

[主页](#) [论坛](#) [导航](#) [MOTO](#) [IMEI](#) [下载](#) [ppi计算](#) [新手教程](#) [手机商城](#) [京东](#) [积分充值](#)[登录](#) [注册](#)[设为首页](#) [收藏本站](#) [微博](#) [导读](#)[商务合作](#) [申请版主](#) [黑武故事](#)

搜索

热门关键字: MOTO X ROOT MOTO G ROOT 刷机教程

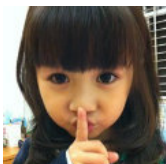
[论坛](#) [资源分享区](#) [Android开发/入门](#) [高通、猎户机型Android典型bootloader分析](#)

发帖

[返回列表](#)

查看: 5148 | 回复: 9

尘封之泪



[入门了解] 高通、猎户机型Android典型bootloader分析 [\[复制链接\]](#) [微博分享](#)

发表于 2014-2-4 11:26 | 只看该作者 | 只看大图

[楼主](#) [电梯直达](#)

本帖最后由 尘封之泪 于 2014-2-4 11:31 编辑

1、bootloader是什么?

简单地说, bootloader 就是在操作系统内核运行之前运行的一段小程序。通过这段小程序, 我们可以初始化硬件设备、建立内存空间的映射图, 从而将系统的软硬件环境带到一个合适的状态, 以便为最终调用操作系统内核准备好正确的环境。

Android系统基于Linux, 所以bootloader部分也是与传统的嵌入式设备上运行的Linux没有什么区别。由于除Google外的大部分Android厂商都没有提供bootloader的源代码, 所以分析手机设备的bootloader需要使用逆向工程的手段, 当然由于有了Google官方的开源bootloader代码做参考, 能让分析工作轻松不少。本文中使用的分析工具为IDA 6.5, 针对的手机设备为N9006, 固件版本为N9006ZCUDMK2。

2、bootloader典型结构

这部分会以高通MSM8960为例子介绍下Bootloader的典型结构。

高通MSM8960中包含多个运算单元, 分别负责引导过程中的不同功能, sbl1的代码负责加载sbl2, sbl2加载tz和sbl3, sbl3加载appsbl, appsbl加载HLOS (基带)。

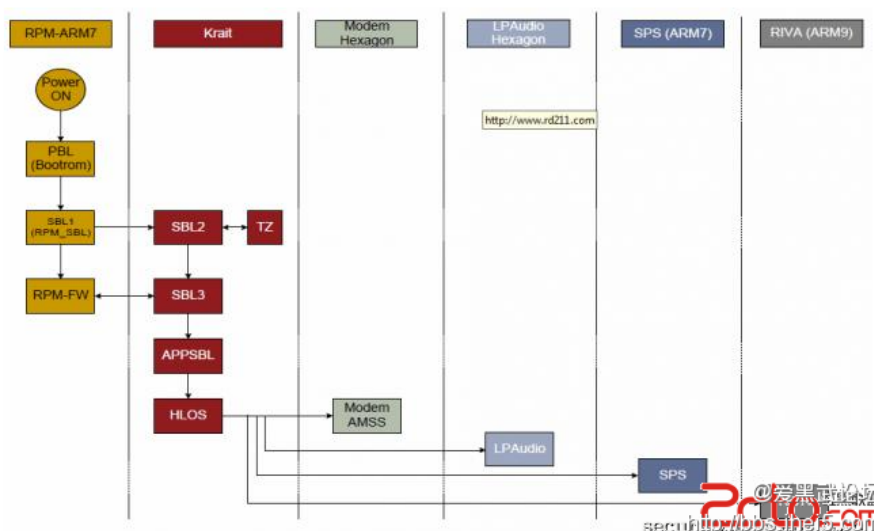


图1 SecureBoot 3.0 的Code Flow

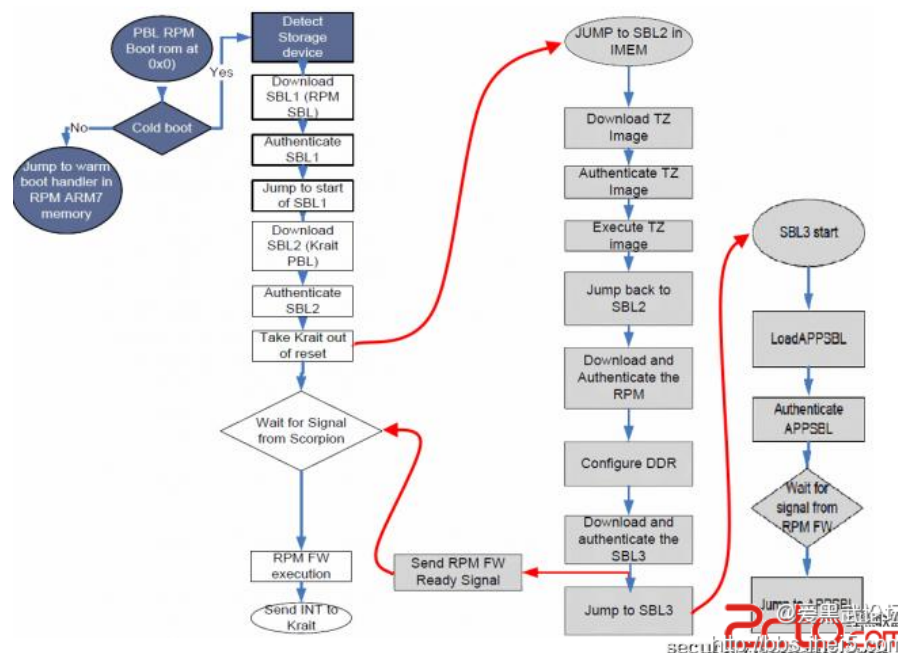


图2 MSM8960引导过程简化流程图

3、Note3的bootloader结构分析

国行版Note3 (N9006) 使用的CPU是MSM8974, 它的bootloader结构与典型的MSM8960差不多, 最大的区别就是把sbl1,sbl2,sbl3整合进了一个文件sbl1中, TrustZone和APPSBL都由sbl1进行验证和加载, 以下为几个主要功能的加载代码分析。

sbl1的功能是对硬件进行初始化并加载其他模块, 需要加载的模块信息按顺序保存在sbl1中, 对应每个模块的数据是一段大小为0x64字节的模块信息数据内, sbl1中有一个循环负责验证和加载所有需要的其他模块(tz, rpm, wdt, appsbl), 加载代码会根据模块信息内的数据调用不同的加载器加载和验证的代码, 具体代码如下图。

```

v4 = 10;
if ( !a1 || !pAllModuleData )
{
    sub_F801D834((int)"boot_config.c", 434, 0x3000);
    while ( 1 )
    {
    }
    pModuleData = pAllModuleData;
    for ( result = *(_DWORD *)pAllModuleData; *(_DWORD *)pModuleData; result = *(_DWORD *)pModuleData )
    {
        if ( *(_DWORD *)pModuleData == v4 )
        {
            SUB_N9006SBL_LoadModule(a1, pModuleData);
            pModuleData += 0x64;
        }
    }
    return result;
}

```

图3 sbl1中循环加载全部模块的代码

```

v7 = *(_DWORD *) (pModuleData + 0xC); // 0x0C处数据表示模块类型
if ( v7 )
{
    if ( v7 == 1 )
    {
        if ( sub_F801ED2C() )
        {
            sub_F801D94C(*(_DWORD *) (pModuleData + 24), *(_DWORD *) (pModuleData + 68));
            v13 = *(_DWORD *) (pModuleData + 0x38);
            if ( !v13 )
            {
                sub_F801DB34((int)"boot_config.c", 276, 12301);
                while ( 1 )
                ;
            }
        }
        sub_F801D564(v13, (int)&v21);
        if ( *(_DWORD *) (pModuleData + 0x18) == 1 )// 根据0x18处的数据判断是否需要对该模块进行验证
        {
            SUB_N9006SBL_AuthenticatorInit((int)&v21);
            v14 = sub_F801E294();
            sub_F80212C4(v14);
            v15 = SUB_N9006SBL_AuthenticateModule(v2, *(_DWORD *) (pModuleData + 16));
            if ( v15 )
            {
                sub_F801DB34((int)"boot_config.c", 296, v15);
                while ( 1 )
                ;
            }
        }
    }
}

```

图4 sbl1中对待加载模块进行验证

```

ROM:F8047188 15 00 00 00 g_AllModuleData DCD 0x15 ; DATA XREF: sub_F803D5A4+102↑to
ROM:F8047188 ; ROM:off_F803D738↑to ...
ROM:F804718C 00 00 00 00 DCD 0
ROM:F8047190 1B 00 00 00 DCD 0x1B
ROM:F8047194 01 00 00 00 DCD 1
ROM:F8047198 07 00 00 00 DCD 7
ROM:F804719C 01 00 00 00 DCD 1
ROM:F80471A0 01 00 00 00 DCD 1
ROM:F80471A4 01 00 00 00 DCD 1
ROM:F80471A8 00 00 00 00 DCD 0
ROM:F80471AC C1 20 04 F8 DCD sub_F80420C0+1
ROM:F80471B0 00 00 00 00 DCD 0
ROM:F80471B4 D8 70 04 F8 DCD off_F80470D8
ROM:F80471B8 0C 71 04 F8 DCD off_F804710C
ROM:F80471BC 00 00 00 00 DCD 0
ROM:F80471C0 44 7C 04 F8 DCD unk_F8047C44
ROM:F80471C4 AF 62 04 F8 DCD aTzImageLoadedD ; "TZ Image Loaded, Delta"
ROM:F80471C8 00 00 00 00 DCD 0
ROM:F80471CC 00 00 00 00 DCD 0
ROM:F80471D0 01 00 00 00 DCD 1
ROM:F80471D4 00 00 00 00 DCD 0
ROM:F80471D8 00 00 00 00 DCD 0
ROM:F80471DC 00 00 00 00 DCD 0
ROM:F80471E0 00 00 00 00 DCD 0
ROM:F80471E4 00 00 00 00 DCD 0
ROM:F80471E8 00 00 00 00 DCD 0

```

图5 TZ模块信息数据

图6 APPSBL模块信息数据

固件包里的tz.mbn是加载在TrustZone中的模块，模块格式为elf，这个模块中的代码和系统其他模块代码运行在互相隔离的区域内，权限也比其他模块更高，三星KNOX的很多底层安全特性也是在这部分中实现，关于TrustZone的更多资料可以参考arm官方的说明。

固件包里的aboot.mbn就是APPSBL模块，模块格式为bin，文件最前面的0x28字节的头部描述了bin的加载地址等信息，后面的数据就是实际加载到内存中的映像，整个bootloader中这个模块的代码量最大（很大一部分是openssl的代码），linux内核的验证和加载（正常启动和Recovery模式），ODIN模式等等代码都包含在这个模块内。

图7 aboot.mbn文件头

图8 根据按键和共享内存中的数据确定引导模式

图9 三星特有的ODIN刷机模式代码

4、Note3的bootloader中KNOX系统的底层代码初步分析

Note3提供了一个企业安全套装KNOX，这个系统包含了底层的Customizable Secure Boot和TrustZone-based Integrity Measurement Architecture(TIMa，目前为2.0版本)，系统层的SecurityEnhancements for Android (SE-Android) 和应用层的Samsung KNOX Container，Encrypted File System (EFS)，Virtual Private Network (VPN)，其中Customizable Secure Boot和TIMa的代码包含在Bootloader的aboot.mbn，tz.mbn，NON-HLOS.bin中，功能为保障加载的内核在加载时和运行期的完整性。

通过前面的分析，我们已经知道了tz.mbn和aboot.mbn在加载时已经由sbl1验证过完整性，tz.mbn加载后会在CPU的安全环境下运行，从高权限的隔离区域内对系统的完整性进行监控，而负责加载android内核的aboot.mbn中包含对内核的完整性检测，三星在bootloader每一部分的结尾都会加上自己的签名，加载前会对签名进行验证，以保障系统未被修改过。

图10 tz.mbn中初始化TIMa系统的代码

图11 aboot.mbn中对内核是否使用SEANDROID进行验证

当任何一部分检测代码发现系统异常状况后，就会调用SMC指令通知TrustZone中运行的TIMa系统设置fuse为系统完整性被破坏，此fuse数据一旦被设置后没有办法被重置，系统也无法再次进入KNOX系统。

图12 加载内核前对内核签名和TIMa的测点进行验证

图13 系统完整性检测失败后设置fuse值

当以上所有检测都通过后，bootloader会把内核复制到指定的内存地址并跳到内核的入口继续执行，到此，就进入了系统内核代码的范畴，bootloader的使命也就完成了，跳到linux内核入口的代码见图14。

图14 内核加载和校验完成后跳到内核的入口点继续执行

另外，除了这两个模块外Modem固件相关的NON-HLOS.bin中也有大量TIMa系统相关的文件，由于TIMa系统包含大量硬件相关代码（使用三星猎户座CPU的N900中TIMa系统的实现与高通CPU的N9006差别很大），如果需要进行进一步的分析TIMa在modem中的行为，需要对TrustZone，modem工作方式等有更多了解。

图15 NON-HLOS.bin中包含的大量TIMa相关文件（全文来自网络，有删改）

Android, 高通, bootloader, Android

评分

2



nifa







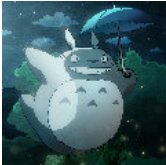




cbhd5233

查看全部评分

分享到:  QQ好友和群  QQ空间  腾讯微博  腾讯朋友

	<div><div><div><div><div><div></div><div>赞同 +0</div></div><div><div></div><div>收藏 +8</div></div></div></div></div></div>
	<div><div>相关帖子</div><div><div><div><div><div></div><div>• 安卓手机明年将会适配3D Touch 是跟风苹果吗?</div><div>• 疯狂喷气机破解版 v1.8.7 一款风靡IOS/Android/WP各种平台的横版跑</div><div>• 第二代Moto X确认将升级Android 6.0</div><div>• 快速定位修改系统不常用字体</div><div>• 不肯去掉黑边的 Moto 360 二代</div></div><div><div><div><div></div><div>• 相似而不相同 谷歌安卓6.0对比苹果iOS9</div><div>• 所有Nexus设备Android 6.0 获取root权限教程</div><div>• android操作系统--好电大户</div><div>• iOS版Android Wear将不支持HealthKit框架!</div><div>• Android Wear国内订制版</div></div></div></div></div></div></div></div>
	<div><div>爱黑武，爱上搞机生活！</div><div><div>回复</div><div>使用道具</div><div>举报</div></div></div>
cs_hebe	<div><div><div><div></div><div>发表于 2014-2-13 13:22 只看该作者</div></div><div>沙发</div></div></div>
<div><div>爱黑武哟</div><div></div></div>	<div><div>感觉我后边很多小朋友会眼冒星星</div><div><div>爱黑武，爱上搞机生活！</div><div><div>回复</div><div>支持</div><div>反对</div><div>使用道具</div><div>举报</div></div></div></div>
wbubian	<div><div><div><div></div><div>发表于 2014-3-21 15:04 只看该作者</div></div><div>板凳</div></div></div>
<div><div>爱黑武哟</div><div></div></div>	<div><div>办公费地方就会给大家个</div><div><div>爱黑武，爱上搞机生活！</div><div><div>回复</div><div>支持</div><div>反对</div><div>使用道具</div><div>举报</div></div></div></div>
自然清淨	<div><div><div><div></div><div>发表于 2014-3-28 09:30 只看该作者</div></div><div>地板</div></div></div>
<div><div></div></div>	<div><div>尘封出品必是精品，始终跟随尘封大大的脚步，认真学习。膜拜.....</div><div><div>爱黑武，爱上搞机生活！</div><div><div>回复</div><div>支持</div><div>反对</div><div>使用道具</div><div>举报</div></div></div></div>
monkey1860	<div><div><div><div></div><div>发表于 2014-6-8 09:39 来自手机 只看该作者</div></div><div>5楼</div></div></div>
<div><div>爱黑武哟</div><div></div></div>	<div><div>真的冒星星了。。</div><div><div>爱黑武，爱上搞机生活！</div><div><div>回复</div><div>支持</div><div>反对</div><div>使用道具</div><div>举报</div></div></div></div>
wsxc009	<div><div><div><div></div><div>发表于 2014-6-17 18:45 来自手机 只看该作者</div></div><div>6楼</div></div></div>

<div>爱黑武呦</div> <div></div>	<div>都是星星啊</div> <div>爱黑武，爱上搞机生活！</div> <div><div>回复支持反对</div><div>使用道具举报</div></div>
wlc001	<div> 发表于 2014-9-30 13:45 只看该作者</div> <div>7楼</div>
<div>爱黑武呦</div> <div></div>	<div>确实都是星星</div> <div>爱黑武，爱上搞机生活！</div> <div><div>回复支持反对</div><div>使用道具举报</div></div>
anyeyinhuo	<div> 发表于 2014-10-25 09:07 只看该作者</div> <div>8楼</div>
<div>爱黑武呦</div> <div></div>	<div>T.T 智商压制</div> <div>爱黑武，爱上搞机生活！</div> <div><div>回复支持反对</div><div>使用道具举报</div></div>
wmslecز	<div> 发表于 2014-11-15 20:09 只看该作者</div> <div>9楼</div>
<div>爱黑武呦</div> <div></div>	<div>果断支持一个..</div> <div>爱黑武，爱上搞机生活！</div> <div><div>回复支持反对</div><div>使用道具举报</div></div>
fanstyle	<div> 发表于 2015-6-11 00:18 来自手机 只看该作者</div> <div>10楼</div>
<div>爱黑武呦</div> <div></div>	<div>bootloader锁这个东西怎么弄得，搞懂了可以来破解一下</div> <div>爱黑武，爱上搞机生活！</div> <div><div>回复支持反对</div><div>使用道具举报</div></div>

发帖

返回列表

Hello, 黑武的好机友！回复想偷个懒？点这里：

请选择快捷回复

 也可以选择最右边 →.→ 的表情哦


高级模式

您需要登录后才可以回帖 登录 | 注册  用QQ帐号登录


发表回复

☐ 回帖后跳转到最后一页

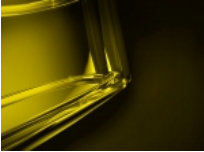
本版积分规则




Moto X Style完美搭配Loui...




Material Lix壁纸 分辨率28...




Droid Turbo 2默认壁纸,分...



质感小岛壁纸静态版, 比...



这颗坚果砸中了谁? -- 坚...



vivo摄影



探索“大人物”的不