

(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
2018 年 10 月 4 日 (04.10.2018)



(10) 国际公布号
WO 2018/177394 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

北省武汉市东湖开发区软件园东路1号软件产业4.1期B1栋11楼, Hubei 430073 (CN)。

(21) 国际申请号: PCT/CN2018/081256

(22) 国际申请日: 2018 年 3 月 30 日 (30.03.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710211363.3 2017年3月31日 (31.03.2017) CN

(71) 申请人: 武汉斗鱼网络科技有限公司
(**WUHAN DOUYU NETWORK TECHNOLOGY CO., LTD.**) [CN/CN]; 中国湖北省武汉市东湖开发区软件园东路1号软件产业4.1期B1栋11楼, Hubei 430073 (CN)。

(72) 发明人: 周志刚(**ZHOU, Zhigang**); 中国湖北省武汉市东湖开发区软件园东路1号软件产业4.1期B1栋11楼, Hubei 430073 (CN)。张文明(**ZHANG, Wenming**); 中国湖北省武汉市东湖开发区软件园东路1号软件产业4.1期B1栋11楼, Hubei 430073 (CN)。陈少杰(**CHEN, Shaojie**); 中国湖

(74) 代理人: 北京众达德权知识产权代理有限公司(**BEIJING ZHONGDA DEQUAN IP AGENCY CO., LTD.**); 中国北京市朝阳区朝外大街乙12号办公楼9层0-1009A, Beijing 100020 (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, 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,

(54) Title: METHOD AND DEVICE FOR PROTECTING ANDROID SO FILE

(54) 发明名称: 一种安卓SO文件的保护方法及装置

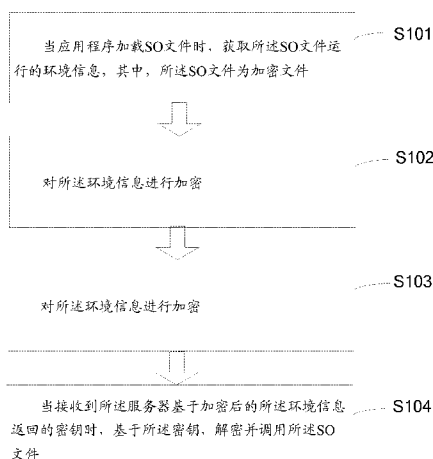


图 1

S101 When an application program loads an SO file, acquire environmental information regarding the environment in which the SO file operates, wherein the SO file is an encrypted file
S102 Encrypt the environmental information
S103 Encrypt the environmental information
S104 Upon receiving a key returned by the server on the basis of the encrypted environmental information, decrypt, on the basis of the key, and invoke the SO file

(57) Abstract: Disclosed are a method and device for protecting an Android SO file. The method comprises: when an application program loads an SO file, acquiring environmental information regarding the environment in which the SO file operates, wherein the SO file is an encrypted file; encrypting the environmental information; transmitting the encrypted environmental information to a server; and upon receiving a key returned by the server on the basis of the encrypted environmental information, decrypting, on the basis of the key, and invoking the SO file. The method and device provided in the present application can address the technical problem of low security in the art resulted from an SO file being easy to be obtained and misappropriated, and thus can improve the security of an SO file.

(57) 摘要: 本发明公开一种安卓SO文件的保护方法及装置, 该方法包括: 当应用程序加载SO文件时, 获取所述SO文件运行的环境信息, 其中, 所述SO文件为加密文件; 对所述环境信息进行加密; 发送加密后的所述环境信息至服务器; 当接收到所述服务器基于加密后的所述环境信息返回的密钥时, 基于所述密钥, 解密并调用所述SO文件。本申请提供的方法和装置可以解决现有技术中SO文件容易被轻易获取和盗用, 存在的安全性低的技术问题。实现了提高SO文件的安全性的技术效果。

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))。

一种安卓 S0 文件的保护方法及装置

技术领域

本发明涉及计算机技术领域，尤其涉及一种安卓（Andriod）S0文件的保护方法及装置。

5

背景技术

随着移动设备的日益普及，移动应用产业尤其是Andriod应用得到飞速的发展，相应的，其开发模式和代码框架也都发生了巨大的变化。由于程序的功能日益丰富，为了节约开发时间，模块化开发已经成为一种开发趋势，且

10 Android系统也提供独立模块的文件以及独立模块的加载和使用方式。

独立的模块文件称为S0文件，该文件可以使用C或者C++语言开发。模块开发者为了保障程序的可用性和易用性，往往会将S0文件的接口设计的更为简洁和好用。在Android程序发布时，独立的S0文件会随之一同发布到用户的终端中，任何人就可以轻易的获取到所有的S0文件，并且通过分析轻易的获取S0
15 文件的所有接口，从而可以将该S0文件使用到自己的Android程序中，以盗取该S0文件程序开发厂商的研发成果。目前，急需一种S0文件的保护方法，来防止其他人员直接盗用厂商辛苦开发出的S0文件。

可见，现有技术中S0文件容易被轻易获取和盗用，存在安全性低的技术问题。

20

发明内容

本发明提供一种安卓S0文件的保护方法及装置，用以解决现有技术中S0文件容易被轻易获取和盗用，存在的安全性低的技术问题。

一方面，本发明提供了一种安卓S0文件的保护方法，包括：

25 当应用程序加载S0文件时，获取所述S0文件运行的环境信息，其中，所述S0文件为加密文件；

对所述环境信息进行加密；

发送加密后的所述环境信息至服务器；

30 当接收到所述服务器基于加密后的所述环境信息返回的密钥时，基于所述密钥，解密并调用所述S0文件。

可选的，所述S0文件中加密的数据包括：常量数据和/或表格数据。

可选的，所述获取所述应用程序中S0文件运行的环境信息，包括：调用S0文件的初始化函数；基于所述初始化函数，获取所述S0文件的运行的环境信息，所述环境信息包括以下任意一种或多种的组合：所述S0文件的加载内存地址范

围、当前内存段的权限或所述S0文件的路径名称。

可选的，所述对所述环境信息进行加密，包括：获取所述应用程序的程序包名称；基于所述程序包名称，对所述环境信息进行加密。

- 5 可选的，所述基于所述程序包名称，对所述环境信息进行加密，包括：计算所述程序包名称的MD5值；基于所述MD5值，对所述环境信息进行加密。

可选的，在所述发送加密后的所述环境信息至服务器后，还包括：当没有接收到所述服务器基于加密后的所述环境信息返回的密钥时，退出对所述S0文件的调用。

另一方面，提供一种安卓S0文件的保护方法，包括：

- 10 接收客户端发送的加密后的环境信息，其中，所述环境信息用于表征应用程序加载的S0文件的运行环境；

判断所述加密后的环境信息是否符合预设要求；

当所述加密后的环境信息符合预设要求时，发送密钥至所述客户端，以使所述客户端能基于所述密钥，解密并调用所述S0文件。

- 15 可选的，所述判断所述加密后的环境信息是否符合预设要求，包括以下任意一种或多种的组合：判断是否能够通过预设应用程序的程序包名称，对所述加密后的环境信息进行解密；或者判断所述环境信息中表征的S0文件的类型是否满足预设类型要求；或者判断所述环境信息中表征的S0文件的参数是否满足预设参数要求。

- 20 再一方面，提供一种安卓S0文件的保护装置，所述装置为客户端，包括：获取模块，用于当应用程序加载S0文件时，获取所述S0文件运行的环境信息，其中，所述S0文件为加密文件；

加密模块，用于对所述环境信息进行加密；

第一发送模块，用于发送加密后的所述环境信息至服务器；

- 25 解密模块，用于当接收到所述服务器基于加密后的所述环境信息返回的密钥时，基于所述密钥，解密并调用所述S0文件。

再一方面，提供一种安卓S0文件的保护装置，所述装置为服务器，包括：

接收模块，用于接收客户端发送的加密后的环境信息，其中，所述环境信息用于表征应用程序加载的S0文件的运行环境；

- 30 判断模块，用于判断所述加密后的环境信息是否符合预设要求；

第二发送模块，用于当所述加密后的环境信息符合预设要求时，发送密钥至所述客户端，以使所述客户端能基于所述密钥，解密并调用所述S0文件。

本发明实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

本申请实施例提供的方法及装置,预先对S0文件进行加密,并设置在客户端的应用程序加载S0文件时,需要先获取所述S0文件运行的环境信息,并将加密后的所述环境信息发送至服务器,以供服务器根据所述环境信息来判断是否允许所述应用程序调用该S0文件,只有收到服务器返回的密钥后,客户端才能根据密钥解密并调用所述S0文件,以避免了不符合要求的应用程序对S0文件的盗用,有效提高了S0文件的安全性。

上述说明仅是本发明技术方案的概述,为了能够更清楚了解本发明的技术手段,而可依照说明书的内容予以实施,并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂,以下特举本发明的具体实施方式。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍,显而易见地,下面描述中的附图是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

图1为本发明实施例中安卓S0文件的保护方法的流程图一;

图2为本发明实施例中安卓S0文件的保护方法的流程图二;

图3为本发明实施例中安卓S0文件的保护装置的结构示意图一;

图4为本发明实施例中安卓S0文件的保护装置的结构示意图二。

具体实施方式

本申请实施例通过提供一种安卓S0文件的保护方法及装置,用以解决现有技术中S0文件容易被轻易获取和盗用,存在的安全性低的技术问题。实现了提高S0文件的安全性的技术效果。

本申请实施例中的技术方案,总体思路如下:

当应用程序加载S0文件时,获取所述S0文件运行的环境信息,其中,所述S0文件为加密文件;对所述环境信息进行加密;发送加密后的所述环境信息至服务器;当接收到所述服务器基于加密后的所述环境信息返回的密钥时,基于所述密钥,解密并调用所述S0文件。

上述方法通过预先对S0文件进行加密,并设置在客户端的应用程序加载S0文件时,需要先获取所述S0文件运行的环境信息,并将加密后的所述环境信息发送至服务器,以供服务器根据所述环境信息来判断是否允许所述应用程序调用该S0文件,只有收到服务器返回的密钥后,客户端才能根据密钥解密并调用所述S0文件,以避免了不符合要求的应用程序对S0文件的盗用,有效提高了S0

文件的安全性。

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作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。

实施例一

本实施例提供一种安卓S0文件的保护方法，如图1所示，该方法包括：

- 步骤S101，当应用程序加载S0文件时，获取所述S0文件运行的环境信息，其中，所述S0文件为加密文件；
- 步骤S102，对所述环境信息进行加密；
- 步骤S103，发送加密后的所述环境信息至服务器；
- 步骤S104，当接收到所述服务器基于加密后的所述环境信息返回的密钥时，基于所述密钥，解密并调用所述S0文件。

- 需要说明的是，本实施例提供的方法应用于客户端，所述客户端与所述服务器通过无线或有限网络进行连接，以实现通信。

在具体实施过程中，所述客户端可以为智能手机，平板电脑或台式机，在此也不作限制。所述服务器可以是一台独立的服务器，也可以是多台服务器组成的服务器群，在此也不作限制。

- 下面，结合图1详细介绍本实施例提供的安卓S0文件的保护方法的具体实施步骤：

首先，执行步骤S101，当应用程序加载S0文件时，获取所述S0文件运行的环境信息，其中，所述S0文件为加密文件。

- 具体来讲，需要预先对S0文件进行加密，具体可以是在编写S0文件时对其进行加密。

进一步，考虑到在编写核心S0文件的模块代码时，其中会使用到一些常量的表格，或者是函数使用的参数等，故可以设置主要对S0文件中使用的常量数据或者表格数据进行加密，以保护最核心的内容。

- 在具体实施过程中，对所述S0文件的加密可以使用非对称加密，也可以使用对称加密算法，在此不作限制。

举例来说，可以预先使用非对称加密算法来对S0文件中表格数据进行加密后存储，调用S0文件时则需要从服务器获取到正确的密钥，即KEY值，才能解密出这些表格数据，从而才能使用S0文件的模块功能，如果获取不到正确的KEY值，则无法使用S0文件的功能。对S0文件的具体加密过程可以如下：

首先，服务器使用RSA算法来生成一对公钥PublicKey和私钥SecretKey。即通过RSA.CreatePairKey(SecretKey, PublicKey)命令，使用RSA算法来生成一对私钥PublicKey和私钥SecretKey。然后，服务器存储这对密钥，以供后续客户端请求下发私钥。

- 5 然后，使用RSA算法来对S0文件中使用的常量数据和表格数据进行加密。即调用RSA算法的加密接口来对常量表格进行加密。例如，Char g_gloabledata[size]为S0文件中使用的表格数据，RSA.encrypt则是RSA加密算法的接口，通过下述命令使用公钥PublicKey来对全局的表格数据进行加密：

```
Char g_gloabledata[size] = {.....};  
10       RSA.encrypt(g_gloabledata, size, PublicKey);
```

其中，Char g_gloabledata[size] = {.....}表征需要加密的表格数据，用加密后的数据替换S0文件中表格数据的内容，从而保证S0文件中存储的表格是已加密状态。

- 15 当对所述S0文件加密后，可以将加密后的S0文件随着Android的应用程序（APP）发布到客户端，当有应用程序要加载S0文件时，必须先获取所述S0文件运行的环境信息。

在本申请实施例中，所述获取所述S0文件运行的环境信息，包括：
调用S0文件的初始化函数；

- 20 基于所述初始化函数，获取所述S0文件的运行的环境信息，所述环境信息包括以下任意一种或多种的组合：所述S0文件的加载内存地址范围、当前内存段的权限或所述S0文件的路径名称。

- 具体来讲，可以预先在S0文件的初始化函数JNI_OnLoad中加入获取所述S0文件运行的环境信息，并对所述环境信息加密后再发送至服务器的指令，当应用程序加载S0文件是，必须调用S0文件的初始化函数JNI_OnLoad，则会触发获取所述S0文件运行的环境信息。
25

- 举例来讲，加入初始化函数中的获取所述环境信息的指令可以是：先定义
ProcessBuilder processBuilder = new ProcessBuilder(“cat
/proc/PID/maps”),以用来创建一个新的进程，其中PID是当前应用程序的ID，
其中“/proc/PID/maps”则标示获取当前程序的内存映射信息，包含S0的加载
30 信息；再执行process = processBuilder.start(),以执行创建的进程；再执行
is = process.getInputStream(),以获取进程的输出信息；然后，执行
ByteArrayOutputStream info = new ByteArrayOutputStream(),来定义一个
输出流；再下来，执行 while (is.read() != -1) { info.write(read); },
以通过编写一个While循环来将进程的输出信息写入到所述输出流中；然后，

执行`byte[] data = info.toByteArray()`，将输出流的信息转换到byte数组中；再执行`String result = new String(data)`，将byte数组的信息转换成一个字符串信息。例如，采用上述步骤获取的信息类似于如下一条SO文件的环境信息：

“4d575000-4d58a000 r-xp 00000000 03:06 736549 /lib/ld.so”

- 5 其中，4d575000-4d58a000标示SO文件的加载内存地址范围；r-xp则标示当前内存段的权限；/lib/ld.so则表示加载的SO文件的路径名称。

因此，根据所述环境信息能较好的判断出SO文件的加载范围和SO文件的路径名称。

在获取了所述环境信息后，执行步骤S102，对所述环境信息进行加密。

- 10 在具体实施过程中，对所述环境信息进行加密后再传送一方面是对所述环境信息的保护，另一方面能通过预先沟通好加密方式来帮助服务器判断所述应用程序是否允许调用所述SO文件。

- 在具体实施过程中，可以直接根据应用程序的程序包名称来对所述环境信息进行加密，即先获取所述应用程序的程序包名称，再基于所述程序包名称，
15 对所述环境信息进行加密。

进一步，可以根据应用程序的程序包名称的MD5值来对所述环境信息进行加密，即先计算所述程序包名称的MD5值，再基于所述MD5值，对所述环境信息进行加密。

- 具体来讲，由于每个应用程序的程序包名称都是不同的，所以获取应用程序
20 的程序包名称，然后对程序包名称计算其MD5值来做为获取到的客户端的环境信息加密使用的KEY值。而服务器存储有允许调用所述SO文件的应用程序的程序包名称，所以服务器会直接使用其认可的程序包名称来解密所述环境信息。而如果客户端是调用SO文件的应用程序不是服务器允许的应用程序，那么获取到的程序包名称则会不一样，从而服务器无法解密出正确的环境信息，从而可以拒绝给客户端发送解密的密钥。只有当服务器对所述环境信息解密成功
25 后，才能继续根据所述环境信息的本文内容来判断是否允许调用SO文件。

在具体实施过程中，应用程序的程序包名称可以采取下述方法获取：

首先，通过在SO文件中使用JNI层的接口来获取程序包名称的方法ID，具体实现代码可以为：

- 30 `jmethodID methodID_pack = (*env)->GetMethodID(env, context_clazz, "getPackageName", "()Ljava/lang/String;");`

然后，通过程序包名称的方法ID来获取当前应用程序的程序包名称，具体实现代码可以为：

`jstring application_package = (*env)->CallObjectMethod(env,`

context, methodID_pack);

其中, application-package则是应用程序的程序包名称。

当然, 应用程序的程序包名还可以通过像应用程序主程序发送请求, 或查询应用程序程序包地址的方式获取, 在此不作限制。

5 在具体实施过程中, 获取了应用程序的程序包名称后, 可以对所述程序包名称使用MD5算法来计算其MD5值, 以作为后续加密使用的KEY值。即设置KEY = MD5.create(application-package)。

10 当然, 在具体实施过程中, 所述KEY值除了可以设置为所述程序包名称和其MD5值外, 还可以为程序的类型标识, 程序名称的首字母或简称等, 在此不作限制。

在具体实施过程中, 确定KEY值后, 对所述环境信息的加密可以采取下述方法实现:

15 使用加密算法, 采用前述步骤确定的KEY值来对获取到的所述环境信息进行加密。例如, 可以采取加密算法AES, 使用AES.encrypt(KEY, result)命令来进行加密, 其中, KEY为之前计算得出的程序包名称或程序包名称的MD5值, result为之前获取的内存映射信息, 即所述环境信息。

当然, 在具体实施过程中, 也可以采用RSA加密算法和DES加密算法来对所述环境信息进行加密, 在此不作限制。

通过上述步骤就实现了在S0文件的初始化中获取环境信息并加密。

20 接下来, 执行步骤S103, 发送加密后的所述环境信息至服务器。

在本申请实施例, 所述服务器与所述客户端实现网络连接, 所述S0文件中存储有服务器的地址, 并设置有与服务器通信的功能, 所述服务器接收到所述环境信息后, 可以通过以下至少一种方式判断是否返回密钥至所述客户端:

第一种, 判断是否能按预设密码解密。

25 具体来讲, 设置客户端以应用程序的信息作为KEY值来对所述环境信息进行加密。而服务器存储有允许调用所述S0文件的应用程序的信息, 所以服务器可以直接使用其认可的应用程序的信息作为KEY值来解密所述环境信息, 例如, 客户端用调用S0文件的当前应用程序的程序包名称的MD5值来加密, 对应的服务器用允许调用S0文件的应用程序的程序包名称的MD5值来解密。如果客户端
30 调用S0文件的当前应用程序不是服务器允许的应用程序, 那么客户端用于加密的程序信息与客户端解密的程序信息则会不一样, 从而服务器无法解密出正确
的环境信息, 从而拒绝给客户端发送解密的密钥。只有当服务器对所述环境信息解密成功后, 才能继续根据所述环境信息的本文内容来判断是否允许调用S0文件。

需要说明的是,服务器端使用的解密算法需要与客户端使用的加密算法预先对应设置。

举例来说,客户端采用AES算法,以当前应用程序的程序包名称的MD5值作为KEY值,来对获得的所述环境信息进行加密,服务器收到客户端上报的加密后环境信息后,使用同样的AES算法并且使用允许调用S0文件的程序包名称的MD5做为KEY值来对所述环境信息进行解密。如果解密失败,拒绝给客户端发送解密的密钥,如果解密成功,再基于所述环境信息的具体内容进行进一步判断或直接发送密钥。

服务器端使用MD5做为KEY值来对所述环境信息进行解密的方法为:

首先,使用允许调用S0文件的应用程序的程序包名称计算MD5值。具体命令为: `KEY = MD5.create(application-package);`

然后,使用AES算法来对上报的数据进行解密。具体命令为:
`AES.decrypt(KEY, result)。`

第二种,或者判断所述环境信息中表征的S0文件的类型或参数是否满足预设要求。

具体来讲,获取的当前环境信息本文是获取当前应用程序所加载的S0文件的环境信息,因为不同的应用程序所需要加载的S0文件是不一样的,所以根据获取加载的S0文件的环境信息可以很好的区分应用程序。

即在解密后,对所述环境信息中加载的S0文件的类型和参数进行判断,由于服务器中预先存储有加载的S0文件的信息,例如,存储有正常的程序会加载哪些必要的S0文件,不会加载哪些S0文件的信息;或者,正常的程序加载的每个S0文件的加载内存区间,故服务器根据预存的加载的S0文件的信息,可以很容易的判断出客户端上报的所述环境信息是否是正确的应用程序加载S0文件时的信息。如果服务器判断出客户端上报的所述环境信息符合正确的应用程序的加载信息,则向客户端下发解密使用的密钥(SecretKey),否则向客户端下发拒绝信息。

当然,在具体实施过程中,结合上述第一种和第二种方法来一同判断是否返回密钥,能够增加判断的准确性。即先采取第一种方法判断能否对所述环境信息进行解密,如果解密失败则拒绝返回密钥,如果解密成功再采取第二种方法进一步判断所述环境信息的具体内容是否符合要求,符合则返回密钥,不符合则拒绝返回密钥。

再下来,执行步骤S104,当接收到所述服务器基于加密后的所述环境信息返回的密钥时,基于所述密钥,解密并调用所述S0文件。

具体来讲,如果客户端接收到所述服务器下发的密钥信息,则对S0文件进

行解密,具体可以是对S0文件中的常量数据或表格数据进行解密,从而S0文件才能正确的使用。具体的解密指令可以为:RSA.decrypt(g_gloabledata,size,SecretKey);

5 进一步,如果客户端没有接收到所述服务器基于加密后的所述环境信息返回的密钥时,退出对所述S0文件的调用。

进一步,退出对所述S0文件的调用后,可以在所述客户端上输出初始化失败信息以提醒用户。

10 本实施例提供的方法,对S0文件中所使用到的关键性的一些常量数据或者表格数据使用加密算法来进行加密,在应用程序调用S0文件时,会对S0文件的使用方程序进行验证,如果验证不成功则无法使用S0文件的所有功能,从而可以对S0文件进行保护。具体来讲,在客户端登陆启动应用程序后,应用程序加载S0文件,而在S0文件进行初始化的同时,会获取当前S0文件所处的环境信息,获取到环境信息后会通过S0文件中编写的与服务器的网络连接功能来进行发送,而服务器则会根据上报的所述环境信息判断当前使用方程序是否是正确的应用程序。只有当服务器校验通过时,才会将解密密钥下发至客户端,才能够正确的解密出需要使用的常量数据或者表格数据,否则无法获取到解密密钥,从而无法使用S0文件中的功能。

15 基于同一发明构思,本申请还提供了与实施例一中安卓S0文件的保护方法对应的应用于服务器端的安卓S0文件的保护方法,详见实施例二。

20 实施例二

本实施例提供了一种安卓S0文件的保护方法,如图2所示,该方法包括:

步骤S201,接收客户端发送的加密后的环境信息,其中,所述环境信息用于表征应用程序加载的S0文件的运行环境;

步骤S202,判断所述加密后的环境信息是否符合预设要求;

25 步骤S203,当所述加密后的环境信息符合预设要求时,发送密钥至所述客户端,以使所述客户端能基于所述密钥,解密并调用所述S0文件。

需要说明的是,本实施例提供的方法应用于服务器端,所述服务器端与实施例一中的客户端通过无线或有限网络进行连接,以实现通信。

30 在具体实施过程中,所述客户端可以为智能手机,平板电脑或台式机,在此也不作限制。所述服务器可以是一台独立的服务器,也可以是多台服务器组成的服务器群,在此也不作限制。

在本申请实施例中,所述判断所述加密后的环境信息是否符合预设要求,包括以下任意一种或多种的组合:

判断是否能通过预设应用程序的程序包名称,对所述加密后的环境信息进行

行解密；或者

判断所述环境信息中表征的S0文件的类型是否满足预设类型要求；或者判断所述环境信息中表征的S0文件的参数是否满足预设参数要求。

5 由于本发明实施例二所介绍的方法与实施例一中所介绍的方法属于同一发明构思，而实施例二中判断所述加密后的环境信息是否符合预设要求的具体实施步骤及原理也在实施例一中做了详细描述，基于实施例一本领域技术人员应该了解实施例二提供方法的实施步骤及原理，故而在不再赘述。

基于同一发明构思，本申请还提供了与实施例一中安卓S0文件的保护方法对应的装置，详见实施例三。

10 实施例三

本实施例提供一种安卓S0文件的保护装置，所述装置为客户端，如图3所示，包括：

获取模块301，用于当应用程序加载S0文件时，获取所述S0文件运行的环境信息，其中，所述S0文件为加密文件；

15 加密模块302，用于对所述环境信息进行加密；

第一发送模块303，用于发送加密后的所述环境信息至服务器；

解密模块304，用于当接收到所述服务器基于加密后的所述环境信息返回的密钥时，基于所述密钥，解密并调用所述S0文件。

20 在具体实施过程中，所述客户端可以为智能手机，平板电脑或台式机，在此不作限制。

由于本发明实施例三所介绍的装置，为实施本发明实施例一的安卓S0文件的保护方法所采用的装置，故而基于本发明实施例一所介绍的方法，本领域所属人员能够了解该装置的具体结构及变形，故而在不再赘述。凡是本发明实施例一的方法所采用的装置都属于本发明所欲保护的范围。

25 基于同一发明构思，本申请还提供了与实施例二中安卓S0文件的保护方法对应的装置，详见实施例四。

实施例四

本实施例提供一种安卓S0文件的保护装置，所述装置为服务器，如图4所示，包括：

30 接收模块401，用于接收客户端发送的加密后的环境信息，其中，所述环境信息用于表征应用程序加载的S0文件的运行环境；

判断模块402，用于判断所述加密后的环境信息是否符合预设要求；

第二发送模块403，用于当所述加密后的环境信息符合预设要求时，发送密钥至所述客户端，以使所述客户端能基于所述密钥，解密并调用所述S0文件。

在本申请实施例中，所述服务器可以是一台独立的服务器，也可以是多台服务器组成的服务器群，在此不作限制。

5 由于本发明实施例四所介绍的装置，为实施本发明实施例二的安卓S0文件的保护方法所采用的装置，故而基于本发明实施例二所介绍的方法，本领域所属人员能够了解该装置的具体结构及变形，故而在此不再赘述。凡是本发明实施例二的方法所采用的装置都属于本发明所欲保护的范围。

本申请实施例中提供的技术方案，至少具有如下技术效果或优点：

10 本申请实施例提供的方法及装置，预先对S0文件进行加密，并设置在客户端的应用程序加载S0文件时，需要先获取所述S0文件运行的环境信息，并将加密后的所述环境信息发送至服务器，以供服务器根据所述环境信息来判断是否允许所述应用程序调用该S0文件，只有收到服务器返回的密钥后，客户端才能根据密钥解密并调用所述S0文件，以避免了不符合要求的应用程序对S0文件的盗用，有效提高了S0文件的安全性。

15 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

20 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

25 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

30 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基

本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

- 显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的精神和范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。
- 5

权 利 要 求

1、一种安卓S0文件的保护方法，其特征在于，包括：

当应用程序加载S0文件时，获取所述S0文件运行的环境信息，其中，所述S0文件为加密文件；

5 对所述环境信息进行加密；

发送加密后的所述环境信息至服务器；

当接收到所述服务器基于加密后的所述环境信息返回的密钥时，基于所述密钥，解密并调用所述S0文件。

10 2、如权利要求1所述的方法，其特征在于，所述S0文件中加密的数据包括：常量数据和/或表格数据。

3、如权利要求1所述的方法，其特征在于，所述获取所述S0文件运行的环境信息，包括：

调用S0文件的初始化函数；

15 基于所述初始化函数，获取所述S0文件的运行的环境信息，所述环境信息包括以下任意一种或多种的组合：所述S0文件的加载内存地址范围、当前内存段的权限或所述S0文件的路径名称。

4、如权利要求1所述的方法，其特征在于，所述对所述环境信息进行加密，包括：

获取所述应用程序的程序包名称；

20 基于所述程序包名称，对所述环境信息进行加密。

5、如权利要求4所述的方法，其特征在于，所述基于所述程序包名称，对所述环境信息进行加密，包括：

计算所述程序包名称的MD5值；

基于所述MD5值，对所述环境信息进行加密。

25 6、如权利要求1-5任一所述的方法，其特征在于，在所述发送加密后的所述环境信息至服务器后，还包括：

当没有接收到所述服务器基于加密后的所述环境信息返回的密钥时，退出对所述S0文件的调用。

7、一种安卓S0文件的保护方法，其特征在于，包括：

30 接收客户端发送的加密后的环境信息，其中，所述环境信息用于表征应用程序加载的S0文件的运行环境；

判断所述加密后的环境信息是否符合预设要求；

当所述加密后的环境信息符合预设要求时，发送密钥至所述客户端，以使所述客户端能基于所述密钥，解密并调用所述S0文件。

8、如权利要求7所述的方法，其特征在于，所述判断所述加密后的环境信息是否符合预设要求，包括以下任意一种或多种的组合：

判断是否能够通过预设应用程序的程序包名称，对所述加密后的环境信息进行解密；或者

- 5 判断所述环境信息中表征的S0文件的类型是否满足预设类型要求；或者
 判断所述环境信息中表征的S0文件的参数是否满足预设参数要求。

9、一种安卓S0文件的保护装置，其特征在于，所述装置为客户端，包括：获取模块，用于当应用程序加载S0文件时，获取所述S0文件运行的环境信息，其中，所述S0文件为加密文件；

- 10 加密模块，用于对所述环境信息进行加密；
 第一发送模块，用于发送加密后的所述环境信息至服务器；
 解密模块，用于当接收到所述服务器基于加密后的所述环境信息返回的密
 钥时，基于所述密钥，解密并调用所述S0文件。

- 10、一种安卓S0文件的保护装置，其特征在于，所述装置为服务器，包括：
15 接收模块，用于接收客户端发送的加密后的环境信息，其中，所述环境信
 息用于表征应用程序加载的S0文件的运行环境；

 判断模块，用于判断所述加密后的环境信息是否符合预设要求；

 第二发送模块，用于当所述加密后的环境信息符合预设要求时，发送密钥
 至所述客户端，以使所述客户端能基于所述密钥，解密并调用所述S0文件。

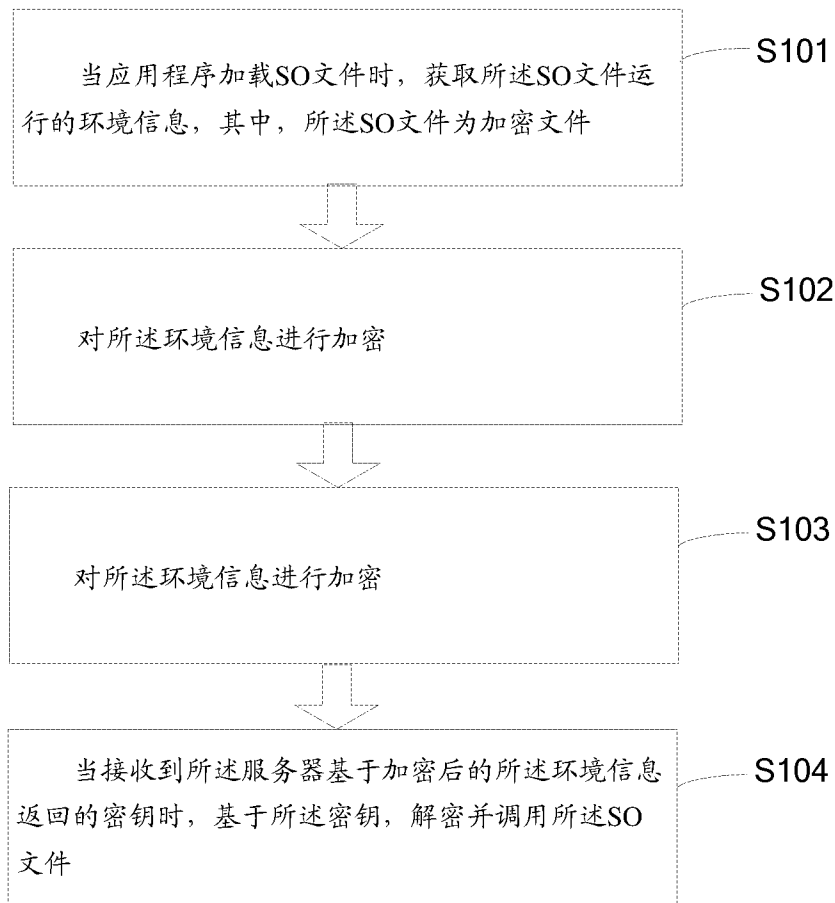


图 1

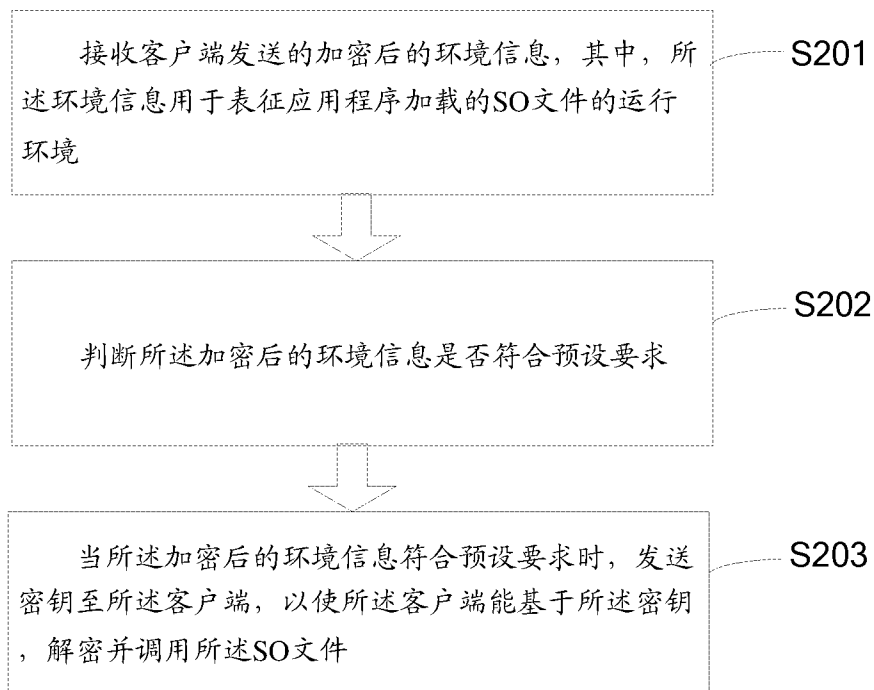


图 2

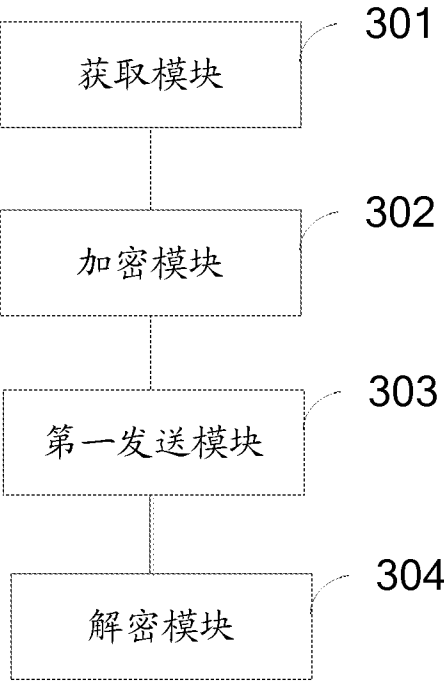


图 3



图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/081256

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

H04L; H04W

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)

CPRSABS; CNTXT; VEN; CNKI: 应用, 程序, 文件, 安卓, 加密, 解密, 密钥, 环境, 信息, 终端, 客户端, 服务器, 发送, 接收, application, file, andriod, encrypt, decrypt, key, circumstance, information, terminal, client, server, send, receive

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107196907 A (WUHAN DOUYU NETWORK TECHNOLOGY CO., LTD.) 22 September 2017 (22.09.2017), claims1-10	1-10
A	CN 107135408 A (WUHAN DOUYU NETWORK TECHNOLOGY CO., LTD.) 05 September 2017 (05.09.2017), entire document	1-10
A	CN 106899463 A (NINGXIA KAISUDE TECHNOLOGY CO., LTD.) 27 June 2017 (27.06.2017), entire document	1-10
A	CN 106203009 A (ZHUHAI MEIZU TECHNOLOGY CO., LTD.) 07 December 2016 (07.12.2016), entire document	1-10

☐ 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 03 May 2018	Date of mailing of the international search report 23 May 2018
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 CHENG, Dong Telephone No. (86-10) 62411276

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/081256

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 107196907 A	22 September 2017	None	
CN 107135408 A	05 September 2017	None	
CN 106899463 A	27 June 2017	None	
CN 106203009 A	07 December 2016	None	

国际检索报告

国际申请号

PCT/CN2018/081256

A. 主题的分类 H04L 29/06 (2006.01) 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) H04L; H04W 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)) CPRSABS; CNTXT; VEN; CNKI: 应用, 程序, 文件, 安卓, 加密, 解密, 密钥, 环境, 信息, 终端, 客户端, 服务器, 发送, 接收, application, file, andriod, encrypt, decrypt, key, circumstance, information, terminal, client, server, send, receive																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 107196907 A (武汉斗鱼网络科技有限公司) 2017年 9月 22日 (2017 - 09 - 22) 权利要求书1-10</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 107135408 A (武汉斗鱼网络科技有限公司) 2017年 9月 5日 (2017 - 09 - 05) 全文</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 106899463 A (宁夏凯速德科技有限公司) 2017年 6月 27日 (2017 - 06 - 27) 全文</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 106203009 A (珠海市魅族科技有限公司) 2016年 12月 7日 (2016 - 12 - 07) 全文</td> <td>1-10</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 107196907 A (武汉斗鱼网络科技有限公司) 2017年 9月 22日 (2017 - 09 - 22) 权利要求书1-10	1-10	A	CN 107135408 A (武汉斗鱼网络科技有限公司) 2017年 9月 5日 (2017 - 09 - 05) 全文	1-10	A	CN 106899463 A (宁夏凯速德科技有限公司) 2017年 6月 27日 (2017 - 06 - 27) 全文	1-10	A	CN 106203009 A (珠海市魅族科技有限公司) 2016年 12月 7日 (2016 - 12 - 07) 全文	1-10
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
PX	CN 107196907 A (武汉斗鱼网络科技有限公司) 2017年 9月 22日 (2017 - 09 - 22) 权利要求书1-10	1-10															
A	CN 107135408 A (武汉斗鱼网络科技有限公司) 2017年 9月 5日 (2017 - 09 - 05) 全文	1-10															
A	CN 106899463 A (宁夏凯速德科技有限公司) 2017年 6月 27日 (2017 - 06 - 27) 全文	1-10															
A	CN 106203009 A (珠海市魅族科技有限公司) 2016年 12月 7日 (2016 - 12 - 07) 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 2018年 5月 3日		国际检索报告邮寄日期 2018年 5月 23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		授权官员 程东 电话号码 86-(010)-62411276															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/081256

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	107196907	A	2017年 9月 22日	无	
CN	107135408	A	2017年 9月 5日	无	
CN	106899463	A	2017年 6月 27日	无	
CN	106203009	A	2016年 12月 7日	无	