(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
2016 年 6 月 23 日 (23.06.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/095796 A1

(51) 国际专利分类号:
G06F 21/57 (2013.01)

(21) 国际申请号: PCT/CN2015/097362

(22) 国际申请日: 2015 年 12 月 15 日 (15.12.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410778171.7 2014 年 12 月 17 日 (17.12.2014) CN

(71) 申请人: **中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.)** [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: **何朔 (HE, Shuo)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **郭伟 (GUO, Wei)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **周钰 (ZHOU, Yu)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **陈成钱 (CHEN, Chengqian)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: **中国专利代理（香港）有限公司 (CHINA PATENT AGENT (HK) LTD.)**; 中国香港特别行政区香港湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (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。

(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,

[见续页]

(54) **Title**: SECURE OPERATING SYSTEM UPDATE METHOD USED IN RELIABLE EXECUTION ENVIRONMENT

(54) **发明名称** : 用于可信执行环境的安全操作系统更新方法

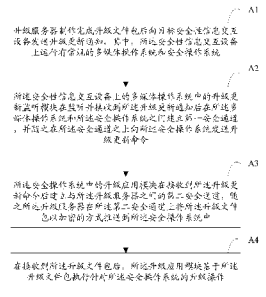


图 1 / Fig. 1

A1 After an upgrade server produces an upgrade file package, send an upgrade update notification to a target security information interaction device, and a regular multi-media operating system and the secure operating system are operated on the security information interaction device

A2 After an upgrade update monitor module in a multi-media operating system on the security information interaction device monitors and receives the upgrade update notification, establish a first secure channel between the multi-media operating system and the secure operating system, then send an upgrade update command to the secure operating system above the secure channel

A3 After an upgrade application module of the secure operating system receives the upgrade update command, establishing a second secure channel with the upgrade server, then the upgrade server pushes the upgrade file package to the secure operating system on the second secure channel in an encrypted way

A4 After the upgrade file package is received, the upgrade application module, on the basis of the upgrade file package, conducts an upgrade operation on the secure operating system

(57) **Abstract**: A secure operating system update method used in a reliable execution environment, the method comprising: after an upgrade server produces an upgrade file package, sending an upgrade update notification to a target security information interaction device (A1); after an upgrade update monitor module in a multi-media operating system on the security information interaction device monitors and receives the upgrade update notification, sending an upgrade update command to the secure operating system (A2); after an upgrade application module of the secure operating system receives the upgrade update command, establishing a second secure channel with the upgrade server, then the upgrade server pushes the upgrade file package to the secure operating system on the second secure channel in an encrypted way (A3); and after the upgrade file package is received, the upgrade application module, on the basis of the upgrade file package, conducts an upgrade operation on the secure operating system (A4). The above method can continuously update and maintain the secure operating system.

(57) **摘要**: 一种用于可信执行环境的安全操作系统更新方法，所述方法包括：升级服务器制作完成升级文件包后向目标安全性信息交互设备发送升级更新通知（A1）；安全性信息交互设备上的多媒体操作系统中的升级更新监听模块在监听并接收到所述升级更新通知后向所述安全操作系统发送升级更新命令（A2）；安全操作系统中的升级应用模块在接收到所述升级更新命令后建立与所述升级服务器之间的第二安全通道，随之所述升级服务器在所述第二安全通道上将所述升级文件包以加密的方式推送到所述安全操作系统中（A3）；在接收到所述升级文件包后，所述升级应用模块基于所述升级文件包执行针对所述安全操作系统的升级操作（A4）。上述方法能够对安全操作系统进行持续的更新和维护。

WO 2016/095796 A1

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))。

用于可信执行环境的安全操作系统更新方法

技术领域

本发明涉及操作系统更新方法，更具体地，涉及用于可信执行环境的安全操作系统更新方法。

背景技术

目前，随着计算机和网络应用的日益广泛以及不同领域的业务种类的日益丰富，用于安全性信息交互（即对安全性要求较高的信息交互，例如金融领域中的交易处理过程）的设备（尤其是基于移动终端的安全性信息交互设备）变得越来越重要。

在现有的基于可信执行环境的技术方案中，安全性信息交互设备（例如移动终端）通常包含为常规的应用提供运行环境的第一系统管理装置（例如常规的多媒体操作系统）和为安全性应用提供安全模式下的运行环境的第二系统管理装置（即安全操作系统），并且在第一系统管理装置中运行的常规应用/设备与在第二系统管理装置中运行的安全应用/设备进行数据交互时，在所述第一和第二系统管理装置在该常规应用/设备和该安全应用/设备之间建立安全通道并随之基于该安全通道完成后续的数据交互过程。

然而，现有的技术方案存在如下问题：当安全操作系统被发布并在设备上运行之后，难于对安全操作系统在较高的安全机制下进行更新，例如针对安全操作系统增加功能或者修补漏洞。

因此，存在如下需求：提供能够对安全操作系统进行持续的更新和维护的用于可信执行环境的安全操作系统更新方法。

发明内容

为了解决上述现有技术方案所存在的问题，本发明提出了能够对安全操作系统进行持续的更新和维护的用于可信执行环境的安全操作系统更新方法。

本发明的目的是通过以下技术方案实现的：

一种用于可信执行环境的安全操作系统更新方法，所述用于可信执行环境

的安全操作系统更新方法包括下列步骤：

（A1）升级服务器制作完成升级文件包后向目标安全性信息交互设备发送升级更新通知，其中，所述安全性信息交互设备上运行有常规的多媒体操作系统和安全操作系统，所述多媒体操作系统为常规的应用和附属设备提供运行环境。所述安全操作系统为安全性应用和附属设备（即对安全性要求较高的应用和附属设备，例如金融领域中的支付应用）提供安全模式下的运行环境，以执行安全性信息交互过程；

（A2）所述安全性信息交互设备上的多媒体操作系统中的升级更新监听模块在监听并接收到所述升级更新通知后在所述多媒体操作系统和所述安全操作系统之间建立第一安全通道，并随之在所述安全通道之上向所述安全操作系统发送升级更新命令；

（A3）所述安全操作系统中的升级应用模块在接收到所述升级更新命令后建立与所述升级服务器之间的第二安全通道，随之所述升级服务器在所述第二安全通道上将所述升级文件包以加密的方式推送到所述安全操作系统中；

（A4）在接收到所述升级文件包后，所述升级应用模块基于所述升级文件包执行针对所述安全操作系统的升级操作。

在上面所公开的方案中，优选地，所述升级文件包包括升级文件、升级文件版本号、安全操作系统校验文件以及升级文件安装脚本，其中，所述安全操作系统校验文件用于验证安全操作系统的完整性，所述升级文件安装脚本用于指示升级文件的安装方式和位置。

在上面所公开的方案中，优选地，所述步骤（A4）进一步包括：（1）在接收到所述升级文件包后，所述升级应用模块解密所述升级文件包，并从所述升级文件包提取出升级文件、升级文件版本号、安全操作系统校验文件以及升级文件安装脚本；(2)所述升级应用模块验证提取出的升级文件版本号，并在验证通过后运行所述升级文件安装脚本以执行针对所述安全操作系统的升级操作。

在上面所公开的方案中，优选地，所述执行针对所述安全操作系统的升级操作包括执行升级文件的安装操作、安全操作系统校验文件的替换操作以及其他由所述升级文件安装脚本指定的更新操作。

在上面所公开的方案中，优选地，升级文件的安装操作的过程如下：（1）将所述升级文件安装到更新保留内存区中；（2）针对所述升级文件中的增加功能类函数，直接将所述增加功能类函数在更新保留内存区中的地址添加到系统中，而针对所述升级文件中的补丁类函数，则首先查找内核符号表以获取被修补函数的入口地址，随后将该被修补函数重定向到其对应的补丁函数，随之将被修补函数的入口处的指令替换为跳转指令，由此将被修补函数重定向到其对应的补丁函数。

在上面所公开的方案中，优选地，在升级文件的安装操作完成之后执行安全操作系统校验文件的替换操作，即将对应于未更新前的安全操作系统的安全操作系统校验文件替换为对应于已更新的安全操作系统的安全操作系统校验文件。

在上面所公开的方案中，优选地，在所述安全操作系统启动时，引导加载器根据安全操作系统校验文件校验所述安全操作系统的完整性。

在上面所公开的方案中，优选地，所述安全操作系统校验文件包含其所对应的安全操作系统的哈希值。

本发明所公开的用于可信执行环境的安全操作系统更新方法具有下列优点：能够在安全操作系统被发布和运行于设备上之后对安全操作系统进行持续的更新和维护，从而显著地提高了系统性能和安全性。

附图说明

结合附图，本发明的技术特征以及优点将会被本领域技术人员更好地理解，其中：

图1是根据本发明的实施例的用于可信执行环境的安全操作系统更新方法的流程图。

具体实施方式

图1是根据本发明的实施例的用于可信执行环境的安全操作系统更新方法的流程图。如图1所示，本发明所公开的用于可信执行环境的安全操作系统更新方法包括下列步骤：（A1）升级服务器（根据维护人员的指令）制作完成升

级文件包后向目标安全性信息交互设备发送升级更新通知，其中，所述安全性信息交互设备上运行有常规的多媒体操作系统和安全操作系统，所述多媒体操作系统为常规的应用和附属设备提供运行环境。所述安全操作系统为安全性应用和附属设备（即对安全性要求较高的应用和附属设备，例如金融领域中的支付应用）提供安全模式下的运行环境，以执行安全性信息交互过程；（A2）所述安全性信息交互设备上的多媒体操作系统中的升级更新监听模块在监听并接收到所述升级更新通知后在所述多媒体操作系统和所述安全操作系统之间建立第一安全通道，并随之在所述安全通道之上向所述安全操作系统发送升级更新命令；（A3）所述安全操作系统中的升级应用模块在接收到所述升级更新命令后建立与所述升级服务器之间的第二安全通道，随之所述升级服务器在所述第二安全通道上将所述升级文件包以加密的方式推送到所述安全操作系统中；（A4）在接收到所述升级文件包后，所述升级应用模块基于所述升级文件包执行针对所述安全操作系统的升级操作。

优选地，在本发明所公开的用于可信执行环境的安全操作系统更新方法中，所述升级文件包包括升级文件（即针对该操作系统的替换程序或者待增加程序）、升级文件版本号（其指示升级文件的发布次数以及先后顺序）、安全操作系统校验文件以及升级文件安装脚本，其中，所述安全操作系统校验文件用于验证安全操作系统的完整性，所述升级文件安装脚本用于指示升级文件的安装方式和位置。

优选地，在本发明所公开的用于可信执行环境的安全操作系统更新方法中，所述步骤（A4）进一步包括：（1）在接收到所述升级文件包后，所述升级应用模块解密所述升级文件包，并从所述升级文件包提取出升级文件、升级文件版本号、安全操作系统校验文件以及升级文件安装脚本；(2)所述升级应用模块验证提取出的升级文件版本号，并在验证通过后运行所述升级文件安装脚本以执行针对所述安全操作系统的升级操作。

优选地，在本发明所公开的用于可信执行环境的安全操作系统更新方法中，所述执行针对所述安全操作系统的升级操作包括执行升级文件的安装操作、安全操作系统校验文件的替换操作以及其他由所述升级文件安装脚本指定的更新操作。

优选地，在本发明所公开的用于可信执行环境的安全操作系统更新方法中，升级文件的安装操作的过程如下：（1）将所述升级文件安装到更新保留内存区中；（2）针对所述升级文件中的增加功能类函数，直接将所述增加功能类函数在更新保留内存区中的地址添加到系统中，而针对所述升级文件中的补丁类函数，则首先查找内核符号表以获取被修补函数的入口地址，随后将该被修补函数重定向到其对应的补丁函数（在该补丁函数中被修补函数的缺陷被修正），随之将被修补函数的入口处的指令替换为跳转指令，由此将被修补函数重定向到其对应的补丁函数。

优选地，在本发明所公开的用于可信执行环境的安全操作系统更新方法中，在升级文件的安装操作完成之后执行安全操作系统校验文件的替换操作，即将对应于未更新前的安全操作系统的安全操作系统校验文件替换为对应于已更新的安全操作系统的安全操作系统校验文件。

优选地，在本发明所公开的用于可信执行环境的安全操作系统更新方法中，在所述安全操作系统启动时，引导加载器（bootloader）根据安全操作系统校验文件校验所述安全操作系统的完整性。

优选地，在本发明所公开的用于可信执行环境的安全操作系统更新方法中，所述安全操作系统校验文件包含其所对应的安全操作系统的哈希值。

由上可见，本发明所公开的用于可信执行环境的安全操作系统更新方法具有下列优点：能够在安全操作系统被发布和运行于设备上之后对安全操作系统进行持续的更新和维护，从而显著地提高了系统性能和安全性。

尽管本发明是通过上述的优选实施方式进行描述的，但是其实现形式并不局限于上述的实施方式。应该认识到：在不脱离本发明主旨和范围的情况下，本领域技术人员可以对本发明做出不同的变化和修改。

权利要求

1. 一种用于可信执行环境的安全操作系统更新方法，所述用于可信执行环境的安全操作系统更新方法包括下列步骤：

（A1）升级服务器制作完成升级文件包后向目标安全性信息交互设备发送升级更新通知，其中，所述安全性信息交互设备上运行有常规的多媒体操作系统和安全操作系统，所述多媒体操作系统为常规的应用和附属设备提供运行环境。所述安全操作系统为安全性应用和附属设备提供安全模式下的运行环境，以执行安全性信息交互过程；

（A2）所述安全性信息交互设备上的多媒体操作系统中的升级更新监听模块在监听并接收到所述升级更新通知后在所述多媒体操作系统和所述安全操作系统之间建立第一安全通道，并随之在所述安全通道之上向所述安全操作系统发送升级更新命令；

（A3）所述安全操作系统中的升级应用模块在接收到所述升级更新命令后建立与所述升级服务器之间的第二安全通道，随之所述升级服务器在所述第二安全通道上将所述升级文件包以加密的方式推送到所述安全操作系统中；

（A4）在接收到所述升级文件包后，所述升级应用模块基于所述升级文件包执行针对所述安全操作系统的升级操作。

2. 根据权利要求1所述的用于可信执行环境的安全操作系统更新方法，其特征在于，所述升级文件包包括升级文件、升级文件版本号、安全操作系统校验文件以及升级文件安装脚本，其中，所述安全操作系统校验文件用于验证安全操作系统的完整性，所述升级文件安装脚本用于指示升级文件的安装方式和位置。

3. 根据权利要求2所述的用于可信执行环境的安全操作系统更新方法，其特征在于，所述步骤（A4）进一步包括：（1）在接收到所述升级文件包后，所述升级应用模块解密所述升级文件包，并从所述升级文件包提取出升级文件、升级文件版本号、安全操作系统校验文件以及升级文件安装脚本；(2)所述升级应用模块验证提取出的升级文件版本号，并在验证通过后运行所述升级文件安装脚本以执行针对所述安全操作系统的升级操作。

4. 根据权利要求3所述的用于可信执行环境的安全操作系统更新方法，其特征在于，所述执行针对所述安全操作系统的升级操作包括执行升级文件的安装操作、安全操作系统校验文件的替换操作以及其他由所述升级文件安装脚本指定的更新操作。

5. 根据权利要求4所述的用于可信执行环境的安全操作系统更新方法，其特征在于，升级文件的安装操作的过程如下：（1）将所述升级文件安装到更新保留内存区中；（2）针对所述升级文件中的增加功能类函数，直接将所述增加功能类函数在更新保留内存区中的地址添加到系统中，而针对所述升级文件中的补丁类函数，则首先查找内核符号表以获取被修补函数的入口地址，随后将该被修补函数重定向到其对应的补丁函数，随之将被修补函数的入口处的指令替换为跳转指令，由此将被修补函数重定向到其对应的补丁函数。

6. 根据权利要求5所述的用于可信执行环境的安全操作系统更新方法，其特征在于，在升级文件的安装操作完成之后执行安全操作系统校验文件的替换操作，即将对应于未更新前的安全操作系统的安全操作系统校验文件替换为对应于已更新的安全操作系统的安全操作系统校验文件。

7. 根据权利要求6所述的用于可信执行环境的安全操作系统更新方法，其特征在于，在所述安全操作系统启动时，引导加载器根据安全操作系统校验文件校验所述安全操作系统的完整性。

8. 根据权利要求7所述的用于可信执行环境的安全操作系统更新方法，其特征在于，所述安全操作系统校验文件包含其所对应的安全操作系统的哈希值。

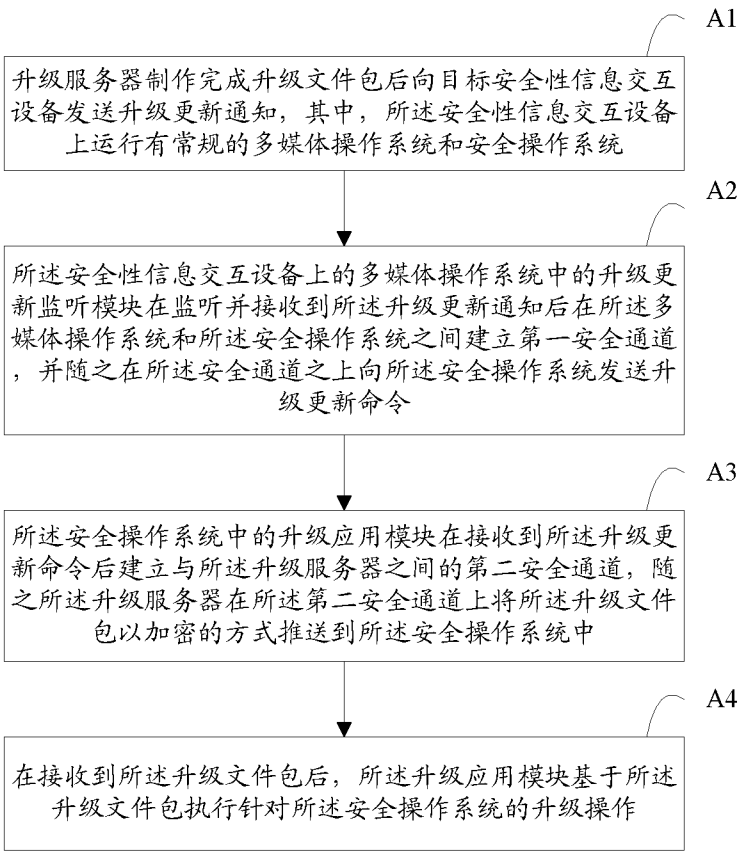

A1
升级服务器制作完成升级文件包后向目标安全性信息交互设备发送升级更新通知，其中，所述安全性信息交互设备上运行有常规的多媒体操作系统和安全操作系统
A2
所述安全性信息交互设备上的多媒体操作系统中的升级更新监听模块在监听并接收到所述升级更新通知后在所述多媒体操作系统和所述安全操作系统之间建立第一安全通道，并随之在所述安全通道之上向所述安全操作系统发送升级更新命令
A3
所述安全操作系统中的升级应用模块在接收到所述升级更新命令后建立与所述升级服务器之间的第二安全通道，随之所述升级服务器在所述第二安全通道上将所述升级文件包以加密的方式推送到所述安全操作系统中
A4
在接收到所述升级文件包后，所述升级应用模块基于所述升级文件包执行针对所述安全操作系统的升级操作

图 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/097362

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)

WPI, EPODOC, CNPAT, CNKI: update, patch, application, program, software, operating system, safe, security, authentic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104168557 A (COOLPAD SOFTWARE TECHNOLOGY (SHENZHEN) CO., LTD.) 26 November2014 (26.11.2014) description, paragraphs [0037]-[0075], and figures 1-4	1-8
A	CN 104040498 A (CONTINENTAL AUTOMOTIVE GMBH) 10 September 2014 (10.09.2014) the whole document	1-8
A	CN 103282911 A (SK PLANET CO., LTD.) 04 September 2013 (04.09.2013) the whole document	1-8
A	CN 101021795 A (NTT DOCOMO INC.) 22 August 2007 (22.08.2007) the whole document	1-8
A	US 2003070162 A1 (OSHIMA, SATOSHI) 10 April 2003 (10.04.2003) the whole document	1-8

☐ 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
24 February 2016	14 March 2016
Name and mailing address of the ISA 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 LI, Na Telephone No. (86-10) 62414068

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/097362

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104168557 A	26 November 2014	None	
CN 104040498 A	10 September 2014	DE 102012200155 A1	11 July 2013
		US 2014372999 A1	18 December 2014
		WO 2013102564 A1	11 July 2013
		EP 2801027 A1	12 November 2014
CN 103282911 A	04 September 2013	WO 2013065915 A1	10 May 2013
		US 2014245013 A1	28 August 2014
		EP 2618266 A1	24 July 2013
		JP 2014505283 A	27 February 2014
		US 9100172 B2	04 August 2015
		JP 5583857 B2	03 September 2014
		KR 20130049343 A	14 May 2013
		KR 20130053867 A	24 May 2013
		KR 20130053868 A	24 May 2013
		ID 201301176 A	25 April 2013
CN 101021795 A	22 August 2007	EP 1821205 A3	27 May 2009
		TW 200818017 A	16 April 2008
		CN 100440149 C	03 December 2008
		US 2007220242 A1	20 September 2007
		US 7827395 B2	02 November2010
		JP 2007213494 A	23 August 2007
		EP 1821205 A2	22 August 2007
		TW 1348644 B	11 September 2011
US 2003070162 A1	10 April 2003	JP 2003114806 A	18 April 2003

国际检索报告

国际申请号
PCT/CN2015/097362

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）)

WPI, EPODOC, CNPAT, CNKI: 升级，更新，补丁，应用，程序，软件，操作系统，安全，可信，认证，update, patch, application, program, operating system, safe, security, authentic

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
A	CN 104168557 A (酷派软件技术深圳有限公司) 2014年 11月 26日 (2014-11-26) 说明书第[0037]-[0075]段，图1-4	1-8
A	CN 104040498 A (大陆汽车有限责任公司) 2014年 9月 10日 (2014-09-10) 全文	1-8
A	CN 103282911 A (SK 普兰尼特有限公司) 2013年 9月 4日 (2013-09-04) 全文	1-8
A	CN 101021795 A (株式会社NTT都科摩) 2007年 8月 22日 (2007-08-22) 全文	1-8
A	US 2003070162 A1 (OSHIMA, SATOSHI) 2003年 4月 10日 (2003-04-10) 全文	1-8

☐ 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 2月 24日	2016年 3月 14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 李娜 电话号码 (86-10)62414068

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/097362

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	104168557	A	2014年 11月 26日	无			
CN	104040498	A	2014年 9月 10日	DE	102012200155	A1	2013年 7月 11日
				US	2014372999	A1	2014年 12月 18日
				WO	2013102564	A1	2013年 7月 11日
				EP	2801027	A1	2014年 11月 12日
CN	103282911	A	2013年 9月 4日	WO	2013065915	A1	2013年 5月 10日
				US	2014245013	A1	2014年 8月 28日
				EP	2618266	A1	2013年 7月 24日
				JP	2014505283	A	2014年 2月 27日
				US	9100172	B2	2015年 8月 4日
				JP	5583857	B2	2014年 9月 3日
				KR	20130049343	A	2013年 5月 14日
				KR	20130053867	A	2013年 5月 24日
				KR	20130053868	A	2013年 5月 24日
				ID	201301176	A	2013年 4月 25日
CN	101021795	A	2007年 8月 22日	EP	1821205	A3	2009年 5月 27日
				TW	200818017	A	2008年 4月 16日
				CN	100440149	C	2008年 12月 3日
				US	2007220242	A1	2007年 9月 20日
				US	7827395	B2	2010年 11月 2日
				JP	2007213494	A	2007年 8月 23日
				EP	1821205	A2	2007年 8月 22日
				TW	I348644	B	2011年 9月 11日
US	2003070162	A1	2003年 4月 10日	JP	2003114806	A	2003年 4月 18日