

(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 21 日 (21.02.2019)



(10) 国际公布号
WO 2019/033973 A1

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2018/099397

(22) 国际申请日: 2018 年 8 月 8 日 (08.08.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710712801.4 2017 年 8 月 18 日 (18.08.2017) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

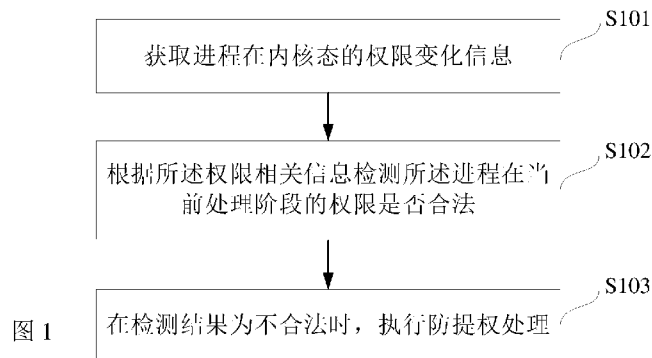
(72) 发明人: 李雪峰 (LI, Xuefeng); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。郭志鹏 (GUO, Zhipeng); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(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,

(54) Title: PRIVILEGE ESCALATION PREVENTION DETECTION METHOD AND DEVICE

(54) 发明名称: 防提权检测方法及设备



S101 ACQUIRE PRIVILEGE CHANGE INFORMATION ABOUT A PROCESS IN A KERNEL STATE
S102 DETECT, ACCORDING TO THE PRIVILEGE CHANGE INFORMATION, WHETHER THE PRIVILEGE OF THE PROCESS IN A CURRENT PROCESSING PHASE IS LEGITIMATE
S103 IF A DETECTION RESULT INDICATES THAT THE PRIVILEGE IS ILLEGITIMATE, EXECUTING PRIVILEGE ESCALATION PREVENTION PROCESSING

(57) Abstract: A privilege escalation prevention detection method and device. The method comprises: firstly acquiring privilege change information about a process in a kernel state; detecting the privilege change information to determine whether the privilege of the process in a current processing phase is legitimate, so as to identify a condition where privilege information is illegitimately modified; and if a detection result indicates that the privilege is illegitimate, taking into consideration the fact that the condition where the privilege information is illegitimately modified may exist, and thus executing privilege escalation prevention processing so that a malicious user cannot obtain illegitimately escalated privilege without being detected.

(57) 摘要: 一种防提权检测的方法和设备, 该方法首先获取进程在内核态的权限变化信息, 通过对所述权限变化信息进行检测, 来判断所述进程在当前处理阶段的权限是否合法, 从而对非法修改权限信息的情况进行识别, 若检测结果为不合法, 则认为可能存在非法修改权限信息的情况, 进而执行防提权处理, 使得恶意用户无法在不被感知的情况下非法提升权限。

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, 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))。

防提权检测方法及设备

本申请要求 2017 年 08 月 18 日递交的申请号为 201710712801.4、发明名称为“防提权检测方法及设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本申请涉及信息技术领域，尤其涉及一种防提权检测的方案。

背景技术

在现有操作系统中，进程在进入内核态工作时，在任务的不同处理阶段会进行不同的操作，同时对应的权限信息也会发生变化。而进程的权限信息通常会通过特定的数据结构进行维护，例如 Linux 系统中通过数据结构 `struct cred` 来记录用户信息（uid）、用户组信息（gid）以及权限等信息，并由内核负责维护修改这些信息，并以及作为判断进程具体操作权限的依据。系统根据权限信息对进程相关处理的权限进行校验，进而提供针对对象操作安全性保障的权限检查机制。

在操作系统的权限检查机制中，权限判断仅依赖于数据结构中保存的权限信息，并不感知这些权限信息的变化情况与其合理性，一旦数据结构中的权限信息被恶意用户非法修改，极易造成非法提权，并且无法被系统感知。例如黑客通过一些非法手段，绕过系统正常修改流程，直接对 `struct cred` 中的权限信息进行非法修改，从而获得额外权限，完成提权，进而对系统造成更大破坏与威胁。而权限检查机制由于无法对非法修改权限信息的情况进行识别，往往一旦恶意用户成功修改了权限信息，就在操作系统中获得了更大的权限，可以轻松的对操作系统进行进一步的入侵而不被拦截和感知。

发明内容

本申请的一个目的是提供一种防提权检测方法及设备，用以解决无法对非法修改权限信息的情况进行识别的问题。

为实现上述目的，本申请提供了一种防提权检测方法，该方法包括：

获取进程在内核态的权限变化信息；

根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法；

若检测结果为不合法，执行防提权处理。

基于本申请的另一方面，还提供了一种防提权检测设备，该设备包括：

安全信息收集模块，用于获取进程在内核态的权限变化信息；

安全信息分析引擎，用于根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法；

安全处理模块，用于在检测结果为不合法时，执行防提权处理。

5 此外，本申请还提供了一种防提权检测设备，该设备包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：获取进程在内核态的权限变化信息；根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法；若检测结果为不合法，执行防提权处理。

10 本申请提供了一种防提权检测的方案，该方案首先获取进程在内核态的权限变化信息，通过对所述权限变化信息进行检测，来判断所述进程在当前处理阶段的权限是否合法，从而对非法修改权限信息的情况进行识别，若检测结果为不合法，则认为可能存在非法修改权限信息的情况，进而执行防提权处理，使得恶意用户无法在不被感知的情况下非法提升权限。

15

附图说明

通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

图 1 为本申请实施例提供的一种防提权检测方法的处理流程图；

20 图 2 为基于本申请实施例中的防提权检测方案提供的提权安全事件处理构架的原理示意图；

图 3 为本申请实施例提供的一种防提权检测设备的结构示意图；

附图中相同或相似的附图标记代表相同或相似的部件。

25 具体实施方式

下面结合附图对本申请作进一步详细描述。

在本申请一个典型的配置中，终端、服务网络的设备均包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

30 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介

质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体，可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘(CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。

在操作系统的权限检查机制中，权限判断仅依赖于数据结构中保存的权限信息，并不感知这些权限信息的变化情况与其合理性，一旦数据结构中的权限信息被恶意用户非法修改，例如黑客通过一些非法手段，绕过系统正常修改流程，直接对进程数据结构中的权限信息进行非法修改，这将使得黑客能够在不被感知的情况下非法提升权限。而本申请实施例提供了一种防提权检测方法，通过对进程在当前处理阶段的权限进行合法性判断，从而对非法修改权限信息的情况，避免恶意用户在不被感知的情况下非法提升权限，该方法的处理流程如图 1 所示，包括以下步骤：

步骤 S101，获取进程在内核态的权限变化信息。

在进程的运行过程中，会在特定情况下（例如进程执行系统调用时）从用户态进入到内核态，在进入内核态至退出内核态的整个过程中，进程在不同的处理阶段会需要对不同的操作对象执行不同的操作，由此需要不同的权限从操作系统获取相应的系统资源。

权限变化信息是用来表示进程在内核态的权限或者权限变化情况的信息，可以是进程在内核态中各个处理阶段的权限或者权限变化的情况，还可以是两者的结合。由于进程的数据结构中保存了与该进程的权限，通过收集每个处理阶段时数据结构中的权限信息，可以确定用户进程在内核态中各个处理阶段的权限或者权限变化的情况。例如，一进程在内核态至少包括三个处理阶段 p1-p3，分别进行三个不同的操作，由于需要获取不同的系统资源，每个处理阶段需要的权限也不相同，因此获取到的权限变化信息可以是进程在每个处理阶段的权限 L2、L1 和 L3，也可以使由 L2 到 L1，再到 L3 的变化过程，或者两者的结合。

步骤 S102，根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法。基于获取到的权限变化信息进行检测，可以判断进程在当前处理阶段的权限合法性，对

于前述的进程，在正常情况下三个处理阶段 p1-p3 的权限应当是 L2、L1 和 L3，若实际获取到的权限变化信息为该进程在三个处理阶段 p1-p3 的权限分别是 L2、L1 和 L2，由于该进程 p3 处理阶段的权限高于正常情况，因此会判定为不合法。

在本申请的一种实施例中，该方法还可以获取安全策略信息，其中，所述安全策略
5 包括判断规则信息，由此在检测进程权限合法性时可以根据所述权限变化信息和所述判断规则信息，检测所述进程在当前处理阶段的权限是否合法。在实际场景中，针对不同的应用场景，可以单独配置不同的安全策略，使得判断规则信息可以适用于不同的检测需求，当应用场景切换时，可以重新获取有针对性的安全策略，以适应场景的需求。例如，判断规则信息所确定的检测规则中，除了基于前述的权限或者权限变化，还可以结合
10 合进程在运行过程中可以检测到的其它任何信息。

在对进程权限合法性进行检测时，判断规则信息可以表征为一项或者多项非法条件，当获取到的权限变化信息符合该任一非法条件时，则确定进程在当前处理阶段的权限不合法。例如，判断规则信息对应的非法条件包括：进程在 p3 处理阶段的权限为 L2 或 L1，或者进程在 p2 至 p3 处理阶段的权限变化情况为 L2 至 L3、L3 至 L3、L1 至 L1 或 L1 至
15 L2 等。在处理时可以将权限变化信息与相同类型的非法条件进行逐一对比，来判断是否符合其中任意一项，进而判断进程在当前处理阶段的权限不合法。

本申请实施例还提供另一形式的检测方式，由于判断规则信息也可以表征为一项或者多项合法条件，仅当获取到的权限变化信息符合所有的合法条件时，判定进程在当前处理阶段的权限合法，否则确定进程在当前处理阶段的权限不合法。例如，判断规则信息
20 对应的合法条件包括：进程在 p3 处理阶段的权限为 L3 以及进程在 p2 至 p3 处理阶段的权限变化情况为 L1 至 L3。在处理时可以将权限变化信息与相同类型的非法条件进行逐一对比，来判断是否符合所有的合法条件，进而判断进程在当前处理阶段的权限的合法性。

步骤 S103，在检测结果为不合法时，执行防提权处理。在实际场景中，防提权处理
25 可以根据不合法的检测结果，可以根据该次非法提权的威胁程度，选择不同的处理方式。在本申请的一种实施方式中可以在生成提示信息、判定进程在内核态的本次处理失败、变更进程在当前处理阶段的权限、上报本次检测结果等方式中，根据实际应用场景的需求，选取其中一种或者几种作为特定情况下的防提权处理方式。例如，在多项非法条件中每项非法条件的所对应的威胁程度可能不同，根据该次检测所符合的特定非法条件可以
30 确定本次非法提权的威胁，进而选择不同的处理方式。

例如，对于威胁程度较低的情况，可以仅发出报警，生成提示信息告知用户。对于威胁程度较高的情况，可以在发出报警、生成提示信息的前提下，判定进程在内核态的本次处理失败，使得进程无法得到非法提升的权限，进而获取相应的系统资源，或者也可以变更进程在当前处理阶段的权限，使得进程的权限恢复为正常应有的等级。此外，
5 还可以向服务器上报本次检测结果，使得各个单机设备上的非法提权情况可以在服务器中汇集，综合各项信息，帮助用户及时有效地掌握整体的安全威胁情况。

在实际场景中，获取到的安全策略中还可以包含处理配置信息，该处理配置信息可以是预先配置完成的针对各种不同应用场景所使用的防提权处理方式，可以在初始化时根据不同的应用场景下发，使得在确定检测结果为不合法时，可以根据处理配置信息，
10 执行相应的防提权处理。

基于同一发明构思，本申请实施例中还提供了防提权检测设备，该设备对应的方法是前述实施例中的防提权检测方法，并且其解决问题的原理与方法相似。

本申请实施例提供了一种防提权检测设备，该设备包括安全信息收集模块、安全信息分析引擎以及安全处理模块，在进行防提权检测处理时，首先由安全信息收集模块获取进程在内核态的权限变化信息。
15

在进程的运行过程中，会在特定情况下（例如进程执行系统调用时）从用户态进入到内核态，在进入内核态至退出内核态的整个过程中，进程在不同的处理阶段会需要对不同的操作对象执行不同的操作，由此需要不同的权限从操作系统获取相应的系统资源。

权限变化信息是用来表示进程在内核态的权限或者权限变化情况的信息，可以是进程在内核态中各个处理阶段的权限或者权限变化的情况，还可以是两者的结合。由于进程的数据结构中保存了与该进程的权限，通过收集每个处理阶段时数据结构中的权限信息，可以确定用户进程在内核态中各个处理阶段的权限或者权限变化的情况。例如，一进程在内核态至少包括三个处理阶段 p1-p3，分别进行三个不同的操作，由于需要获取不同的系统资源，每个处理阶段需要的权限也不相同，因此获取到的权限变化信息可以是
20 进程在每个处理阶段的权限 L2、L1 和 L3，也可以使由 L2 到 L1，再到 L3 的变化过程，或者两者的结合。

而后，安全信息分析引擎根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法。基于获取到的权限变化信息进行检测，可以判断进程在当前处理阶段的权限合法性，对于前述的进程，在正常情况下三个处理阶段 p1-p3 的权限应当是 L2、L1
30 和 L3，若实际获取到的权限变化信息为该进程在三个处理阶段 p1-p3 的权限分别是 L2、

L1 和 L2，由于该进程 p3 处理阶段的权限高于正常情况，因此会判定为不合法。

在本申请的一种实施例中，该安全信息分析引擎还可以获取安全策略信息，其中，所述安全策略包括判断规则信息，由此安全信息分析引擎在检测进程权限合法性时可以根据所述权限变化信息和所述判断规则信息，检测所述进程在当前处理阶段的权限是否合法。在实际场景中，针对不同的应用场景，可以单独配置不同的安全策略，使得判断规则信息可以适用于不同的检测需求，当应用场景切换时，可以重新获取有针对性的安全策略，以适应场景的需求。例如，判断规则信息所确定的检测规则中，除了基于前述的权限或者权限变化，还可以结合进程在运行过程中可以检测到的其它任何信息。

安全信息分析引擎在对进程权限合法性进行检测时，判断规则信息可以表征为一项或者多项非法条件，当获取到的权限变化信息符合该任一非法条件时，则安全信息分析引擎确定进程在当前处理阶段的权限不合法。例如，判断规则信息对应的非法条件包括：进程在 p3 处理阶段的权限为 L2 或 L1，或者进程在 p2 至 p3 处理阶段的权限变化情况为 L2 至 L3、L3 至 L3、L1 至 L1 或 L1 至 L2 等。在处理时可以将权限变化信息与相同类型的非法条件进行逐一对比，来判断是否符合其中任意一项，进而判断进程在当前处理阶段的权限不合法。

本申请实施例还提供另一形式的检测方式，由于判断规则信息也可以表征为一项或者多项合法条件，仅当获取到的权限变化信息符合所有的合法条件时，安全信息分析引擎判定进程在当前处理阶段的权限合法，否则确定进程在当前处理阶段的权限不合法。例如，判断规则信息对应的合法条件包括：进程在 p3 处理阶段的权限为 L3 以及进程在 p2 至 p3 处理阶段的权限变化情况为 L1 至 L3。在处理时可以将权限变化信息与相同类型的非法条件进行逐一对比，来判断是否符合所有的合法条件，进而判断进程在当前处理阶段的权限的合法性。

在检测结果为不合法时，安全处理模块执行防提权处理。在实际场景中，防提权处理可以根据不合法的检测结果，可以根据该次非法提权的威胁程度，选择不同的处理方式。在本申请的一种实施方式中安全处理模块可以在生成提示信息、判定进程在内核态的本次处理失败、变更进程在当前处理阶段的权限、上报本次检测结果等方式中，根据实际应用场景的需求，选取其中一种或者几种作为特定情况下的防提权处理方式。例如，在多项非法条件中每项非法条件的所对应的威胁程度可能不同，根据该次检测所符合的特定非法条件可以确定本次非法提权的威胁，进而选择不同的处理方式。

例如，对于威胁程度较低的情况，可以仅发出报警，生成提示信息告知用户。对于

威胁程度较高的情况，可以在发出报警、生成提示信息的前提下，判定进程在内核态的本次处理失败，使得进程无法得到非法提升的权限，进而获取相应的系统资源，或者也可以变更进程在当前处理阶段的权限，使得进程的权限恢复为正常应有的等级。此外，还可以向服务器上报本次检测结果，使得各个单机设备上的非法提权情况可以在服务器中汇集，综合各项信息，帮助用户及时有效地掌握整体的安全威胁情况。

在实际场景中，获取到的安全策略中还可以包含处理配置信息，该处理配置信息可以是预先配置完成的针对各种不同应用场景所使用的防提权处理方式，可以在初始化时根据不同的应用场景下发，使得在确定检测结果为不合法时，安全处理模块可以根据处理配置信息，执行相应的防提权处理。

基于本申请实施例的方案，还提供一套完整的提权安全事件处理构架，用于在大规模计算的场景下进行提权安全事件的防护和监控。如图 2 所示，整个处理构架中包括内核态的安全信息收集模块（Security information collection）210 与安全信息分析引擎（Security information analysis engine）220，用户态的安全事件管理客户端（Security Event Client）230，上述三个组件在每个单机设备上运行，用于对单机设备上的提权安全事件的防护和监控，此外还包括远端的安全信息收集服务器（Security Event Server）240，运行于网络侧，用于对整个集群的所有安全提权事件进行收集。工作流程如下：

步骤 S1，安全事件管理客户端 230 下发安全信息分析的规则，根据不同的工作场景灵活配置，配置有针对性的安全策略。

步骤 S2，用户（Actor）创建进程后，在用户态执行处理，然后通过系统调用进入内核态，内核的任务处理模块（task handler）200 开始处理。

步骤 S3，在内核态处理开始后，安全信息收集模块 210 收集保存此时用户的权限信息，作为后面判断非法提权的依据。

步骤 S4，在进程在内核执行的过程中至执行结束返回之前，安全信息收集模块 220 持续收集各个处理阶段的权限信息的变化情况。

步骤 S5，将收集到的不同处理阶段的权限信息或者权限信息的变化情况，交由安全信息分析引擎 220，按照已配置的安全策略，判断这一处理阶段的权限变化情况是否合法，有效识别出非法提权操作。

步骤 S6，根据非法提权的识别情况，通知安全信息收集模块 210 最终的识别结果。

步骤 S7，一旦判定出现非法提权的情况，系统的内核判定进程的操作在内核态执行失败，不允许该进程获得非法的权限与系统资源。

步骤 S8, 用户无法完成非法提权, 也就阻止了恶意用户对系统资源的进一步威胁。

步骤 S9, 同时安全信息分析引擎 220 会向用户态的安全事件管理客户端 230 通报非法提权威胁。

步骤 S10, 安全事件管理客户端 230 会向安全信息收集服务器上报告非法提权威胁,

5 最终各个单机设备上的非法提权情况, 将在远端的安全信息收集服务器 230 中汇集, 综合各项信息, 帮助管理人员及时有效地掌握集群整体的安全威胁情况。

综上所述, 本申请提供了一种防提权检测的方案, 该方案首先获取进程在内核态的权限变化信息, 通过对所述权限变化信息进行检测, 来判断所述进程在当前处理阶段的权限是否合法, 从而对非法修改权限信息的情况进行识别, 若检测结果为不合法, 则认为可能存在非法修改权限信息的情况, 进而执行防提权处理, 使得恶意用户无法在不被感知的情况下非法提升权限。

另外, 本申请的一部分可被应用为计算机程序产品, 例如计算机程序指令, 当其被计算机执行时, 通过该计算机的操作, 可以调用或提供根据本申请的方法和/或技术方案。而调用本申请的方法的程序指令, 可能被存储在固定的或可移动的记录介质中, 和/或通过广播或其他信号承载媒体中的数据流而被传输, 和/或被存储在根据程序指令运行的计算机设备的工作存储器中。在此, 根据本申请的一个实施例包括一个如图 3 所示的防提权检测设备, 该设备包括用于存储计算机程序指令的存储器 320 和用于执行程序指令的处理器 310, 其中, 当该计算机程序指令被该处理器执行时, 触发该设备运行基于前述根据本申请的多个实施例的方法和/或技术方案。

20 需要注意的是, 本申请可在软件和/或软件与硬件的组合体中被实施, 例如, 可采用专用集成电路 (ASIC)、通用目的计算机或任何其他类似硬件设备来实现。在一个实施例中, 本申请的软件程序可以通过处理器执行以实现上文步骤或功能。同样地, 本申请的软件程序 (包括相关的数据结构) 可以被存储到计算机可读记录介质中, 例如, RAM 存储器, 磁或光驱动器或软磁盘及类似设备。另外, 本申请的一些步骤或功能可采用硬件来实现, 例如, 作为与处理器配合从而执行各个步骤或功能的电路。

对于本领域技术人员而言, 显然本申请不限于上述示范性实施例的细节, 而且在不背离本申请的精神或基本特征的情况下, 能够以其他的具体形式实现本申请。因此, 无论从哪一点来看, 均应将实施例看作是示范性的, 而且是非限制性的, 本申请的范围由所附权利要求而不是上述说明限定, 因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本申请内。不应将权利要求中的任何附图标记视为限制所涉及的权

30

利要求。此外，显然“包括”一词不排除其他单元或步骤，单数不排除复数。装置权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

权 利 要 求 书

1. 一种防提权检测方法，其中，该方法包括：

获取进程在内核态的权限变化信息；

根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法；

若检测结果为不合法，执行防提权处理。

2. 根据权利要求 1 所述的方法，其中，所述权限变化信息包括进程在内核态中各个处理阶段的权限和/或权限变化。

3. 根据权利要求 1 所述的方法，其中，该方法还包括：

获取安全策略信息，其中，所述安全策略包括判断规则信息；

根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法，包括：

根据所述权限变化信息和所述判断规则信息，检测所述进程在当前处理阶段的权限是否合法。

4. 根据权利要求 3 所述的方法，其中，根据所述权限变化信息和所述判断规则信息，检测所述进程在当前处理阶段的权限是否合法，包括：

将所述权限变化信息和所述判断规则信息比较，若所述权限变化信息符合所述判断规则信息对应的非法条件或所述权限变化信息不符合所述判断规则信息对应的合法条件，则确定所述进程在当前处理阶段的权限不合法。

5. 根据权利要求 3 所述的方法，其中，所述安全策略还包括处理配置信息；

执行防提权处理，包括：

根据所述处理配置信息，执行防提权处理。

6. 根据权利要求 1 至 5 中任意一项所述的方法，其中，执行所述防提权处理，包括以下任意一项或多项：

生成提示信息；

判定进程在内核态的本次处理失败；

变更进程在当前处理阶段的权限；

上报本次检测结果。

7. 一种防提权检测设备，其中，该设备包括：

安全信息收集模块，用于获取进程在内核态的权限变化信息；

安全信息分析引擎，用于根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法；

安全处理模块，用于在检测结果为不合法时，执行防提权处理。

8. 根据权利要求7所述的设备，其中，所述权限变化信息包括进程在内核态中各个处理阶段的权限和/或权限变化。

9. 根据权利要求7所述的设备，其中，所述安全信息分析引擎，用于获取安全策略信息，并根据所述权限变化信息和判断规则信息，检测所述进程在当前处理阶段的权限是否合法，其中，所述安全策略包括判断规则信息。

10. 根据权利要求9所述的设备，其中，所述安全信息分析引擎，用于将所述权限变化信息和所述判断规则信息比较，若所述权限变化信息符合所述判断规则信息对应的非法条件或所述权限变化信息不符合所述判断规则信息对应的合法条件，则确定所述进程在当前处理阶段的权限不合法。

11. 根据权利要求9所述的设备，其中，所述安全策略还包括处理配置信息；
所述安全处理模块，用于根据所述处理配置信息，执行防提权处理。

12. 根据权利要求7至11中任意一项所述的设备，其中，所述安全处理模块执行的所述防提权处理，包括以下任意一项或多项：

生成提示信息；

判定进程在内核态的本次处理失败；

变更进程在当前处理阶段的权限；

上报本次检测结果。

13. 一种防提权检测设备，其中，该设备包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：获取进程在内核态的权限变化信息；根据所述权限变化信息检测所述进程在当前处理阶段的权限是否合法；若检测结果为不合法，执行防提权处理。

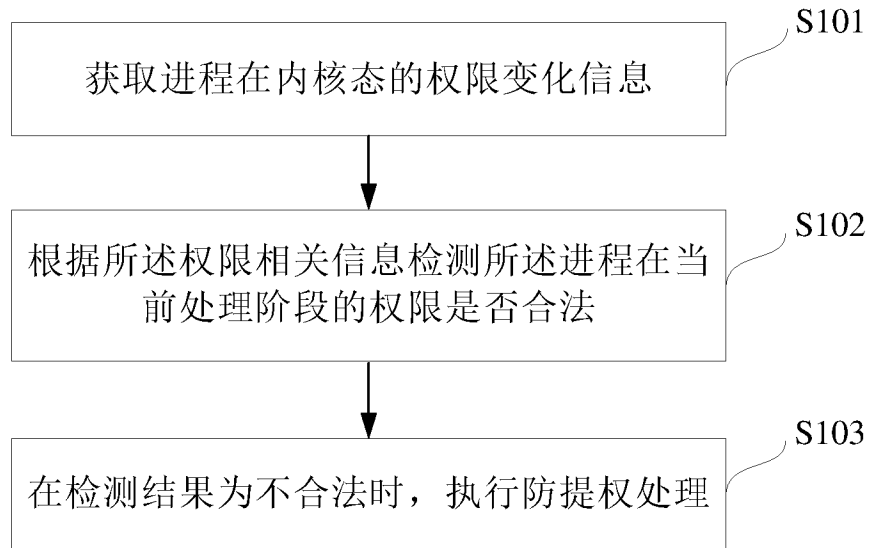


图 1

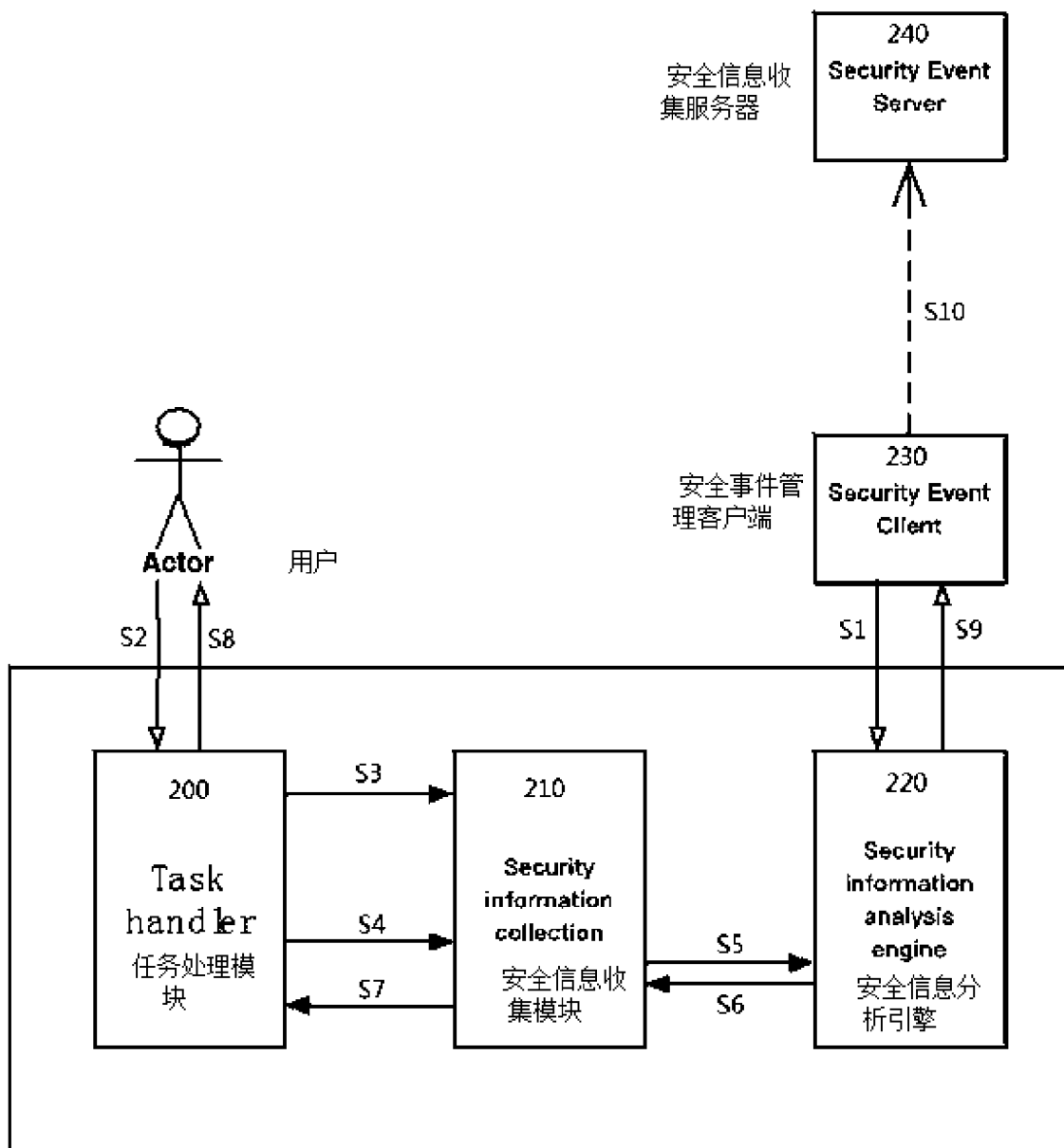


图 2

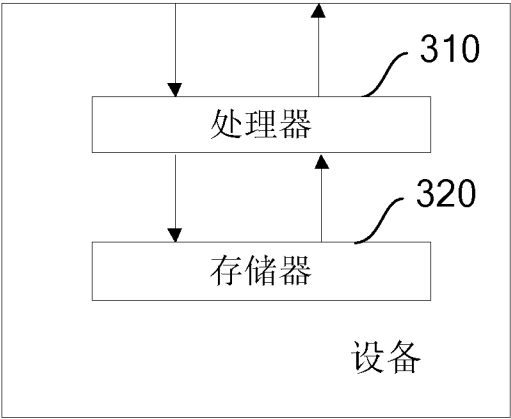


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/099397

A. CLASSIFICATION OF SUBJECT MATTER		
G06F 21/56(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)		
CNPAT; EPODOC; WPI; IEEE: 权限, 提权, 内核, 进程, 检测, 监测, root, rootkit, kernel, process, detect		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106560832 A (HARBIN ANTIY TECHNOLOGY CO., LTD.) 12 April 2017 (2017-04-12) description, paragraphs [0003]-[0012]	1-13
A	US 2007079178 A1 (COMPUTER ASSOCIATES THINK, INC.) 05 April 2007 (2007-04-05) entire document	1-13
A	US 2007078915 A1 (COMPUTER ASSOCIATES THINK, INC.) 05 April 2007 (2007-04-05) entire document	1-13
A	CN 102930205 A (BEIJING QIHOO TECHNOLOGY CO., LTD. ET AL.) 13 February 2013 (2013-02-13) entire document	1-13
A	CN 104318156 A (SHANGHAI FEIXUN COMMUNICATION CO., LTD.) 28 January 2015 (2015-01-28) entire document	1-13
A	CN 103699839 A (TCL CORPORATION) 02 April 2014 (2014-04-02) entire document	1-13
☐ 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
25 October 2018		14 November 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/CN2018/099397

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106560832	A	12 April 2017	None			
US	2007079178	A1	05 April 2007	WO	2007044498	A1	19 April 2007
				US	7841006	B2	23 November 2010
US	2007078915	A1	05 April 2007	WO	2007044499	A1	19 April 2007
				US	8572371	B2	29 October 2013
CN	102930205	A	13 February 2013	None			
CN	104318156	A	28 January 2015	CN	104318156	B	25 July 2017
CN	103699839	A	02 April 2014	None			

国际检索报告

国际申请号

PCT/CN2018/099397

A. 主题的分类 G06F 21/56 (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)) CNPAT; EPDOC; WPI; IEEE: 权限, 提权, 内核, 进程, 检测, 监测, root, rootkit, kernel, process, detect		
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
X	CN 106560832 A (哈尔滨安天科技股份有限公司) 2017年 4月 12日 (2017 - 04 - 12) 说明书第 [0003] - [0012] 段	1-13
A	US 2007079178 A1 (COMPUTER ASSOCIATES THINK, INC.) 2007年 4月 5日 (2007 - 04 - 05) 全文	1-13
A	US 2007078915 A1 (COMPUTER ASSOCIATES THINK, INC.) 2007年 4月 5日 (2007 - 04 - 05) 全文	1-13
A	CN 102930205 A (北京奇虎科技有限公司 等) 2013年 2月 13日 (2013 - 02 - 13) 全文	1-13
A	CN 104318156 A (上海斐讯数据通信技术有限公司) 2015年 1月 28日 (2015 - 01 - 28) 全文	1-13
A	CN 103699839 A (TCL集团股份有限公司) 2014年 4月 2日 (2014 - 04 - 02) 全文	1-13
☐ 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 10月 25日		2018年 11月 14日
ISA/CN的名称和邮寄地址		授权官员
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 传真号 (86-10) 62019451		欧晓丹 电话号码 86-(10)-53961416

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/099397

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	106560832	A	2017年 4月 12日	无			
US	2007079178	A1	2007年 4月 5日	WO	2007044498	A1	2007年 4月 19日
				US	7841006	B2	2010年 11月 23日
US	2007078915	A1	2007年 4月 5日	WO	2007044499	A1	2007年 4月 19日
				US	8572371	B2	2013年 10月 29日
CN	102930205	A	2013年 2月 13日	无			
CN	104318156	A	2015年 1月 28日	CN	104318156	B	2017年 7月 25日
CN	103699839	A	2014年 4月 2日	无			