Accessibility。Serwice外如心,事例中外.tuicool.com/sites/ho

时间 2016-12-13 11:04:31 **主题 (https://www.tuicool.com/topics)** 活动 (https://huodong.tuicool.com/)

原文

http://blog.csdn.net/eclipsexys/article/https://www.tuicool.com/mobile) 周刊▼ 更多 ▼

(http://blog.csdn.net/eclipsexys/article/details/53560013?utm_source=tuicool&utm_medium=referral)

主题 安卓开发 (/topics/110800%)

AccessibilityService从入门到出轨

AccessibilityService根据官方的介绍,是指开发者通过增加类似contentDescription的属性,从而在不修改代码的 情况下,让残障人士能够获得使用体验的优化,大家可以打开AccessibilityService来试一下,点击区域,可以有 语音或者触摸的提示,帮助残障人士使用App。

当然,现在AccessibilityService已经基本偏离了它设计的初衷,至少在国内是这样,越来越多的App借用 AccessibilityService来实现了一些其它功能,甚至是灰色产品。

使用入门

老规矩,官网镇楼

https://developer.android.com/guide/topics/ui/accessibility/services.html (https://developer.android.com/guide/topics/ui/accessibility/services.html)

https://developer.android.com/training/accessibility/service.html

(https://developer.android.com/training/accessibility/service.html)

要使用AccessibilityService实际上非常简单,一般来说,只需要以下三步即可。

继承系统AccessibilityService



(http://cpp-summit.org/?channel=tuicool)

2017全球C++及系统软件技术大会

其中有两个必须实现的方法:onAccessibilityEvent和onInterrupt。

在onAccessibilityEvent中,我们可以接收所监听的事件。不熟悉这些事件的话,只需要使用toString把这些信息打出来,自己多看几个Log,就大概能够了解了。

新建配置文件

在资源目录res下新建xml文件夹,新建accessibility.xml文件,写入:

里面有一些比较简单的配置。

其中 description 为 用户允许应用的辅助功能的说明字符串,这里没有指定所要辅助的应用packageNames,当没有指定时,默认辅助所有的应用,建议大家在使用时,指定需要监听的包名(你可以通过|来进行分隔),而不是所有的包名。typeAllMask是设置响应事件的类型,feedbackGeneric是设置回馈给用户的方式,有语音播出



推酷 (https://www.tuicool.com/)

注册

文章 (https://www.tuicool.com/ah)

在AndroidMainifest中注册:

活动 (https://huodong.tuicool.com/) 主题 (https://www.tuicool.com/topics) <service

android:name=".MyAccessibility"

android:permissiap="#"(https://www.tuicoop.com/mobile)" # [https://www.tuicoop.com/mobile)

<intent-filter>

<action

android:name="android"器ccessibilityservice.AccessibilityService"/>

</intent-filter>

<meta-data

android:name="android.accessibilityservice" android:resource="@xml/accessibility"/>

</service>

完成以上步骤后,一个AccessibilityService就可以使用了,你要知道的是,AccessibilityService具有很高的系统 权限,所以,系统不会让App直接设置是否启用,需要用户进入设置-辅助功能中去手动启用,这样在一定程度 上,保护了用户数据的安全。

如何理解AccessibilityService

很多人可能对AccessibilityService了解的不是很深入,所以认为AccessibilityService是在调用一些系统服务来自 动执行一些操作,实际上,这个理解不能算错,当然也不全对,我觉得你可以把AccessibilityService理解为—— 『按键精灵』。相信很多开发者都玩过PC上的这款软件,他的作用,就是将你一次操作的整个记录,录制下 来,然后就可以根据这个记录,重复的执行这些操作,例如:先点击某个输入框,再输入XXXX,再输入验证 码,最后点击某按钮,这些操作如果需要重复执行,那么显然是一套机械的步骤,那么通过按键精灵,记录下这 些操作后,直接通过脚本就可以完成这些操作。其实AccessibilityService跟这个是一样的,我们记录的,实际上 就是我们的操作步骤,或者称之为『脚本』,那么系统在监控整个手机的各种AccessibilityService事件时,就会 根据我们的逻辑来判断该使用哪一个脚本。



(https://

因此,我们完全可以抽象出一个基类AccessibilityService,并抽象出一些脚本的事件,例如,根据Text查找对应的View、点击某个View、清缺一返回等;从所以从我也这里到袋可加入BaseAccessibilityService,这里就不贴具体的代码了,大家可以参考我的Github:

文章 (https://www.tuicool.com/ah) 站点 (https://www.tuicool.com/sites/hot) 问里云 https://github.com/xuyisheng/AccessibilityUtil (https://github.com/xuyisheng/AccessibilityUtil)

入门

主题 (https://www.tuicool.com/topics) 活动 (https://huodong.tuicool.com/

不知道从什么时候开始,AccessibilityService来做的事情,也越来越偏离了AccessibilityService设计的初衷,各种安全问题也随之暴露出来,Google的理想是好的,愿天下都是安分守己的程序员。

免Root自动安装

这个也许是能考证的最早利用AccessibilityService的使用场景了,最早在一些应用市场中出现,例如用户一次下载了很多App,那么每个App下载完毕后都会弹出安装界面,而且需要用户手动去处理,确实体验不太好,所以后来就出现了利用Root权限来静默安装App的功能,但现在普通用户Root的需求越来越少,所以,AccessibilityService来实现免Root自动安装的黑科技,才走上了桌面。

那么按照我们前面的思路,要实现自动安装,实际上就是把手动安装的步骤脚本化。一般来说,我们要安装一个 App,会通过以下几个步骤:

- 1. 调用系统的安装Intent
- 2. 在安装界面上寻找『安装』、『下一步』这些操作按钮
- 3. 点击『安装』、『下一步』按钮
- 4. 完成安装

那么这些流程化的操作,我们就完全可以通过脚本来实现,下面就是一些简单的代码实现。

调用系统安装Intent:

```
public void autoInstall(View view) {
   String apkPath = Environment.getExternalStorageDirectory() + "/test.apk";
   Uri uri = Uri.fromFile(new File(apkPath));
   Intent localIntent = new Intent(Intent.ACTION_VIEW);
   localIntent.setDataAndType(uri, "application/vnd.android.package-archive");
   startActivity(localIntent);
```



监控安装界面,并根据逻辑处理点击: 推**皓** (https://www.tuicool.com/)

@Override

代码写完才发现,看似很牛逼的自动安装,其实不过十几行代码。唯一复杂的,就是抽象化这些流程了。

抢红包

抢红包应该是AccessibilityService火起来的最大因素。网上借助AccessibilityService来实现的抢红包插件也是数不胜数,又是一个看上去很牛逼的功能。那么我们再来分析下,你是怎么抢红包的。

加入你现在在桌面,怎么知道有红包了呢?哦,看通知栏,出现了『微信红包』这几个关键字,然后,你点击这条通知进去,点击红包的那条消息,然后再点击拆红包的按钮,返回,回到桌面。

这样一看,抢红包完全是一个体力活啊,如果有个机器人能帮助我完成上面的动作,根本不用我抢啊,对的,这个机器人就是AccessibilityService,我们同样把抢红包流程化。

- 1. 获取通知栏通知事件
- 2. 点击通知栏消息
- 3. 找到红包消息
- 4. 点击
- 5. 点击拆红包
- 6. 返回

这每个步骤,也都不难啊,我们的工具类中,所有的方法都实现了,唯一要做的,就是写几个ifelse把逻辑拼起来就行了,具体代码就不贴了,毕竟是微信严打的一件事,大家适可而止就好了。



当然,这个Demo同样可以做的更完善一点,例如,增加WakeLock和Keyguard,实现在锁屏情况下的自动抢红包等功能。 **推酷 (https://www.tuicool.com/)**

微信自动回复 文章 (https://www.tuicool.com/ah) 站点 (https://www.tuicool.com/sites/hot) 阿里云 📯

在了解了微信抢红包的方式之后,再看看微信自动回复,是不是就更是小菜一碟了?我们只要把抢红包的流程稍 微改一下,就完成了整个功能的实现ttps://www.tuicool.com/topics) 活动 (https://huodong.tuicool.com/

1. 获取通知栏通知事件

2. 点击通知栏消息

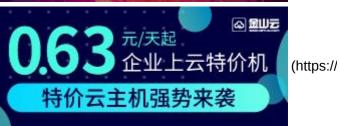
- APP ^荐 (https://www.tuicool.com/mobile) 周刊 ▼ 更多 ▼
- 3. 找到红包消息 ——> 输入自动回复的消息
- 4. 点击 ——> 点击发送 (搜索
- 5. 点击拆红包 ——> 不需要了
- 6. 返回

是不是非常简单?唯一一个有价值的代码如下:

```
private void notifyWechat(AccessibilityEvent event) {
    if (event.getParcelableData() != null && event.getParcelableData() instanceo
f Notification) {
        Notification notification = (Notification) event.getParcelableData();
        String content = notification.tickerText.toString();
        String[] msg = content.split(":");
        name = msg[0].trim();
        text = msg[1].trim();
        PendingIntent pendingIntent = notification.contentIntent;
        try {
            pendingIntent.send();
        } catch (PendingIntent.CanceledException e) {
            e.printStackTrace();
        }
    }
}
```

一个简单的Trick而已,借用notification.contentIntent来唤起Notification对应的App。





实际上,我们能做的事情还有很多,当我们拿到对应的聊天信息时,可以通过聊天对象的筛选,来实现对『特别 对象的监控。,例如你离开的时候,可以还是给你的老婆自知应是你就爱的我在忙呢,等等哈。,而对其它人自 动回复『滚,LZ忙』。再例如,可以对聊天信息进行分词、识别,从而实现对内容的精准回复,当然,这里还

检查微信好友

主题 (https://www.tuicool.com/topics) 活动 (https://huodong.tuicool.com/)建网站 搭应用

那么再比如去年比较火的一个方法,通过拉好友进群组来检查是否还有好友关系。PC、Chrome上已经有很多软 件来做这个检查了,其核心原理P. 都是通过球球场的方式形像co那么右折相上,围槽可以通道多种方式来实现, 如果现在你还不知道该怎么做,那么后面的文章就没有看的必要了.....

进程清理

搜索

大家应该都用过冯老师的『绿色守护』,这个App的最基本无Root功能,就是通过在应用管理界面『结束进程』 的方式来停止一个后台运行的App,大家都知道天朝的App,基本都是全家桶,所以这种方式对释放系统资源确 实还是有一定的帮助的,那么我们就来看看简单的实现。

核心原理非常简单,在应用详情页面,通过停止服务来禁止App服务。OK,那么我们要做的,实际上,就是下 面的流程:

- 1. 通过Intent打开对应App的管理详情信息页面
- 2. 点击停止运行
- 3. 返回,处理下一个

流程要比抢红包什么的简单多了,下面列出2个关键代码,大家应用详情界面:

```
public void cleanProcess(View view) {
   for (String mPackage : mPackages) {
       Intent intent = new Intent();
       intent.setAction(Settings.ACTION_APPLICATION_DETAILS_SETTINGS);
       Uri uri = Uri.fromParts("package", mPackage, null);
       intent.setData(uri);
       startActivity(intent);
```

监控详情页面,进行停止操作:



```
@Override
woverride 推酷 (https://www.tuicool.com/)
public void onAccessibilityEvent(AccessibilityEvent event) {
   if (event.getEventType() == AccessibilityEvent.TYPE_WINDOW_STATE_CHANGED &&
           event.getPackagenalmewww.tuicool.com/sites/hot) 可见云
       CharSequence className = event.getClassName();
       if (classNam<del>主题叫机的的!/AAWWARd[cool.eent/toolcos]</del>ppl活动 interstabling to the comp
ilsTop")) {
          performViewClick(info);
                                                                               2017全球软件架构技术大会
                                                                 登录 (https://www.tuicool.com/login)
           } else {搜索
              performBackClick();
                                                                                     点击免费领取大会PPI
       if (className.equals("android.app.AlertDialog")) {
           clickTextViewByText("确定");
          performBackClick();
```

另外,还有一个兼容性的问题,大家都懂的,国内各种第三方的ROM厂家,经常会修改一些系统的Activity,甚 至不同系统版本同一个功能的Activity都有可能不一样,所以,使用AccessibilityService的一个比较大的麻烦就是 兼容性的处理,需要使用dumpsys和uiautomator这些工具来进行详细的分析,这些工具的使用以及分析方法, 在我的新书《Android群英传:神兵利器》中都有详细的讲解,想深入了解的开发者可以参考下。

判断应用当前状态

这个App唯一的难点,应该就剩下怎么把UI做的好看一点了。

借助AccessibilityService同样可以做一些比较有用的事情,例如监控App当前的状态,例如前台、后台的切换, 通过TYPE WINDOW STATE CHANGED即可进行判断,特别是在5.0以上,原先的getRunningTasks这个方法 被升级到系统权限。

当然,AccessibilityService或多或少会存在一些性能问题,所以现在并不推荐使用这种方式来监控应用状态,更 多的是通过activitylifecyclecallbacks来实现对App状态的跟踪与监控。

(http://s

(https://

ふ 金山元

出轨 推酷 (https://www.tuicool.com/)

其实一旦我们了解了Accessi**刘琦:(Intips的)使网原理ic例处的很难的**到不**追與 (https://里的)透现的透现次页了。Co当形第es/hot) 一)阿里云** 到这里时,甚至有种不寒而栗的感觉,**所以这里申明:

本文所有内容仅供学习、技术现间,如此并他的各种问题I,对有体及流染。*活动(https://huodong.tuicool.com/)建网站搭应用

防卸载

APP ^荐 (https://www.tuicool.com/mobile) 周刊 ▼ 更多 ¬

据我所知,已经有些App或者称之为恶意软件实现了这样的功能,这个功能难吗,不难,估计都不超过20行代 **2017全球软件**码,但确实很恶心,特别是对要整普通、小白用户,压根都不知道AccessibilityService是什么,莫名**要录作诚称s://www.tuicool.com/login/** 启用,写的可能比较好看,什么帮助你清理系统,优化资源,但实际上,在后面做一些见不得人的事情。

我们来分析下如何实现,当用户想要卸载你的App的时候,一般会来到设置界面,找到你的App然后选择卸载,那么如果我们监控这个页面,如果发现是自己的App,就直接退出,这样不就无法卸载了吗?是的,代码如下, 没几行代码:

那么有人要说了,如果是用的一些第三方ROM,直接在桌面就能卸载呢?同样的,只不过会稍微麻烦点,需要判断的东西更多了,要处理的兼容性更复杂了而已。



这里不得不说,虽然国内各种第三方ROM百花齐放、肆意妄为,但这也给AccessibilityService造成了很大的兼容

浏览器劫持 站点 (https://www.tuicool.com/sites/hot) 一 阿里云 文章 (https://www.tuicool.com/ah)

实际上并不局限于浏览器,各种App都能被劫持,因为AccessibilityService监控的是全局App,良心点的可能会 指定包名进行监控。所以,我们们如整件整个TApp,例如浏览器,但并并可以标识就输入指定的例址,或是com/ 是一打开一些App,就输入一些查询内容,这里我以鄙司的沪江网校为例,进入后直接进行搜索。

算了代码还是不贴了,完全都是Copy film right www.tuicool.com/mobile)

监控密码框

搜索

呵呵呵,这个你还真是想多了,系统再天真也不会把这个权限开放给你,所有的设置为password类型的EditText 都是无法被监控的,系统还算有点良心。

这里我只列举了一些非常简单的Hack方式,但实际上,还有很多,例如通过拉取指定网站的内容后自动安装App 并模拟点击等,当然,AccessibilityService也可以用在自动化测试中,这完全就是一把双刃剑,是利是弊,完全 取决于使用他的人。

跳过用户授权

一般来说,AccessibilityService是需要用户手动操作授权才可以执行的,但是,如果是在Root的情况下,或者是 在ADB连接PC的情况下,甚至都不用用户授权,就可以完成AccessibilityService的授权操作。

Root的情况就不说了,通过修改Setting的数据库就可以更改这个设置了,当然,有Root的情况下,就根本不需 要AccessibilityService了。

在没有Root的情况下,如果PC通过ADB发出指令,同样是可以自动完成授权的,这个可以参考360的一篇文 章:

http://www.freebuf.com/articles/terminal/114045.html (http://www.freebuf.com/articles/terminal/114045.html)

我这里就不多说了,大家看看就懂了,并没有太多的技术含量,应该算是系统的一个小的漏洞。

AccessibilityService一般分析步骤

前面我们分析了那么多AccessibilityService好的不好的使用方法,实际上,总结下就这么几步。



- 1. 分析操作的流程,拆解成单步可实现的过程 2. 通过UIAutomator和adb shell cultures shell
- 3. 通过逻辑组合进行代码编写
- 站点 (https://www.tuicool.com/sites/hot) 一 阿里云 文章 (https://www.tuicool.com/ah) 4. 调试、兼容性处理

通过上面的这些方式,基本就可以实现一些固定流程的操作自动化了。关于AccessibilityService的工具类,我放 到了Github上,虽然功能已经主题。但trps但必没有绝过很多的兼容性测试,同活动,确实时间和精力的失源ic绝出com 的Demo示例也不多,希望大家可以多提PR,共同完善。

https://github.com/xuvishences/kers/bittps://www.tuicoplecom/unsbile/Acc風動ilityUti更多。

欢迎大家关注我的微信公众号:

0.73元 (http://c 百选云服务器 2017全球软件架构技术大会 登录 (https://www.tuicool.com/login) 点击免费领取大会PPT

(http://s



(https://

ch=00033.00018.6666&hmsr=%E6%8E%A8%E9%85%I





▲ 纠错

性能云服务器2折起 (一) 阿里云

0.73元/日, 节省80%运维成本



了解详细

(http://click.aliyun.com/m/32076/)

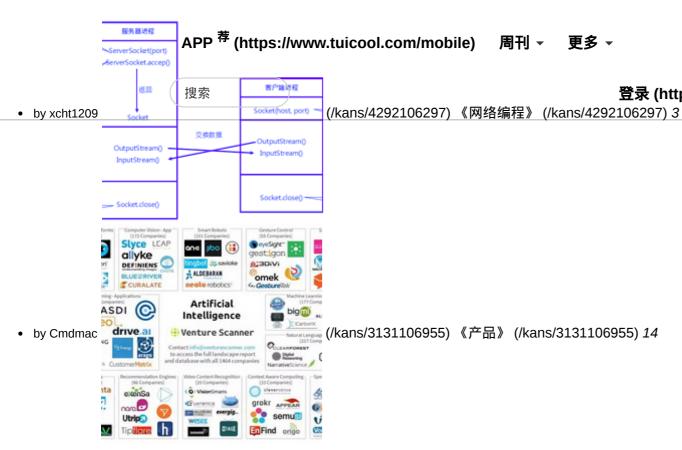
推荐文章

• 1. 设计师说, 我们要在 App 里用十种字体!!! (/articles/aMfqaiR)

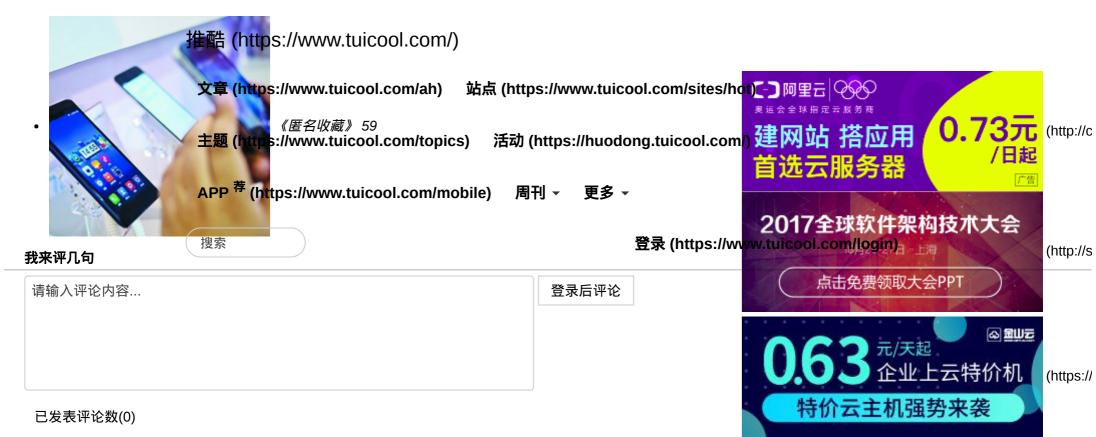
- 4. 美团App 插件化实践 (/articles/3qMRV3Z)
- 5. 像 npm 一样在 Andrio 文章 目 中的 \$**/\burade t**\@parade t\@parade t\
- 6. Kotlin 将超越 Java 成为 Android 开发的第一语言? (/articles/RnIJ7ne)

相关推刊

活动 (https://huodong.tuicool.com/ 主题 (https://www.tuicool.com/topics)







ch=00033.00018.6666&hmsr=%E6%8E%A8%E9%85%I

关于我们 (https://www.tuicool.com/about) 移动应用 (https://www.tuicool.com/mobile) 意见反馈 (https://www.tuicool.com/bbs/go/issues) 官方微博 (https://weibo.com/tuicool2012)