

(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
2015 年 5 月 14 日 (14.05.2015)



(10) 国际公布号
WO 2015/067170 A1

- (51) 国际专利分类号:
G06F 21/52 (2013.01)
- (21) 国际申请号: PCT/CN2014/090302
- (22) 国际申请日: 2014 年 11 月 5 日 (05.11.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201310542708.5 2013 年 11 月 6 日 (06.11.2013) CN
- (71) 申请人: 中国银联股份有限公司 (CHINA UNION-PAY 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: 柴洪峰 (CHAI, Hongfeng); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 束骏亮 (SHU, Junliang); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 鲁志军 (LU, Zhijun); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 李卷濡 (LI, Juanru); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 刘发章

(LIU, Fazhang); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 林培胜 (LIN, Peisheng); 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,

[见续页]

(54) Title: METHOD AND SYSTEM FOR ANALYZING ANDROID APPLICATION PROGRAM

(54) 发明名称: 一种分析 Android 应用程序的方法和系统

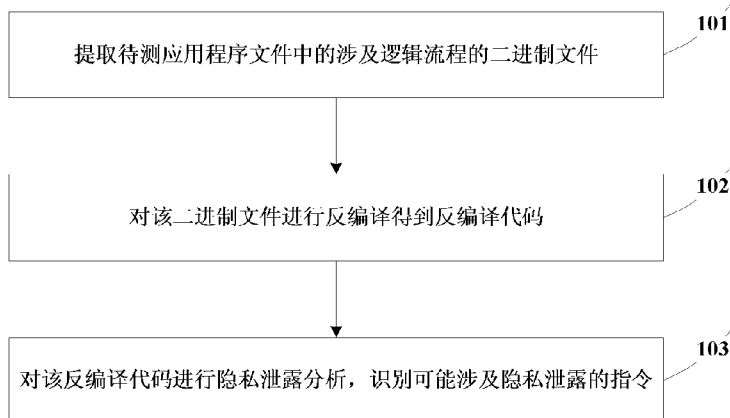


图 1 / Fig. 1

- 101 EXTRACTING A BINARY FILE RELATING TO A LOGICAL FLOW IN AN APPLICATION PROGRAM FILE TO BE TESTED
- 102 CONDUCTING DE-COMPILATION ON THE BINARY FILE TO OBTAIN A DE-COMPILATION CODE
- 103 CONDUCTING PRIVACY DISCLOSURE ANALYSIS ON THE DE-COMPILATION CODE, AND RECOGNIZING AN INSTRUCTION POSSIBLY RELATING TO PRIVACY DISCLOSURE

(57) Abstract: Disclosed are a method and device for analyzing an Android application program. The method comprises the following step: performing static analysis before operation, and the step comprises: extracting a binary file relating to a logical flow in an application program file; conducting de-compilation on the binary file to obtain a de-compilation code; and conducting privacy disclosure analysis on the de-compilation code, and recognizing an instruction possibly relating to privacy disclosure.

(57) 摘要: 本发明公开一种分析 Android 应用程序的方法和系统。该方法包括以下步骤: 运行前静态分析, 该步骤包括: 提取应用程序文件中的涉及逻辑流程的二进制文件, 对该二进制文件进行反编译得到反编译代码, 对该反编译代码进行隐私泄露分析, 识别可能涉及隐私泄露的指令。



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))。

一种分析 Android 应用程序的方法和系统

技术领域

[0001] 本发明涉及信息安全，并且尤其涉及分析 Android 应用程序的方法和系统。

背景技术

[0002] 在现有技术中，查明隐私泄露通常在隐私泄露事件发生后进行。例如，在运行 Android 平台的设备发生了隐私泄露之后，对 Android 平台上的应用程序进行分析检测（例如分析检测该应用程序使用过的资源，收发过的数据）从而查明隐私泄露。

[0003] 现有的技术方案根据应用程序运行的结果数据以补救的形式来处理隐私泄露，应对时间滞后而且无法预防隐私泄露。因此，需要一种能够预防隐私泄露的技术方案。

发明内容

[0004] 根据本发明的一个目的，公开一种分析 Android 应用程序的方法，包括以下步骤：
运行前静态分析，该步骤包括：

提取应用程序文件中的涉及逻辑流程的二进制文件，

对该二进制文件进行反编译得到反编译代码，

对该反编译代码进行隐私泄露分析，识别可能涉及隐私泄露的指令。

[0005] 优选地，上述隐私泄露分析步骤包括：

在反编译代码中查找涉及隐私数据的关键指令，

判断关键指令和与该关键指令相关的其它指令是否执行与外界进行数据交换的操作，

将关键指令和与该关键指令相关的其它指令中的执行与外界进行数据交换的操作的指令标记为可能涉及隐私泄露的指令。

[0006] 优选地，该方法还包括以下步骤：

运行中动态分析，该步骤包括：

记录应用程序在运行时的动态数据，

分析动态数据的行为，识别涉及隐私泄露的行为。

[0007] 优选地，分析动态数据的行为的步骤包括：

分析动态数据中的与通过静态分析识别的可能涉及隐私泄露的指令相关的部分，

根据预定的分析算法识别涉及隐私泄露的行为。

[0008] 优选地，上述隐私泄露分析步骤还包括：

生成静态分析报告。

[0009] 优选地，运行中动态分析的步骤还包括：

生成隐私泄露安全分析报告。

[0010] 根据本发明的一个目的，公开一种分析 Android 应用程序的系统，包括：

运行前静态分析装置，该装置包括：

提取单元，用于提取应用程序文件中的涉及逻辑流程的二进制文件，

反编译单元，用于对该二进制文件进行反编译得到反编译代码，

第一分析单元，用于对该反编译代码进行隐私泄露分析，识别可能涉及隐私泄露的指令。

[0011] 优选地，所述第一分析单元被配置成：

在反编译代码中查找涉及隐私数据的关键指令，

判断关键指令和与该关键指令相关的其它指令是否执行与外界进行数据交换的操作，

将关键指令和与该关键指令相关的其它指令中的执行与外界进行数据交换的操作的指令标记为可能涉及隐私泄露的指令。

[0012] 优选地，该系统还包括：

运行中动态分析装置，该装置包括：

监控单元，用于记录应用程序在运行时的动态数据，

第二分析单元，用于分析动态数据的行为，识别涉及隐私泄露的行为。

[0013] 优选地，所述第二分析单元被配置成：

分析动态数据中的与通过静态分析识别的可能涉及隐私泄露的指令相关的部分，

根据预定的分析算法识别涉及隐私泄露的行为。

[0014] 优选地，所述第一分析单元还被配置成：

生成静态分析报告。

[0015] 优选地，所述第二分析单元还被配置成：

生成隐私泄露安全分析报告。

[0016] 本发明的一个优势在于，能够进行运行前静态分析与运行时动态分析来检测隐私泄露。本发明的一个优势在于，能够综合使用运行前静态分析和运行过程中触发应用程序的行为的动态分析，根据预定的算法分析统计应用中涉及到隐私泄露的相关指令及其操作从而判定是否存隐私泄露。本发明的一个优势在于，生成隐私泄露分析报告。本发明的一个优势在于，能够在应用程序的层面对隐私数据的泄漏进行检测，无需对 Android 系统底层进行修改，也不会对 Android 系统造成额外的负担。

附图说明

[0017] 在参照附图阅读了本发明的具体实施方式以后，本领域技术人员将会更清楚地了解本发明的各个方面。本领域技术人员应当理解的是，这些附图仅仅用于配合具体实施方式说明本发明的技术方案，而并非意在对本发明的保护范围构成限制。

[0018] 图 1 是根据本发明一个实施例的分析 Android 应用程序的方法的步骤示意图。

[0019] 图 2 是根据本发明一个实施例的分析 Android 应用程序的方法的步骤示意图。

[0020] 图 3 是根据本发明一个实施例的分析 Android 应用程序的方法的步骤示意图。

[0021] 图 4 是根据本发明一个实施例的分析 Android 应用程序的系统的结构示意图。

具体实施方式

[0022] 下面参照附图，对本发明的具体实施方式作进一步的详细描述。在下面的描述中，为了解释的目的，陈述许多具体细节以便提供对实施例的一个或多个方面的透彻理解。然而，对于本领域技术人员可以显而易见的是，可以这些具体细节的较少程度来实践各实施例的一个或多个方面。因此下面的描述不被视为局限性的，而是通过所附权利要求来限定保护范围。

[0023] 图 1 是根据本发明一个实施例的分析 Android 应用程序的方法的步骤示意图。如图所示，该方法包括以下步骤：

步骤 101：提取应用程序文件中的涉及逻辑流程的二进制文件，

步骤 102：对该二进制文件进行反编译得到反编译代码，

步骤 103：对该反编译代码进行隐私泄露分析，识别可能涉及隐私泄露的指令。

[0024] 上述 3 个步骤是应用程序的运行前静态分析。这里，隐私泄露是指将关于 Android 设备和用户的敏感信息泄露给第三方的情况。

[0025] 图 2 是根据本发明另一个实施例的分析 Android 应用程序的方法的步骤示意图。图 2 进一步描述关于图 1 中步骤 103 的情况。如图所示，隐私泄露分析步骤包括：

步骤 1031：在反编译代码中查找涉及隐私数据的关键指令，

步骤 1032：判断关键指令和与该关键指令相关的其它指令是否执行与外界进行数据交换的操作，

步骤 1033：将关键指令和与该关键指令相关的其它指令中的执行与外界进行数据交换的操作的指令标记为可能涉及隐私泄露的指令。

[0026] 这里，与外界进行数据交换是指与第三方进行隐私数据的交换。在一个示例中，可以生成静态分析报告。

[0027] 图 3 是根据本发明另一个实施例的分析 Android 应用程序的方法的步骤示意图。在该

方法中，描述应用程序的运行中动态分析。如图 3 所示，该方法包括以下步骤：

步骤 201：记录应用程序在运行时的动态数据，

步骤 202：分析动态数据的行为，识别涉及隐私泄露的行为。

[0028] 这里，动态数据的行为是指与该动态数据相关的操作。通过分析动态数据能够对应应用程序运行中的一切操作进行监控和判断，从而识别应用程序在运行期间是否进行了泄漏隐私数据的操作。

[0029] 在一个示例中，可以主动触发应用程序的行为，从而记录尽可能完全的运行时的动态数据。

[0030] 在一个示例中，可以根据动态数据获取例如运行中应用程序的 Class、Method、Opcode、String 等信息，并从中识别出可能存在的泄漏隐私数据的行为。例如，可以配置策略来进行不同类型的行为分析。

[0031] 在一个实施例，将上述的运行前静态分析和运行中动态分析相结合。此时，对于上述实施例中的步骤 202 来说，分析动态数据的行为的步骤可以包括：分析动态数据中的与通过静态分析识别的可能涉及隐私泄露的指令相关的部分，以及根据预定的分析算法识别涉及隐私泄露的行为。

[0032] 该实施例通过综合分析提高了识别隐私泄露的行为的效率。在一个示例中，还生成隐私泄露安全分析报告。

[0033] 图 4 是根据本发明一个实施例的分析 Android 应用程序的系统的结构示意图。如图所示，该系统包括运行前静态分析装置，该装置包括：提取单元，用于提取应用程序文件中的涉及逻辑流程的二进制文件，反编译单元，用于对该二进制文件进行反编译得到反编译代码，第一分析单元，用于对该反编译代码进行隐私泄露分析，识别可能涉及隐私泄露的指令。

[0034] 在一个实施例中，第一分析单元被配置成：

在反编译代码中查找涉及隐私数据的关键指令，

判断关键指令和与该关键指令相关的其它指令是否执行与外界进行数据交换的操作，

将关键指令和与该关键指令相关的其它指令中的执行与外界进行数据交换的操作的指令标记为可能涉及隐私泄露的指令。

[0035] 再如图所示，该系统还可以包括运行中动态分析装置，该装置包括：

监控单元，用于记录应用程序在运行时的动态数据，

第二分析单元，用于分析动态数据的行为，识别涉及隐私泄露的行为。

[0036] 这里，监控单元可以被部署在 Android 系统底层从而避免给系统带来过多的负载。被加载到 Android 系统的监控单元将记录的动态数据发送到第二分析单元以供进一步分析。

[0037] 在一个实施例中，所述第二分析单元被配置成：

分析动态数据中的与通过静态分析识别的可能涉及隐私泄露的指令相关的部分，
根据预定的分析算法识别涉及隐私泄露的行为。

[0038] 这里，第二分析单元还从第一分析单元接收可能涉及隐私泄露的指令。

[0039] 通过以上实施方式的描述，本领域中的普通技术人员能够理解，在不偏离本发明的精神和范围的情况下，还可以对本发明的具体实施方式作各种变更和替换。这些变更和替换都落在本发明权利要求书所限定的范围内。

权利要求

1. 一种分析 Android 应用程序的方法，其特征在于，包括以下步骤：

运行前静态分析，该步骤包括：

提取应用程序文件中的涉及逻辑流程的二进制文件，

对该二进制文件进行反编译得到反编译代码，

对该反编译代码进行隐私泄露分析，识别可能涉及隐私泄露的指令。

2. 如权利要求 1 所述的方法，其特征在于，

上述隐私泄露分析步骤包括：

在反编译代码中查找涉及隐私数据的关键指令，

判断关键指令和与该关键指令相关的其它指令是否执行与外界进行数据交换的操作，

将关键指令和与该关键指令相关的其它指令中的执行与外界进行数据交换的操作的指令标记为可能涉及隐私泄露的指令。

3. 如权利要求 1 或 2 所述的方法，其特征在于，该方法还包括以下步骤：

运行中动态分析，该步骤包括：

记录应用程序在运行时的动态数据，

分析动态数据的行为，识别涉及隐私泄露的行为。

4. 如权利要求 3 所述的方法，其特征在于，

分析动态数据的行为的步骤包括：

分析动态数据中的与通过静态分析识别的可能涉及隐私泄露的指令相关的部分，

根据预定的分析算法识别涉及隐私泄露的行为。

5. 如权利要求 4 所述的方法，其特征在于，

上述隐私泄露分析步骤还包括：

生成静态分析报告。

6. 如权利要求 5 所述的方法，其特征在于，

运行中动态分析的步骤还包括：

生成隐私泄露安全分析报告。

7. 一种分析 Android 应用程序的系统，其特征在于，包括：

运行前静态分析装置，该装置包括：

提取单元，用于提取应用程序文件中的涉及逻辑流程的二进制文件，

反编译单元，用于对该二进制文件进行反编译得到反编译代码，

第一分析单元，用于对该反编译代码进行隐私泄露分析，识别可能涉及隐私泄露的指令。

8. 如权利要求 1 所述的系统，其特征在于，

所述第一分析单元被配置成：

在反编译代码中查找涉及隐私数据的关键指令，

判断关键指令和与该关键指令相关的其它指令是否执行与外界进行数据交换的操作，

将关键指令和与该关键指令相关的其它指令中的执行与外界进行数据交换的操作的指令标记为可能涉及隐私泄露的指令。

9. 如权利要求 7 或 8 所述的系统，其特征在于，该系统还包括：

运行中动态分析装置，该装置包括：

监控单元，用于记录应用程序在运行时的动态数据，

第二分析单元，用于分析动态数据的行为，识别涉及隐私泄露的行为。

10. 如权利要求 9 所述的系统，其特征在于，

所述第二分析单元被配置成：

分析动态数据中的与通过静态分析识别的可能涉及隐私泄露的指令相关的部分，

根据预定的分析算法识别涉及隐私泄露的行为。

11. 如权利要求 10 所述的系统，其特征在于，

所述第一分析单元还被配置成：

生成静态分析报告。

12. 如权利要求 11 所述的系统，其特征在于，

所述第二分析单元还被配置成：

生成隐私泄露安全分析报告。

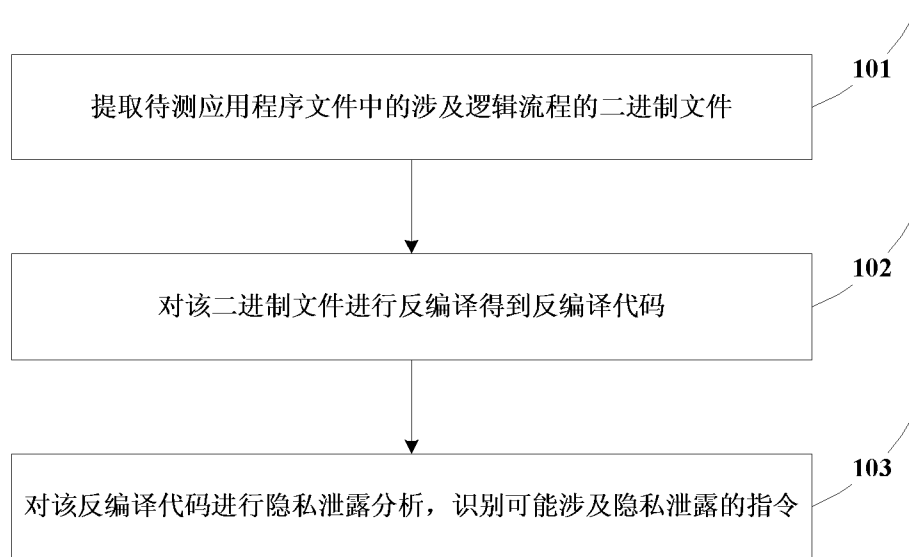


图 1

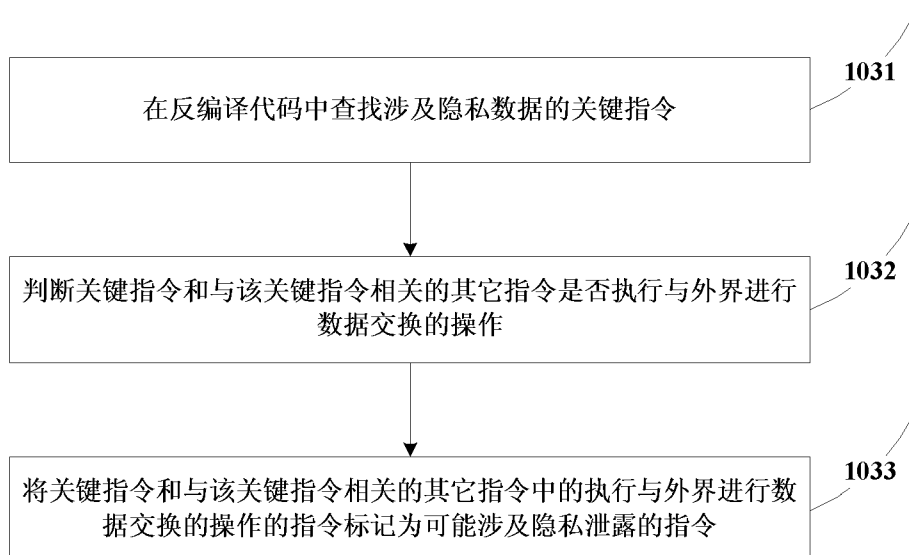


图 2

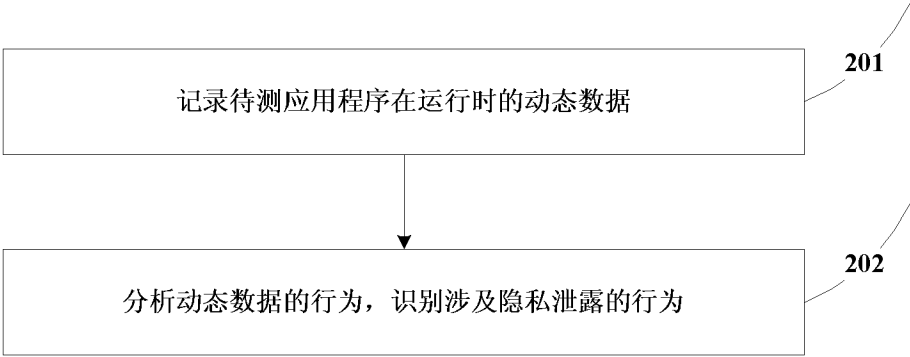


图 3

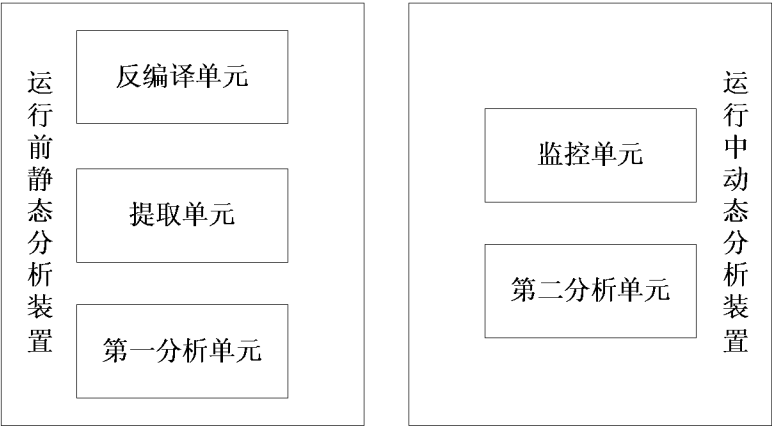


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/090302**A. CLASSIFICATION OF SUBJECT MATTER**

G06F 21/52 (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)

IPC: G06F 21

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, DWPI: android, application, APK, analyze, decompile, binary, privacy, leakage

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102737190 A (FUDAN UNIVERSITY), 17 October 2012 (17.10.2012), description, paragraphs [0007]-[0027]	1-12
Y	CN 102779255 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 14 November 2012 (14.11.2012), description, paragraphs [0048]-[0051] and [0071]-[0079]	1-12
A	CN 103309808 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES et al.), 18 September 2013 (18.09.2013), the whole document	1-12

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

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search
15 January 2015 (15.01.2015)Date of mailing of the international search report
04 February 2015 (04.02.2015)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

JIA, YongTelephone No.: (86-10) **62411850**

International application No.
PCT/CN2014/090302

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2014/090302

A. 主题的分类

G06F 21/52 (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 21

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, DWPI: 安卓, 应用, 分析, 反编译, 二进制, 隐私, 泄露, android, application, APK, analyze, decompile, binary, privacy, leakage

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
Y	CN 102737190 A (复旦大学) 2012年 10月 17日 (2012 - 10 - 17) 说明书第【0007】-【0027】段	1-12
Y	CN 102779255 A (腾讯科技深圳有限公司) 2012年 11月 14日 (2012 - 11 - 14) 说明书第【0048】-【0051】、【0071】-【0079】段	1-12
A	CN 103309808 A (中国科学院信息工程研究所等) 2013年 9月 18日 (2013 - 09 - 18) 全文	1-12

☐ 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

2015年 1月 15日

国际检索报告邮寄日期

2015年 2月 04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)
北京市海淀区蓟门桥西土城路6号
100088 中国

授权官员

贾勇

传真号 (86-10) 62019451

电话号码 (86-10) 62411850

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/090302

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	102737190	A	2012年 10月 17日	无			
CN	102779255	A	2012年 11月 14日	US	2014165199	A1	2014年 6月 12日
				CN	102779255	B	2014年 11月 12日
				WO	2014012441	A1	2014年 1月 23日
CN	103309808	A	2013年 9月 18日	WO	2014198171	A1	2014年 12月 18日

表 PCT/ISA/210 (同族专利附件) (2009年7月)