INFORMATION SECURITY LABORATORIES

Android behind the scenes

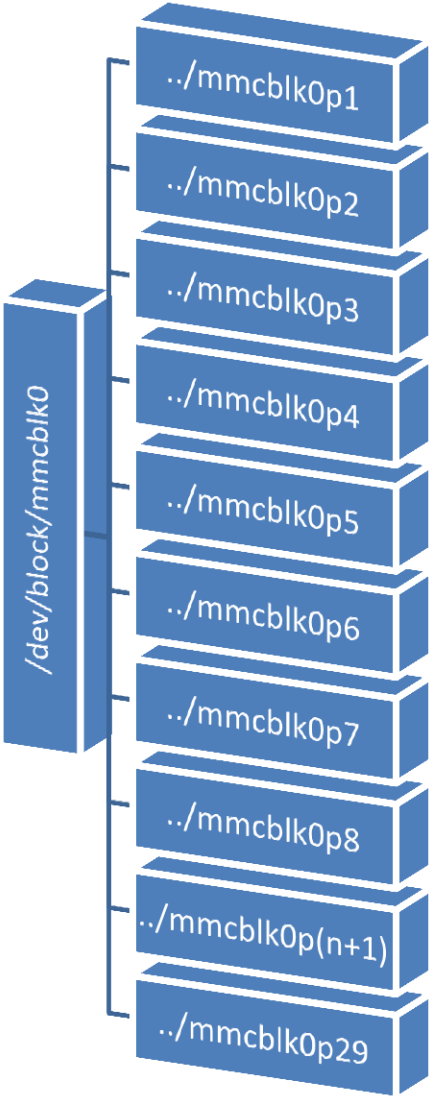
possible attacks
and radical defense
measures

INFORMATION SECURITY LABORATORIES

1. From A to Z:

Low-level hack of the HTC Desire HD Read-Only eMMC partition story

eMMC structure



- /dev/block/mmcblk0p1 - 512 000 - dbl
- /dev/block/mmcblk0p3 - 4 608 000 - osbl
- /dev/block/mmcblk0p4 - 1 024 - header_rex_amss
- /dev/block/mmcblk0p5 - 30 720 000 - rex_amss
- /dev/block/mmcblk0p6 - 12 800 000 - modem_DSP
- /dev/block/mmcblk0p7 - 2 097 152 - CID, Secure_Flag, IMEI, rcdata.img
- /dev/block/mmcblk0p8 - 3 145 728
- /dev/block/mmcblk0p9 - 2 097 152
- /dev/block/mmcblk0p10 - 1 048 576
- /dev/block/mmcblk0p11 - 1 048 576
- /dev/block/mmcblk0p12 - 8 961 536
- /dev/block/mmcblk0p13 - 3 145 728 - reserved for modem storage
- /dev/block/mmcblk0p14 - 3 145 728 - reserved for modem storage
- /dev/block/mmcblk0p15 - 1 048 576
- /dev/block/mmcblk0p16 - 9 172 480
- /dev/block/mmcblk0p17 - 262 144 - misc
- /dev/block/mmcblk0p18 - 1 048 576 - hboot
- /dev/block/mmcblk0p19 - 1 048 576 - sp1
- /dev/block/mmcblk0p20 - 1 310 720 - wifi
- /dev/block/mmcblk0p21 - 8 909 824 - recovery
- /dev/block/mmcblk0p22 - 4 194 304 - boot
- /dev/block/mmcblk0p23 - 262 144 - mfg
- /dev/block/mmcblk0p24 - 2 096 128 - sp2
- /dev/block/mmcblk0p25 - 585 104 896 - system
- /dev/block/mmcblk0p26 - 1 232 076 288 - userdata
- /dev/block/mmcblk0p27 - 314 572 288 - cache
- /dev/block/mmcblk0p28 - 21 757 440 - devlog
- /dev/block/mmcblk0p29 - 262 144 - pdata

Secure Flag 0/1, opportunities

INFORMATION SECURITY LABORATORIES

S-ON

- eMMC read, writing only to user-available partitions
- Flashing only HTC-signed firmware

S-OFF

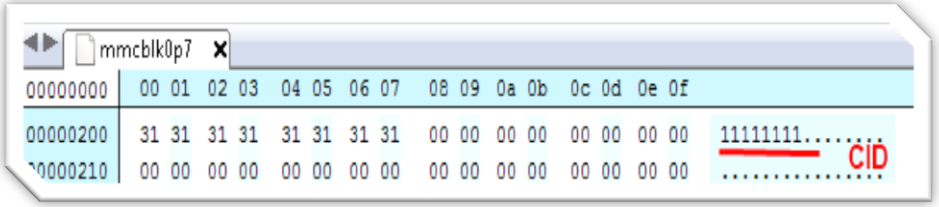
- Writing in any eMMC partition, except partition 7
- Flashing any third-party modified firmware, including hboot, recovery and custom roms

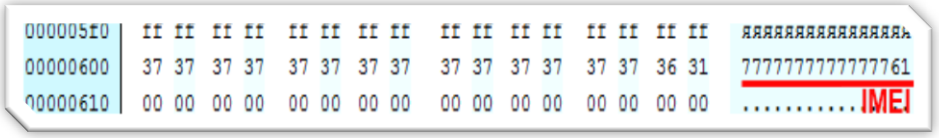
mmcblk0p7

INFORMATION SECURITY LABORATORIES

mmcblk0p7

- CID
- IMEI
- S-Flag





XTC Dongle

INFORMATION SECURITY LABORATORIES

IMEI repair

S-OFF

Unlock

In the deep: how it works

wpthis.ko

- **void powercycle_emmc()**
  {
  gpio_tlmm_config(PCOM_GPIO_CFG(88, 0, GPIO_OUTPUT, GPIO_NO_PULL, GPIO_2MA), 0);

  // turn off.
  gpio_set_value(88, 0);
  mdelay(200);

  // turn back on.
  gpio_set_value(88, 1);
  mdelay(200);
  }

Kernel Filter removal

INFORMATION SECURITY LABORATORIES

drivers/mmc/card/block.c

#if 1 → #if 0

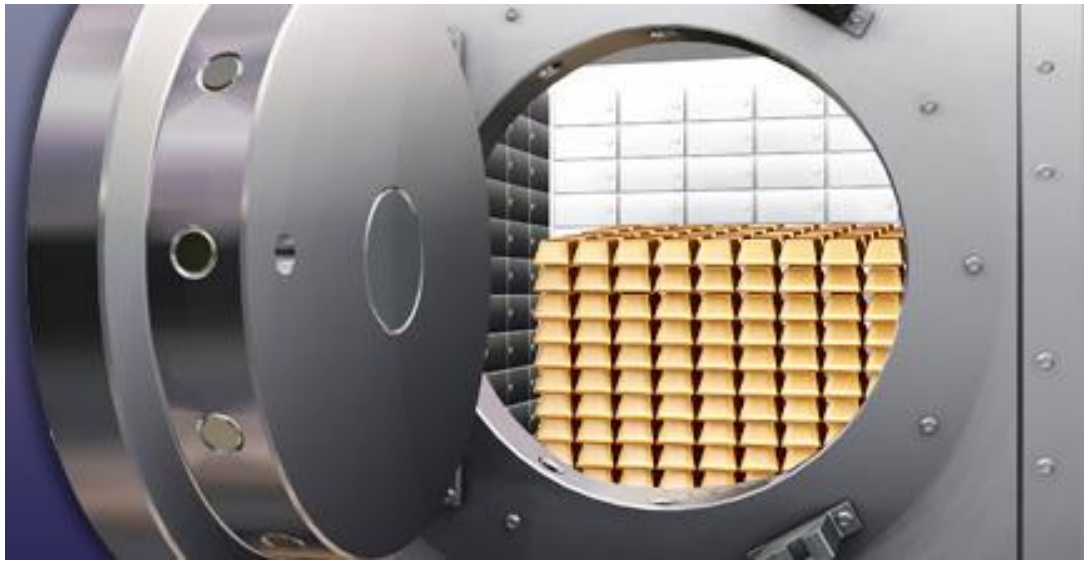
```
 if (board_emmc_boot())
   if (mmc_card_mmc(card)) {
     if (brq.cmd.arg < 131073) {/* should not write any value before
131073 */
       pr_err("%s: pid %d(tgid %d)(%s)\n", func, (unsigned)(current->pid),
                 (unsigned)(current->tgid), current->comm);
       pr_err("ERROR! Attemp to write radio partition start %d size %d\n",
                  brq.cmd.arg, blk_rq_sectors(req));

       BUG();
       return 0;
      }
#endif
```

2. Paranoid Android

INFORMATION SECURITY LABORATORIES

Making of werephone with encrypted data



Preparations

INFORMATION SECURITY LABORATORIES

Android 2.3-4.1

- Rooted Android OS, stock or custom

Busybox

- Android console utility pack installed

lm.cryptsetup

- Android console LUKS-manager installed

USB Debugging Enabled

- Access to device's shell by USB

"reboot" binary

- Reboot binary from the ROM Manager contents

Step one: creating encrypted containers

INFORMATION SECURITY LABORATORIES

In the Android Shell:

```
#busybox dd if=/dev/zero of=/data/secure0 bs=1M count 800
#losetup /dev/block/loop3 /data/secure0
#lm.cryptsetup luksFormat –c aes-plain /dev/block/loop3
#lm.cryptsetup luksOpen /dev/block/loop3 data
#mke2fs –T ext4 –L Secure0 -F /dev/mapper/data
#lm.cryptsetup luksClose  data
```

In the CWM Recovery:

```
parted /dev/block/mmcblk1
print
rm 1
mkpartfs primary fat32 0 4032
mkpartfs primary ext2 4032 8065
quit
```

In the Android Shell:

```
#lm.cryptsetup luksFormat –c aes-plain /dev/block/mmcblk1p2
#lm.cryptsetup luksOpen /dev/block/mmcblk1p2 sdcard
#mkfs.vfat -n Seccard0 /dev/mapper/sdcard
#lm.cryptsetup luksClose sdcard
```

Second step: copying data to container

In the Android Shell:

```
#losetup /dev/block/loop3 /data/secure0
#lm.cryptsetup luksOpen /dev/block/loop3 data
#mount –o remount,rw /
#mkdir /DATA
#mount –t ext4 /dev/mapper/data /DATA
# cp -a /data/app /DATA
# cp -a /data/app-private /DATA
# cp -a /data/backup /DATA
# cp -a /data/data /DATA
# cp -a /data/dontpanic /DATA
# cp -a /data/drm /DATA
# cp -a /data/etc /DATA
# cp -a /data/htcfs /DATA
# cp -a /data/local /DATA
# cp -a /data/misc /DATA
# cp -a /data/property /DATA
# cp -a /data/secure /DATA
# cp -a /data/system /DATA
# cp -a /data/zipalign.log /DATA
# mkdir /DATA/d
# mkdir /DATA/dalvik-cache
# umount /DATA
# lm.cryptsetup luksClose data
```

Third step : proper startup and shutdown of the encrypted mode

INFORMATION SECURITY LABORATORIES

Entering encrypted mode:

```
#setprop ctl.stop zygote
#mount -o remount,rw rootfs /
#mkdir /DATA
#mkdir /mnt/SDCARD
#mount -o move /mnt/sdcard /mnt/SDCARD
#lm.cryptsetup luksOpen /dev/block/mmcblk1p2 sdcard
#mount -t vfat /dev/mapper/sdcard /mnt/sdcard
#mount -o remount,ro rootfs /
#mount /dev/block/mmcblk0p26 /DATA
#losetup /dev/block/loop5 /DATA/secure0
#lm.cryptsetup luksOpen /dev/block/loop5 data
#umount /data -l
#mount -t ext4 /dev/mapper/data /data
#setprop ctl.start zygote
#killall zygote
```

Leaving encrypted mode:

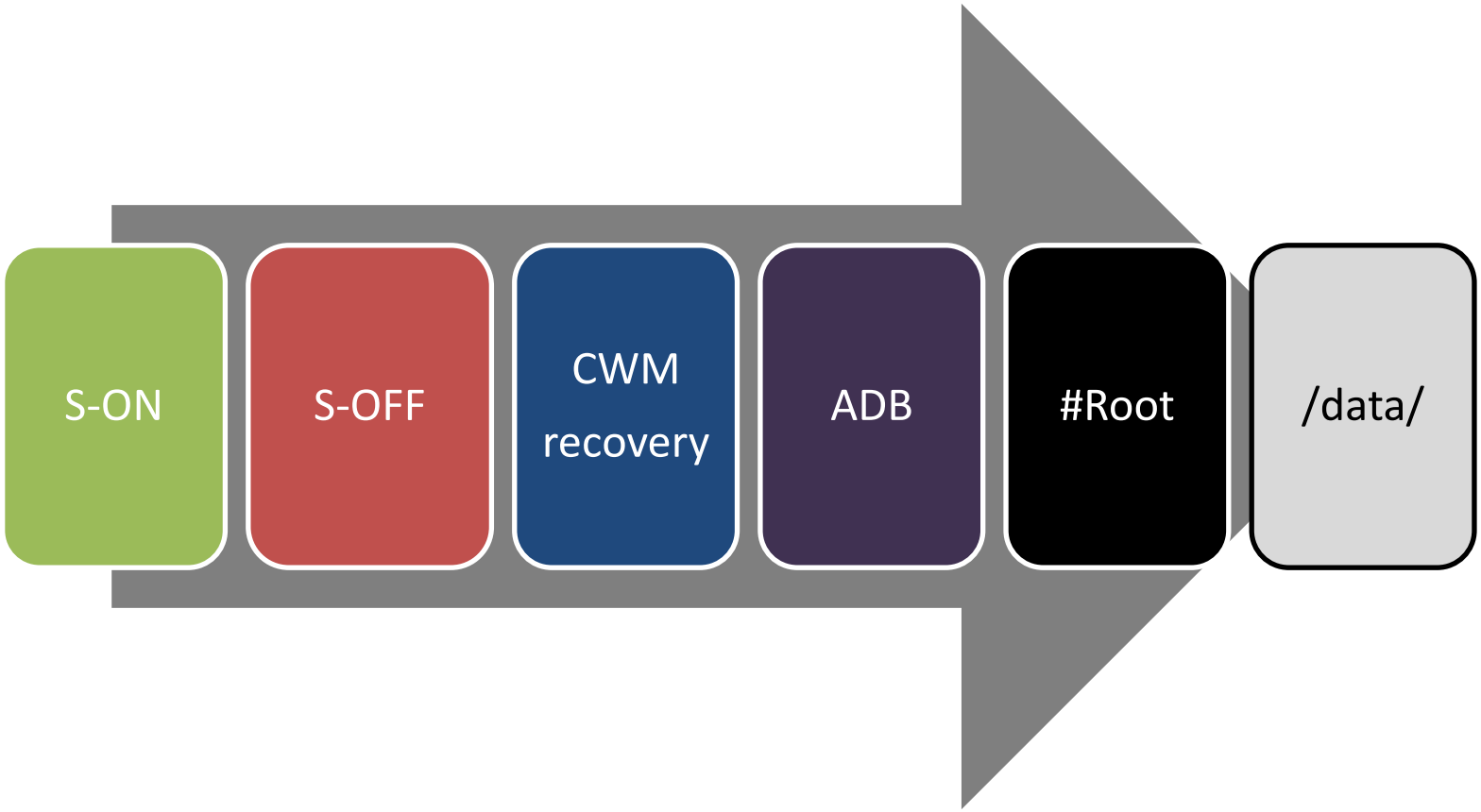
```
#sync
#setprop ctl.stop zygote
#setprop ctl.stop runtime
#setprop ctl.stop keystore
#fuser /data –m -k
#umount /data
#/lm.cryptsetup luksClose data
#/system/bin/reboot
```

3. FALSE SAFETY

INFORMATION SECURITY LABORATORIES

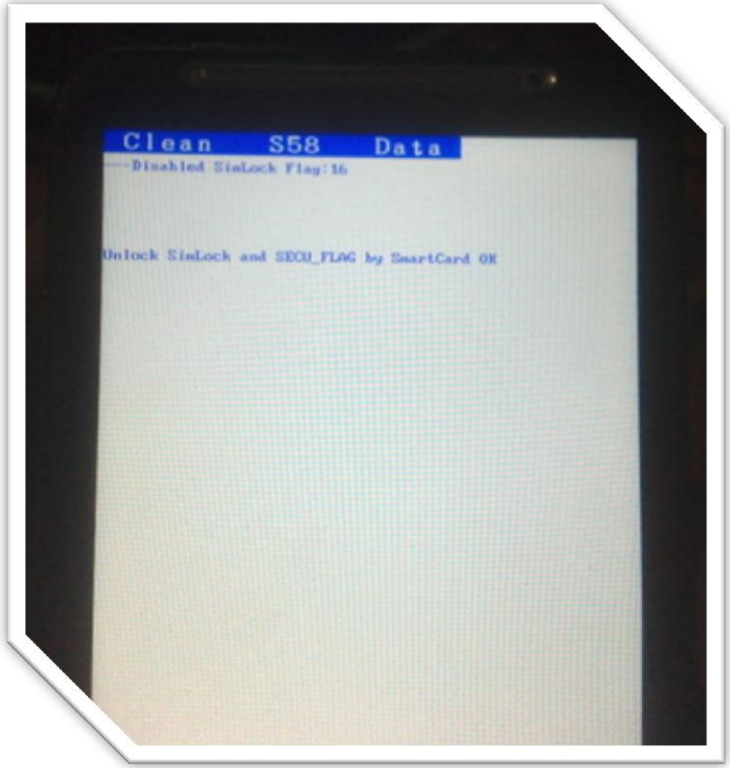
Data extraction methods review.

Getting access to data



Universal lockpick: XTC Clip

INFORMATION SECURITY LABORATORIES



Andoid POI

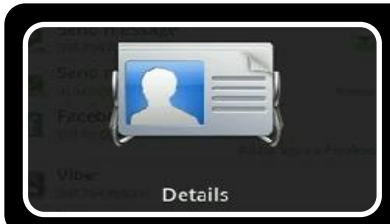
INFORMATION SECURITY LABORATORIES

/data/system/accounts.db

SQLit
File E
Database

Table: accounts

	id	name	type	password
1	1	Weather	com.htc.sync.provider.weather	
2	2	Stocks	com.htc.android.Stock	
3	3	[redacted]	com.google	[redacted]
4	4	News	com.htc.newsreader	
5	5	[redacted]	com.skype.contacts.sync	[redacted]
6	6	[redacted]	com.htc.android.mail	[redacted]



/data/data/com.android.providers.contacts/databases/contacts2.db

- Contacts
- Call history

/data/data/com.android.providers.telephony/databases/mmssms.db

- Sms

Pinlock removal

```
adb shell
# sqlite3 /data/data/com.android.providers.settings/databases/settings.db
sqlite> update secure set value=65536 where name='lockscreen.password_type';
sqlite> .exit
# exit
adb reboot
```

Security measures

INFORMATION SECURITY LABORATORIES

Basic	Moderate	Recomended
• USB Debugging Disable • Unknown Sources Off • PinLock	• S-ON • Stock Firmware	• Data Encryption

INFORMATION SECURITY LABORATORIES

Thank you for listening!

See you next time.