神奇的面具 Magisk

作者：bugless
原文链接：https://ld246.com/article/1621851304892
来源网站：链滴

Magisk

A Magic Mask to Alter System Systemless-ly

神奇的面具Magisk

今天为大家介绍一款神奇的 Android 第三方接口 —— Magisk

Root —— 玩家与厂商间的博弈

Android 从诞生之日起就高举着开源的大旗，这也是它成功的原因之一。而它的开放性也成功的吸引了一大批爱折腾的人，从而诞生出了 root（此处特制 Android 中的 root）。

根据 Wikipedia 的释义，root 指的是使用户取得 Android 操作系统的超级用户（Super User）许可的技术。用户通过 root，可以越过手机制造商的限制，卸载手机制造商预装在手机中某些应用，以及行一些需要超级用户权限的应用程序。同时,root 也可能会让手机变得“不安全”（并不是说 root 使机变得不安全，而是一些用户的使用习惯会使 root 后的手机变得危险）。

但是从棉花糖（Android 6.0）开始，Google 基本阻止了以前版本中最流行的 root 方法 —— 即，将 su守护程序 放置到 /system 分区，并在启动时取得所需的权限。道高一尺，魔高一丈，于是就出现了 systemless 的 root 方式，因为它不采取任何方式修改 /system 分区。

出于增加安全性的考虑，Google 推出了 SafetyNet 这样的检测，以确保 Android Pay 等一些 App 安全运行，玩家不得不在 root 权限和一些有价值的 App 之间作出选择。

这个时候 Magisk 诞生了。

Magisk

什么是 Magisk

Magisk 是出自一位台湾学生 @topjohnwu 开发的 Android 框架，是一个通用的第三方 systemless 接口，通过这样的方式实现一些较强大的功能。

看似很简单的一个框架，甚至与大名鼎鼎的 Xposed 框架在功能性上有点重复。很多人批评 Magisk 模块太少了，想替代 Xposed 根本不可能（在那个 Xposed Framework for Android 7.0 难产的时，很多人将 Magisk 看是做是 Xposed 的替代品）。这是不正确的，因为 Magisk 从来没有想过要代 Xposed，Magisk 与 Xposed 是可以互相兼容的，你甚至可以通过 Magisk 来安装 Xposed（安装 posed 后就不能绕过 SafetyNet 了）。

Magisk 的厉害之处在于它实现了一种绕过 SafetyNet 使用 root 的方法。

实现原理： 由于它是通过启动时在 boot 中创建钩子，把 /data/magisk.img 挂载到 /magisk，构建一个在 system 基础上能够自定义替换，增加以及删除的文件系统，所有操作都在启动的时候完成，

际上并没有对 /system 分区进行修改（即 systemless 接口，以不触动 /system 的方式修改 /syste
）。

功能

截至目前版本（v14.0），Magisk 可以实现的功能包括：

- 集成 root（MagiskSU）
- root 和 Magisk 的日志功能
- Magisk Hide（隐藏 Magisk 的 root 权限，针对 Snapchat、Android Pay、PokémonGo、Netfli
等）
- 为广告屏蔽应用提供 systemless hosts 支持
- 通过 SafetyNet 检查
- Magisk 功能模块

支持的版本：Android 5.0+

安装方法

安装 Magisk 需要解锁 Bootloader 并刷入第三方 Recovery。所以每个品牌的手机都或多或少的有
不一样，这里只介绍一个标准的流程，具体操作方法请自行 Google（只需要 Google 你使用的手机
锁 Bootloader 和刷入第三方 Recovery 的方法就可以了，其他的安我说的做）。

1. 解锁手机 Bootloader（BL）

方法：自行 Google

2. 刷入第三方 Recovery（例如 TWRP）

方法：自行 Google

3. 下载官方 Magisk 包，然后通过第三方 Recovery 刷入

方法：首先将下好的包放入手机的硬盘中（你可以使用 QQ数据线 也可以使用 XX手机助手，whateve
）然后，进入第三方 Recovery（以 twrp 为例），安装刷机包 -> 找到我让你放在硬盘中的那个包（
缀为 .zip）-> 滑动滑块，开始刷机 -> 刷好后立即重启

4. 享受完整 Magisk 的 systemless root 和神奇的 Magisk 模块

重启后找到一个名为 Magisk Manager（图标是一个面具，绿色背景），这是 Magisk 的管理程序，
可以在这里下载、安装、升级、卸载你的 Magisk 和 Magisk 模块。

5. 卸载 Magisk

卸载 Magisk 有两种方法：在 Magisk Manager 中卸载，或者通过第三方 Recovery 刷入卸载包卸
。通过 Magisk Manager 卸载很好理解，通过第三方 Recovery 卸载的意思是刷一个名为Magisk-un
nstaller.zip 的刷机包，方法和刷 Magisk 一样。两种方法我都没试过。

一些推荐的功能模块

App Systemizer

这是一个能把用户 App 挂载为系统 App 的模块，如 Google Play 服务、绿色守护、蟒蛇音效等。

Magisk SELinux Permissive Script

使 Android 的 SELinux 默认以 Permissive 运行，关于 SELinux 模式的介绍，请点击这里。

ViPER4Android FX

大名鼎鼎的蝰蛇音效的 Magisk 模块，需要配合 VIPERFX 的管理器使用，请在 XDA 论坛搜索下载。于ViPER4Android。

Xposed

强大的 Xposed 框架的 systemless 实现，关于 Xposed 的介绍点击这里。

- 作者：bugless
- 时间：2021-02-02 10:41:55
- 主页：bugless.site