重建二进制映像的编译标志，上述基本信息可以由终端准备，继而可以将上述基本信息发送至服务器。可选的，服务器可以根据接收到的基本信息构建第一内核文件和第二内核文件，例如，服务器可以使用与基本信息相同的编译信息构建得到第一内核文件和第二内核文件。

[0058] 步骤S110，根据第一内核文件和第二内核文件得到目标补丁函数。

[0059] 其中，目标补丁函数可以是需要得到的补丁修复函数。可选的，可以根据第一内核文件和第二内核文件进行比较，提取得到目标补丁函数。例如，根据第一内核文件和第二内核文件分别生成相应的函数调用图，比较所得函数调用图即可提取得到目标补丁函数。

[0060] 步骤S120，对目标补丁函数进行预处理，生成目标修补文本。

[0061] 其中，目标修补文本可以是处理后所得的初始二进制补丁。可选的，在终端的操作系统内核使用所得补丁代码修复内核之前，需要对补丁代码进行必要的预处理，即对目标补丁函数进行预处理，得到初步受信任的实时修补程序，即得到目标修补文本。可以在服务器对目标补丁函数进行预处理得到初步受信任的实时修补程序，即得到目标修补文本。

[0062] 步骤S220，将目标修补文本发送至终端。

[0063] 可选的，当服务器预处理得到初步受信任的实施修补程序，及得到目标修补文本后，可以将目标修补文本发送至终端，使得终端可以根据该目标修补文本进行操作系统内核修复。可以通过加密数据传输，将目标修补文本发送至终端。

[0064] 上述内核修复方法，首先，根据终端发送的基本信息可以构建得到第一内核文件和第二内核文件，其次，根据第一内核文件和第二内核文件提取得到目标补丁函数；再次，可以对目标补丁函数进行预处理，生成目标修补文本；最后，将所述目标修补文本发送至终端，可以增强内核修补的可靠性、有效性，提高实时修补性能。

[0065] 在本发明的一些实施例中，根据第一内核文件和第二内核文件提取得到目标补丁函数，包括：

[0066] 基于第一内核文件创建第一函数调用图和第二函数调用图。其中，第一函数调用图可以是基于第一内核文件创建得到的原始代码在编译前的代码级函数调用图，即补丁修补前源代码对应的函数调用图；第二函数调用图可以是基于第一内核文件创建得到的原始代码在编译后所得的二进制函数调用图，即补丁修复前二进制文件对应的函数调用图。可选的，为阅读第一内核文件，可以结合使用现有的算法和技术，例如使用codeviz工具，根据第一内核文件构建得到原始代码编译前的函数调用图，即得到第一函数调用图；又如使用

IDA Pro(交互式反汇编器专业版,Interactive Disassembler Professional),根据第一内核文件来创建得到原始代码编译后的二进制函数调用图。由此可以得到第一函数调用图和第二函数调用图。

[0067] 基于第二内核文件创建第三函数调用图和第四函数调用图。其中,第三函数调用图可以是基于第二内核文件创建得到的补丁修复后代码在编译前的代码级函数调用图,即补丁修补后源代码对应的函数调用图;第四函数调用图可以是基于第二内核文件创建得到的补丁修复后代码在编译后的二进制函数调用图,即补丁修补后二进制文件对应的函数调用图。可选的,为阅读第二内核文件,可以使用codeviz工具,根据第二内核文件构建得到第三函数调用图;可以使用IDA Pro,根据第二内核文件构建得到第四函数调用图,由此可以得到第三函数调用图和第四函数调用图。

[0068] 将第一函数调用图和所述第二函数调用图进行比对,得到第一比对结果,将第三函数调用图和所述第四函数调用图进行比对,得到第二比对结果。其中,第一比对结果可以是表示第一函数调用图和第二函数调用图之间的差异;第二比对结果可以是表示第三函数调用图和第四函数调用图之间的差异。可选的,可以通过源代码级函数调用图和二进制函数调用图之间的差异说明某些编译器优化,所以可以分别比较第一函数调用图和第二函数调用图、比较第三函数调用图和第四函数调用图,由此可以得到第一比对结果和第二比对结果。

[0069] 根据第一比对结果和第二比对结果提取得到目标补丁函数。可选的,所得的第一比对结果和第二比对结果中可以包括在操作系统内核中特别常见的内联函数,因此可以根据第一比对结果和第二比对结果提取该内联函数,即得到目标补丁函数。例如,可以将第一函数调用图和第二函数调用图进行比对,将第三函数调用图和第四函数调用图进行比对,具体的,利用现有的二进制签名匹配方法,如iBinHunt和FIBER来对齐和识别二进制内核图像的相关部分,并通过算法迭代地标识包含的函数,直到不能添加新的包含的函数为止。为了便于讨论和评估,可以将所得包含的函数分为三大类(通过内核实时修补增加支持难度),例如分为Type 1函数、Type 2函数和Type 3函数,其中Type 1函数不涉及内联,Type 2函数确实涉及内联,Type 3函数修改全局或共享变量。可以重点考虑Type1和Type2的函数作为目标补丁函数,Type 3函数则需要根据变量修改情形确定目标补丁函数:在Type3函数中,可以考虑补丁中更改的全局或共享变量(这样的变量可以被删除、添加或修改),如果未修改变量的大小,则修补程序代码不受影响。只能提取Type 3函数中的部分作为目标补丁函数进行补丁修复。根据第一内核文件创建得到第一函数调用图和第二函数调用图,根据第二内核文件创建得到第三函数调用图和第四函数调用图,然后分别比较第一函数调用图和第二函数调用图、比较第三函数调用图和第四函数调用图,从而可以提取得到目标补丁函数,从而可以得到高效目标补丁函数。

[0070] 在本发明的一些实施例中,对目标补丁函数进行预处理,生成目标修补文本,包括:

[0071] 获取对称密钥。其中,对称密钥可以是服务器与终端通过共享内存交互生成的共享密钥加密,服务器与终端在发送和接收数据时双方对明文进行加密和解密运算所使用相同的密钥。该共享内存可以是操作系统中的预留内存,例如操作系统上Intel SGX和Intel SMM两个可信执行环境的共享内存。可选的,可以在服务器对目标补丁函数进行预处理,得

到初步受信任的实时修补程序。因此，可以获取对称密钥即Deffie-Hellman密钥，该对称密钥可以用于加密传输目标修补文本。

[0072] 根据对称密钥加密目标补丁函数，得到目标修补文本。可选的，可以根据对称密钥对目标补丁函数进行加密处理，得到初步受信任的实时修补程序，即得到目标修补文本。通过获取的对称密钥可以对目标补丁函数进行加密处理，得到初步受信任的二进制补丁，即得到目标修补文本，可以初步构建可信任的补丁修补执行环境，从而可以避免来自内核本身对修复过程的干扰或攻击。

[0073] 参照图2，根据本发明第二方面实施例提出的内核修复方法，用于终端，包括：

[0074] 步骤S200，获取操作系统的基本信息，将基本信息发送至服务器。

[0075] 其中，操作系统的基本信息可以是终端的有关操作系统的信息，例如内核版本、配置和足以重建二进制映像的编译标志。可选的，可以在终端系统启动时安全地收集有关当前操作系统内核的信息，即得到基本信息，继而可以将搜集的基本信息发送至远程补丁服务器，使得远程补丁服务器可以根据该基本信息使用相同的编译信息构建第一内核文件及第二内核文件。

[0076] 步骤S210，获取服务器发送的目标修补文本，对目标修补文本进行处理得到目标补丁。

[0077] 其中，目标补丁可以是用于进行内核修复的可正确执行修复的二进制补丁。可选的，为避免直接使用目标修补文本进行实时修补可能会更改函数大小并导致内核一致性问题，可以通过服务器获取初步的二进制补丁，即获取目标修补文本，可以将该目标修补文本发送到本终端操作系统的Intel SGX飞地中做进一步处理成可正确执行的二进制补丁，即得到目标补丁。

[0078] 步骤S220，根据目标补丁进行内核修复。

[0079] 可选的，当处理得到目标补丁后，即得到可正确执行的二进制补丁，又因该二进制补丁已经加密，所以能够在确保安全性的情况下，根据该目标补丁进行内核修复。例如，终端的SGX飞地接收处理得到的二进制补丁(即目标补丁)，并准备修复函数，可以在目标补丁添加外部消息字段以确保SMM(System Management Mode，即系统管理模式，是一个对所有Intel处理器都统一的标准体系结构特性)系统处理程序能够正确处理目标补丁，并将处理后的目标补丁放在可执行内存空间中，即放在共享内存中(操作系统中的预留内存)，则操作系统可以调用该目标补丁进行内核修复，如Intel SMM处理程序通过读共享内存获取可执行的二进制补丁进行内核修复。

[0080] 在一些具体的实施例中，为了保证内核修复时系统运行时状态不改变，可以利用硬件特性暂停系统当前执行程序并保存状态，待补丁修复后自动恢复系统状态，保证系统执行的一致性。例如，通过SMM系统保存运行时进程的状态，在SMM完成补丁修补程序后恢复该状态，即通过SMM硬件确保将最新的运行时状态和寄存器值保存到受保护的内存SMRAM区域。通过使用SMM自然地存储操作系统的运行时状态，从而减少外部存储开销并提高实时修补性能，支持更快的恢复，而不需要外部检查和恢复。

[0081] 上述内核修复方法，首先，获取操作系统的基本信息，将基本信息发送至服务器；其次，获取服务器发送的目标修补文本，对目标修补文本进行处理得到目标补丁；最后，根据目标补丁进行内核修复，可以支持受损内核进行实时补丁修复，减少存储开销，还可以保

证操作系统和软件执行状态的一致性。

[0082] 在本发明的一些实施例中,根据目标修补文本处理得到目标补丁,包括:

[0083] 验证目标修补文本的完整性,得到第一验证结果。其中,第一验证结果可以是验证目标修补文本是否完整的结果,例如目标修补文本完整的结果。可选的,可以检测从服务器接收到的目标修补文本的完整性,确保目标修补文本的安全性,例如可以得到目标修补文本完整的第一验证结果。

[0084] 对目标修补文本中的分支指令进行简化处理,得到简化处理结果。其中,简化处理结果可以简化目标修补文本中的分支指令跳转偏移量的重置计算的结果。可选的,可以标识目标修补文本中的分支指令,简化该分支指令跳转偏移量的重置计算,得到简化处理结果,例如完成简化处理的结果。

[0085] 补充目标修补文本的标识信息,得到补充结果。其中,标识信息可以是用于识别目标修补文本的信息,补充结果可以是为目标修补文本补充标识信息完成的结果。可选的,为得到可执行的目标补丁,便于在操作系统中识别目标补丁并正确实施,可以补充目标修补文本的标识信息,例如可以生成标准的补丁报文,补充目标修补文本的版本、类型、hash值等标识信息,得到补充完毕的结果。

[0086] 根据第一验证结果、简化处理结果和补充结果进行加密处理,得到目标补丁。可选的,在对目标修补文本处理完毕后,即完成完整性验证、简化目标修补文本中的分支指令跳转偏移量的重置计算、补充目标修补文本的标识信息之后,可以根据所得第一验证结果、简化处理结果和补充结果得到加密处理后的目标补丁。

[0087] 在一些具体的实施例中,可以加密处理所得目标补丁并传递到操作系统预留的共享内存区域,使得操作系统可以通过共享内存调用该目标补丁进行内核修复。例如,可以通过以下方式得到共享内存:首先配置引导加载程序(例如,GRUB。GNU GRUB,GRand Unified Bootloader,简称"GRUB",是一个来自GNU项目的多操作系统启动程序),以保留操作系统中适当的内核内存分配空间(假设原型实现为18MB);其次,可以将页属性操作代码添加到paging_init函数中,以便为该共享内存提供适当的访问限制。可以通过下述方式将目标补丁存储到共享内存中:假设共享内存包括三个逻辑部分:mem_RW、mem_W和mem_X。其中,mem_RW是用于进行对称密钥交换的读/写区域,假设使用Diffie-Hellman密钥交换算法进行对称密钥交换;较大的区域mem_W是只写的区域,用于存储加密的目标修补文本,不受信任的应用程序将数据从SGX飞地写入mem_W,但是不受信任的应用程序无法解密此输出数据;更大的mem_X区域只能执行,用于将解密得到的目标补丁存储为本地操作系统的内核文本。为了保持完整性,可以禁止对内核文本进行读写访问。此外,还可以使用现有的基于SMM的运行时检查系统来进一步确保该区域的完整性,使得控制机制访问权限只限于本地操作系统内核。

[0088] 通过上述方法,可以在确保目标修补文本的完整性和安全性的前提下,对目标修补文本进行处理,得到目标补丁,以防止网络传输错误导致的内核本身对内核修复的干扰或攻击;且将目标补丁存储到共享内存中,可以在可信执行环境中存储目标补丁,从而可以提供高效安全的目标补丁。

[0089] 在本发明的一些实施例中,根据目标补丁进行内核修复,包括:

[0090] 验证目标补丁的完整性,得到第二验证结果。其中,第二验证结果可以是在调用目

标补丁进行内核修复时对目标补丁的完整性进行验证的结果。可选的，为防止网络传输错误，可以对目标补丁进行完整性验证，例如，可以先为目标补丁添加外部消息字段以确保SMM处理程序能够正确处理该目标补丁，并将处理后的目标补丁放置于正确的内存位置和对齐方式，然后对目标补丁的完整性进行验证，得到完整性验证完成的第二验证结果。

[0091] 根据第二验证结果将目标补丁进行写出，并获取修补指令。其中，修补指令可以是触发内核修补的指令。例如，可以将目标补丁作为可执行内存块写出，并用外部头信息打包这个内存块；然后可以在SGX飞地加密写出的数据，继而可以将加密的数据传递给mem_W段；最后，可以触发SMI将控制权转移到基于SMM的实时修补组件，同时得到修补指令。

[0092] 根据修补指令进行内核修复。可选的，当系统接收到修补指令时，可以切换到系统管理模式，进行内核修复。同时SMM硬件可以将最新的运行时状态和寄存器值保存到受保护的内存SMRAM区域，即利用硬件特性暂停系统当前执行程序并保存状态，待内核修复后自动恢复系统状态，保证系统执行的一致性。根据目标补丁进行完整性验证并写出，同时根据获取的修补指令触发内核修复，使得内核即使被破坏也可以被可靠而正确地进行修补，可以实现内核修复的最小的停机时间，提高修补的可靠性和一致性。

[0093] 根据本发明第三方面实施例提出的内核修复方法，用于服务器和终端，包括：

[0094] 服务器执行如本发明第一方面实施例的内核修复方法；对应的，终端执行如本发明第二方面实施例的内核修复方法。

[0095] 上述内核修复方法，通过服务器执行本发明第一方面实施例的内核修复方法，通过终端执行本发明第二方面实施例的内核修复方法，可以提高实时修补性能，减少存储开销，保护补丁隐私。

[0096] 参照图3，根据本发明第四方面实施例提出的内核修复装置，包括：

[0097] 获取模块300，用于获取终端发送的基本信息，根据基本信息构建第一内核文件和第二内核文件；

[0098] 提取模块310，用于根据第一内核文件和第二内核文件提取得到目标补丁函数；

[0099] 第一处理模块320，用于对目标补丁函数进行预处理，生成目标修补文本；

[0100] 第一发送模块330，用于将目标修补文本发送至终端。

[0101] 上述内核修复装置，通过执行本发明第一方面实施例的内核修复方法，可以增强内核修补的可靠性、有效性，提高实时修补性能。

[0102] 参照图4，根据本发明第五方面实施例提出的内核修复装置，包括：

[0103] 第二发送模块400，用于获取操作系统的基本信息，将基本信息发送至服务器；

[0104] 第二处理模块410，用于获取服务器发送的目标修补文本，对目标修补文本进行处理得到目标补丁；

[0105] 修复模块420，用于根据目标补丁进行内核修复。

[0106] 上述内核修复装置，通过执行本发明第二方面实施例的内核修复方法，可以支持受损内核进行实时补丁修复，减少存储开销，还可以保证操作系统和软件执行状态的一致性。

[0107] 参照图5，本发明第六方面实施例还提供了一种内核修复电子设备内部结构图，包括：至少一个处理器500，以及与至少一个处理器500通信连接的存储器510；还可以包括数据传输模块520、摄像头530、显示屏540。

[0108] 其中，所述处理器500通过调用存储器510中存储的计算机程序，用于执行第一方面实施例和/或第二方面实施例和/或第三方面实施例中的内核修复方法。

[0109] 存储器作为一种非暂态存储介质，可用于存储非暂态软件程序以及非暂态性计算机可执行程序，如本发明第一方面实施例和/或第二方面实施例和/或第三方面实施例中的内核修复方法。处理器通过运行存储在存储器中的非暂态软件程序以及指令，从而实现上述第一方面实施例和/或第二方面实施例和/或第三方面实施例中的内核修复方法。

[0110] 存储器可以包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需要的应用程序；存储数据区可存储执行上述第一方面实施例和/或第二方面实施例和/或第三方面实施例中的内核修复方法。此外，存储器可以包括高速随机存取存储器，还可以包括非暂态存储器，例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施方式中，存储器可选包括相对于处理器远程设置的存储器，这些远程存储器可以通过网络连接至该终端。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0111] 实现上述第一方面实施例和/或第二方面实施例和/或第三方面实施例中的内核修复方法所需的非暂态软件程序以及指令存储在存储器中，当被一个或者多个处理器执行时，执行上述第一方面实施例和/或第二方面实施例和/或第三方面实施例中的内核修复方法。

[0112] 本发明第七方面实施例还提供了计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令用于：执行第一方面实施例和/或第二方面实施例和/或第三方面实施例中的内核修复方法。

[0113] 在一些实施例中，该存储介质存储有计算机可执行指令，该计算机可执行指令被一个或多个控制处理器执行，例如，被第六方面实施例的电子设备中的一个处理器执行，可使得上述一个或多个处理器执行上述第一方面实施例和/或第二方面实施例和/或第三方面实施例中的内核修复方法。

[0114] 上面结合附图对本发明实施例作了详细说明，但是本发明不限于上述实施例，在所属技术领域普通技术人员所具备的知识范围内，还可以在不脱离本发明宗旨的前提下作出各种变化。

[0115] 本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统可以被实施为软件、固件、硬件及其适当的组合。某些物理组件或所有物理组件可以被实施为由处理器，如中央处理器、数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

[0116] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示意性实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0117] 尽管已经示出和描述了本发明的实施例，本领域的普通技术人员可以理解：在不脱离本发明的原理和宗旨的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由权利要求及其等同物限定。

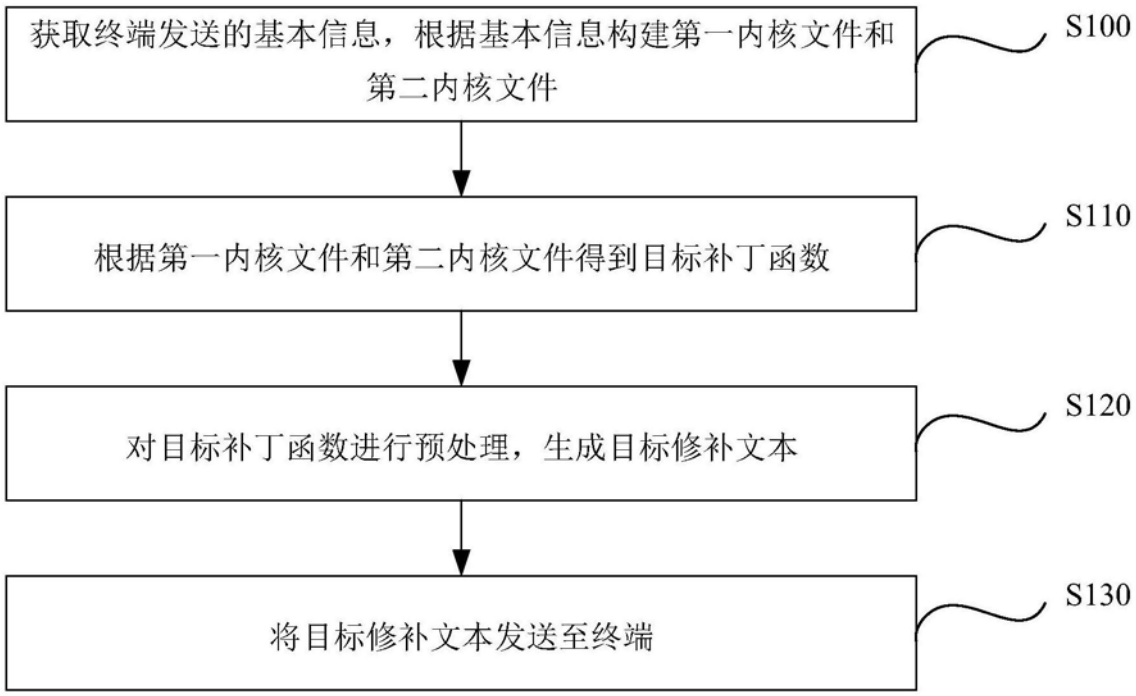

获取终端发送的基本信息，根据基本信息构建第一内核文件和第二内核文件
S100
根据第一内核文件和第二内核文件得到目标补丁函数
S110
对目标补丁函数进行预处理，生成目标修补文本
S120
将目标修补文本发送至终端
S130

图1

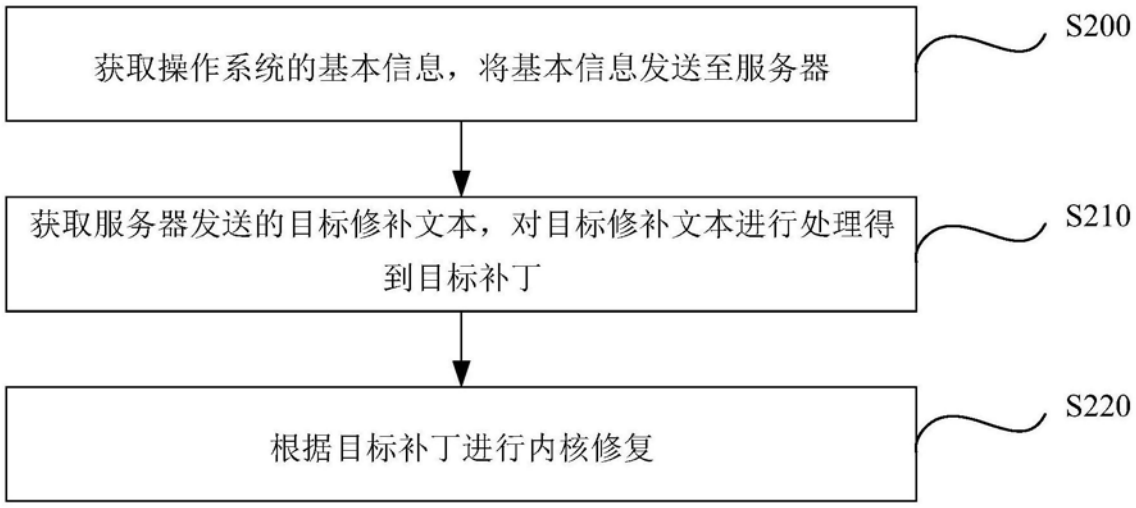

获取操作系统的基本信息，将基本信息发送至服务器
S200
获取服务器发送的目标修补文本，对目标修补文本进行处理得到目标补丁
S210
根据目标补丁进行内核修复
S220

图2

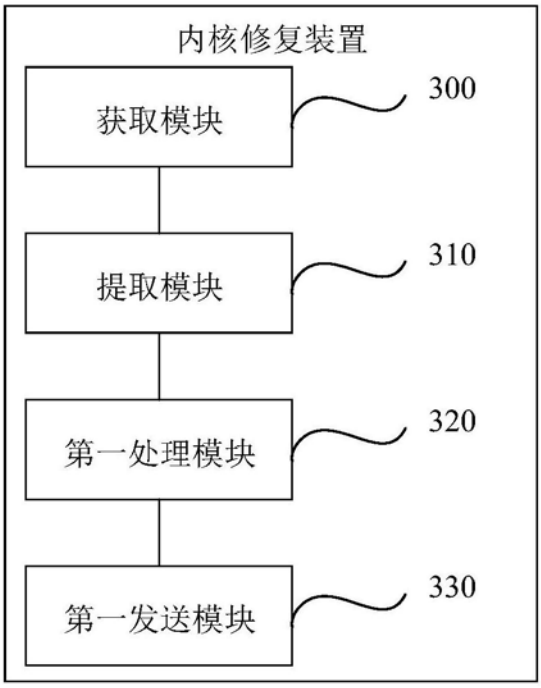

内核修复装置
获取模块
300
提取模块
310
第一处理模块
320
第一发送模块
330

图3

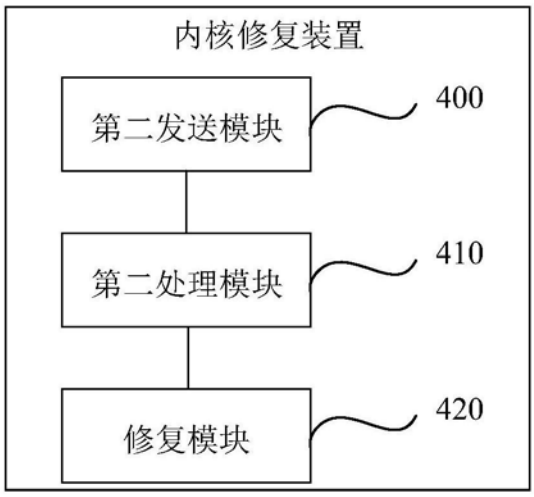

内核修复装置
第二发送模块
400
第二处理模块
410
修复模块
420

图4

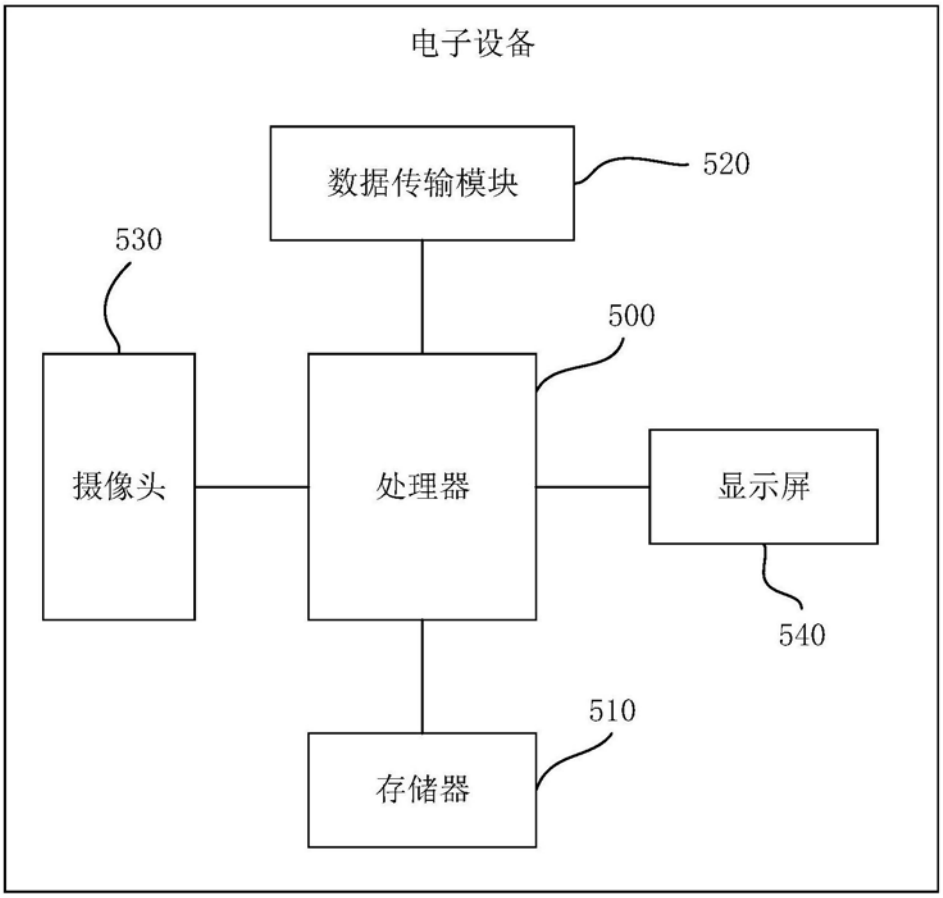


图5