华为解锁码手工获取

首先，华为的解锁码是存在系统分区内的，这点不用怀疑，至于是否加密暂时不清楚

根据安智上的神贴所给的信息，我这里再总结一下，

和手机状态和解锁码有关的分区就是nvme，oeminfo，这两个分区，没有涉及到aboot，也就是说aboot是没有加锁的，

其次就是提取解锁码的过程，这里使用的是strings nvme | grep WVDEVID -B 1 这个命令，也就是nvme其实就是个文本文件，里面有一行含有WVDEVID = W V DEV ID，这个值就是所需要的devid，这一点其实是比较难发现的，因为只有官方获取解锁码之后才有机会来验证，还要排除华为对数据进行加密的可能性。

不过也算是学习了，Bootloader锁如果被大范围破解了的话，应该后续华为还是会对其算法进行改进的，不过不会移除倒是真的，因为移除了这个解锁码机制的话那以后如果有客户大量投诉华为不是只有吃大亏？所以移除是不可能移除的。

其次就是新算法的大致可能性，因为在lk阶段是没办法获取手机imei和meid等信息的，所以除非是使用非常手段，能够使用的算法还是预置解锁信息到某个特定位置，不可能是刷机包中的某个文件，因为这些文件是统一分发的，所以只能在出场时候写入到某个特定分区中比如乐视的letvconfig，oeminfo，华为的nvme，小米的….，中兴的factory，等等厂商自定义分区中，然后就是额外加密手段，即通过读取预置的信息，对信息进行某种加密来作为解锁码，这种可能性是有的，而且出现之后可能需要一段时间才能破解，不过都是加密算法，总有高手可以搞定的，自己也该学学这方面的东西了…

华为bootloader需要解锁后才能刷第三方recovery，解锁需要在华为官网上申请解锁码，而且解锁后重新上锁，bootloader的显示不是unlocked，而是relocked，这点不知道是否影响保修，下面介绍如何绕开华为官网解锁bootloader，以及将bootloader恢复成unlocked状态  
首先，你的手机需要未解锁，但需要获得root权限(目前我测下来唯一能实现这个目标的是360root，http://down.360safe.com/360PermRoot/PermRoot.apk)  
其次，需要有一台安装了adb的机器  
下面从adb shell登录到手机开始

1. 255|shell@hwp7:/ $ su
2. root@hwp7:/ # cd /storage/sdcard1/
3. root@hwp7:/storage/sdcard1 # mkdir -p PartitionBackup
4. root@hwp7:/storage/sdcard1 # cd PartitionBackup
5. root@hwp7:/storage/sdcard1/PartitionBackup # dd of=nvme \
6. > if=/dev/block/platform/hi\_mci.0/by-name/nvme
7. 8192+0 records in
8. 8192+0 records out
9. 4194304 bytes transferred in 0.916 secs (4578934 bytes/sec)
10. root@hwp7:/storage/sdcard1/PartitionBackup # dd of=oeminfo \
11. > if=/dev/block/platform/hi\_mci.0/by-name/oeminfo
12. 65536+0 records in
13. 65536+0 records out
14. 33554432 bytes transferred in 8.768 secs (3826919 bytes/sec)
15. root@hwp7:/storage/sdcard1/PartitionBackup # dd of=recovery \
16. > if=/dev/block/platform/hi\_mci.0/by-name/recovery
17. 32768+0 records in
18. 32768+0 records out
19. 16777216 bytes transferred in 4.419 secs (3796609 bytes/sec)
20. root@hwp7:/storage/sdcard1/PartitionBackup # strings nvme | grep WVDEVID -B 1
21. <font color="#ff0000">1234567890123456</font>

复制代码

这里得到的16位红色数字就是解锁码，可直接用于bootloader的解锁  
上面还在/storage/sdcard1/PartitionBackup目录下面得到三个文件：nvme oeminfo recovery  
这三个文件一定要保存好，当需要将bootloader恢复成unlocked状态时，只需运行如下命令

1. root@hwp7:/ # cd /storage/sdcard1/PartitionBackup
2. root@hwp7:/storage/sdcard1/PartitionBackup # dd if=nvme of=/dev/block/platform/hi\_mci.0/by-name/nvme
3. root@hwp7:/storage/sdcard1/PartitionBackup # dd if=oeminfo of=/dev/block/platform/hi\_mci.0/by-name/oeminfo

复制代码

再重启到bootloader，就可以看到是unlocked状态了  
注：bootloader恢复成unlocked状态后，第三方recovery、第三方boot.img都不能正常工作。需要用如下命令恢复recovery

1. root@hwp7:/storage/sdcard1/PartitionBackup # dd if=recovery of=/dev/block/platform/hi\_mci.0/by-name/recovery

华为bootloader需要解锁后才能刷第三方recovery，解锁需要在华为官网上申请解锁码，而且解锁后重新上锁，bootloader的显示不是unlocked，而是relocked，这点不知道是否影响保修，下面介绍如何绕开华为官网解锁bootloader，以及将bootloader恢复成unlocked状态  
首先，你的手机需要未解锁，但需要获得root权限(目前我测下来唯一能实现这个目标的是kingroot，大家有兴趣可以用替换kingrootsupersu试试。  
其次，需要有一台安装了adb的机器  
下面从adb shell登录到手机开始

1. 255|shell@hw[P7](http://club.huawei.com/forum-402-1.html):/ $ su
2. root@hwp7:/ # cd /storage/sdcard1/
3. root@hwp7:/storage/sdcard1 # mkdir -p PartitionBackup
4. root@hwp7:/storage/sdcard1 # cd PartitionBackup
5. root@hwp7:/storage/sdcard1/PartitionBackup # dd of=nvme \
6. > if=/dev/block/platform/hi\_mci.0/by-name/nvme
7. 8192+0 records in
8. 8192+0 records out
9. 4194304 bytes transferred in 0.916 secs (4578934 bytes/sec)
10. root@hwp7:/storage/sdcard1/PartitionBackup # dd of=oeminfo \
11. > if=/dev/block/platform/hi\_mci.0/by-name/oeminfo
12. 65536+0 records in
13. 65536+0 records out
14. 33554432 bytes transferred in 8.768 secs (3826919 bytes/sec)
15. root@hwp7:/storage/sdcard1/PartitionBackup # dd of=recovery \
16. > if=/dev/block/platform/hi\_mci.0/by-name/recovery
17. 32768+0 records in
18. 32768+0 records out
19. 16777216 bytes transferred in 4.419 secs (3796609 bytes/sec)
20. root@hwp7:/storage/sdcard1/PartitionBackup # strings nvme | grep WVDEVID -B 1
21. <font color="#ff0000">1234567890123456</font>

*复制代码*  
这里得到的16位红色数字就是解锁码，可直接用于bootloader的解锁  
上面还在/storage/sdcard1/PartitionBackup目录下面得到三个文件：nvme oeminfo recovery  
这三个文件一定要保存好，当需要将bootloader恢复成unlocked状态时，只需运行如下命令

1. root@hwp7:/ # cd /storage/sdcard1/PartitionBackup
2. root@hwp7:/storage/sdcard1/PartitionBackup # dd if=nvme of=/dev/block/platform/hi\_mci.0/by-name/nvme
3. root@hwp7:/storage/sdcard1/PartitionBackup # dd if=oeminfo of=/dev/block/platform/hi\_mci.0/by-name/oeminfo

*复制代码*  
再重启到bootloader，就可以看到是unlocked状态了  
注：bootloader恢复成unlocked状态后，第三方recovery、第三方boot.img都不能正常工作。需要用如下命令恢复recovery

1. root@hwp7:/storage/sdcard1/PartitionBackup # dd if=recovery of=/dev/block/platform/hi\_mci.0/by-name/recovery

*复制代码*