

标准与合规

App安全合规的思考（七）iOS下App权限检测方法

原创

文章目录

Moench 2021-10-26 16:51:35 25506 1

iOS最近逐渐也进入监管范围内，而市面上的隐私合规产品针对iOS的测试能力十分有限，下文是利用iOS15隐私新功能给大家提供一个简单又能解决一定问题的iOS下权限合规检测的方法。

本身没有任何技术含量，最近简单接触了下ios下的合规测试，记个流水账，希望有大佬可以提供更好的解决方案~

0 环境及工具

环境：Mac、iphone（iOS15.0及以上）

Mac工具：Xcode、Apple Configurator 2

iphone工具：App活动日志查看的辅助工具

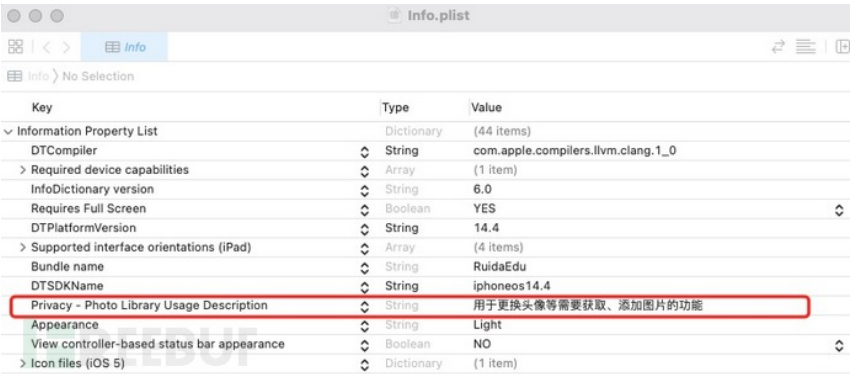
1 常见权限

	常见权限	字段名
1	麦克风	Privacy - Microphone Usage Description
2	相机	Privacy - Camera Usage Description
3	相册(读权限)	Privacy - Photo Library Usage Description
4	相册(写权限)	Privacy - Photo Library Additions Usage Description
5	通讯录	Privacy - Contacts Usage Description
6	蓝牙	Privacy - Bluetooth Peripheral Usage Description
7	语音转文字	Privacy - Speech Recognition Usage Description
8	日历权限	Privacy - Calendars Usage Description
9		Privacy - Location When In Use Usage Description
10	定位权限	Privacy - Location Always Usage Description
11		Privacy - Location Always and When In Use Usage Description
12	媒体库	Privacy - Media Library Usage Description
13	运动与健身	Privacy - Motion Usage Description
14	健康(分享权限)	Privacy - Health Share Usage Description
15	健康(更新权限)	Privacy - Health Update Usage Description
16	提醒事项	Privacy - Reminders Usage Description
17	语音识别(Siri)	Privacy - Siri Usage Description
18	本地网络	Privacy - Local Network Usage Description
19	面容/指纹	Privacy - Face ID Usage Description

2 info.plist 文件

2.1 info.plist

iOS应用和Android应用一样，权限列表都能在包里的文件找到（Android：AndroidManifest.xml，iOS：info.plist）。但是iOS比Android贴心的地方在于苹果下对于权限调用的目的说明都在此文件里，对于安全合规人员审核调用权限的目的提供了便利。



Key	Type	Value
Information Property List	Dictionary	(44 items)
DTCompiler	String	com.apple.compilers.llvm.clang.1_0
Required device capabilities	Array	(1 item)
InfoDictionary version	String	6.0
Requires Full Screen	Boolean	YES
DTPlatformVersion	String	14.4
Supported interface orientations (iPad)	Array	(4 items)
Bundle name	String	RuidaEdu
DTSDKName	String	iphones14.4
Privacy - Photo Library Usage Description	String	用于更换头像等需要获取、添加图片的功能
Appearance	String	Light
View controller-based status bar appearance	Boolean	NO
Icon files (iOS 5)	Dictionary	(1 item)

上图中Value值就是获取权限弹窗中显示出来的内容（目的）。当然，很多时候因为功能变更导致有些权限不使用也在info.plist文件中声明，还是建议开发人员进行删除不使用的权限，避免检查过程中出现问题。

2.2 如何获取info.plist文件

- 0 环境及工具
- 1 常见权限
- 2 info.plist 文件
 - 2.1 info.plist
 - 2.2 如何获取info.plist文件
- 3 权限使用情况
 - 3.1 记录App活动
 - 3.2 测试用例
- 4 其他

品调研

2021-05-27

App安全合规的思考

2021-05-26

浏览更多

请登录 / 注册后在FreeBuf发布内容哦

5 1 + 收入专辑 ...

标准与合规



文章目录

- 0 环境及工具
- 1 常见权限
- 2 info.plist 文件
 - 2.1 info.plist
 - 2.2 如何获取info
- 3 权限使用情况
 - 3.1 记录App活动
 - 3.2 测试用例
- 4 其他

2.2.2 没有ipa包
合规同学在日常线上巡查时，为了不强打扰业务，可以通过Apple Configurator 2工具搞到ipa包。因为没办法放链接，可以搜Apple Configurator 2提取ipa文件，找详细方法，这里简单说一下。

打开应用，连手机，登录Apple ID。
点击添加按钮，选择要测试的App（保证本机已安装）
弹出本机已存在xxxx的应用时，Finder打开如下路径，复制出来ipa：

```
~/Library/Group  
Containers/K36BKF7T3D.group.com.apple.configurator/Library/Caches/Assets/TemporaryItems  
/MobileApps/
```

按2.2.1的方式

2.2.3 其他方式
如果越狱了，应该可以用爱思助手什么的肯定是可以的。

3 权限使用情况

3.1 记录App活动功能

iOS15以上，也有了类似小米照明弹的功能，可以下载辅助类的App进行App访问活动日志查看，例如极简小组件-无广告桌面小组件、隐私洞见等等（商店一搜隐私有好多）。网上也有很多关于网友也通过这个功能，曝光国民App滥用权限的新闻。

使用方法：设置-隐私-记录App活动-存储App活动-导入到你下载的辅助查看的App，即可即可查看

3.2 测试用例

可以通过如下测试用例分别进行测试：

- 同意前信息上传、权限使用情况
 - 下载app后，打开，不做后续操作，放置（可后台运行）
 - 查看是否有权限申请情况
 - 导出活动记录，查看是否有网络活动
- 权限使用频率
 - 同意隐私政策后，正常使用App一段时间
 - 导出活动记录，查看访问记录，评估权限使用频率
- 后台运行情况
 - 同意隐私政策后，登录App后，放置后台运行一段时间（记录后台放置时间点）
 - 导出活动记录，查看访问记录中，后台放置后是否有权限使用情况

4 其他

- 企业级证书ipa包怎么安装
 - 扫码
 - 扫码装不上可以下ipa，用xcode装（window-Devices&Simulators）
- 权限是否是基于场景触发
 - 没办法，只能安装好，一步一步找到触发点。

- App安全合规的思考（一）：APP安全认证的工作流程梳理
- App安全合规的思考（二） 监管的重点变化梳理
- App安全合规的思考（三）如何做好App整改应急响应工作
- App安全合规的思考（四） 权限问题
- App安全合规的思考（五） 隐私合规产品调研

本文作者：Moench，转载请注明来自FreeBuf.COM

标准与合规

- # 安全合规
- # App合规
- # App安全合规检测

文章目录

- 0 环境及工具
- 1 常见权限
 - 2 info.plist 文件
 - 2.1 info.plist
 - 2.2 如何获取info
- 3 权限使用情况
 - 3.1 记录App活动
 - 3.2 测试用例
- 4 其他

被以下专辑收录，发现更多精彩内容

+ 收入我的专辑

1

评论 1


按热度排序



白小仙bbb LV.1（这家伙太懒了，还未填写个人描述！）
听着语气像个小姐姐
2021-11-10 17:37:16

 亮了

 回复



请 [登录](#) / [注册](#) 后在FreeBuf发布内容哦

相关推荐

戴尔BIOS更新后可能导致电脑无法正常启动



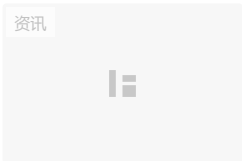
戴尔最近发布的BIOS更新在多个笔记本电脑和台式机型号上引起严重启动问题。

 wzb123


已有 2034 人围观

2021-12-22

《上海市建设网络安全产业创新高地行动计划（2021-2023年）》全文发布



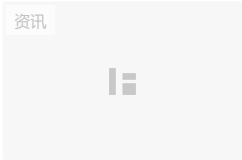
总的来说，《行动计划》共提出4项主要目标，3大建设高地，10项建设任务，以及7项保障措施。

 FreeBuf政策发布

已有 7348 人围观

2021-12-22

谷歌警告称，超过35000个Java包受 Log4j 漏洞影响



谷歌扫描Maven Central Java软件包库，发现35863个软件包使用的Log4j库版本易受Log4Shell漏洞攻击。

 Zicheng

已有 13713 人围观

2021-12-22

FreeBuf早报 | 阿里云被暂停工信部网络安全威胁信息共享平台合作单位；摩根员工使...



全球各地麻烦事儿都不少，FreeBuf早报，安全早知道。

 yannichen

已有 29879 人围观 · 发现 1 个不明物体

2021-12-22

请 [登录](#) / [注册](#) 后在FreeBuf发布内容哦

51+ 收入专辑...

App安全合规的思考（七）iOS下App权限检测...

 Moe

标准与合规



 腾讯安全

已有 9808 人围观

2021-12-21

 5

 FREEBUF

本站由 阿里云 提供计算与安全服务

 FreeBuf社群入口

用户服务

有奖投稿

提交漏洞

参与众测

商城

企业服务

企业空间

企业SRC

漏洞众测

威胁检测

合作信息

寻求服务

广告投放

联系我们

友情链接

关于我们

关于我们

加入我们

微信公众号

新浪微博

文章目录

0 环境及工具

1 常见权限

2 info.plist 文件

2.1 info.plist

2.2 如何获取info

3 权限使用情况

3.1 记录App活动

3.2 测试用例

4 其他

斗象科技

FreeBuf

漏洞盒子

斗象智能安全平台

免责条款

协议条款

Copyright © 2020 WWW.FREEBUF.COM All Rights Reserved

沪ICP备13