



(12)发明专利

(10)授权公告号 CN 104036193 B

(45)授权公告日 2017.02.01

(21)申请号 201410210259.9

(22)申请日 2014.05.16

(65)同一申请的已公布的文献号

申请公布号 CN 104036193 A

(43)申请公布日 2014.09.10

(73)专利权人 北京金山安全软件有限公司

地址 100085 北京市海淀区小营西路33号  
二层东区

(72)发明人 刘文柱 沈江波 张楠 陈勇

(74)专利代理机构 广州三环专利代理有限公司

44202

代理人 郝传鑫 熊永强

(51)Int.Cl.

G06F 21/57(2013.01)

(56)对比文件

CN 103001817 A,2013.03.27,

CN 101296087 A,2008.10.29,

US 6073241 A,2000.06.06,

CN 102411690 A,2012.04.11,

Yajin zhou 等.《Detecting Passive

Content Leaks and Pollution in Android Applications》.《In Proceedings of the 20th Network and Distributed System Security Symposium》.2013,第1-16页.

审查员 张文波

权利要求书3页 说明书11页 附图5页

(54)发明名称

一种应用程序的本地跨域漏洞检测方法及装置

(57)摘要

本发明实施例公开了一种应用程序的本地跨域漏洞检测方法，包括：指示待检测应用程序访问第一通用资源标识符所指向的共享文件，所述共享文件不是所述待检测应用程序的共享文件；指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件，所述私有文件为所述待检测应用程序的非共享文件；若成功访问所述私有文件，则确定所述待检测应用程序存在本地跨域漏洞。本发明实施例还公开了一种应用程序的本地跨域漏洞检测装置。采用本发明实施例，可自动检测待检测应用程序的本地跨域漏洞，检测效率高。

S101  
指示待检测应用程序访问第一通用资源标识符所指向的共享文件，所述共享文件不是所述待检测应用程序的共享文件

S102  
指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件，所述私有文件为所述待检测应用程序的非共享文件

S103  
若成功访问所述私有文件，则确定所述待检测应用程序存在本地跨域漏洞

1. 一种应用程序的本地跨域漏洞检测方法,其特征在于,包括:

指示待检测应用程序访问第一通用资源标识符所指向的共享文件,所述共享文件不是所述待检测应用程序的共享文件,所述共享文件包括或加载有第二通用资源标识符;

指示所述待检测应用程序访问所述第二通用资源标识符所指向的私有文件,所述私有文件为所述待检测应用程序的非共享文件;

若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。

2. 如权利要求1所述的方法,其特征在于,所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件之前,所述方法还包括:

将所述待检测应用程序的安装包文件导入装有手机模拟器的计算机中;

根据所述安装包文件在所述手机模拟器中安装所述待检测应用程序。

3. 如权利要求2所述的方法,其特征在于,所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件之前,所述方法还包括:

检测所述待检测应用程序是否具有提供访问文件的功能;

若是,执行所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件的步骤;

若否,则确定所述待检测应用程序不存在本地跨域漏洞。

4. 如权利要求3所述的方法,其特征在于,所述检测所述待检测应用程序是否具有提供访问文件的功能之前,所述方法还包括:

对所述待检测应用程序进行解包处理,获取所述待检测应用程序的配置文件,所述配置文件记录有所述待检测应用程序是否具有提供访问文件的功能。

5. 如权利要求1-4任一项所述的方法,其特征在于,所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件,包括:

通过adb调试工具给所述待检测应用程序发送包括访问所述第一通用资源标识符所指向的共享文件的操作指令。

6. 如权利要求5所述的方法,其特征在于,所述指示所述待检测应用程序访问所述第二通用资源标识符所指向的私有文件,包括:

所述共享文件中包括访问所述第二通用资源标识符所指向的私有文件的JavaScript脚本程序,所述待检测应用程序访问所述共享文件后,通过所述JavaScript脚本程序自动去访问所述第二通用资源标识符所指向的私有文件。

7. 如权利要求5所述的方法,其特征在于,所述指示所述待检测应用程序访问所述第二通用资源标识符所指向的私有文件,包括:

所述共享文件中加载有所述第二通用资源标识符,所述第二通用资源标识符指向所述待检测应用程序的私有文件;

所述待检测应用程序访问所述共享文件后,若接收到访问所述私有文件的确认指令,访问所述第二通用资源标识符所指向的私有文件。

8. 如权利要求6或7所述的方法,其特征在于,所述方法还包括:

输出所述待检测应用程序的检测结果,所述检测结果包括漏洞信息和检测时间。

9. 如权利要求1所述的方法,其特征在于,所述待检测应用程序为Android浏览器或内置浏览器的Android应用程序。

10. 如权利要求1或9所述的方法,其特征在于,所述方法还包括:

记录所述待检测应用程序的特征信息,并将所述特征信息和所述检测结果上传至服务器。

11. 如权利要求10所述的方法,其特征在于,所述特征信息为所述待检测应用程序的包名和/或MD5值。

12. 如权利要求1所述的方法,其特征在于,所述方法还包括:

提示用户所述待检测应用程序存在所述本地跨域漏洞。

13. 如权利要求1或12所述的方法,其特征在于,所述方法还包括:

修复所述待检测应用程序中存在的本地跨域漏洞。

14. 如权利要求13所述的方法,其特征在于,所述修复所述待检测应用程序中存在的本地跨域漏洞,包括:

下载所述待检测应用程序的升级包文件,将所述升级包文件替换掉所述待检测应用程序中对应的原始文件。

15. 一种应用程序的本地跨域漏洞检测装置,其特征在于,包括:

第一指示模块,用于指示待检测应用程序访问第一通用资源标识符所指向的共享文件,所述共享文件不是所述待检测应用程序的共享文件,所述共享文件包括或加载有第二通用资源标识符;

第二指示模块,用于指示所述待检测应用程序访问所述第二通用资源标识符所指向的私有文件,所述私有文件为所述待检测应用程序的非共享文件;

确定模块,用于若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。

16. 如权利要求15所述的装置,其特征在于,所述装置还包括:

导入模块,用于将所述待检测应用程序的安装包文件导入装有手机模拟器的计算机中;

安装模块,用于根据所述安装包文件在所述手机模拟器中安装所述待检测应用程序。

17. 如权利要求16所述的装置,其特征在于,所述装置还包括:

检测模块,用于检测所述待检测应用程序是否具有提供访问文件的功能;

若是,指示所述待检测应用程序访问所述第一通用资源标识符所指向的共享文件;

若否,则确定所述待检测应用程序不存在本地跨域漏洞。

18. 如权利要求17所述的装置,其特征在于,所述装置还包括:

获取模块,用于对所述待检测应用程序进行解包处理,获取所述待检测应用程序的配置文件,所述配置文件记录有所述待检测应用程序是否具有提供访问文件的功能。

19. 如权利要求15-18任一项所述的装置,其特征在于,所述第一指示模块,还用于通过adb调试工具给所述待检测应用程序发送包括访问所述第一通用资源标识符所指向的共享文件的操作指令。

20. 如权利要求19所述的装置,其特征在于,所述第二指示模块还用于:

所述共享文件中包括访问所述第二通用资源标识符所指向的私有文件的JavaScript脚本程序,所述待检测应用程序访问所述共享文件后,通过所述JavaScript脚本程序自动去访问所述第二通用资源标识符所指向的私有文件。

21. 如权利要求19所述的装置，其特征在于，所述第二指示模块包括：

加载单元，用于所述共享文件中加载有所述第二通用资源标识符，所述第二通用资源标识符指向所述待检测应用程序的私有文件；

访问单元，用于所述待检测应用程序访问所述共享文件后，若接收到访问所述私有文件的确认指令，访问所述第二通用资源标识符所指向的私有文件。

22. 如权利要求20或21所述的装置，其特征在于，所述装置还包括：

输出模块，用于输出所述待检测应用程序的检测结果，所述检测结果包括漏洞信息和检测时间。

23. 如权利要求15所述的装置，其特征在于，所述待检测应用程序为Android浏览器或内置浏览器的Android应用程序。

24. 如权利要求15或23所述的装置，其特征在于，所述装置还包括：

上传模块，用于记录所述待检测应用程序的特征信息，并将所述特征信息和所述检测结果上传至服务器。

25. 如权利要求24所述的装置，其特征在于，所述特征信息为所述待检测应用程序的包名和/或MD5值。

26. 如权利要求15所述的装置，其特征在于，所述装置还包括：

提示模块，用于提示用户所述待检测应用程序存在所述本地跨域漏洞。

27. 如权利要求15或26所述的装置，其特征在于，所述装置还包括：

修复模块，用于修复所述待检测应用程序中存在的本地跨域漏洞。

28. 如权利要求27所述的装置，其特征在于，所述修复模块还用于下载所述待检测应用程序的升级包文件，将所述升级包文件替换掉所述待检测应用程序中对应的原始文件。

## 一种应用程序的本地跨域漏洞检测方法及装置

### 技术领域

[0001] 本发明涉及信息安全技术领域,尤其涉及一种应用程序的本地跨域漏洞检测方法及装置。

### 背景技术

[0002] 通常,应用程序的私有文件不允许其它任何文件或应用程序访问,只有应用程序本身可以访问该私有文件,若该私有文件被非自身应用程序的其它文件或应用程序所访问时,说明该应用程序存在本地跨域漏洞。

[0003] 当应用程序存在本地跨域漏洞时,黑客可利用该漏洞使终端自动执行一些黑客命令,如后台下载恶意软件、获取用户隐私,甚至篡改用户的重要信息等。因此,对该类漏洞的检测尤为重要。目前,常采用的解决方法是手动触发的方式来检测,对应用程序的安装文件进行反编译,然后在反编译后的原文件中查找特定代码,从而确定该应用程序是否存在本地跨域漏洞。然而,该方法需人工检测,检测效率低。

### 发明内容

[0004] 本发明实施例提供一种应用程序的本地跨域漏洞检测方法及装置,可自动检测待检测应用程序是否存在本地跨域漏洞,检测效率高。

[0005] 本发明实施例提供一种应用程序的本地跨域漏洞检测方法,包括:

[0006] 指示待检测应用程序访问第一通用资源标识符所指向的共享文件,所述共享文件不是所述待检测应用程序的共享文件;

[0007] 指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件,所述私有文件为所述待检测应用程序的非共享文件;

[0008] 若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。

[0009] 其中,所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件之前,所述方法还包括:

[0010] 将所述待检测应用程序的安装包文件导入装有手机模拟器的计算机中;

[0011] 根据所述安装包文件在所述手机模拟器中安装所述待检测应用程序。

[0012] 其中,所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件之前,所述方法还包括:

[0013] 检测所述待检测应用程序是否具有提供访问文件的功能;

[0014] 若是,执行所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件的步骤;

[0015] 若否,则确定所述待检测应用程序不存在本地跨域漏洞。

[0016] 其中,所述检测所述待检测应用程序是否具有提供访问文件的功能之前,还包括:

[0017] 对所述待检测应用程序进行解包处理,获取所述待检测应用程序的配置文件,所述配置文件记录有所述待检测应用程序是否具有提供访问文件的功能。

- [0018] 其中,所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件,包括:
- [0019] 通过adb调试工具给所述待检测应用程序发送包括访问所述第一通用资源标识符所指向的共享文件的操作指令。
- [0020] 其中,所述指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件,包括:
- [0021] 所述共享文件中包括访问所述第二通用资源标识符所指向的私有文件的JavaScript脚本程序,所述待检测应用程序访问所述共享文件后,通过所述JavaScript脚本程序自动去访问所述第二通用资源标识符所指向的私有文件。
- [0022] 其中,所述指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件,包括:
- [0023] 所述共享文件中加载有所述第二通用资源标识符,所述第二通用资源标识符指向所述待检测应用程序的私有文件;
- [0024] 所述待检测应用程序访问所述共享文件后,若接收到访问所述私有文件的确认指令,访问所述第二通用资源标识符所指向的私有文件。
- [0025] 其中,所述方法还包括:
- [0026] 输出所述待检测应用程序的检测结果,所述检测结果包括漏洞信息和检测时间。
- [0027] 其中,所述待检测应用程序为Android浏览器或内置浏览器的Android应用程序。
- [0028] 其中,所述方法还包括:
- [0029] 记录所述待检测应用程序的特征信息,并将所述特征信息和所述检测结果上传至服务器。
- [0030] 其中,所述特征信息为所述待检测应用程序的包名和/或MD5值。
- [0031] 其中,所述方法还包括:
- [0032] 提示用户所述待检测应用程序存在所述本地跨域漏洞。
- [0033] 其中,所述方法还包括:
- [0034] 修复所述待检测应用程序中存在的本地跨域漏洞。
- [0035] 其中,所述修复模块还用于下载所述待检测应用程序的升级包文件,将所述升级包文件替换掉所述待检测应用程序中对应的原始文件。
- [0036] 相应的,本发明实施例还提供一种应用程序的本地跨域漏洞检测装置,包括:
- [0037] 第一指示模块,用于指示待检测应用程序访问第一通用资源标识符所指向的共享文件,所述共享文件不是所述待检测应用程序的共享文件;
- [0038] 第二指示模块,用于指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件,所述私有文件为所述待检测应用程序的非共享文件;
- [0039] 确定模块,用于若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。
- [0040] 其中,所述装置还包括:
- [0041] 导入模块,用于将所述待检测应用程序的安装包文件导入装有手机模拟器的计算机中;
- [0042] 安装模块,用于根据所述安装包文件在所述手机模拟器中安装所述待检测应用程

序。

[0043] 其中,所述装置还包括:

[0044] 检测模块,用于检测所述待检测应用程序是否具有提供访问文件的功能;

[0045] 若是,指示所述待检测应用程序访问所述第一通用资源标识符所指向的共享文件;

[0046] 若否,则确定所述待检测应用程序不存在本地跨域漏洞。

[0047] 其中,所述装置还包括:

[0048] 获取模块,用于对所述待检测应用程序进行解包处理,获取所述待检测应用程序的配置文件,所述配置文件记录有所述待检测应用程序是否具有提供访问文件的功能。

[0049] 其中,所述第一指示模块,还用于通过adb调试工具给所述待检测应用程序发送包括访问所述第一通用资源标识符所指向的共享文件的操作指令。

[0050] 其中,所述第二指示模块还用于所述共享文件中包括访问所述第二通用资源标识符所指向的私有文件的JavaScript脚本程序,所述待检测应用程序访问所述共享文件后,通过所述JavaScript脚本程序自动去访问所述第二通用资源标识符所指向的私有文件。

[0051] 其中,所述第二指示模块包括:

[0052] 加载单元,用于所述共享文件中加载有所述第二通用资源标识符,所述第二通用资源标识符指向所述待检测应用程序的私有文件;

[0053] 访问单元,用于所述待检测应用程序访问所述共享文件后,若接收到访问所述私有文件的确认指令,访问所述第二通用资源标识符所指向的私有文件。

[0054] 其中,所述装置还包括:

[0055] 输出模块,用于输出所述待检测应用程序的检测结果,所述检测结果包括漏洞信息和检测时间。

[0056] 其中,所述待检测应用程序为Android浏览器或内置浏览器的Android应用程序。

[0057] 其中,所述装置还包括:

[0058] 上传模块,用于记录所述待检测应用程序的特征信息,并将所述特征信息和所述检测结果上传至服务器。

[0059] 其中,所述特征信息为所述待检测应用程序的包名和/或MD5值。

[0060] 其中,所述装置还包括:

[0061] 提示模块,用于提示用户所述待检测应用程序存在所述本地跨域漏洞。

[0062] 其中,所述装置还包括:

[0063] 修复模块,用于修复所述待检测应用程序中存在的本地跨域漏洞。

[0064] 其中,所述修复所述待检测应用程序中存在的本地跨域漏洞,包括:

[0065] 替换模块,用于下载所述待检测应用程序的升级包文件,将所述升级包文件替换掉所述待检测应用程序中对应的原始文件。

[0066] 实施本发明实施例,具有如下有益效果:

[0067] 通过利用URI通用资源标识符指示待检测应用程序访问不属于待检测应用程序的共享文件,该共享文件又指示待检测应用程序访问属于待检测应用程序的非共享文件,若成功访问该非共享文件,则确定所述待检测应用程序存在本地跨域漏洞。采用本发明实施例,可自动检测待检测应用程序的本地跨域漏洞,检测效率高。

## 附图说明

- [0068] 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简单地介绍,显而易见地,下面描述中的附图仅仅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。
- [0069] 图1是本发明实施例提供的一种应用程序的本地跨域漏洞检测方法的流程示意图;
- [0070] 图2是本发明实施例提供的一种应用程序的本地跨域漏洞检测方法的另一流程示意图;
- [0071] 图3是本发明实施例提供的一种应用程序的本地跨域漏洞检测方法的又一流程示意图;
- [0072] 图4是本发明实施例提供的一种应用程序的本地跨域漏洞检测装置的结构示意图;
- [0073] 图5是本发明实施例提供的一种应用程序的本地跨域漏洞检测装置的另一结构示意图;
- [0074] 图6是图5提供的其中一种第二指示模块的结构示意图;
- [0075] 图7是本发明实施例提供的一种应用程序的本地跨域漏洞检测装置的又一结构示意图。

## 具体实施方式

[0076] 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,所描述的实施例仅是本发明的一部分实施例,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做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。

[0077] 在本发明实施例中,待检测应用程序可以是基于Android、塞班或苹果IOS等手机操作系统的应用程序,也可以是基于计算机操作系统的应用程序,本发明实施例对此不作任何限制。为方便说明,本发明实施例以基于手机操作系统的应用程序为例。

[0078] 请参见图1,图1是本发明实施例提供的一种应用程序的本地跨域漏洞检测方法的流程示意图,在本发明实施例中,该方法包括以下步骤。

[0079] S101:指示待检测应用程序访问第一通用资源标识符所指向的共享文件,所述共享文件不是所述待检测应用程序的共享文件。

[0080] Web上可用的每种资源(HTML文档、图像、视频片段、程序等)都可由一个通用资源标识符(Uniform Resource Identifier,URI)进行定位。本发明实施例的实施方式可以是终端上具体的检测软件中对待检测应用程序进行本地跨域漏洞的检测,也可以是将待检测应用程序导入装有手机模拟器的计算机中进行本地跨域漏洞的检测,本发明实施例对此不作任何限制。为方便说明,本发明实施例以在手机模拟器中进行检测为例。具体的,在计算机中安装手机模拟器,其中,手机模拟器基于手机的操作系统分为基于Android系统的手机模拟器、基于塞班系统的手机模拟器和基于苹果系统的手机模拟器等,在本发明实施例中,

手机模拟器的具体安装类型应根据待检测应用程序的类别来选择，本发明实施例对此不作任何限制。例如：若待检测应用程序的安装包为apk文件，则在计算机中安装基于Android系统的手机模拟器。将待检测应用程序的安装包文件导入装有手机模拟器的计算机中，同时，在手机模拟器中安装待检测应用程序。其中，待检测应用程序的安装路径中包括共享文件和非共享文件（即私有文件，只有待检测应用程序自身可以访问的文件）。在手机模拟器所处的存储卡的根目录上创建一个共享文件，该共享文件可以被所有的应用程序访问，根据该共享文件的保存路径可以获知指向该共享文件的第一通用资源标识符，且该共享文件中包括或加载有第二通用资源标识符，该第二通用资源标识符指向待检测应用程序的私有文件，指示待检测应用程序访问第一通用资源标识符所指向的共享文件。

[0081] 作为一种优选的实施方式，通过adb调试工具给待检测应用程序发送包括访问所述第一通用资源标识符所指向的共享文件的操作指令，指示待检测应用程序访问第一通用资源标识符所指向的共享文件，其中，所述共享文件不是该待检测应用程序的共享文件。adb(Android Debug Bridge，调试桥)是Android提供的一个通用的调试工具，借助该工具，通过命令管理设备或手机模拟器的状态。

[0082] 优选的，在执行所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件之前，还包括：检测所述待检测应用程序是否具有提供访问文件的功能，若是，执行所述指示待检测应用程序访问第一通用资源标识符所指向的共享文件；若否，则可直接确定待检测应用程序不存在本地跨域漏洞。一般的，若应用程序不提供访问文件的功能，则其它任何程序均无法访问该应用程序所提供的文件，因此，若应用程序不提供访问文件的功能，则可直接确定待检测应用程序不存在本地跨域漏洞，而无需继续执行S102，提高检测效率。具体的，对所述待检测应用程序进行解包处理，其中，解包即压包的反过程，将压包文件还原成原来的初始文件，扫描待检测应用程序包括的所有文件，获取待检测应用程序的配置文件，其中，所述配置文件中记录有待检测应用程序是否具有提供访问文件的功能。

[0083] S102：指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件，所述私有文件为所述待检测应用程序的非共享文件。

[0084] 具体的，由于第一通用资源标识符所指向的共享文件是系统根目录下所有应用程序都可以访问的共享文件，因此，在S101中，待检测应用程序是可以成功访问所述共享文件的。进一步的，待检测应用程序成功访问第一通用资源标识符所指向的共享文件后，该共享文件可自动指示待检测应用程序继续访问该共享文件中包括的第二通用资源标识符所指向的私有文件，例如：通过Javascript脚本的方式自动去访问第二通用资源标识符所指向的私有文件。可选的，也可以由用户点击该共享文件中设置的包括第二通用资源标识符的链接后再去访问第二通用资源标识符所指向的私有文件。

[0085] S103：若成功访问所述私有文件，则确定所述待检测应用程序存在本地跨域漏洞。

[0086] 具体的，应用程序在进行文件操作时，系统均会根据操作结果返回一个日志信息，获取访问第二通用资源标识符所指向的私有文件后的日志信息，所述日志信息中记录有是否成功访问该私有文件的状态信息，若从该状态信息中获取到已成功访问该私有文件，则确定所述待检测应用程序存在本地跨域漏洞，即该待检测应用程序的私有文件可以被除自己外的其它应用程序或文件向该待检测应用程序发起访问请求，且该待检测应用程序根据该访问请求成功访问该私有文件。相应的，若获取到访问所述私有文件失败，则确定所述待

检测应用程序不存在本地跨域漏洞。

[0087] 若待检测应用程序存在本地跨域漏洞,将导致黑客获取到该本地跨域漏洞后,给安装了该待检测应用程序的终端执行一些恶意操作,从而给终端带来风险,因此,若检测出该应用程序存在本地跨域漏洞,开发人员应及时修复该漏洞。通常,开发者开发完一个新的应用程序后,在进行软件发布前会对该应用程序进行本地跨域漏洞的检测,若在手机模拟器中检测出该应用程序存在本地跨域漏洞,则根据检测结果可指示开发者对该应用程序进行修改,进行漏洞修复;若该应用程序发布后,终端在使用该应用程序的过程中,通过具体的检测软件获取到该应用程序存在本地跨域漏洞,该终端可以获取该应用程序的特征信息,例如:应用程序的包名和/或MD5值,将特征信息和检测结果上传至服务器,以使服务器获知该特征信息所指定的应用程序存在本地跨域漏洞,从而提示开发人员针对该漏洞对应应用程序进行修改。开发人员对该应用程序的本地跨域漏洞进行修复后,可重新发布升级包文件,服务器可基于消息推送的机制使终端下载该升级包文件,将下载过来的升级包文件替换掉应用程序中对应的原始文件,从而对存在本地跨域漏洞的应用程序进行升级,修复该漏洞。

[0088] 在本发明实施例所描述的应用程序的本地跨域漏洞检测方法中,通过利用URI通用资源标识符指示待检测应用程序访问不属于待检测应用程序的共享文件,该共享文件又指示待检测应用程序访问属于待检测应用程序的非共享文件,若成功访问该非共享文件,则确定所述待检测应用程序存在本地跨域漏洞。采用本发明实施例,可自动检测待检测应用程序的本地跨域漏洞,检测效率高。

[0089] 请参见图2,图2是本发明实施例提供的一种应用程序的本地跨域漏洞检测方法的另一流程示意图,在本发明实施例中,该方法包括以下步骤。

[0090] S201:对所述待检测应用程序进行解包处理,获取所述待检测应用程序的配置文件。

[0091] 具体的,将所述待检测应用程序的安装包文件导入装有手机模拟器的计算机中,并根据所述安装包文件在所述手机模拟器中安装所述待检测应用程序。然后对待检测应用程序进行解包处理,解包即压包的反过程,将压包文件还原成原来的初始文件,扫描待检测应用程序包括的所有文件,获取待检测应用程序的配置文件,其中,所述配置文件中记录有待检测应用程序是否具有提供访问文件的功能。

[0092] S202:检测所述待检测应用程序是否具有提供访问文件的功能。

[0093] 具体的,根据获取到的配置文件检测待检测应用程序是否具有提供访问文件的功能,若是,执行S203;若否,则直接确定所述待检测应用程序不存在本地跨域漏洞,执行S206。

[0094] S203:指示待检测应用程序访问第一通用资源标识符所指向的共享文件。

[0095] 优选的,通过adb调试工具给待检测应用程序发送包括访问所述第一通用资源标识符所指向的共享文件的操作指令,指示待检测应用程序访问第一通用资源标识符所指向的共享文件,其中,所述共享文件不是该待检测应用程序的共享文件。

[0096] S204:指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件。

[0097] 作为一种可能的实施方式,待检测应用程序成功访问第一通用资源标识符所指向

的共享文件后,该共享文件可自动指示待检测应用程序继续访问该共享文件中包括的第二通用资源标识符所指向的私有文件,其中,所述私有文件为所述待检测应用程序的非共享文件。

[0098] 作为一种优选的实施方式,所述第一通用资源标识符所指向的共享文件中包括访问第二通用资源标识符所指向的私有文件的JavaScript脚本程序,执行该JavaScript脚本程序自动去访问第二通用资源标识符所指向的私有文件。因此,待检测应用程序访问所述共享文件后,通过所述JavaScript脚本程序自动去访问第二通用资源标识符所指向的私有文件。

[0099] 作为另一种优选的实施方式,所述第一通用资源标识符所指向的共享文件中加载有第二通用资源标识符,所述第二通用资源标识符指向待检测应用程序的私有文件;待检测应用程序访问所述共享文件后,若接收到访问所述私有文件的确认指令,访问所述第二通用资源标识符所指向的私有文件。具体的,可以是测试人员点击该第二通用资源标识符发出访问该私有文件的确认指令,也可以是通过程序设置成共享文件被访问后,进而自动发出访问该私有文件的确认指令,访问所述第二通用资源标识符所指向的私有文件。

[0100] S205:若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。

[0101] 具体的,若获取到成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞;若获取到访问所述私有文件失败,则确定所述待检测应用程序不存在本地跨域漏洞。

[0102] S206:输出所述待检测应用程序的检测结果,所述检测结果包括漏洞信息和检测时间。

[0103] 具体的,待确定完待检测应用程序是否存在本地跨域漏洞后,将检测结果进行输出,所述检测结果包括漏洞信息和检测时间。例如:假设检测时间为2000年1月1日13:27,若待检测应用程序不存在本地跨域漏洞,可输出:该应用程序不存在本地跨域漏洞,检测时间为2000年1月1日13:27;若待检测应用程序存在本地跨域漏洞,可输出:该应用程序存在本地跨域漏洞,检测时间为2000年1月1日13:27。

[0104] 优选的,待确定完待检测应用程序是否存在本地跨域漏洞后,保存该待检测应用程序的检测结果,并标记该待检测应用程序已检测,方便下次检测时直接根据已保存的信息获取该应用程序的检测信息,减少重复操作。具体的,在系统中给待检测应用程序创建一个标记文件,其中,用“1”标识所述待检测应用程序已完成本地跨域漏洞的检测,用“0”标识所述待检测应用程序未进行本地跨域漏洞的检测,将该状态标志位默认置为“0”,当确定完待检测应用程序是否存在本地跨域漏洞后,再将该状态标志位置为“1”,并将检测结果保存在指定的保存路径中。当下一次对该待检测应用程序进行本地跨域漏洞的检测时,首先去获取系统中是否有该待检测应用程序的标记文件,若有,查看状态标志位是否为1,若状态标志位为“1”,直接去指定的存储单元中获取该待检测应用程序的检测结果;若系统中没有该待检测应用程序的标记文件,为该待检测应用程序创建一个标记文件,将状态标志位默认置为“0”,执行S201,待确定完待检测应用程序是否存在本地跨域漏洞后,将状态标志位更新为1并保存检测结果;若系统中有该待检测应用程序的标记文件,但状态标志位为“0”,执行S201,待确定完待检测应用程序是否存在本地跨域漏洞后,将状态标志位更新为1并保存检测结果。

[0105] 在本发明实施例所描述的应用程序的本地跨域漏洞检测方法中,通过利用URI通用资源标识符指示待检测应用程序访问不属于待检测应用程序的共享文件,该共享文件又指示待检测应用程序访问属于待检测应用程序的非共享文件,若成功访问该非共享文件,则确定所述待检测应用程序存在本地跨域漏洞。采用本发明实施例,可自动检测待检测应用程序的本地跨域漏洞,检测效率高。

[0106] 请参见图3,图3是本发明实施例提供的一种应用程序的本地跨域漏洞检测方法的又一流程示意图,在本发明实施例中,该方法包括以下步骤。

[0107] S301:检测所述待检测应用程序是否具有提供访问文件的功能。

[0108] 若是,执行S302;若否,则确定所述待检测应用程序不存在本地跨域漏洞。

[0109] S302:指示待检测应用程序访问第一通用资源标识符所指向的共享文件。

[0110] 优选的,通过adb调试工具给待检测应用程序发送包括访问所述第一通用资源标识符所指向的共享文件的操作指令,指示待检测应用程序访问第一通用资源标识符所指向的共享文件,其中,所述共享文件不是该待检测应用程序的共享文件。进一步优选的,待检测应用程序为Android浏览器或内置浏览器的Android应用程序。

[0111] S303:指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件。

[0112] 作为一种可能的实施方式,待检测应用程序成功访问第一通用资源标识符所指向的共享文件后,该共享文件可自动指示待检测应用程序继续访问该共享文件中包括的第二通用资源标识符所指向的私有文件,其中,所述私有文件为所述待检测应用程序的非共享文件。

[0113] 作为一种优选的实施方式,所述第一通用资源标识符所指向的共享文件中包括访问第二通用资源标识符所指向的私有文件的JavaScript脚本程序,执行该JavaScript脚本程序自动去访问第二通用资源标识符所指向的私有文件。因此,待检测应用程序访问所述共享文件后,通过所述JavaScript脚本程序自动去访问第二通用资源标识符所指向的私有文件。

[0114] 作为另一种优选的实施方式,所述第一通用资源标识符所指向的共享文件中加载有第二通用资源标识符,所述第二通用资源标识符指向待检测应用程序的私有文件;待检测应用程序访问所述共享文件后,若接收到访问所述私有文件的确认指令,访问所述第二通用资源标识符所指向的私有文件。具体的,可以是测试人员点击该第二通用资源标识符发出访问该私有文件的确认指令,也可以是通过程序设置成共享文件被访问后,进而自动发出访问该私有文件的确认指令,访问所述第二通用资源标识符所指向的私有文件。

[0115] S304:若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。

[0116] 若待检测应用程序存在本地跨域漏洞,将导致黑客获取到该本地跨域漏洞后,给安装了该待检测应用程序的终端执行一些恶意操作,从而给终端带来风险,因此,若检测出该应用程序存在本地跨域漏洞,开发人员应及时修复该漏洞。

[0117] S305:记录所述待检测应用程序的特征信息,并将所述特征信息和所述检测结果上传至服务器。

[0118] 优选的,所述特征信息为待检测应用程序的包名和/或MD5值。

[0119] 具体的,终端在使用该应用程序的过程中,通过具体的检测软件获取到该应用程

序存在本地跨域漏洞,该终端可以获取该应用程序的特征信息,例如:应用程序的包名和/或MD5值,将特征信息和检测结果上传至服务器,以使服务器获知该特征信息所指定的应用程序存在本地跨域漏洞后,提示开发人员针对该漏洞对应用程序进行修改。开发人员对该应用程序的本地跨域漏洞进行修复后,可重新发布升级包文件,服务器可基于消息推送的机制使终端下载该升级包文件,将下载过来的升级包文件替换掉应用程序中对应的原始文件,从而对存在本地跨域漏洞的应用程序进行升级,修复该漏洞。

[0120] S306:提示用户所述待检测应用程序存在所述本地跨域漏洞。

[0121] S307:修复所述待检测应用程序中存在的本地跨域漏洞。

[0122] 优选的,若接收到修复该漏洞的确认请求,所在终端可以下载修复所述待检测应用程序中的本地跨域漏洞的升级包文件,将所述升级包文件替换掉所述待检测应用程序中对应的原始文件,完成漏洞修复。

[0123] 在本发明实施例所描述的应用程序的本地跨域漏洞检测方法中,通过利用URI通用资源标识符指示待检测应用程序访问不属于待检测应用程序的共享文件,该共享文件又指示待检测应用程序访问属于待检测应用程序的非共享文件,若成功访问该非共享文件,则确定所述待检测应用程序存在本地跨域漏洞。采用本发明实施例,可自动检测待检测应用程序的本地跨域漏洞,检测效率高。

[0124] 请参见图4,图4是本发明实施例提供的一种应用程序的本地跨域漏洞检测装置的结构示意图,在本发明实施例中,该装置包括:第一指示模块101、第二指示模块102和确定模块103。

[0125] 第一指示模块101,用于指示待检测应用程序访问第一通用资源标识符所指向的共享文件,所述共享文件不是所述待检测应用程序的共享文件。

[0126] 第二指示模块102,用于指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件,所述私有文件为所述待检测应用程序的非共享文件。

[0127] 确定模块103,用于若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。

[0128] 在本发明实施例所描述的应用程序的本地跨域漏洞检测装置中,通过利用URI通用资源标识符指示待检测应用程序访问不属于待检测应用程序的共享文件,该共享文件又指示待检测应用程序访问属于待检测应用程序的非共享文件,若成功访问该非共享文件,则确定所述待检测应用程序存在本地跨域漏洞。采用本发明实施例,可自动检测待检测应用程序的本地跨域漏洞,检测效率高。

[0129] 请参见图5,图5是本发明实施例提供的一种应用程序的本地跨域漏洞检测装置的另一结构示意图,在本发明实施例中,该装置包括:第一指示模块201、第二指示模块202、确定模块203、导入模块204、安装模块205、检测模块206、获取模块207和输出模块208。

[0130] 第一指示模块201,用于指示待检测应用程序访问第一通用资源标识符所指向的共享文件,所述共享文件不是所述待检测应用程序的共享文件。具体的,第一指示模块201通过adb调试工具给所述待检测应用程序发送包括访问所述第一通用资源标识符所指向的共享文件的操作指令。

[0131] 第二指示模块202,用于指示所述待检测应用程序访问所述共享文件中包括的第

第二通用资源标识符所指向的私有文件,所述私有文件为所述待检测应用程序的非共享文件。具体的,第二指示模块202还用于所述共享文件中包括访问所述第二通用资源标识符所指向的私有文件的JavaScript脚本程序,所述待检测应用程序访问所述共享文件后,通过所述JavaScript脚本程序自动去访问所述第二通用资源标识符所指向的私有文件。

[0132] 确定模块203,用于若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。

[0133] 导入模块204,用于将所述待检测应用程序的安装包文件导入装有手机模拟器的计算机中。

[0134] 安装模块205,用于根据所述安装包文件在所述手机模拟器中安装所述待检测应用程序。

[0135] 检测模块206,用于检测所述待检测应用程序是否具有提供访问文件的功能;若是,指示所述待检测应用程序访问所述第一通用资源标识符所指向的共享文件;若否,则确定所述待检测应用程序不存在本地跨域漏洞。

[0136] 获取模块207,用于对所述待检测应用程序进行解包处理,获取所述待检测应用程序的配置文件,所述配置文件记录有所述待检测应用程序是否具有提供访问文件的功能。

[0137] 输出模块208,用于输出所述待检测应用程序的检测结果,所述检测结果包括漏洞信息和检测时间。

[0138] 作为一种可能的实施方式,第二指示模块202包括:加载单元2021和访问单元2022。如图6所示,图6是图5提供的其中一种第二指示模块的结构示意图。

[0139] 加载单元2021,用于所述共享文件中加载有所述第二通用资源标识符,所述第二通用资源标识符指向所述待检测应用程序的私有文件。

[0140] 访问单元2022,用于所述待检测应用程序访问所述共享文件后,若接收到访问所述私有文件的确认指令,访问所述第二通用资源标识符所指向的私有文件。

[0141] 在本发明实施例所描述的应用程序的本地跨域漏洞检测装置中,通过利用URI通用资源标识符指示待检测应用程序访问不属于待检测应用程序的共享文件,该共享文件又指示待检测应用程序访问属于待检测应用程序的非共享文件,若成功访问该非共享文件,则确定所述待检测应用程序存在本地跨域漏洞。采用本发明实施例,可自动检测待检测应用程序的本地跨域漏洞,检测效率高。

[0142] 请参见图7,图7是本发明实施例提供的一种应用程序的本地跨域漏洞检测装置的结构示意图,在本发明实施例中,该装置包括:检测模块301、第一指示模块302、第二指示模块303、确定模块304、上传模块305、提示模块306和修复模块307。

[0143] 检测模块301,用于检测所述待检测应用程序是否具有提供访问文件的功能。若是,指示所述待检测应用程序访问所述第一通用资源标识符所指向的共享文件;若否,则确定所述待检测应用程序不存在本地跨域漏洞。

[0144] 第一指示模块302,用于指示待检测应用程序访问第一通用资源标识符所指向的共享文件,所述共享文件不是所述待检测应用程序的共享文件。

[0145] 第二指示模块303,用于指示所述待检测应用程序访问所述共享文件中包括的第二通用资源标识符所指向的私有文件,所述私有文件为所述待检测应用程序的非共享文件。

[0146] 确定模块304,用于若成功访问所述私有文件,则确定所述待检测应用程序存在本地跨域漏洞。

[0147] 上传模块305,用于记录所述待检测应用程序的特征信息,并将所述特征信息和所述检测结果上传至服务器。

[0148] 提示模块306,用于提示用户所述待检测应用程序存在所述本地跨域漏洞。

[0149] 修复模块307,用于修复所述待检测应用程序中存在的本地跨域漏洞。优选的,修复模块307还用于下载所述待检测应用程序的升级包文件,将所述升级包文件替换掉所述待检测应用程序中对应的原始文件。

[0150] 在本发明实施例所描述的应用程序的本地跨域漏洞检测装置中,通过利用URI通用资源标识符指示待检测应用程序访问不属于待检测应用程序的共享文件,该共享文件又指示待检测应用程序访问属于待检测应用程序的非共享文件,若成功访问该非共享文件,则确定所述待检测应用程序存在本地跨域漏洞。采用本发明实施例,可自动检测待检测应用程序的本地跨域漏洞,检测效率高。

[0151] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random Access Memory, RAM)等。

[0152] 以上所揭露的仅为本发明一种较佳实施例而已,当然不能以此来限定本发明之权利范围,本领域普通技术人员可以理解实现上述实施例的全部或部分流程,并依本发明专利要求所作的等同变化,仍属于发明所涵盖的范围。

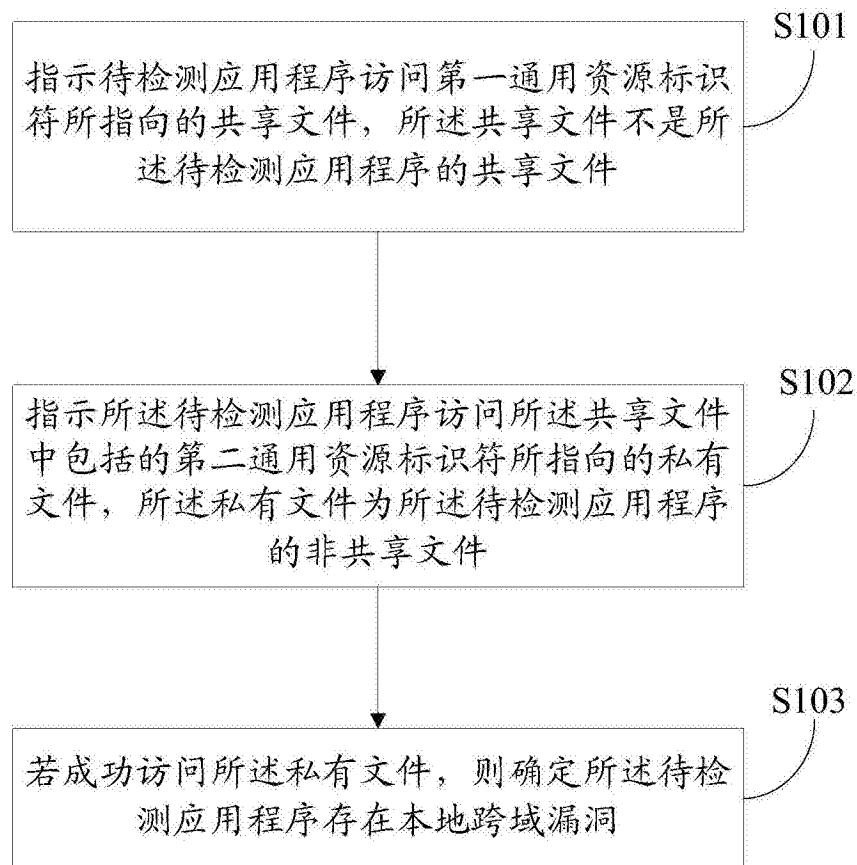


图1

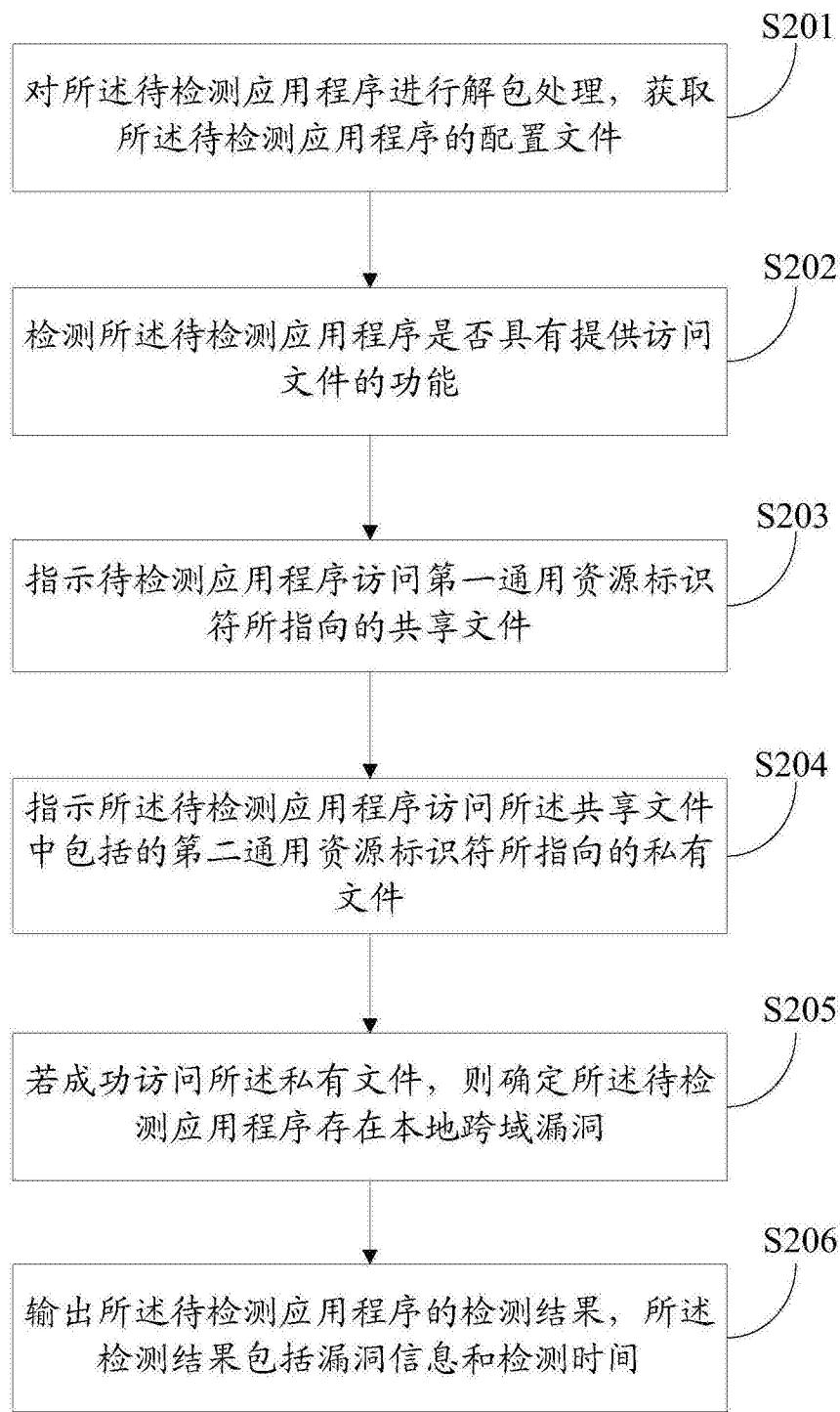


图2

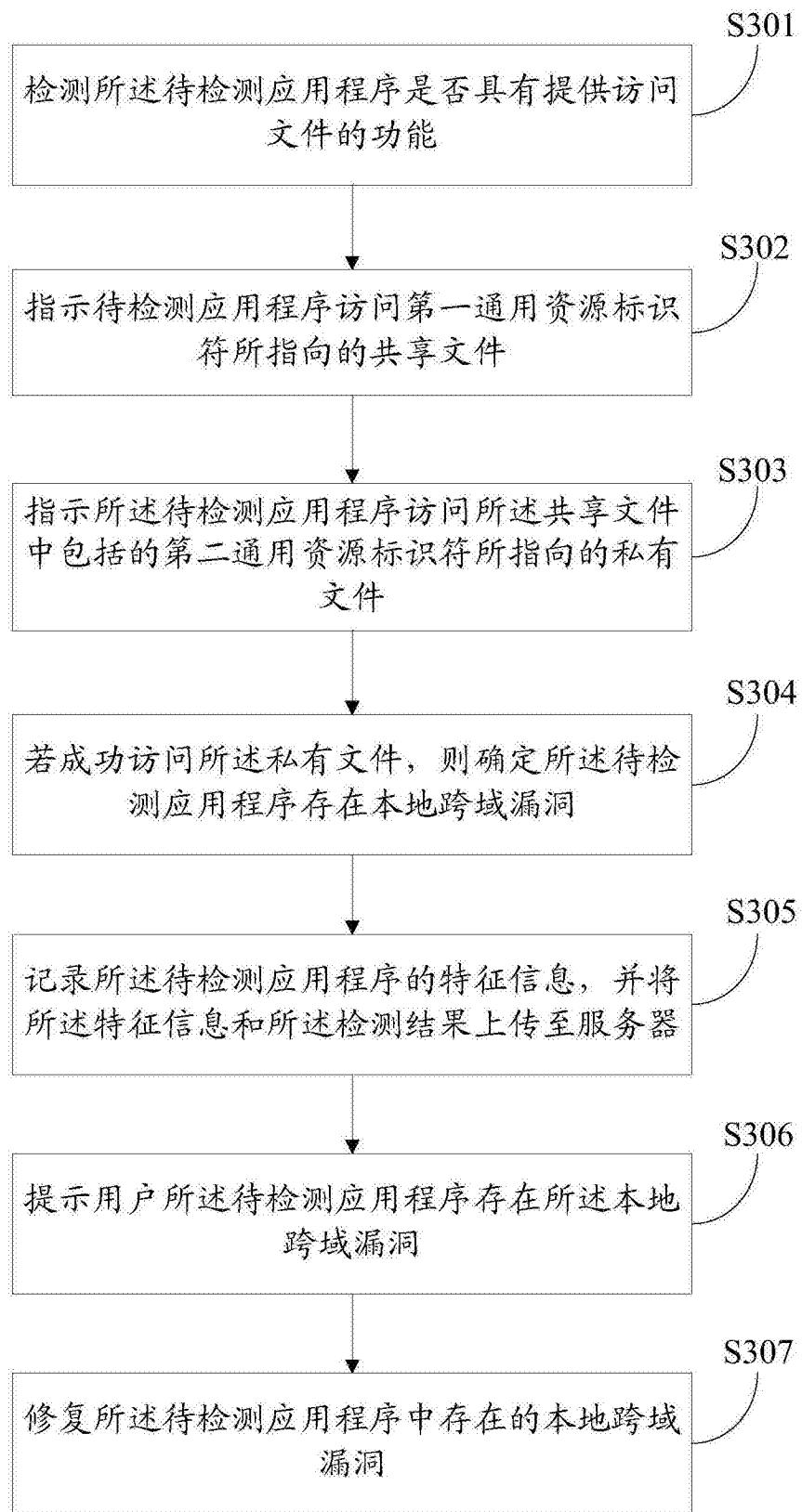


图3

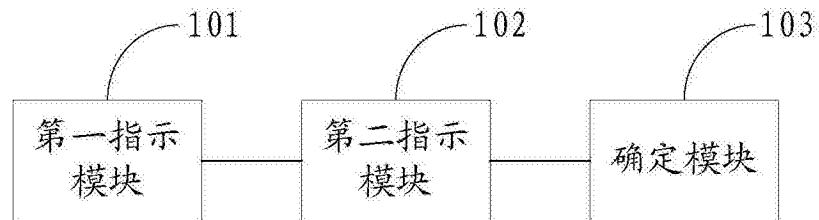


图4

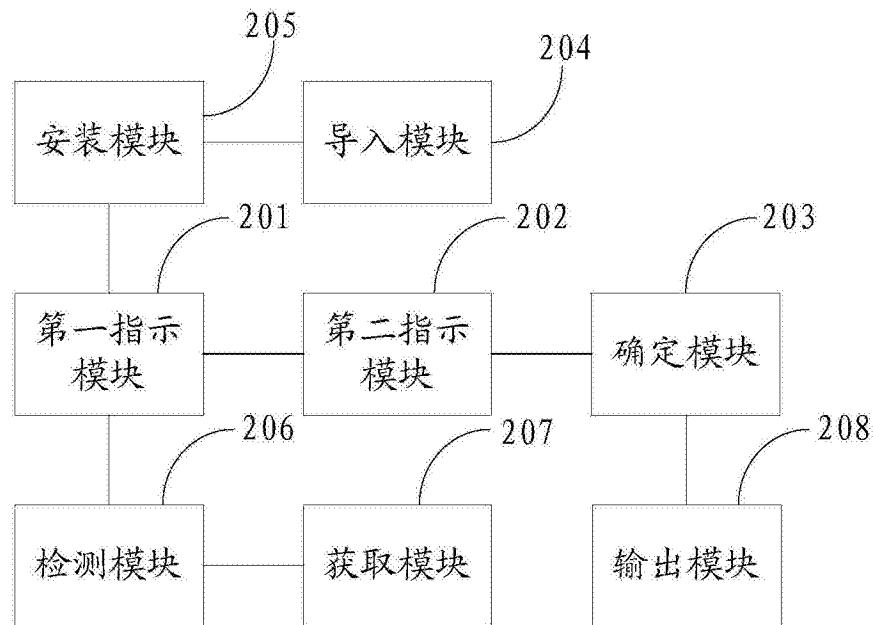


图5

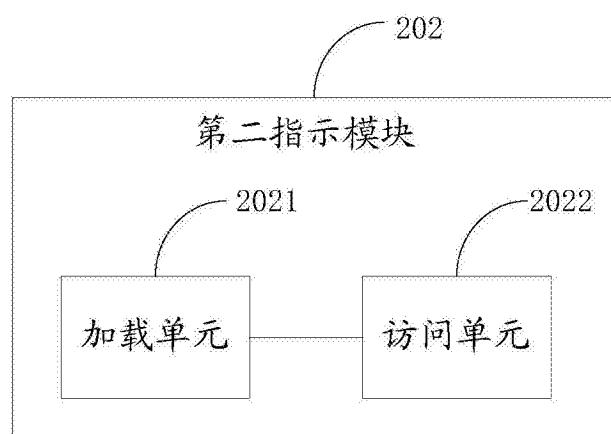


图6

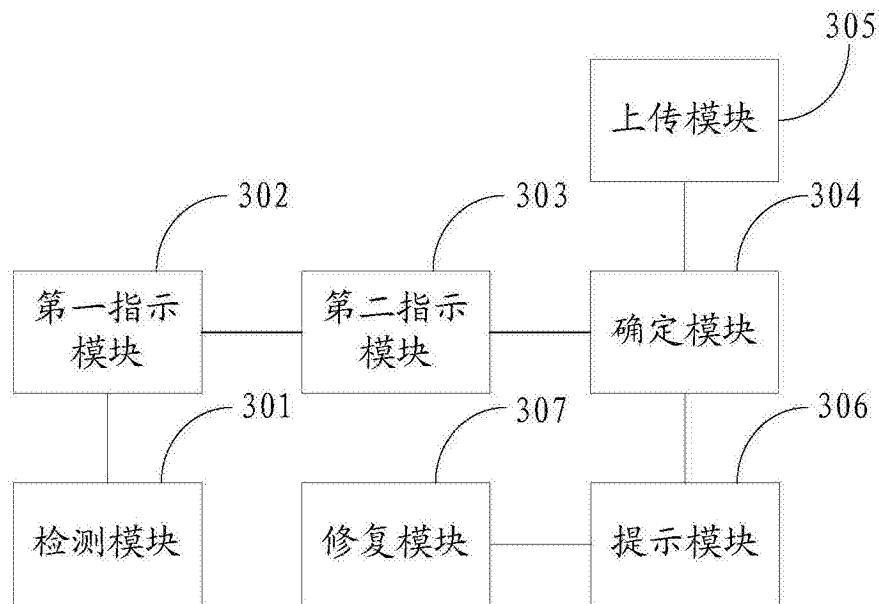


图7