(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
2017 年 10 月 5 日 (05.10.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/166446 A1

(51) 国际专利分类号:
G06F 21/57 (2013.01)

(21) 国际申请号: PCT/CN2016/086410

(22) 国际申请日: 2016 年 6 月 20 日 (20.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610193039.9 2016 年 3 月 30 日 (30.03.2016) CN

(71) 申请人: **百度在线网络技术（北京）有限公司 (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.)** [CN/CN]; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。

(72) 发明人: **夏良钊 (XIA, Liangzhao)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **郑龙日 (ZHENG, Longri)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **卢永强 (LU, Yongqiang)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **包沉浮 (BAO, Chenfu)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **张煜龙 (ZHANG, Yulong)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **韦韬 (WEI, Tao)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。

(74) 代理人: **北京英赛嘉华知识产权代理有限责任公司 (INSIGHT INTELLECTUAL PROPERTY LIMITED)**; 中国北京市海淀区知春路甲 48 号盈都大厦 A 座 19A, Beijing 100098 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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。

[见续页]

(54) Title: VULNERABILITY-FIXING METHOD AND DEVICE

(54) 发明名称 : 漏洞修复方法和装置

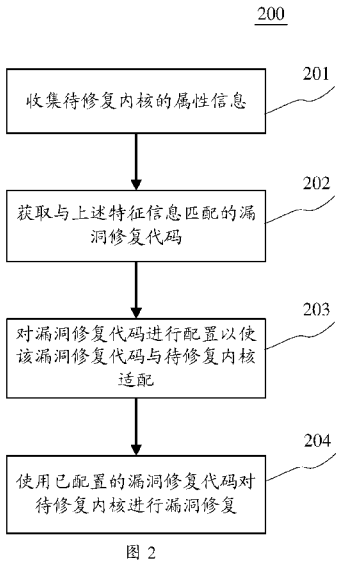

图 2

201 Collecting attribute information about a kernel to be fixed
202 Acquiring a vulnerability-fixing code matching feature information
203 Configuring the vulnerability-fixing code so that the vulnerability-fixing code is adapted to the kernel to be fixed
204 Using the configured vulnerability-fixing code to perform vulnerability fixing on the kernel to be fixed

(57) **Abstract**: Disclosed are a vulnerability-fixing method and device. The method comprises: collecting attribute information about a kernel to be fixed (201), the attribute information comprising feature information used for characterizing a code-loading method supported by the kernel to be fixed; acquiring a vulnerability-fixing code matching the feature information (202); based on the attribute information, configuring the vulnerability-fixing code so that the vulnerability-fixing code is adapted to the kernel to be fixed (203); and using the configured vulnerability-fixing code to perform vulnerability fixing on the kernel to be fixed (204). This method is compatible with a plurality of methods for loading a kernel fixing code.

(57) **摘要**: 漏洞修复方法和装置，所述方法包括：收集待修复内核的属性信息（201），所述属性信息包括用于表征所述待修复内核所支持代码加载方式的特征信息；获取与所述特征信息匹配的漏洞修复代码（202）；基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配（203）；使用已配置的漏洞修复代码对所述待修复内核进行漏洞修复（204）。该方法兼容于多个内核修复代码加载方法。

WO 2017/166446 A1

(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))。

说 明 书

漏洞修复方法和装置

相关申请的交叉引用

本申请要求于 2016 年 3 月 30 日提交的中国专利申请号为“201610193039.9”的优先权，其全部内容作为整体并入本申请中。

技术领域

本申请涉及计算机技术领域，具体涉及信息安全技术领域，尤其涉及漏洞修复方法和装置。

背景技术

操作系统内核经常被发现各种安全漏洞，由于安全漏洞本身原理的复杂性，会消耗大量人力资源来应对。有些厂商会延迟更新甚至放弃了旧版本的维护，给用户带来了极大的安全风险。以 Linux 内核为例，各种安卓设备中使用的内核版本呈现碎片化特征，不同内核之间差异较大，所以缺乏良好的代码通用性，Linux 内核本身和厂商还设置一些安全机制对代码加载进行限制。

由于上述原因，现有技术中的修复方法依赖于运行系统的源代码或者需要原始内核提供相应的机能进行配合才能使用，生成的补丁也只能用于修补特定的内核编译版本，极大的限制了其应用场景和兼容性。

发明内容

本申请的目的在于提出一种改进的漏洞修复方法和装置，来解决以上背景技术部分提到的技术问题。

第一方面，本申请提供了一种漏洞修复方法，所述方法包括：收集待修复内核的属性信息，所述属性信息包括用于表征所述待修复内核所支持代码加载方式的特征信息；获取与所述特征信息匹配的漏洞

修复代码；基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配；使用已配置的漏洞修复代码对所述待修复内核进行漏洞修复。

在一些实施例中，所述获取与所述特征信息匹配的漏洞修复代码，包括：获取服务器中存储的、与所述特征信息匹配的漏洞修复代码，其中所述服务器存储的漏洞修复代码是实时更新的。

在一些实施例中，所述特征信息包括：用于描述所述待修复内核中是否存在预设的系统调用的信息以及用于描述所述待修复内核中是否存在预设的物理内存设备的信息；以及所述获取与所述特征信息匹配的漏洞修复代码，包括：当所述特征信息指示预设的系统调用存在时所匹配的漏洞修复代码包括内核模块类型的漏洞修复代码，当所述特征信息指示预设的物理内存设备存在时所匹配的漏洞修复代码包括指令序列类型的漏洞修复代码。

在一些实施例中，所述属性信息还包括内核符号校验参数；以及当所获取的漏洞修复代码为内核模块时，所述基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配，包括：使用所述内核符号校验参数配置所述内核模块对应的可执行文件中的内核符号校验参数字段。

在一些实施例中，所述属性信息还包括待修复内核中内核符号的地址信息；以及所述基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配包括：使用所述地址信息配置所述指令序列中的内核符号的地址。

在一些实施例中，在所述获取与所述特征信息匹配的漏洞修复代码之后，所述方法还包括：对所获取的漏洞修复代码进行合法性校验，以确认所述漏洞修复代码未被篡改。

在一些实施例中，所述方法还包括：生成用于表示漏洞修复成功或失败的信息。

在一些实施例中，所述收集待修复内核的属性信息，包括：响应于待修复内核的启动操作，收集所述待修复内核的属性信息。

在一些实施例中，所述方法还包括：若漏洞修复失败，则将待修

复内核恢复至修复之间的状态。

第二方面，本申请提供了一种漏洞修复装置，所述装置包括：收集单元，用于收集待修复内核的属性信息，所述属性信息包括用于表征所述待修复内核所支持代码加载方式的特征信息；获取单元，用于获取与所述特征信息匹配的漏洞修复代码；配置单元，用于基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配；修复单元，用于使用已配置的漏洞修复代码对所述待修复内核进行漏洞修复。

在一些实施例中，所述获取单元进一步用于获取服务器中存储的、与所述特征信息匹配的漏洞修复代码，其中所述服务器存储的漏洞修复代码是实时更新的。

在一些实施例中，所述特征信息包括：用于描述所述待修复内核中是否存在预设的系统调用的信息以及用于描述所述待修复内核中是否存在预设的物理内存设备的信息；以及所述获取单元进一步用于：当所述特征信息指示预设的系统调用存在时所匹配的漏洞修复代码包括内核模块类型的漏洞修复代码，当所述特征信息指示预设的物理内存设备存在时所匹配的漏洞修复代码包括指令序列类型的漏洞修复代码。

在一些实施例中，所述属性信息还包括内核符号校验参数；以及所述配置单元进一步用于：当所获取的漏洞修复代码为内核模块时，使用所述内核符号校验参数配置所述内核模块对应的可执行文件中的内核符号校验参数字段。

在一些实施例中，所述属性信息还包括待修复内核中内核符号的地址信息；以及所述配置单元进一步用于：使用所述地址信息配置所述漏洞修复代码中的内核符号的地址。

在一些实施例中，所述装置还包括：校验单元，用于对所获取的漏洞修复代码进行合法性校验，以确认所述漏洞修复代码未被篡改。

在一些实施例中，所述装置还包括生成单元：生成用于表示漏洞修复成功或失败的信息。

在一些实施例中，所述收集单元进一步用于：响应于待修复内核

的启动操作，收集所述待修复内核的属性信息。

在一些实施例中，所述装置还包括：恢复单元，用于若漏洞修复失败，则将待修复内核恢复至修复之间的状态。

本申请提供的漏洞修复方法和装置，获取到与内核所支持的加载方式匹配的漏洞修复代码并对该漏洞修复代码进行相应的配置，使得配置后的漏洞修复代码可以在内核中加载以实现对内核的漏洞修复。这种漏洞修复方法可以兼容于多个内核修复代码加载方法，不依赖于内核源码及其内核功能，生成的补丁可自适配不同的内核编译版本，克服了 Linux 系统碎片化的影响。

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 是本申请可以应用于其中的示例性系统架构图；

图 2 是根据本申请的漏洞修复方法的一个实施例的流程图；

图 3 是根据本申请的漏洞修复方法的又一个实施例的流程图；

图 4 是根据本申请的漏洞修复装置的一个实施例的结构示意图；

图 5 是适于用来实现本申请实施例的终端设备或服务器的计算机系统的结构示意图。

具体实施方式

下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。

需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

图 1 示出了可以应用本申请的漏洞修复方法或漏洞修复装置的实施例的示例性系统架构 100。

如图 1 所示，系统架构 100 可以包括终端设备 101、102、103，网络 104 和服务器 105。网络 104 用以在终端设备 101、102、103 和服务器 105 之间提供通信链路的介质。网络 104 可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

用户可以使用终端设备 101、102、103 通过网络 104 与服务器 105 交互，以接收或发送消息等。终端设备 101、102、103 上可以安装有安全软件等通讯客户端应用。

终端设备 101、102、103 可以是各种电子设备，包括但不限于智能手机、平板电脑、电子书阅读器、MP3 播放器(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面 3)、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面 4)播放器、膝上型便携计算机和台式计算机等等。

服务器 105 可以是提供各种服务的服务器，例如对终端设备 101、102、103 提供数据支持的云端服务器。云端服务器可以对接收到的漏洞修复代码请求等数据进行分析等处理，并将处理结果（例如预设的漏洞修复代码）反馈给终端设备 101、102、103。

需要说明的是，本申请实施例所提供的漏洞修复方法一般由终端设备 101、102、103 执行，一些步骤也可以由服务器 105 执行；相应地，漏洞修复装置一般设置于终端设备 101、102、103 中，漏洞修复装置的一些单元也可以设置在服务器 105 中。

应该理解，图 1 中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

继续参考图 2，示出了根据本申请的漏洞修复方法的一个实施例的流程 200。所述的漏洞修复方法，包括以下步骤：

步骤 201，收集待修复内核的属性信息。

在本实施例中，漏洞修复方法运行于其上的电子设备（例如图 1 所示的终端设备）可以首先对该电子设备中待修复内核进行分析，从而收集该内核的属性信息。待修复内核可以是各种操作系统的内核，相应的操作系统可以是 Windows、Linux 等。其中，该属性信息可以是各种用于描述内核相关属性的信息，例如内核版本信息、内核配置

信息等。其中，该属性信息中包括待修复内核所支持代码加载方式的特征信息。不同的内核编译版本，其支持的代码加载方式可能不同，待修复内核所支持的代码加载方式即可以通过上述特征信息进行表征。其中代码记载方式可以是内核记载代码的各种方式，例如加载内核模块方式、操作内存方式以及其他系统可能支持的代码加载方式。

在本实施例的一些可选实现方式中，上述属性信息包括以下至少一项：系统版本信息；用于指示系统调用是否存在的信息；用于指示物理内存设备是否存在的信息；内核配置信息；内核符号地址；校验和信息。

步骤 202，获取与上述特征信息匹配的漏洞修复代码。

在本实施例中，电子设备可以在预先设置的一个或多个漏洞修复代码中，获取与上述特征信息匹配的漏洞修复代码。通常，预先设置的一个或多个漏洞修复代码可以是与用于对待修复内核进行修复的各种漏洞修复代码。这些预先设置的一个或多个漏洞修复代码可以是存储在电子设备本地，也可以存储在服务器上，且可以是各种形式的。其中，所获取的漏洞修复代码可以是内核模块形式，也可以是指令序列形式，还可以是预先约定的、且可被电子设备解释与执行的指令组合。内核模块形式是指可在内核运行时加载到内核的一组目标代码，在重构和使用可装载模块时并不需要重新编译内核。漏洞修复代码与特征信息之间的匹配关系可以是预先设置的。电子设备在获取漏洞修复代码时，即可以根据上述匹配关系获取到与上述特征信息匹配的漏洞修复代码。例如，当特征信息指示内核支持以预先约定的指令组合加载代码时，所匹配的漏洞修复代码可以是相应的指令组合形式。

在本实施例的一些可选实现方式中，步骤 202 可以具体包括：获取服务器中存储的、与上述特征信息匹配的漏洞修复代码，其中服务器存储的漏洞修复代码是实时更新的。在本实施例中，电子设备可以通过有线连接方式或者无线连接方式从服务器中获取与上述特征信息匹配的漏洞修复代码。该服务器中存储的漏洞修复代码可以是实时更新的，因此。在具体获取时，电子设备可以向服务器发送对漏洞修复代码的请求，服务器可以根据该请求向分发相应的漏洞代码。可选的，

电子设备还可以将相应的属性信息通过请求发送至服务器，使服务器返回的漏洞修复代码与上述特征信息匹配。上述无线连接方式可以包括但不限于 3G/4G 连接、WiFi 连接、蓝牙连接、WiMAX 连接、Zigbee 连接、UWB（ultra wideband）连接、以及其他现在已知或将来开发的无线连接方式。通过这种方式，电子设备可以获取到实时更新的漏洞修复代码，使得对内核漏洞的修复具有更强的实时性，进一步保证内核的安全性。

步骤 203，对漏洞修复代码进行配置以使该漏洞修复代码与待修复内核适配。

在本实施例中，基于步骤 202 获取到与上述特征信息匹配的漏洞修复代码后，上述电子设备可以对该漏洞修复代码进行相应地配置，以使该漏洞修复代码可以与上述待修复内核适配，例如使版本号匹配。上述属性信息中可以包括待修复内核所加载的代码应当符合的配置信息。因此，基于该属性信息，电子设备可以对漏洞修复代码进行相应的配置。上述配置可以是在漏洞修复代码中加入一些设定的符号地址、对漏洞修复代码的某些信息进行修改、确定漏洞修复代码将加载在内存中的地址等。

步骤 204，使用已配置的漏洞修复代码对待修复内核进行漏洞修复。

在本实施例中，基于步骤 203 中配置好的漏洞修复代码，上述电子设备可以使用已配置的漏洞修复代码对待修复内核进行漏洞修复。具体的修复可以与漏洞修复代码类型对应的方式执行。例如，当漏洞修复代码是内核模块形式时，可以使用设定的系统调用在待修复内核中加载相应的内核模块；当漏洞修复代码是指令序列形式，可以通过操作内存的方式进行加载；当漏洞修复代码是预先约定的指令组合时，电子设备可以直接解释并执行。

在本实施例的一些可选实现方式中，步骤 201 中的特征信息可以包括：用于描述待修复内核中是否存在预设的系统调用的信息以及用于描述待修复内核中是否存在预设的物理内存设备的信息；以及步骤 202 包括：当上述特征信息指示预设的系统调用存在时所匹配的漏洞

修复代码包括内核模块类型的漏洞修复代码，当特征信息指示预设的物理内存设备存在时所匹配的漏洞修复代码包括指令序列类型的漏洞修复代码。

以 Linux 操作系统为例进行说明。例如，有的内核编译版本中存在预设的系统调用，该预设的系统调用可用于加载内核模块。当特征信息指示预设的系统调用存在时，意味着该内核模块可以支持内核模块的加载，则在获取漏洞修复代码时，可以获取内核模块类型的漏洞修复代码。上述预设的系统调用可以是模块加载与卸载函数，例如 init_module、finite_module、delete_module，也可以是其他各种用于加载或卸载内核模块的系统调用。

又例如，有的内核编译版本中存在预设的物理内存设备，该预设的物理内存设备可用于对内存进行操作来加载和移除代码 。当特征信息指示预设的物理内存设备存在时，意味着内核支持使用该物理内存设备进行操作内存以加载代码，则所获取的漏洞修复代码可以是可在内存中直接加载执行的指令序列。上述预设的物理内存设备可以是 /dev/kmem。

可选的，当特征信息指示预设的系统调用与预设的物理内存设备均存在时，内核模块类型与指令序列类型的漏洞修复代码均匹配，电子设备可以选择任意一项。

在本实施例的一些可选实现方式中，上述属性信息还包括内核符号校验参数；以及当所获取的漏洞修复代码为内核模块时，上述步骤 203 还包括：使用内核符号校验参数配置内核模块对应的可执行文件中的内核符号校验参数字段。通常，内核在加载内核模块时，会利用各种内核符号校验参数对内核模块进行校验。因此，电子设备在获取到内核模块形式的漏洞修复代码后，可以将该内核模块对应的可执行文件中的内核符号校验参数字段的数值配置为内核符号校验参数，以使该内核模块在后续加载时通过内核的校验，从而得以顺利加载。上述校验参数可以是 vermagic 字符串、module 结构体、符号 CRC 或者其他各种用于验证的校验参数。

在本实施例的一些可选实现方式中，上述属性信息还包括待修复

内核中内核符号的地址信息，上述步骤 203 还包括：使用上述地址信息配置漏洞修复代码中的内核符号的地址。在该实现方式中，电子设备可以使用上述地址信息对漏洞修复代码中的内核符号的地址进行配置，使得配置后的漏洞修复代码可以与待修复内核适配。

本申请的上述实施例提供的方法获取到与内核所支持的加载方式匹配的漏洞修复代码并对该漏洞修复代码进行相应的配置，使得配置后的漏洞修复代码可以在内核中加载以实现对内核的漏洞修复。这种漏洞修复方法可以兼容于多个内核修复代码加载方法，不依赖于内核源码及其内核功能，生成的补丁可自适配不同的内核编译版本，克服了 Linux 系统碎片化的影响。

进一步参考图 3，其示出了漏洞修复方法的又一个实施例的流程 300。该漏洞修复方法的流程 300，包括以下步骤：

步骤 301，收集待修复内核的属性信息。

在本实施例中，步骤 301 中的具体处理可以参考图 2 对应实施例中的步骤 201，这里不再赘述。

在本实施例的一些可选实现方式中，电子设备可以在待修复内核启动时响应于待修复内核的启动操作，收集待修复内核的属性信息。该实现方式中，可以通过修改系统配置，使该漏洞修复方法在系统重新启动时及早运行，无需用户再次介入，即可及时保护系统。

步骤 302，获取与特征信息匹配的漏洞修复代码。

在本实施例中，步骤 302 中的具体处理可以参考图 2 对应实施例中的步骤 202，这里不再赘述。

步骤 303，对所获取的漏洞修复代码进行合法性校验，以确认漏洞修复代码未被篡改。

在本实施例中，电子设备可以通过各种信息对所获取的漏洞修复代码进行合法性校验，以确认漏洞修复代码未被篡改。通常，电子设备可以预先设定合法的验证参数，该验证参数可以对确定合法的漏洞修复代码进行设定的算法所形成的，例如通过 CRC，RSA 等算法所形成的 CRC 值、RSA 值。在进行合法性验证时，电子设备可以使用相

同的校验算法对获取到的漏洞修复代码进行计算，并对所生成的校验值与上述验证参数是否一致。具体的校验算法时，不限于 CRC 算法、RSA 算法。

步骤 304，对漏洞修复代码进行配置以使该漏洞修复代码与待修复内核适配。

在本实施例中，步骤 304 中的具体处理可以参考图 2 对应实施例中的步骤 203，这里不再赘述。

步骤 305，使用已配置的漏洞修复代码对待修复内核进行漏洞修复。

在本实施例中，步骤 305 中的具体处理可以参考图 2 对应实施例中的步骤 204，这里不再赘述。

在本实施例的一些可选实现方式中，电子设备还生成用于表示漏洞修复成功或失败的信息。该信息可以供用户对漏洞修复是否成功进行查询。

在本实施例的一些可选实现方式中，若漏洞修复失败，电子设备可以将待修复内核恢复至修复之间的状态。通过这种方式，电子设备可以在修复失败后自动恢复至修复前的初始状态，以免对系统产生无不良影响。

从图 3 中可以看出，与图 2 对应的实施例相比，本实施例中的漏洞修复方法的流程 300 对所获取的漏洞修复代码进行了合法性校验，可以保证未被篡改，从而进一步提高漏洞修复的安全性。

进一步参考图 4，作为对上述各图所示方法的实现，本申请提供了一种漏洞修复装置的一个实施例，该装置实施例与图 2 所示的方法实施例相对应，该装置具体可以应用于各种电子设备中。

如图 4 所示，本实施例所述的漏洞修复装置 400 包括：收集单元 401、获取单元 402、配置单元 403 和修复单元 404。其中，收集单元 401 用于收集待修复内核的属性信息，属性信息包括用于表征待修复内核所支持代码加载方式的特征信息；获取单元 402 用于获取与特征信息匹配的漏洞修复代码；配置单元 403 用于基于属性信息，对漏洞

修复代码进行配置以使漏洞修复代码与待修复内核适配；而修复单元404用于使用已配置的漏洞修复代码对待修复内核进行漏洞修复。

在本实施例中，漏洞修复装置400的收集单元401、获取单元402、配置单元403和修复单元404的具体处理可以参考图2对应实施例中的步骤201、步骤202、步骤203、步骤204。

在本实施例的一些可选实现方式中，上述获取单元402进一步用于获取服务器中存储的、与特征信息匹配的漏洞修复代码，其中服务器存储的漏洞修复代码是实时更新的。具体处理可以参考图2对应实施例中相应的处理步骤。

在本实施例的一些可选实现方式中，上述特征信息包括：用于描述待修复内核中是否存在预设的系统调用的信息以及用于描述待修复内核中是否存在预设的物理内存设备的信息；以及上述获取单元402进一步用于当特征信息指示预设的系统调用存在时所匹配的漏洞修复代码包括内核模块类型的漏洞修复代码，当特征信息指示预设的物理内存设备存在时所匹配的漏洞修复代码包括指令序列类型的漏洞修复代码。具体处理可以参考图2对应实施例中相应的实现方式。

在本实施例的一些可选实现方式中，上述属性信息还包括内核符号校验参数；以及上述配置单元403进一步用于当所获取的漏洞修复代码为内核模块时，使用内核符号校验参数配置内核模块对应的可执行文件中的内核符号校验参数字段。具体处理可以参考图2对应实施例中相应的实现方式。

在本实施例的一些可选实现方式中，上述属性信息还包括待修复内核中内核符号的地址信息；以及配置单元403进一步用于使用地址信息配置漏洞修复代码中的内核符号的地址。具体处理可以参考图2对应实施例中相应的实现方式。

在本实施例的一些可选实现方式中，上述漏洞修复装置400还包括：校验单元（未示出），用于对所获取的漏洞修复代码进行合法性校验，以确认漏洞修复代码未被篡改。具体处理可以参考图3对应实施例中的步骤303。

在本实施例的一些可选实现方式中，漏洞修复装置400还包括生

成单元（未示出），生成用于表示漏洞修复成功或失败的信息。具体处理可以参考图 3 对应的实现方式。

在本实施例的一些可选实现方式中，收集单元 401 进一步用于：响应于待修复内核的启动操作，收集待修复内核的属性信息。具体处理可以参考图 3 对应的实现方式。

在本实施例的一些可选实现方式中，漏洞修复装置 400 还包括：恢复单元（未示出），用于若漏洞修复失败，则将待修复内核恢复至修复之间的状态。具体处理可以参考图 3 对应的实现方式。

下面参考图 5，其示出了适于用来实现本申请实施例的终端设备或服务器的计算机系统 500 的结构示意图。

如图 5 所示，计算机系统 500 包括中央处理单元（CPU）501，其可以根据存储在只读存储器（ROM）502 中的程序或者从存储部分 508 加载到随机访问存储器（RAM）503 中的程序而执行各种适当的动作和处理。在 RAM 503 中，还存储有系统 500 操作所需的各种程序和数据。CPU 501、ROM 502 以及 RAM 503 通过总线 504 彼此相连。输入/输出（I/O）接口 505 也连接至总线 504。

以下部件连接至 I/O 接口 505：包括键盘、鼠标等的输入部分 506；包括诸如阴极射线管（CRT）、液晶显示器（LCD）等以及扬声器等的输出部分 507；包括硬盘等的存储部分 508；以及包括诸如 LAN 卡、调制解调器等的网络接口卡的通信部分 509。通信部分 509 经由诸如因特网的网络执行通信处理。驱动器 510 也根据需要连接至 I/O 接口 505。可拆卸介质 511，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器 510 上，以便于从其上读出的计算机程序根据需要被安装入存储部分 508。

特别地，根据本公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括有形地包含在机器可读介质上的计算机程序，所述计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分 509 从网络上被下载和安装，

和/或从可拆卸介质 511 被安装。

附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，所述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

描述于本申请实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中，例如，可以描述为：一种处理器包括收集单元、获取单元、配置单元和修复单元。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定，例如，收集单元还可以被描述为“待修复内核的属性信息的单元”。

作为另一方面，本申请还提供了一种非易失性计算机存储介质，该非易失性计算机存储介质可以是上述实施例中所述装置中所包含的非易失性计算机存储介质；也可以是单独存在，未装配入终端中的非易失性计算机存储介质。上述非易失性计算机存储介质存储有一个或者多个程序，当所述一个或者多个程序被一个设备执行时，使得所述设备：收集待修复内核的属性信息，所述属性信息包括用于表征所述待修复内核所支持代码加载方式的特征信息；获取与所述特征信息匹配的漏洞修复代码；基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配；将已配置的漏洞修复代码加载值所述待修复内核中进行漏洞修复。

以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本申请中所涉及的发明范围，并不限

于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离所述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

权 利 要 求 书

1、一种漏洞修复方法，其特征在于，所述方法包括：

收集待修复内核的属性信息，所述属性信息包括用于表征所述待修复内核所支持代码加载方式的特征信息；

获取与所述特征信息匹配的漏洞修复代码；

基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配；

使用已配置的漏洞修复代码对所述待修复内核进行漏洞修复。

2、根据权利要求 1 所述的方法，其特征在于，所述获取与所述特征信息匹配的漏洞修复代码，包括：

获取服务器中存储的、与所述特征信息匹配的漏洞修复代码，其中所述服务器存储的漏洞修复代码是实时更新的。

3、根据权利要求 1 所述的方法，其特征在于，所述特征信息包括：用于描述所述待修复内核中是否存在预设的系统调用的信息以及用于描述所述待修复内核中是否存在预设的物理内存设备的信息；以及

所述获取与所述特征信息匹配的漏洞修复代码，包括：

当所述特征信息指示预设的系统调用存在时所匹配的漏洞修复代码包括内核模块类型的漏洞修复代码，当所述特征信息指示预设的物理内存设备存在时所匹配的漏洞修复代码包括指令序列类型的漏洞修复代码。

4、根据权利要求 3 所述的方法，其特征在于，所述属性信息还包括内核符号校验参数；以及

当所获取的漏洞修复代码为内核模块时，所述基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配，包括：

使用所述内核符号校验参数配置所述内核模块对应的可执行文件

中的内核符号校验参数字段。

5、根据权利要求 1 所述的方法，其特征在于，所述属性信息还包括待修复内核中内核符号的地址信息；以及

所述基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配包括：

使用所述地址信息配置所述漏洞修复代码中的内核符号的地址。

6、根据权利要求 1 所述的方法，其特征在于，在所述获取与所述特征信息匹配的漏洞修复代码之后，所述方法还包括：

对所获取的漏洞修复代码进行合法性校验，以确认所述漏洞修复代码未被篡改。

7、一种漏洞修复装置，其特征在于，所述装置包括：

收集单元，用于收集待修复内核的属性信息，所述属性信息包括用于表征所述待修复内核所支持代码加载方式的特征信息；

获取单元，用于获取与所述特征信息匹配的漏洞修复代码；

配置单元，用于基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配；

修复单元，用于使用已配置的漏洞修复代码对所述待修复内核进行漏洞修复。

8、根据权利要求 7 所述的装置，其特征在于，所述获取单元进一步用于获取服务器中存储的、与所述特征信息匹配的漏洞修复代码，其中所述服务器存储的漏洞修复代码是实时更新的。

9、根据权利要求 7 所述的装置，其特征在于，所述特征信息包括：用于描述所述待修复内核中是否存在预设的系统调用的信息以及用于描述所述待修复内核中是否存在预设的物理内存设备的信息；以及

所述获取单元进一步用于：当所述特征信息指示预设的系统调用

存在时所匹配的漏洞修复代码包括内核模块类型的漏洞修复代码，当所述特征信息指示预设的物理内存设备存在时所匹配的漏洞修复代码包括指令序列类型的漏洞修复代码。

10、根据权利要求 9 所述的装置，其特征在于，所述属性信息还包括内核符号校验参数；以及

所述配置单元进一步用于：当所获取的漏洞修复代码为内核模块时，使用所述内核符号校验参数配置所述内核模块对应的可执行文件中的内核符号校验参数字段。

11、根据权利要求 7 所述的装置，其特征在于，所述属性信息还包括待修复内核中内核符号的地址信息；以及

所述配置单元进一步用于：使用所述地址信息配置所述漏洞修复代码中的内核符号的地址。

12、根据权利要求 7 所述的装置，其特征在于，所述装置还包括：

校验单元，用于对所获取的漏洞修复代码进行合法性校验，以确认所述漏洞修复代码未被篡改。

13、一种设备，包括：

处理器；和

存储器，

所述存储器中存储有能够被所述处理器执行的计算机可读指令，在所述计算机可读指令被执行时，所述处理器执行漏洞修复方法，所述方法包括：

收集待修复内核的属性信息，所述属性信息包括用于表征所述待修复内核所支持代码加载方式的特征信息；

获取与所述特征信息匹配的漏洞修复代码；

基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配；

使用已配置的漏洞修复代码对所述待修复内核进行漏洞修复。

14、一种非易失性计算机存储介质，所述计算机存储介质存储有能够被处理器执行的计算机可读指令，当所述计算机可读指令被处理器执行时，所述处理器执行漏洞修复方法，所述方法包括:

收集待修复内核的属性信息，所述属性信息包括用于表征所述待修复内核所支持代码加载方式的特征信息;

获取与所述特征信息匹配的漏洞修复代码;

基于所述属性信息，对所述漏洞修复代码进行配置以使所述漏洞修复代码与所述待修复内核适配;

使用已配置的漏洞修复代码对所述待修复内核进行漏洞修复。

说 明 书 附 图

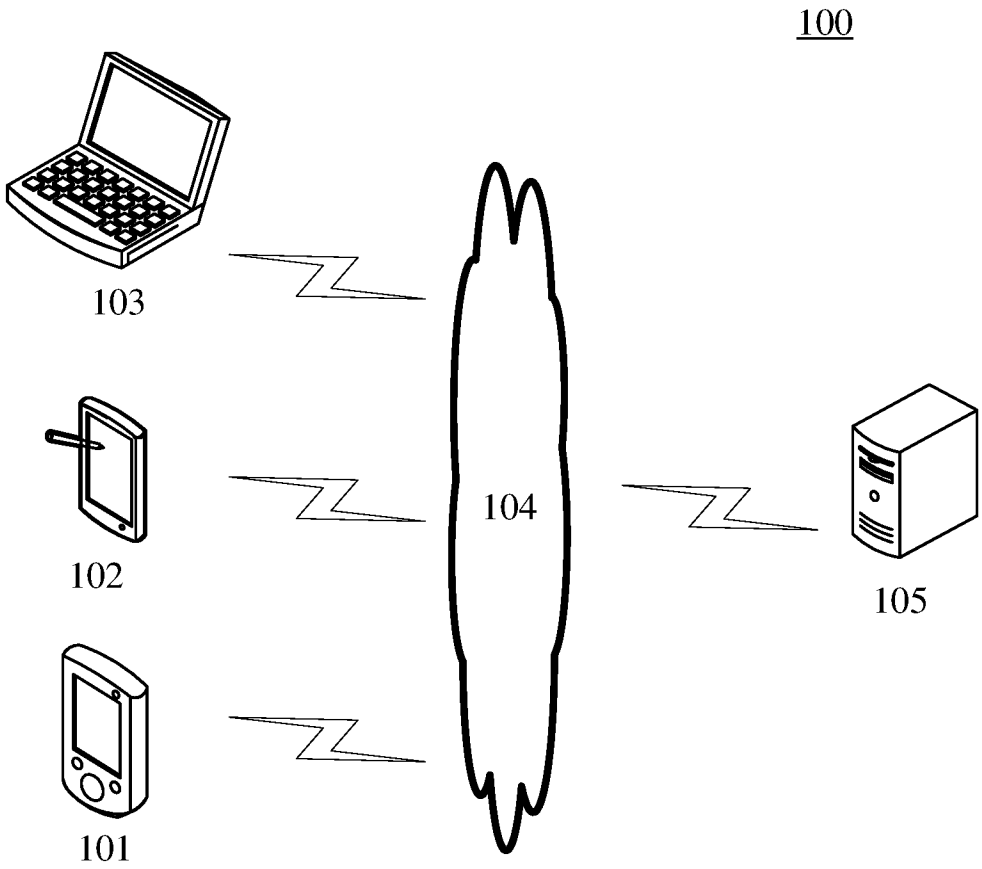

图 1

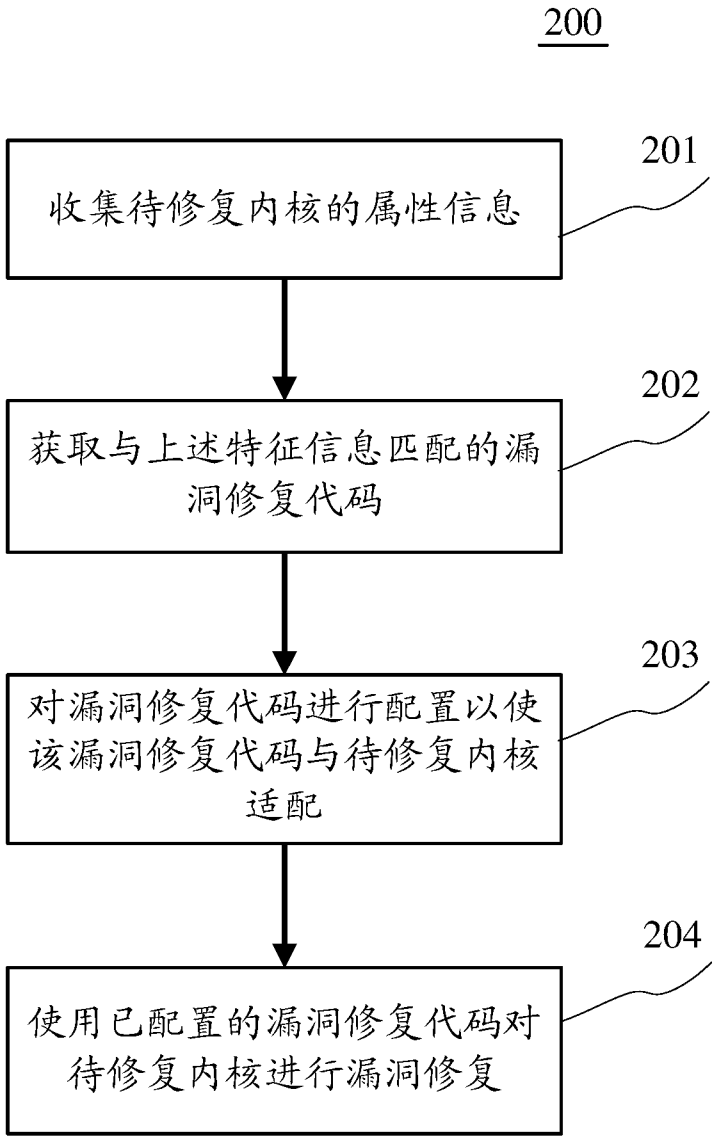
200
201
收集待修复内核的属性信息
202
获取与上述特征信息匹配的漏洞修复代码
203
对漏洞修复代码进行配置以使该漏洞修复代码与待修复内核适配
204
使用已配置的漏洞修复代码对待修复内核进行漏洞修复

图 2

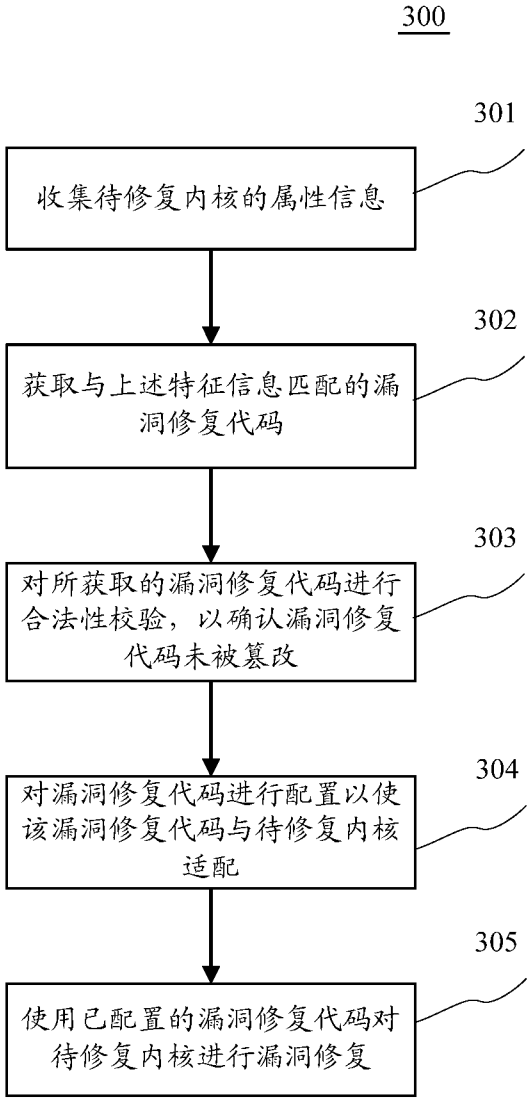
300
301
收集待修复内核的属性信息
302
获取与上述特征信息匹配的漏洞修复代码
303
对所获取的漏洞修复代码进行合法性校验，以确认漏洞修复代码未被篡改
304
对漏洞修复代码进行配置以使该漏洞修复代码与待修复内核适配
305
使用已配置的漏洞修复代码对待修复内核进行漏洞修复

图 3

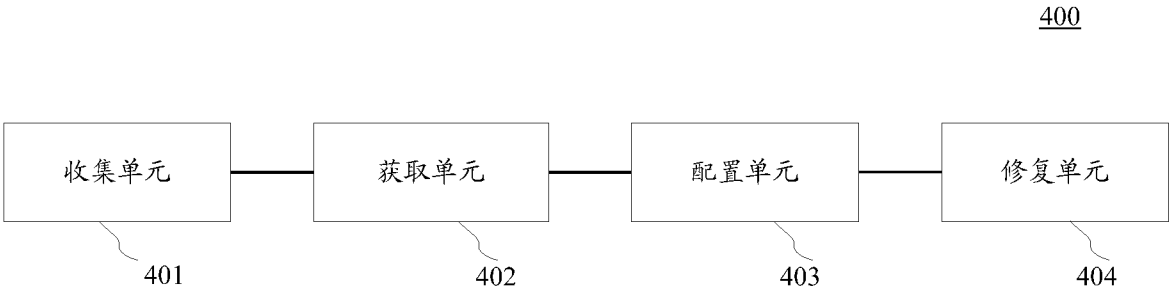

图 4

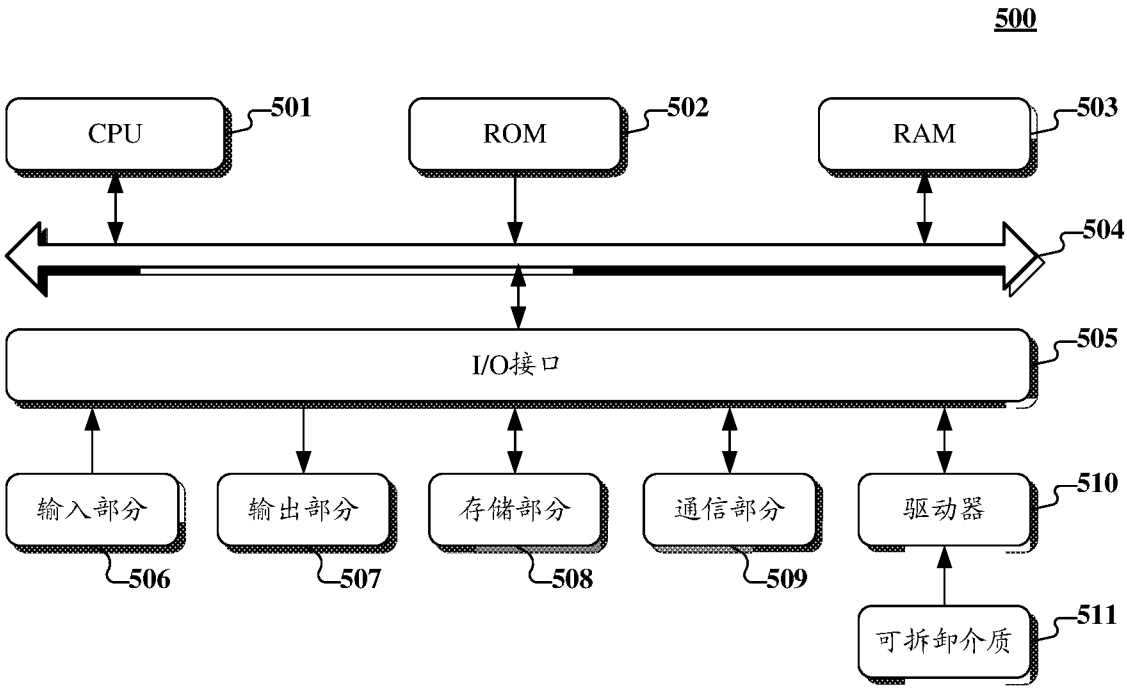
500
CPU
501
ROM
502
RAM
503
504
I/O接口
505
输入部分
506
输出部分
507
存储部分
508
通信部分
509
驱动器
510
可拆卸介质
511

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/086410

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57 (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; CNKI; WPI; EPODOC: vulnerability, patch, feature, match, adaptation, repair+, updat+, verify+, system, file

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103324494 A (KINGDEE SOFTWARE (CHINA) COMPANY LIMITED), 25 September 2013 (25.09.2013), description, paragraphs [0043]-[0063]	1-14
X	CN 104679532 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 03 June 2015 (03.06.2015), description, paragraphs [0003] and [0021]-[0060]	1-14
A	CN 103678032 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 26 March 2014 (26.03.2014), the whole document	1-14
A	CN 103309768 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 18 September 2013 (18.09.2013), the whole document	1-14

☐ 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
30 November 2016 (30.11.2016)	**03 January 2017 (03.01.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **LIU, Man** Telephone No.: (86-10) **62414025**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/086410

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103324494 A	25 September 2013	None	
CN 104679532 A	03 June 2015	WO 2015078294 A1	04 June 2015
CN 103678032 A	26 March 2014	TW 201413472 A	01 April 2014
		KR 20150017385 A	16 February 2015
		US 2014101482 A1	10 April 2014
		WO 2014040458 A1	20 March 2014
CN 103309768 A	18 September 2013	US 2014136893 A1	15 May 2014
		WO 2013135137 A1	19 September 2013
		HK 1187430 A0	04 April 2014
		VN 40540 A	26 January 2015

国际检索报告

国际申请号
PCT/CN2016/086410

A. 主题的分类

G06F 21/57(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;CNKI;WPI;EPODOC:漏洞, 补丁, 修复, 特征, 匹配, 适配, repair+, updat+, verify+, system, file

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 103324494 A (金蝶软件中国有限公司) 2013年 9月 25日 (2013-09-25) 说明书第[0043]-[0063]段	1-14
X	CN 104679532 A (腾讯科技深圳有限公司) 2015年 6月 3日 (2015-06-03) 说明书第[0003], [0021]-[0060]段	1-14
A	CN 103678032 A (腾讯科技深圳有限公司) 2014年 3月 26日 (2014-03-26) 全文	1-14
A	CN 103309768 A (腾讯科技深圳有限公司) 2013年 9月 18日 (2013-09-18) 全文	1-14

☐ 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
2016年 11月 30日	2017年 1月 3日
ISA/CN的名称和邮寄地址 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	受权官员 刘曼 电话号码 (86-10)62414025

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/086410

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	103324494	A	2013年 9月 25日	无			
CN	104679532	A	2015年 6月 3日	WO	2015078294	A1	2015年 6月 4日
CN	103678032	A	2014年 3月 26日	TW	201413472	A	2014年 4月 1日
				KR	20150017385	A	2015年 2月 16日
				US	2014101482	A1	2014年 4月 10日
				WO	2014040458	A1	2014年 3月 20日
CN	103309768	A	2013年 9月 18日	US	2014136893	A1	2014年 5月 15日
				WO	2013135137	A1	2013年 9月 19日
				HK	1187430	A0	2014年 4月 4日
				VN	40540	A	2015年 1月 26日