目录

瑞芯微android固件包介绍

一、解包、打包

二、固件升级

三、固件修改

１、固件精减、添加APK软件

２、提取Root权限

３、修改用户分区大小

A．修改HWDEF文件：

B．修改parameter文件

5、美化界面

A．界面美化

B．修改开机LOGO（Android启动时，出现闪动的ANDROID字样的动画图片）

６、桌面美化

瑞芯微android固件包介绍

瑞芯微的android固件包分两种：

一种为量产升级包（暂且如此称呼吧，PS：其实称之为开发包较为合适，因为是使用开发工具进行升级。），使用量产升级工具RKAndroidTool.exe进行升级，量产升级包的文件包含：HWDEF、package-file、parameter、recover-script、Rock28Boot(L).bin、update-script和一个Image文件夹，里边又包含boot.img、 kernel.img、 misc.img、 recovery.img 、system.img五个镜像文件。

System.img包含所有用户资源，大部分情况下修改system.img文件就能达到我们的目的。本文也是重点围绕system.img的修改。

另一种为用户升级包（也暂且如此称呼吧），即将上述量产升级包的文件用工具打包成一个文件――update.img，使用用户升级工具RKAndroidDM.exe进行升级。此文件包需通过解包成量产升级包后才能修改，修改后再打包成update.img进行升级。

一、解包、打包

对于update.img的解包、打包，需用到附件“打包解包工具”中的AFPTool.exe、mkupdate.bat、unpack.bat三个文件，其中unpack.bat为解包工具，

mkupdate.bat为打包工具。将用户升级包update.img和上述三个文件放在同一目录下，双击unpack.bat后，就可以将用户升级包解包成6个文件和一个Image文件夹，即和量产升级包完全相同的文件。此时可对相应的文件进行修改，修改完成后，再双击mkupdate.bat，会在Image文件夹下产生一个update.img，此文件就是打包后新生成的用户升级包文件。

对于system.img的解包、打包，需用到cramfsck、mkcramfs两个工具，此img文件和工具需在Linux（Ubuntu、RedHat等）系统下操作和使用，来进行解包、打包，cramfsck为解包工具，mkcramfs为打包工具。

先通过本地硬盘、Ｕ盘或者Live CD启动到Linux下（Linux相关知识和安装不在本篇介绍范围内，请自行Google），然后将system.img、cramfsck、mkcramfs三个文件拷贝到系统的root文件夹下。（有些Linux系统对挂载的其它分区或磁盘兼容性不好，所以拷贝到系统分区进行操作可减少出问题的可能性，本文涉及到Linux部分的操作以BackTrack3操作系统为示例。部分人反映用Ubuntu的精简等版本时用不了已编译好的cramfsck和mkcramfs，所以在教程包中又放入了一个deb的文件，在启动到Linux后双击就可以像Windows一样安装它了。）

打开一个shell，在shell中输入：

cramfsck -x system system.img

对system.img文件进行解包，执行完成后，会产生一个名为system的文件夹，如下图所示：

也可以采用以下方法进行解包，原理就是mount这个镜像文件，然后再拷贝出来，命令如下：

mkdir system

sudo mount -t cramfs -o loop system.img system

tar cvzf system.tgz system

sudo umount system

rm -r system

tar xzvf system.tgz

用这个方法的好处是可以避免某种情况下出错的可能，第一种方法在某些情况下会造成某些文件损坏，有碰到过。

解包后的System文件夹内包含9个文件夹和1个文件，简单说明如下：

/system/app 系统应用程序存放目录

/system/bin 系统的本地程序，是binary二进制的程序，里面主要是Linux系统自带的组件。

/system/etc 系统的配置文件，比如APN接入点设置等核心配置。 /system/fonts 字体文件夹。

/system/framework 主要是一些核心的文件，从后缀名为jar可以看出是系统平台框架。

/system/lib 存放的主要是系统底层库，如平台运行时库。

/system/media 铃声音乐文件夹，除了常规的铃声外还有一些系统提示事件音

/system/usr 用户文件夹，包含共享、键盘布局、时间区域文件等。

/system/xbin 存放系统管理工具，他们都是为系统管理员准备的，是一些系统管理和配置工具。

/system/build.prop 属性文件，“关于MID”中所显示的软件版本、内核、机型等信息。

通过上面进行简单的介绍，相信你已有了一个大概的了解了。

此时可对system文件夹下的文件进行其它修改了，比如提取root权限、固件精减、APK替换修改等操作。

修改完成后，需要对system文件夹进行打包，在shell中输入：

mkcramfs system system02.img

(为了便于区分原先的img文件，所以建议重新生成的文件不要与原文件名一样。)

此时会在root目录下生成一个新文件system02.img，这个文件就是我们修改好并重新打包OK的文件了。

此时，对于update.img和system.img两个文件的解包、打包操作就介绍完了。对于system.img和相应的文件是否需要打包成用户升级包update.img就看各位是否有需要了。

二、固件升级

固件升级有两种工具可实现（其实还有第三种升级――即通过MID本机进行升级，不过需要原生软件和硬件支持才可以实现，目前发现上市的机子还无此功能。所以略过 ），即量产升级、用户升级。

量产升级：将量产升级包的6个文件和一个文件夹，放入../升级工具/量产升级工具\_RKAndroidTool/rockdev文件夹下，然后打开量产工具

RKAndroidTool.exe，如下图所示：

（如有需要勾选Loader、Backup选项，对于软件跨版本较大或修改过分区等情况可勾选Loader，如果你的MID没有Recover功能，Backup选项无需勾选。题外话太多了，现转移到正题。）

关机状态下长按ESC键或菜单键（视机型而定，具体请自行查找相应信息）的同时连接PC，按提示安装驱动(首次使用)，驱动路径指向.. /升级工具/rk28usb‐Driver，安装好驱动后按“执行”即可完成升级。

注意：如果是Vista、Windows7系统需用管理员权限运行本工具，否则会提示“测试设备失败”，造成升级失败。

用户升级：打开用户升级工具RKAndroidDM.exe，如下图所示：

点击“ ”按钮，选择电脑中要升级的用户升级文件update.img，然后按量产升级的方法连接你的MID，提示找到设备后按“升级”按钮进行升级，完成后提示“升级成功”后拔掉USB线重新开机即可。

三、固件修改

前面讲解了那么多了，前戏应做的很足了，现在开始介绍各位同鞋最为关心滴事、最最为想做滴事情，我再次手把手滴开始教各位同鞋鸟，希望能和大家一起达到目的，冲向高潮。吼 ！！！

１、固件精减、添加APK软件

将system.img解包，解包后将../system/app目录下的不需要的APK文件进行删除、修改、替换，以制作适合自己的固件包，对于app目录内不清楚用途的APK文件，请勿随意删除，以免引起不必要的问题。

注意：据说个别APK软件需自带的库文件支持才能正常运行，此时可用WinRAR等压缩软件将APK文件打开（将.apk后缀改成.zip，然后用压缩软件打开即可），从里边找到后缀为.so的文件，然后放入../system/lib文件夹下即可。 修改完成后，然后进行打包、升级、测试。

２、提取Root权限

将system.img解包，解包后将“取root权限文件”目录中的Superuser.apk、su两个文件分别放进下列目录：

Superuser.apk ---> ../system/app

su ---> ../system/bin

打开一个shell，然后用chmod 6755修改文件的权限，如图示。

Chmod 6755 /system/app/Superuser.apk

Chmod 6755 /system/bin/su

上述命令需注意大小写，否则有可能会出错。修改完成后打包即可。

我开始在验证过程中，因使用了较老的root explorer版本根本不能进入资源管理器，于是更换了最新版V2.94，是能进资源管理器界面了，但是却不能修改或删除system下的文件，可能有人会怀疑这是否真正的取得了root权限？我可以很负责的告诉你，已经取得了root权限，因为运行drocap2这类root权限的软件是灰常正常滴。

嗯，其实这里又涉及到一个专业知识了，请 坐好捏，哎，后面那位同鞋别看别人了，说的就是你。现在仔细听我讲解：

瑞芯微android系统固件的system分区采用的是cramfs文件系统。

cramfs文件系统是一个压缩式的文件系统，它并不需要一次性地将文件系统中的所有内容都解压缩到内存之中，而只是在系统需要访问某个位置的数据的时侯，马上计算出该数据在cramfs文件系统中的位置，将其实时地解压缩到内存之中，然后通过对内存的访问来获取文件系统中需要读取的数据。cramfs文件系统中的解压缩以及解压缩之后的内存中数据存放位置都是由cramfs文件系统文件系统本身进行维护的，用户并不需要了解具体的实现过程，因此这种方式既方便，又节省了存储空间。cramfs文件系统的数据都是预先经过处理、打包的，这种系统是一种只读、不支持写操作的文件系统，在刷到机器里后，这个分区就是只读的，不能做任何更改。所以，刷机后是不能对这个系统进行修改的，只能在刷机前对system.img进行解包、修改，以达到我们的目的。

３、修改用户分区大小

部分同鞋使用了MID一段时间后，就会为用户区空间太小装不了几个软件而发愁，其实，你不用发愁，只要稍稍修改一下两个文件就可以将分区加大。现在出产的MID一般都是配备2GB以上的内存，划个几百M至1G都不会太影响本机使用的，再者现在TF卡那么便宜，都是标配2~4G以上的容量了。所以即便将用户区再划大些都不会有太大的影响。

（题外话：还有同鞋在寻找APP2SD的功能，个人建议不如修改一下这两个文件，将用户区划大一些来得实在，一来在本机上读取软件稳定性会高些，二来不会因TF卡的问题导至软件出问题嘛！）

言归正传：将用户升级包update.img解包（如果已经是量产升级包，略过此解包操作），找到其中的HWDEF、parameter两个文件并备份。再用UE（UltraEdit32，其实用记事本也可以，不过看起比较乱）修改两个文件的分区偏移量和分区大小，是以16进制表示，前一个分区的偏移量和大小加起来就是后面一个分区的偏移量，我们需让用户分区增大，所以只修改用户分区即可，只需修改userdata、user两个分区的偏移量和大小即可。

A．修改HWDEF文件：

用UE打开HWDEF，找到如下部分的代码（请注意红色部分数据）：

mtd\_id=rk28xxnand

#Format: part\_name offset:size

parameter 0x00000000:0x00001000:fh

misc 0x00001000:0x00001000:f

kernel 0x00002000:0x00003000:f

boot 0x00005000:0x00002000:f

recovery 0x00007000:0x00003000:f

system 0x0000A000:0x0001E000:f

backup 0x00028000:0x00026000:

cache 0x0004E000:0x0001E000:

userdata 0x0006C000:0x0001E000:

user 0x0008A000:0xFFFFFFFF:

END

简单解释一下，上面的userdata分区表示：偏移量为0x0006C000，分区大小为：0x0001E000，比如我们需将使用空间由原来的123M增大一倍到246M，即

0x0001E000＋0x0001E000＝0x0003C000，那么，下一个分区user的偏移量就变成6C000＋3C000＝0x000A8000，修改后新的数据如下：

userdata 0x0006C000: 0x0003C000:

user 0x000A8000:0xFFFFFFFF:

修改后保存。对HWDEF的修改完成了。

B．修改parameter文件

再用UE打开parameter，找到最后一行，其部分代码如下：

CMDLINE: noinitrd c,115200n8n androidboot.c init=/init

root=/dev/mtdblock2 mem=128M@0x60000000

mtdparts=rk28xxnand:0x00001000@0x00001000(misc),0x00003000@0x00002000(kernel),0x00002000@0x00005000(boot),0x00003000@0x00007000(recovery),0x0001E000@0x0000A000(system),0x00026000@0x00028000(backup),0x0001E000@0x0004E000(cache), 0x00040000 @0x0006C000(userdata),-@ 0x000AC000 (user)

此段代码@前面表示分区大小，@后面表示偏移量。userdata前面的6个分区大小和偏移量都能和HWDEF文件中的一一对应起来，但userdata的分区大小明显要大很多，暂不明白为何要加大一些。查看过几个不同机型的这些文件，大小也有差距，在22000-62000（16进制）之间;为了不出问题，我们也依照那样做吧，所以我们也在userdata空间的大小上面也加上22000至62000之间的一个数值吧。

所以，此处userdata的分区大小为：3C000（扩容后的分区大小）

+22000=5E000,那下一个分区user的偏移量也变成了：5E000（新分区大小）+6C000（偏移）=CA000。修改过的数据如下：

0x0005E000@0x0006C000(userdata),-@0x000CA000(user)

修改后保存。对parameter的修改也完成了。用刚才改好的两个文件替换原先的两个文件，然后重新打包、升级。

不同机型分区大小可能会有差别，所以附件中放有原始的和修改好的两个文件，以供参考！此文件仅供参考，请勿直接替换，出了问题概不负责！ ４，修改设置中“关于MID”中的机型型号

将system.img进行解包，解包后在system文件夹下找到

build.prop

将build.prop文件用UE打开，找到ro.product.model=sdkDemo一行，将其中的sdkDemo改成你想要显示的文字，比如BM999，修改后保存，然后重新打包烧录即可。

5、美化界面

这个又涉及到APK文件的修改了，这部分的教程就不作过多的介绍了，有需要的同鞋可以上网去Google下相关资料，大把的教程可供参考。

将system.img进行解包，解包后在../system/framework文件夹下找到

framework-res.apk，将.APK后缀改名为.zip，然后将其中的assets、res两个文件夹解压出来开始我们的美化工作。要注意修改后的图片分辨率大小和图片格式要与原来保持一致，否则会出错的哦。

A．界面美化

找到解压后的下列两个目录，这两个目录存放所有界面的系统图标，可对需要修改的界面小图标进行美化：

../framework-res/res/drawable

../framework-res/res/drawable-land

B．修改开机LOGO（Android启动时，出现闪动的ANDROID字样的动画图片）

Android 的系统登录动画类似于Windows系统的滚动条，是由前景和背景两张PNG图片组成，这两张图片也是位于../system/framework/framework-res.apk文件当中。前景图片（android-logo-mask.png）上的Android文字部分镂空，背景图片（android-logo-shine.png）则是简单的纹理。系统登录时，前景图片在最上层显示，程序代码控制背景图片连续滚动，透过前景图片文字镂空部 分滚动显示背景纹理，从而实现动画效果。以相同的原理修改或替换下面两张图片即可达到目的。

../framework-res/assets/images/android-logo-mask.png

../framework-res/assets/images/android-logo-shine.png

android-logo-mask.png ：Android默认的前景图片，文字部分镂空，大小256×64

android-logo-shine.png ：Android默认的背景图片，有动感效果，大小512×64

美化完成后，将修改过的图片替换掉APK文件中相应的文件，然后将APK文件中META-INF文件夹内的CERT.SF、CERT.RSA两个文件删除，然后用签名工具重新签名。再将签名后的APK文件替换掉原先的文件，之后重新打包成system.img并用工具升级即可。

６、桌面美化

感觉桌面默认的公版壁纸、搜索条、快捷键等图标太难看？没问题，把它都换了吧。

将system.img进行解包，解包后在../system/app文件夹下找到Launcher.apk，将.APK后缀改名为.zip，然后将其中的res文件夹解压出来，将需要美化的图片进行美化、替换，修改好后按照上面的方法将文件替换、签名、打包再升级即可。

基础篇教程完毕！敬请关注进阶篇。因本人水平有限，教程中难免会有错误之处，欢迎指正！

————————————————

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

原文链接：https://blog.csdn.net/qq\_33611327/article/details/104499375