(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 2 月 7 日 (07.02.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/024708 A1

(51) 国际专利分类号:
G06F 21/74 (2013.01)

(21) 国际申请号: PCT/CN2018/096759

(22) 国际申请日: 2018 年 7 月 24 日 (24.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710648239.3 2017年8月1日 (01.08.2017) CN

(71) 申请人: 杭州中天微系统有限公司 (C-SKY MICROSYSTEMS CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼, Zhejiang 310012 (CN)。

(72) 发明人: 崔晓夏 (CUI, Xiaoxia); 中国浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼, Zhejiang 310012 (CN)。 李春强 (LI, Chunqiang); 中国浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼, Zhejiang 310012 (CN)。 侯光恩 (HOU, Guangen); 中国浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼, Zhejiang 310012 (CN)。 陈理 (CHEN, Li); 中国浙江省杭州市西湖区西斗门路3号天堂软件园A幢15楼, Zhejiang 310012 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街35号国际企业大厦A座16层, Beijing 100033 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) **Title:** TRUSTED KERNEL-BASED ATTACK-PREVENTION DATA PROCESSOR

(54) **发明名称:** 一种基于可信内核的防攻击数据处理器

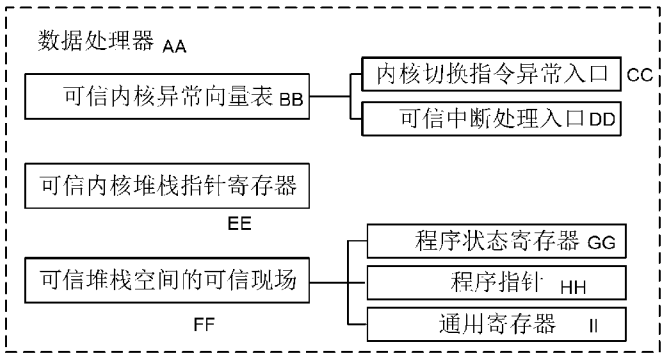

图 1

AA Data processor
BB Trusted kernel exception vector table
CC Kernel switching command exception entry
DD Trusted interruption processing entry
EE Trusted kernel stack pointer register
FF Trusted site of trusted stack space
GG Program status register
HH Program pointer
II Universal register

(57) **Abstract:** Provided in the present invention is a trusted kernel-based attack-prevention data processor, comprising: a trusted kernel exception vector table, which is used to provide a processing entry for kernel switching; a trusted kernel stack pointer register, which is used to store a trusted kernel stack pointer that points to a trusted kernel stack space; and a trusted site within the trusted kernel stack space, wherein the trusted site comprises a program status register that is used to store an initial kernel flag bit of kernel switching, as well as a program pointer and a universal register; when the data processor executes kernel switching from a non-trusted kernel to a trusted kernel, said trusted kernel is addressed to the processing entry of said kernel switching, and switching is executed. The present invention is able to provide an underlying software protection mechanism for a switching entry of a trusted kernel, so that switching between a trusted kernel and a non-trusted kernel is more secure.

WO 2019/024708 A1

[见续页]

LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本发明提供一种基于可信内核的防攻击数据处理器，包括：可信内核异常向量表，用于提供内核切换的处理入口；可信内核堆栈指针寄存器，用于存储指向可信内核堆栈空间的可信内核堆栈指针；可信内核堆栈空间中的可信现场，可信现场包括用于存储内核切换的起始内核标志位的程序状态寄存器、程序指针和通用寄存器；其中，数据处理器在执行非可信内核向可信内核的内核切换时，所述可信内核寻址到所述内核切换的处理入口并执行切换。本发明能够对可信内核切换入口提供底层软件保护机制，使得可信内核和非可信内核切换时更加安全。

一种基于可信内核的防攻击数据处理器

技术领域

本发明涉及信息安全技术领域，尤其涉及一种基于可信内核的防攻击数据处理器。

背景技术

随着移动互联网以及物联网的发展及信息技术在生产、经营、管理方面的广泛应用，人类经济社会越来越依赖网络和信息系统。而不时发生的病毒侵袭、黑客攻入和信息窃取等事件，使得系统安全保障工作日益重要并倍受人们关注。

目前，通过引入安全模式，系统信息的安全得到了一定程度的保障。在安全模式中，系统真正实现了硬件隔离。系统内核运行在整个系统的最高特权层，管理和控制底层硬件资源，为上层应用程序提供安全隔离的资源抽象和访问接口，是整个系统的基础。在安全模式下，运行可信内核的操作系统与在非安全模式下运行的操作系统相互独立。可信内核提供安全认证、加解密、敏感数据存储等服务。通过硬件安全组件进行物理隔离，确保非安全模式下的操作系统无法直接访问安全模式下的资源，从而缩小攻击面。

但是，攻击者依然可以在非安全模式下通过一系列手段对可信内核进行攻击来获取敏感数据等，甚至可以导致系统崩溃。

因此，亟需在可信内核中设计一种程序控制，用于防范此类攻击。

发明内容

本发明提供的一种基于可信内核的防攻击数据处理器，能够针对现有技术的不足，在可信内核中提供底层软件保护机制，增强可信内核的安全性。

本发明提供一种基于可信内核的防攻击数据处理器，其中包括：

可信内核异常向量表，用于提供内核切换的处理入口；

可信内核堆栈指针寄存器，用于存储指向可信内核堆栈空间的可信内核堆栈指针；

可信内核堆栈空间中的可信现场，所述可信现场包括用于存储内核切换的起始内核标志位的程序状态寄存器、程序指针和通用寄存器；

所述数据处理器在执行非可信内核向可信内核的内核切换时，所述可信内核寻址到所述内核切换的处理入口并执行切换。

可选地，上述提供内核切换的处理入口包括内核切换指令异常入口和可信中断处理入口。

可选地，上述可信内核通过内核切换指令、内核切换返回指令或中断响应方式寻址到所述内核切换的处理入口并执行切换。

可选地，上述可信内核通过内核切换返回指令执行切换时，需根据所述程序状态寄存器的起始内核的标志位判断返回所述起始内核或停留在当前内核。

可选地，上述可信内核通过跨内核任务调用的入口向量表寻址到所述内核切换指令异常入口。

可选地，上述可信内核通过所述可信内核异常向量表寻址到可信中断处理入口。

可选地，当上述可信内核响应非可信中断而切换到所述非可信内核时，所述可信内核将可信现场保存在所述可信内核堆栈空间中；

当上述非可信内核处理完非可信中断后，再调用所述内核切换返回指令切换到所述可信内核时，所述可信内核会从所述可信内核堆栈空间恢复可信现场。

可选地，上述可信现场是所述可信内核为响应非可信中断而切换到所述非可信内核前的现场。

可选地，当上述非可信内核修改所述程序状态寄存器的起始内核标志并且执行所述内核切换返回指令切换到所述可信内核时，所述可信内核会从所述可信内核堆栈空间恢复可信现场。

可选地，上述可信现场是所述可信内核第一次主动切换到所述非可信内核前的现场。

本发明实施例提供的基于可信内核的防攻击数据处理器，对所有可信内核切换入口提供了底层软件保护机制，能够使得可信内核和非可信内核切换时更加安全。

附图说明

为了更清楚地说明本申请实施方式或现有技术中的技术方案，下面将对实施方式或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施方式，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明提供的基于可信内核的防攻击数据处理器的基本架构示意图；

图 2 为本发明一实施例的数据处理器正常执行内核切换指令时的运行示意图；

图 3 为本发明一实施例的可信内核响应非可信内核中断后、由非可信内核执行内核切换返回指令返回可信内核的运行示意图；

图 4 为本发明一实施例的非法内核切换异常的运行示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明提供一种基于可信内核的防攻击数据处理器。图 1 示出了本发明提供的数据处理器的基本架构示意图。如图 1 所示，数据处理器包括可信内核异常向量表、可信内核堆栈指针寄存器、可信内核堆栈空间内的可信现场。

具体地，可信内核异常向量表包括两种内核切换的处理入口，即内核切换指令异常入口和可信中断处理入口，数据处理器在执行非可信内核向可信内核的内核切换时，可信内核会根据不同的方式寻址到内核切换的处理入口并执行切换。可信内核堆栈指针寄存器是指可信内核拥有的独立的堆栈指针，其指向可信内核堆栈空间；可信内核堆栈空间保存可信现场，可信现场包含当前可信内核上下文，典型地，包含上次可信内核切换前的程序状态寄存器、程序指针、通用寄存器。特别的，所述程序状态寄存器包含内核切换的起始内核的标志位。

具体地，数据处理器的内核切换方式包括内核切换指令、内核切换返回指令和中断响应三种方式。特别的，在使用内核切换返回指令执行内核切换时，可以根据程序状态寄存器的起始内核标志位置，判断返回起始内核还是停留在当前内核。

特别的，在使用内核切换指令、内核切换返回指令进行内核切换时，可信内核根据可信内核跨内核任务调用的入口向量表，寻址到内核切换指令异常入口。而在中断响应执行内核切换时，可信内核根据可信内核异常向量表寻址到可信中断处理入口。

图 2 示出了本发明一个实施例的数据处理器正常执行内核切换指令时的运行示意图。如图所示，当前数据处理器在非可信内核中正常执行内核切换命令。数据处理器保存位于非可信内核中的非可信现场，并且通过切换过程切换到可信内核。

进一步的，数据处理器在可信内核的异常向量表中寻址到内核切换指令异常入口并执行，可信内核的内核切换异常处理代码执行内核切换指令，通过切换过程返回到非可信内核，数据处理器恢复非可信现场后继续执行。

图 3 示出了本发明一个实施例的可信内核响应非可信内核中断后、由非可信内核执行内核切换返回指令返回可信内核的运行示意图。如图所示，当前数据处理器在可信内核中执行。当非可信内核有中断发生时，数据处理器保存可信现场到可信内核堆栈空间后，通过切换过程切换到非可信内核响应中断，特别的，可信堆栈指针寄存器指向上述

可信内核堆栈空间。

进一步的，非可信内核的中断处理函数执行内核切换指令返回可信内核。数据处理器根据可信内核堆栈指针寄存器指向的可信内核堆栈空间恢复可信现场后继续执行。

图 4 示出了本发明一个实施例的非法内核切换异常的运行示意图。如图所示，在可信内核里设置可信内核第一次切换到非可信内核前的现场，并且保存现场到可信内核堆栈指针寄存器指向的可信内核堆栈空间，然后执行内核切换指令切换到非可信内核。

进一步的，非可信内核修改程序状态寄存器的起始内核标志位，并且执行内核切换返回指令切换到可信内核执行。数据处理器保存非可信内核现场后，切换到可信内核内执行。

进一步的，数据处理器根据可信内核堆栈指针寄存器指向的可信内核堆栈空间恢复可信现场。数据处理器执行非法内核切换异常处理代码后，能够重启或抛出异常，从而防止非法内核侵入。

本发明实施例提供的基于可信内核的防攻击数据处理器，对所有可信内核切换入口提供了底层软件保护机制，能够使得可信内核和非可信内核切换时更加安全。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

权 利 要 求 书

1、一种基于可信内核的防攻击数据处理器，其特征在于，其包括：

可信内核异常向量表，用于提供内核切换的处理入口；

可信内核堆栈指针寄存器，用于存储指向可信内核堆栈空间的可信内核堆栈指针；

可信内核堆栈空间中的可信现场，所述可信现场包括用于存储内核切换的起始内核标志位的程序状态寄存器、程序指针和通用寄存器；

所述数据处理器在执行非可信内核向可信内核的内核切换时，所述可信内核寻址到所述内核切换的处理入口并执行切换。

2、根据权利要求 1 所述的数据处理器，其特征在于，所述提供内核切换的处理入口包括内核切换指令异常入口和可信中断处理入口。

3、根据权利要求 2 所述的数据处理器，其特征在于，所述可信内核通过内核切换指令、内核切换返回指令或中断响应方式寻址到所述内核切换的处理入口并执行切换。

4、根据权利要求 3 所述的数据处理器，其特征在于，所述可信内核通过内核切换返回指令执行切换时，需根据所述程序状态寄存器的起始内核的标志位判断返回所述起始内核或停留在当前内核。

5、根据权利要求 3 所述的数据处理器，其特征在于，所述可信内核通过跨内核任务调用的入口向量表寻址到所述内核切换指令异常入口。

6、根据权利要求 3 所述的数据处理器，其特征在于，所述可信内核通过所述可信内核异常向量表寻址到可信中断处理入口。

7、根据权利要求 3 所述的数据处理器，其特征在于，

当所述可信内核响应非可信中断而切换到所述非可信内核时，所述可信内核将可信现场保存在所述可信内核堆栈空间中；

当所述非可信内核处理完非可信中断后，再调用所述内核切换返回指令切换到所述可信内核时，所述可信内核会从所述可信内核堆栈空间恢复可信现场。

8、根据权利要求 7 所述的数据处理器，其特征在于，所述可信现场是所述可信内核为响应非可信中断而切换到所述非可信内核前的现场。

9、根据权利要求 3 所述的数据处理器，其特征在于，当所述非可信内核修改所述程序状态寄存器的起始内核标志并且执行所述内核切换返回指令切换到所述可信内核时，所述可信内核会从所述可信内核堆栈空间恢复可信现场。

10、根据权利要求 9 所述的数据处理器，其特征在于，所述可信现场是所述可信内

核第一次主动切换到所述非可信内核前的现场。

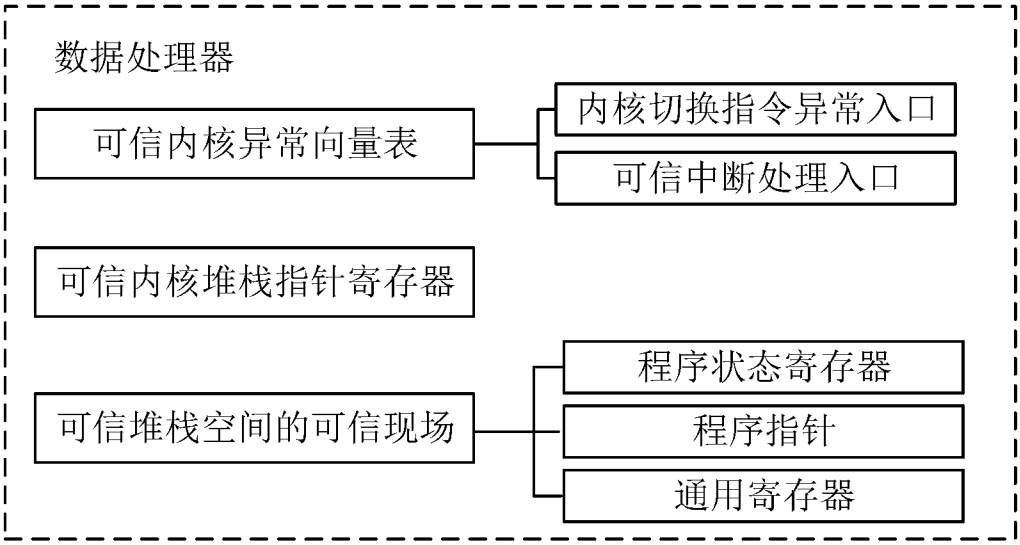
数据处理器
可信内核异常向量表
内核切换指令异常入口
可信中断处理入口
可信内核堆栈指针寄存器
可信堆栈空间的可信现场
程序状态寄存器
程序指针
通用寄存器

图 1

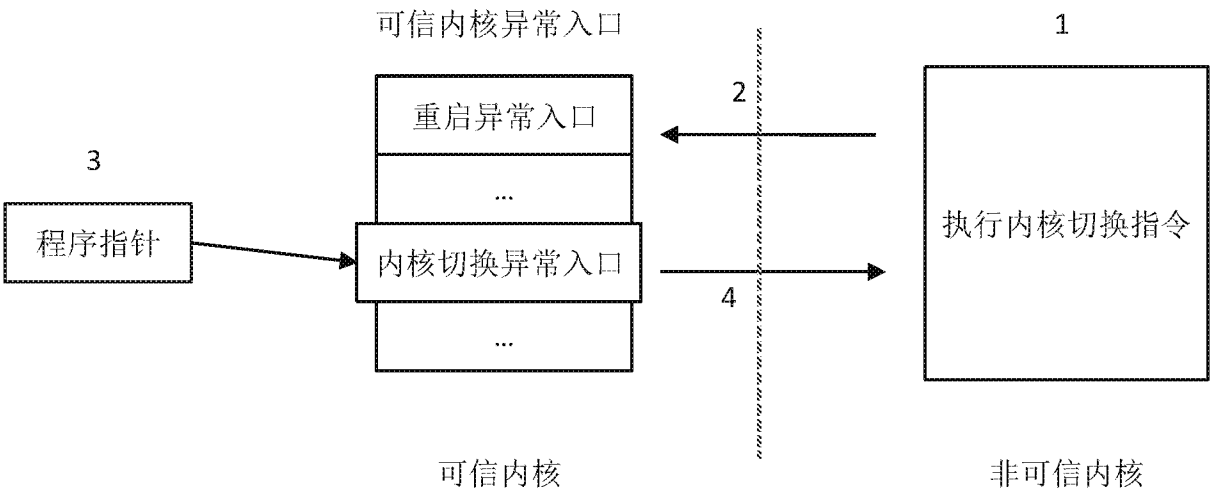
可信内核异常入口
1
2
重启异常入口
...
3
程序指针
内核切换异常入口
...
4
执行内核切换指令
可信内核
非可信内核

图 2

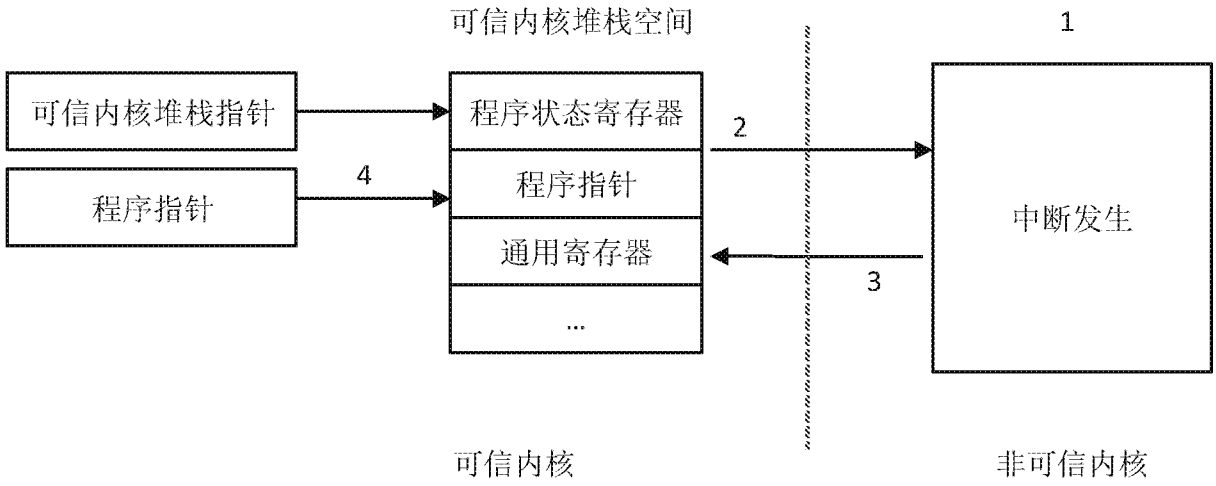
可信内核堆栈空间
1
可信内核堆栈指针
程序状态寄存器
2
程序指针
4
程序指针
通用寄存器
中断发生
3
...
可信内核
非可信内核

图 3

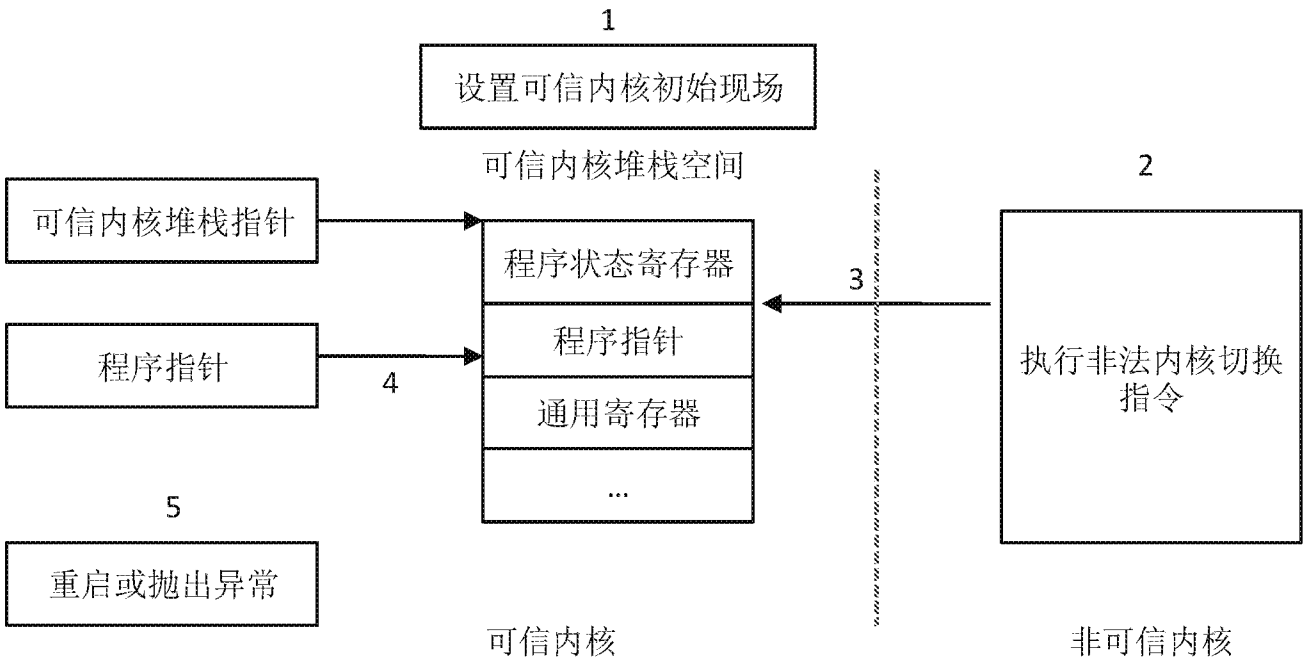
1
设置可信内核初始现场
可信内核堆栈空间
2
可信内核堆栈指针
程序状态寄存器
3
程序指针
程序指针
4
通用寄存器
执行非法内核切换指令
...
5
重启或抛出异常
可信内核
非可信内核

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/096759

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/74(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; SIPOABS; DWPI; CNTXT; EPODOC; CNKI: 处理器, 内核, 可信内核, 安全模式, 攻击, 切换, 异常, 向量表, 入口, 中断, 现场, 堆栈, 指针, 寄存器, 寻址, 标志位, processor, kernel, trusted kernel, security mode, attack, switch, exception, vector table, entry, interrupt, scene, stack, pointer, register, addressing, flag bit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107463856 A (C-SKY MICROSYSTEMS CO., LTD.) 12 December 2017 (2017-12-12) claims 1-10, and figures 1-4	1-10
X	CN 106599717 A (C-SKY MICROSYSTEMS CO., LTD.) 26 April 2017 (2017-04-26) claims 1-4, 6 and 8, description, paragraphs [0024]-[0029], [0036]-[0040] and [0042]-[0047], and figure 2	1-10
A	CN 106778365 A (C-SKY MICROSYSTEMS CO., LTD.) 31 May 2017 (2017-05-31) entire document	1-10
A	US 2003225817 A1 (ISHWAR, P. ET AL.) 04 December 2003 (2003-12-04) entire document	1-10

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 September 2018	**30 September 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/096759

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	107463856	A	12 December 2017	None	
CN	106599717	A	26 April 2017	None	
CN	106778365	A	31 May 2017	None	
US	2003225817	A1	04 December 2003	None	

国际检索报告

国际申请号 PCT/CN2018/096759

A. 主题的分类

G06F 21/74(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;SIPOABS;DWPI;CNTXT;EPODOC;CNKI: 处理器,内核,可信内核,安全模式,攻击,切换,异常,向量表,入口,中断,现场,堆栈,指针,寄存器,寻址,标志位, processor, kernel, trusted kernel, security mode, attack, switch, exception, vector table, entry, interrupt, scene, stack, pointer, register, addressing, flag bit

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 107463856 A (杭州中天微系统有限公司) 2017年 12月 12日 (2017-12-12) 权利要求1-10、图1-4	1-10
X	CN 106599717 A (杭州中天微系统有限公司) 2017年 4月 26日 (2017-04-26) 权利要求1-4，6，8、说明书第[0024]-[0029]，[0036]-[0040]，[0042]-[0047]段、图2	1-10
A	CN 106778365 A (杭州中天微系统有限公司) 2017年 5月 31日 (2017-05-31) 全文	1-10
A	US 2003225817 A1 (ISHWAR P 等) 2003年 12月 4日 (2003-12-04) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 9月 7日	2018年 9月 30日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	李昕宇
传真号 (86-10)62019451	电话号码 (86-10)62089924

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/096759

检索报告引用的专利文件			公布日（年/月/日）	同族专利	公布日（年/月/日）
CN	107463856	A	2017年 12月 12日	无	
CN	106599717	A	2017年 4月 26日	无	
CN	106778365	A	2017年 5月 31日	无	
US	2003225817	A1	2003年 12月 4日	无	