本文PDF版：magisk01.pdf

Magisk官方教程指路：https://topjohnwu.github.io/Magisk/install.html

本文仅为官方教程中最通用的一种方法的个人实践过程(Ramdisk、vbmeta验证和三星手机的问题还请自行查阅上述官方教程)

食材准备：

- 手机一部，本文以 红米K30Pro (MIUI 13 Android 12) 做演示

- 电脑一台，本文以 Windows 11系统 做演示

- USB线一根
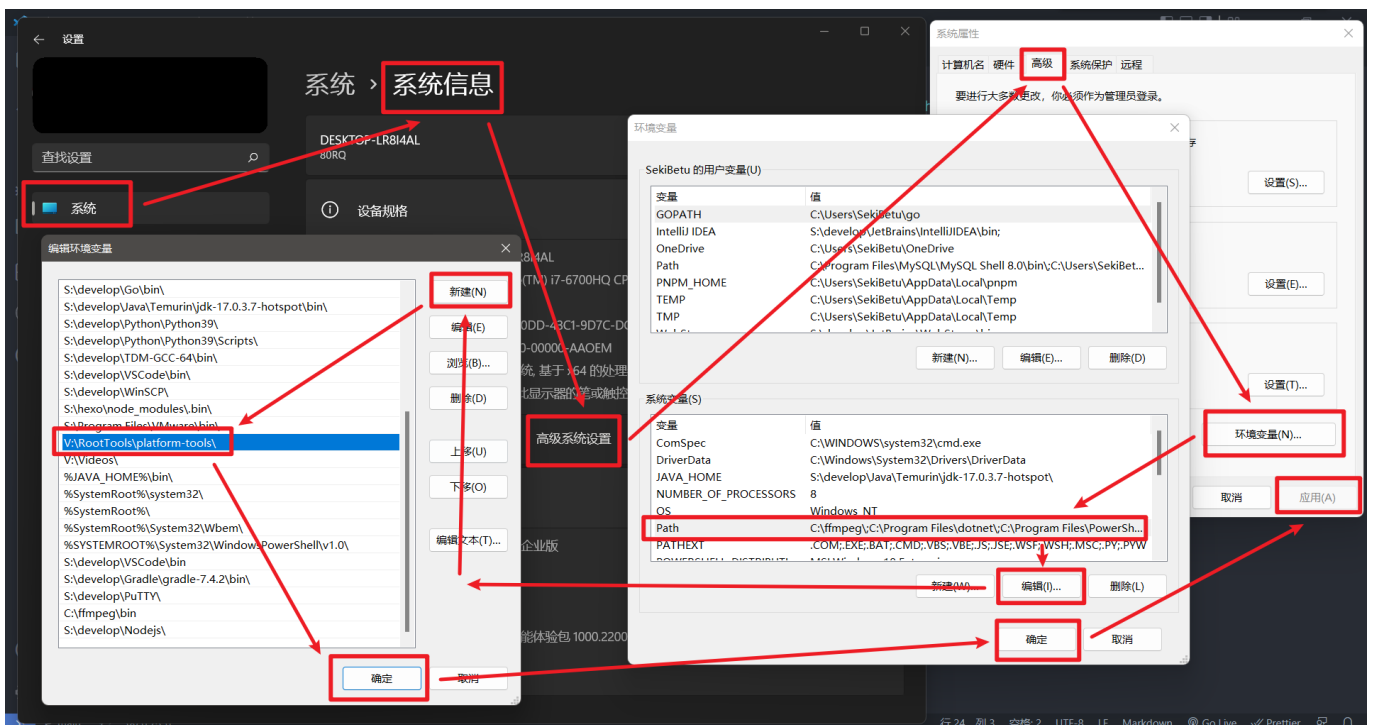
厨具准备：

- Android SDK Platform-Tools

- Google USB

- Magisk

烹饪步骤：

- 通过小米官方的 解锁工具 解锁手机的 BootLoader (不同的厂商有不同的解锁方式，也有一些厂商不支持解锁 BootLoader)

- 把下载好的 Android SDK Platform-Tools 压缩包解压到一个文件夹中

adb.exe	1/1 周二 0:00	应用程序	5,849 KB
AdbWinApi.dll	1/1 周二 0:00	应用程序扩展	96 KB
AdbWinUsbApi.dll	1/1 周二 0:00	应用程序扩展	62 KB
dmtracedump.exe	1/1 周二 0:00	应用程序	236 KB
etc1tool.exe	1/1 周二 0:00	应用程序	426 KB
fastboot.exe	1/1 周二 0:00	应用程序	1,611 KB
hprof-conv.exe	1/1 周二 0:00	应用程序	43 KB
libwinpthread-1.dll	1/1 周二 0:00	应用程序扩展	227 KB
make_f2fs.exe	1/1 周二 0:00	应用程序	479 KB
make_f2fs_casefold.exe	1/1 周二 0:00	应用程序	479 KB
mke2fs.conf	1/1 周二 0:00	CONF 文件	2 KB
mke2fs.exe	1/1 周二 0:00	应用程序	735 KB
NOTICE.txt	1/1 周二 0:00	文本文档	2,768 KB
source.properties	1/1 周二 0:00	Properties 源文件	1 KB
sqlite3.exe	1/1 周二 0:00	应用程序	1,136 KB

- 【可选步骤】将上述文件夹的路径加入到系统环境变量以使 adb 、 fastboot 等程序能够在任意位置调用 (如果不进行此处步骤，则下述步骤中的 cmd 和 powershell 7 请在上述 Android SDK Platform-Tools 解压后的文件夹目录中运行，并替换 adb 和 fastboot 指令为 .\adb.exe 和 .\fastboot.exe 执行)

- 通过手机品牌官网下载或者以抓包的方式获取手机的系统安装包并解压获得 boot.img 文件

- 在手机上安装 Magisk

- 将上述步骤获取到的 `boot.img` 文件传输到手机中，并用 Magisk 对其进行修补

主页 ⚙️

Magisk [安装]

当前 **无法获取**
Zygisk 否
Ramdisk 是

App 📥 安装

最新 25.0 (25000) (31)
当前 25.0 (25000)
包名 com.topjohnwu.magisk

支持开发

Magisk 将一直保持免费且开源，向开发者捐赠以表示支持。

关注我们

关注我们

@topjohnwu

@vvb2060

@yujincheng08

@RikkaW

主页　　超级用户　　日志　　模块

← 安装

⊖　选项　　　　　　　　　　下一步

☑　修补 boot 镜像中的 vbmeta

⊖　方式

2022.6.7 Magisk v25.0

Another major release! A lot of the changes aren't visible at the surface, but v25 is actually a really substantial upgrade!

MagiskInit Rewrite

A significant portion of `magiskinit` (the critical software that runs before your device boots up) is completely rewritten from scratch. Ever since Android introduced [Project Treble](#) in Android 8.0, Magisk has been constantly fighting against the increasingly complex partitioning and early mount setups of all kinds of devices, sometimes with weird OEM specific implementations. It got to a point that `magiskinit` had become so complicated that few people (including myself!) were aware of every detail, and maintaining this piece of software like this was clearly not sustainable. After many months of planning (yes, this whole re-architecture has been in my head for a long time) and some help from external contributors, a whole new `sepolicy` injection mechanism is introduced into Magisk, solving the "SELinux Problem" once and for all.

Since this is a full paradigm shift on how Magisk hot-patch the device at boot, several behaviors that many developers implicitly relied on might not exist. For example, Magisk no longer patches fstabs in most scenarios, which means AVB will remain intact; some custom kernels rely on AVB being stripped out for them by Magisk.

MagiskSU Security Enhancements

The superuser functionality of Magisk has not seen much

← 安装

✓ 选项

⊖ 方式 开始 →

◉ 选择并修补一个文件

2022.6.7 Magisk v25.0

Another major release! A lot of the changes aren't visible at the surface, but v25 is actually a really substantial upgrade!

MagiskInit Rewrite

A significant portion of `magiskinit` (the critical software that runs before your device boots up) is completely rewritten from scratch. Ever since Android introduced [Project Treble](#) in Android 8.0, Magisk has been constantly fighting against the increasingly complex partitioning and early mount setups of all kinds of devices, sometimes with weird OEM specific implementations. It got to a point that `magiskinit` had become so complicated that few people (including myself!) were aware of every detail, and maintaining this piece of software like this was clearly not sustainable. After many months of planning (yes, this whole re-architecture has been in my head for a long time) and some help from external contributors, a whole new `sepolicy` injection mechanism is introduced into

Magisk, solving the "SELinux Problem" once and for all.

Since this is a full paradigm shift on how Magisk hot-patch the device at boot, several behaviors that many developers implicitly relied on might not exist. For example, Magisk no longer patches fstabs in most scenarios, which means AVB will remain intact; some custom kernels rely on AVB being stripped out for them by Magisk.

MagiskSU Security Enhancements

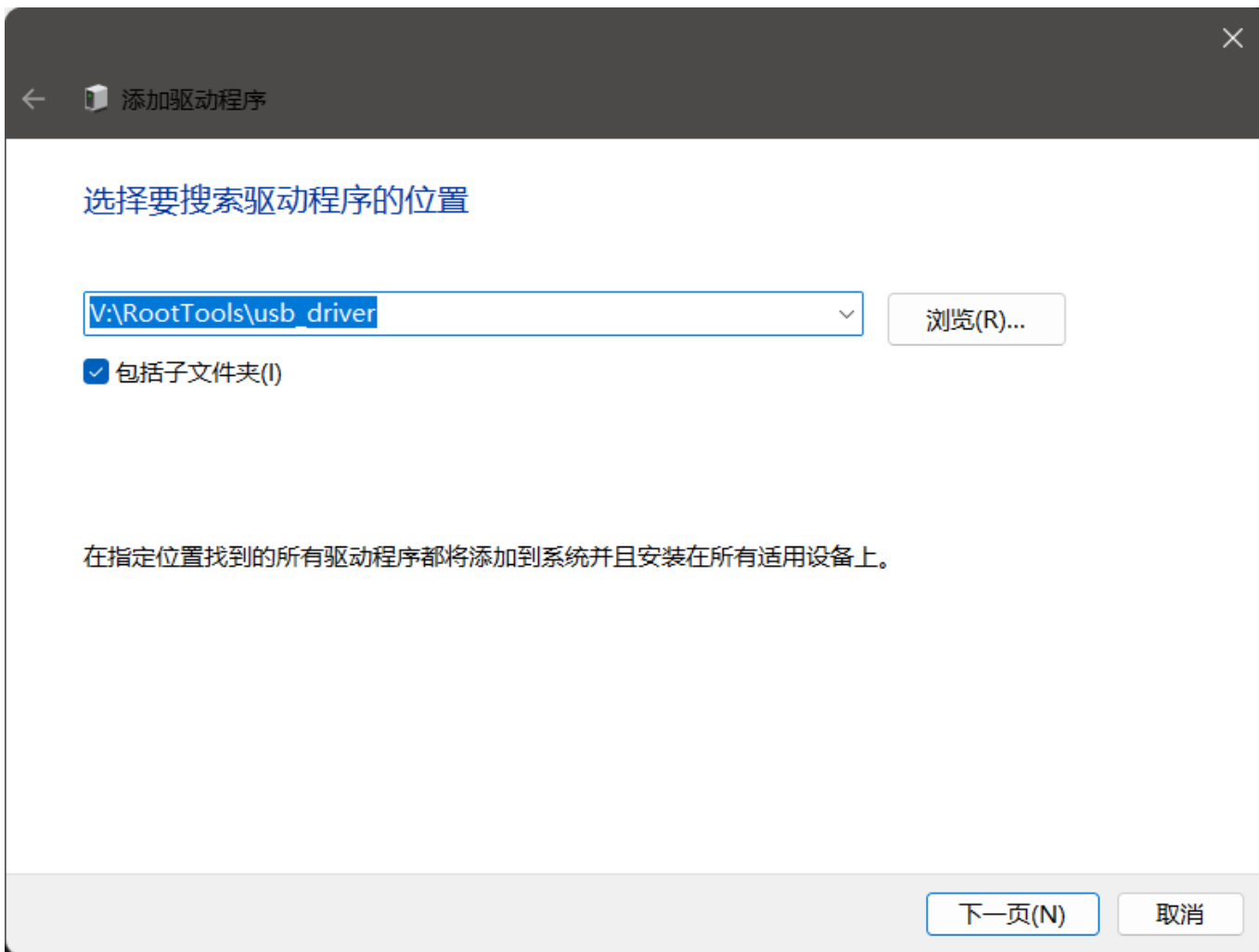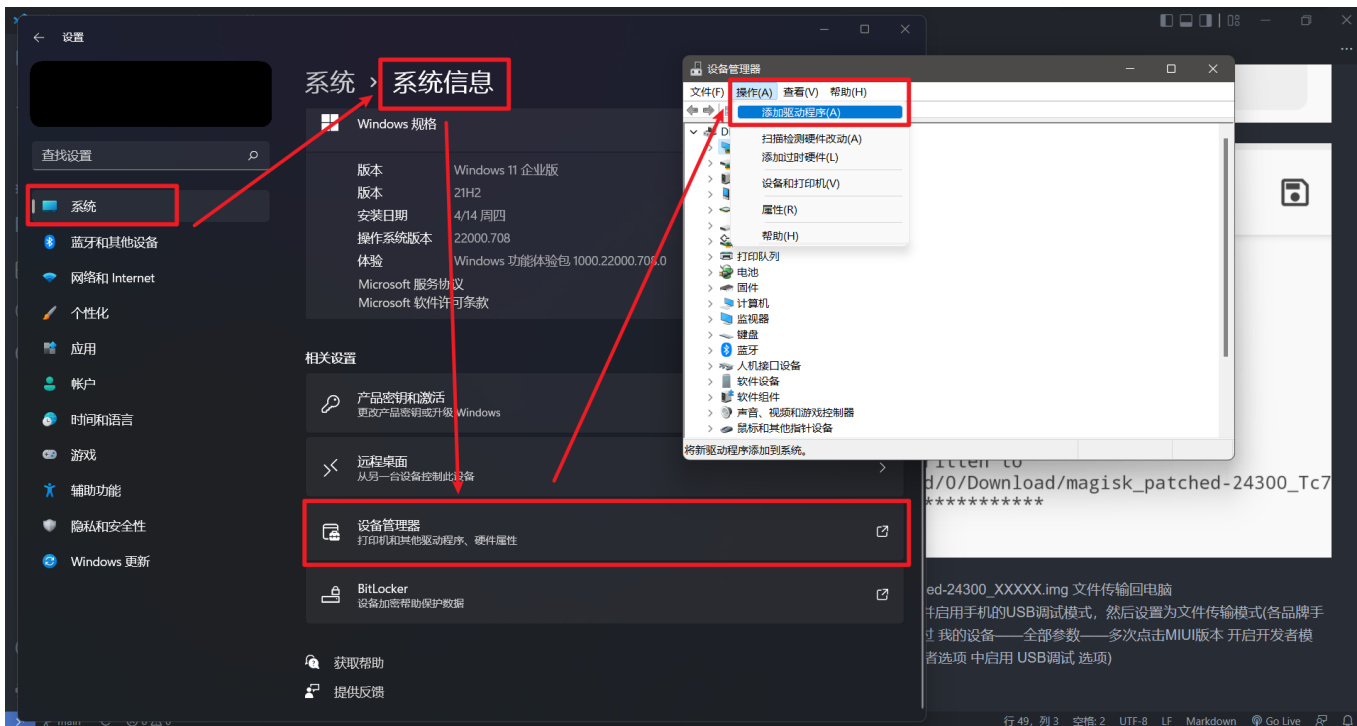The superuser functionality of Magisk has not seen much

---

← **安装**
完成！

🖫

```
- Device platform: arm64-v8a
- Installing: 25.0 (25000)
- Copying image to cache
- Unpacking boot image
- Checking ramdisk status
- Stock boot image detected
- Patching ramdisk
- Repacking boot image


**************************
 Output file is written to
 /storage/emulated/0/Download/magisk_patched-25000_m4t
**************************
- All done!
```

- 将修补后的 `magisk_patched-25000_XXXXX.img` 文件传输回电脑

- 将手机通过USB连上电脑并启用手机的USB调试模式，然后设置为文件传输模式(各品牌手机不同，小米手机可以通过 我的设备 —— 全部参数 —— 多次点击 `MIUI版本` 开启开发者模式，在 更多设置 —— 开发者选项 中启用 `USB调试` 选项)

- 【可选步骤，适用于USB连接有问题的人】下载 Google USB 驱动压缩包并解压到一个文件夹后安装

选择要搜索驱动程序的位置

V:\RootTools\usb_driver

浏览(R)...

☑ 包括子文件夹(I)

在指定位置找到的所有驱动程序都将添加到系统并且安装在所有适用设备上。

下一页(N)　　取消

Windows 安全中心

你想安装这个设备软件吗?

名称: Google, Inc. Android Phone
发布者: Google LLC

☑ 始终信任来自 "Google LLC" 的软件(A)。   安装(I)   不安装(N)

⚠ 你应仅从可信的发布者安装驱动程序软件。我如何确定哪些设备软件可以安全安装?

添加驱动程序

驱动程序已成功安装

Windows 已成功添加和安装所有指定的驱动程序

android_winusb.inf: 已成功添加 oem2.inf 并安装在 1 设备上(s)

关闭(C)

- 在电脑上打开 `cmd` 或者 `powershell 7`，输入 `adb devices` 回车执行查看是否能检测到手机，如果没有检测到则返回上一步安装 Google USB 驱动

- 继续输入 `adb reboot bootloader` 回车执行使手机进入 fastboot 模式(也可以在手机关机状态下，同时按住 电源 和 音量+ 键几秒后进入)

```
PowerShell 7.2.4
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

PS C:\Users\SekiBetu> adb devices
adb server version (31) doesn't match this client (41); killing...
* daemon started successfully
List of devices attached
bb983c01        device

PS C:\Users\SekiBetu> adb reboot bootloader
PS C:\Users\SekiBetu>
```

- 继续输入 `fastboot flash boot 路径\magisk_patched-24300_XXXXX.img` 回车执行刷入通过
  Magisk 修补后的上述文件

- 继续输入 `fastboot reboot` 或者长按电源键关机后重启手机，至此，Magisk 的安装就完成了

```
PS C:\Users\SekiBetu> fastboot flash boot "V:\RootTools\platform-tools\magisk_patched-25000_m4tOA.img"
Sending 'boot' (52736 KB)                    OKAY [  1.184s]
Writing 'boot'                               OKAY [  0.188s]
Finished. Total time: 1.588s
PS C:\Users\SekiBetu> fastboot reboot
Rebooting                                    OKAY [  0.000s]
Finished. Total time: 0.002s
PS C:\Users\SekiBetu> |
```