Android搞机之打开系统调试总开关ro.debuggable

原创 BeilunYang 悖论的技术小屋 2023年10月11日 00:43 新加坡

前言

几乎所有应用市场中的 Android 应用，都处于非可调试状态。如果我们需要调试 Android 应用，往往需要反编译对应的 apk，然后修改 apk 的 AndroidManifest.xml 中的 application 标签，将android:debuggable 属性设置为 true。然后进行回编译

```
<application android:debuggable="true">
</application>
```

这样做不仅麻烦，而且如果对应的 app 做了签名校验，可能会使 app 无法正常运行。

在 Android 系统中一个应用能否被调试是这样判断的：当 android 启动时，系统属性 ro.debuggable 为1，系统中所有的程序都是可以调试的。如果系统中的 ro.debuggable 为 0， 则会判断程序的 AndroidManifest.xml 中 application 标签中的 android:debuggable 属性是否为 true。

所以，我们可以通过修改 default.prop 文件中的 ro.debuggable 属性来调试设备中的所有应用。

下面介绍二种修改 ro.debuggable 的方式

方式一（不推荐）

注入 init 进程，修改内存中的属性值，只要init进程不重启，这些属性值就会生效。但是如果设备重启，则修改的属性值就失效。

前提：需要有 su 命令（root）

具体方法:

1. 在 Github 上搜索 mprop，下载对应的 mprop 工具
2. `adb push ./mprop /data/local/tmp` 将 mprop 推送到手机
3. `adb shell` 进入手机 shell
4. `su` 切换到 root

5. `cd /data/local/tmp & chmod 777 ./mprop`
6. `./mprop ro.debuggable 1`

方式二 （推荐）

前提：需要先安装 Magisk

具体方法:

1. 在 Github 上搜索 MagiskHidePropsConfig，下载对应的 MagiskHidePropsConfig 模块
2. 在 Magisk 中安装下载的 MagiskHidePropsConfig 模块并开启
3. `adb shell`
4. `props`
5. 输入 5 ， Add/edit custom props

```
MagiskHide Props Config v6.1.2
by Didgeridoohan @ XDA Developers

=====================================
 Select an option below.
=====================================

1 - Edit device fingerprint
2 - Force BASIC key attestation
3 - Device simulation (disabled)
4 - Edit MagiskHide props (active)
5 - Add/edit custom props
6 - Delete prop values
7 - Script settings
8 - Collect logs
u - Perform module update check
r - Reset all options/settings
b - Reboot device
e - Exit

See the module readme or the
support thread @ XDA for details.

Enter your desired option: 5
```

6. 输入 n, New custom prop

```
MagiskHide Props Config v6.1.2
by Didgeridoohan @ XDA Developers

====================================
 Custom props
 Select an option below:
====================================

Set or edit custom prop values for your device.

Currently no custom props set.
Please add one by selecting
"New custom prop" below.

n - New custom prop
b - Go back to main menu
e - Exit

See the module readme or the
support thread @ XDA for details.

Enter your desired option: n
```

7. 输入 ro.debuggable

```
MagiskHide Props Config v6.1.2
by Didgeridoohan @ XDA Developers

====================================
 New custom prop
====================================

Enter the prop to set. Example:
ro.sf.lcd_density

b - Go back
e - Exit

Enter your desired option: ro.debuggable
```

8. 输入 y

```
MagiskHide Props Config v6.1.2
by Didgeridoohan @ XDA Developers

====================================
 ro.debuggable
====================================

ro.debuggable is
one of the sensitive props that can be
set by the MagiskHide props option.

Are you sure you want to proceed?

y - Yes
n - No
e - Exit

Enter your desired option: y
```

9. 输入 1

```
MagiskHide Props Config v6.1.2
by Didgeridoohan @ XDA Developers

====================================
 ro.debuggable
====================================

Enter the value you want to set
ro.debuggable to,
or select from the options below.

The currently set value is:
0
Please enter the new value.

b - Go back
e - Exit

Enter your desired option: 1
```

10. 输入 y

```
MagiskHide Props Config v6.1.2
by Didgeridoohan @ XDA Developers

====================================
 ro.debuggable
====================================

This will set ro.debuggable to:

1

Pick an option below to change
what boot stage the prop will
be set in, or set/reset a delay:

1 - Default (current)
2 - post-fs-data
3 - late_start service
4 - Both boot stages
d - Delay

Do you want to continue?

Enter y(es), n(o), e(xit)
or an option from above: y

Working. Please wait...


Working. Please wait...


Working. Please wait...


Working. Please wait...


Working. Please wait...
```

```
MagiskHide Props Config v6.1.2
by Didgeridoohan @ XDA Developers

====================================
 Reboot - ro.debuggable
====================================

Reboot for changes to take effect.

Do you want to reboot now (y/n)?

Enter y(es), n(o) or e(xit): y

Rebooting...
```

结语

通过上述两种方式修改 ro.debuggable 的值后，在手机 shell 中输入 **getprop ro.debuggb**

`le` 应该会得到 1。此时我们就能愉快地调试手机上的所有 app 了。