Xposed精品连载 | 一篇文章彻底搞定安卓刷机与Root

小肩膀 非攻code 2020-06-25

> 阅读本文大概需要 10 分钟。

安卓是基于Linux内核的一个移动操作系统。在Linux这种Unix系统中，通常都有两种账户，一个是普通用户，一个是root用户。一般来说我们在安卓手机上都是普通用户。因为市面上的App良莠不齐，出于安全的考虑，只有开发者才会去获取整个操作系统的更改权限，普通用户是没有高级权限的。

对于我们而言，为了进行App逆向和协议分析，获取整个安卓设备的权限是至关重要的。不论是Frida，Xposed还是Cydia Substrate这类应用，都需要开发者能完全控制自己的文件系统，所以这节教程会让大家彻底搞定安卓刷机与Root。

目录

本文以Google Pixel机型为例，主要解决以下两个问题

- 官方8.1系统线刷
- twrp+Magisk Root方案

adb与fastboot

手机通过USB连接电脑，需要用到adb
刷机包通过线刷刷入手机，需要用到fastboot
这俩个东西在安卓SDK中自带，路径为 SDK\platform-tools 添加到系统环境变量即可
（what? 环境变量有什么用？环境变量怎么添加？本人已与百度达成合作，上百度一键搜索，免费获取答案）

开启开发者选项

选择 【设置 – 系统 – 关于手机 – 版本号】，点击【版本号】7次开启 【开发者选项】。如果是英文系统，自行翻译

开启USB调试

选择 【设置 – 系统 – 开发者选项】，开启【USB调试】。

如果是英文系统，请通过百度或者谷歌自行翻译。

通过数据线将手机连接至电脑，手机端会弹出 USB 调试申请，允许即可

开启成功的标志，cmd中输入adb devices

Bootloader解锁

要想刷机首先要Bootloader解锁，而要Bootloader解锁，又要先开启oem解锁。不过，如果你的手机是淘宝买的二手机，一般都是已经解锁了的。那么可以跳过oem解锁与Bootloader解锁

1. 手机先退出谷歌账号，取消锁屏，指纹识别等
2. 从手机设备中取出sim卡
3. 开启开发者选项
4. 开启USB调试
5. 开启oem解锁 (这个选项也在开发者选项中，但是需要科学上网)
6. 手机连接至电脑，进入Bootloader模式（ 进入方式在下文给出 ）
7. 在cmd中输入fastboot oem unlock 或者 fastboot flashing unlock
8. Bootloader解锁界面中，用音量键 +/- 控制光标，选择【Yes】并按下电源键进行Bootloader解锁
9. 确认完毕后，稍作等待。通过 fastboot reboot 命令重启手机

成功解锁Bootloader后，每次手机启动时，都会出现黑底白字的英文警告页，提示 “Your device software can’t be checked for corruption. Please lock the bootloader”。

这仅仅提示你 Bootloader 被解锁了，忽视即可。

进入Bootloader模式

进入Bootloader默认有两种方式。

1. 关机状态下【按住音量减少键 + 电源键】

2. 开机状态下，在cmd中通过adb命令进入 `adb reboot bootloader` ，可以用 `fastboot devices` 来验证是否成功

刷机详解

本文以pixel机型刷官方工厂镜像包8.1为例

sailfish-opm1.171019.011-factory-56d15350

下载地址如下（需要科学上网）

https://developers.google.com/android/images

其实设备解锁方法，这里面也有写

把下载后的刷机包解压，我们先来认识下刷机包的组成

bootloader-sailfish-8996-012001-1710040120.img
很明显我们进入的bootloader需要这玩意。

radio-sailfish-8996-130091-1710201747.img
基带

image-sailfish-opm1.171019.011.zip
这个就是安卓系统了

有了前面的步骤的铺垫，刷机就更简单了。
进入bootloader，Windows系统双击 `flash-all.bat` ，Linux、mac系统运行 `flash-all.sh` 即可

zip压缩包中的img镜像有很多，其实有一些并不是必须要刷的，如果你编译过安卓系统就知道了。
同样的我们在魔改系统的时候，可以只单独刷其中几个修改过的img镜像。譬如 `fastboot flash boot boot.img`

7.0系统以后连接wifi会出现一个× ，这是由于原生安卓系统验证wifi是否有效，是去访问谷歌的服务器运行以下命令：`adb shell settings put global captive_portal_https_url https://www.google.cn/generate_204`

开启飞行模式，再关闭飞行模式即可解决！

Root详解

安卓系统版本不一样，Root方法也不一样。不过一般高版本安卓系统，都选择用twrp+Magisk的Root方案

其中twrp是第三方recovery，用来卡刷

twrp下载地址：

https://dl.twrp.me/sailfish/

Magisk下载地址 ：

https://github.com/topjohnwu/Magisk/releases

本文使用的版本：

- 临时twrp：twrp-3.2.3-1-sailfish.img
- 永久twrp：twrp-pixel-installer-sailfish-3.2.3-1.zip

- Magisk：Magisk-v20.4.zip

1. 通过 adb push 命令，把 twrp-pixel-installer-sailfish-3.2.3-1.zip 和 Magisk v20.4.zip 拷贝到手机sdcard目录。为电脑端文件所在路径 ，为要推送到手机端哪个地方。
   ```
   adb push twrp-pixel-installer-sailfish-3.2.3-1.zip /sdcard/
   adb push Magisk-v20.4.zip /sdcard/
   ```
2. 进入bootloader模式，刷临时twrp `fastboot boot twrp-3.2.3-1-sailfish.img` ，手机会进入到临时twrp，滑动下面的 Swipe to Allow Modifications 滑条，进入Twrp操作页面
3. 刷入永久twrp
   选择 Install – 找到目录 /sdcard/ – 选择 twrp-pixel-installer-sailfish-3.2.3-1.zip 文件 – 弹出安装界面 – 滑动底部的滑条 Swipe to confirm Flash 安装。最后显示 ...done 的提示。这一步完成
4. 刷入Magisk
   点击顶部的【install Zip】 蓝色条部分左侧图标处，返回 Team Win Recovery Project 界面
   按照第三步的操作，只不过文件换成 Magisk-v20.4.zip
5. 安装完成后，点击下面的 Reboot System 按钮，重启系统。这时候会询问是否安装 twrp app
   这里绝对不要安装，直接点击中间的 Do Not Install 即可
6. 启动手机后，会多一个面具图标的app，这个就可以用来管理Root权限，以及Magisk相关的模块，我们后面要在8.0以后的系统上安装EdXposed就需要用到它

专注于网络爬虫，JavaScript与App安全防护与逆向分析
包括Frida与Xposed教程发布

喜欢此内容的人还喜欢

体育老师给你的寒假家庭锻炼计划

体育老师

麦读书单 | 薛政：从法官与律师的视角，推荐一份行政法实务书单

麦读