RSA Conference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: FLE-W03

Battling Snapdragon and Kirin: Data Extraction from Chinese Android Phones

James Lan

Officer-In-Charge (OC) Team,
Technology Crime Forensic Branch,
Singapore Police Force

#RSAC

The Presentation outline

- Introduction to basic terminology
- Attack surfaces on
  - Xiaomi Android smartphone powered by Qualcomm Snapdragon pre-msm8994
  - Huawei Android smartphone powered by Kirin pre-970
- Demonstration
- Conclusion

DISCLAIMER

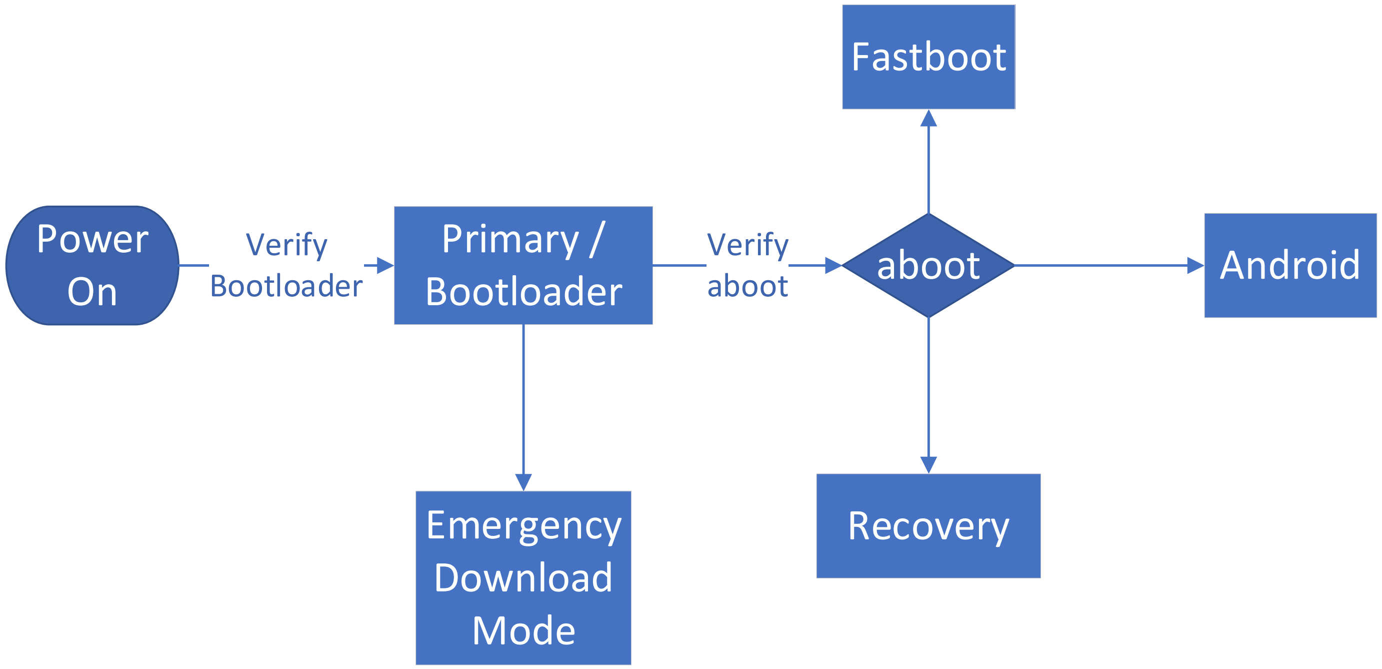
This research is solely based on open source information and reverse-engineering of executables

Introduction

Overview of Qualcomm boot process for Xiaomi phone (Qualcomm Snapdragon pre-msm8994)

Qualcomm boot process for Xiaomi phone in a Nutshell

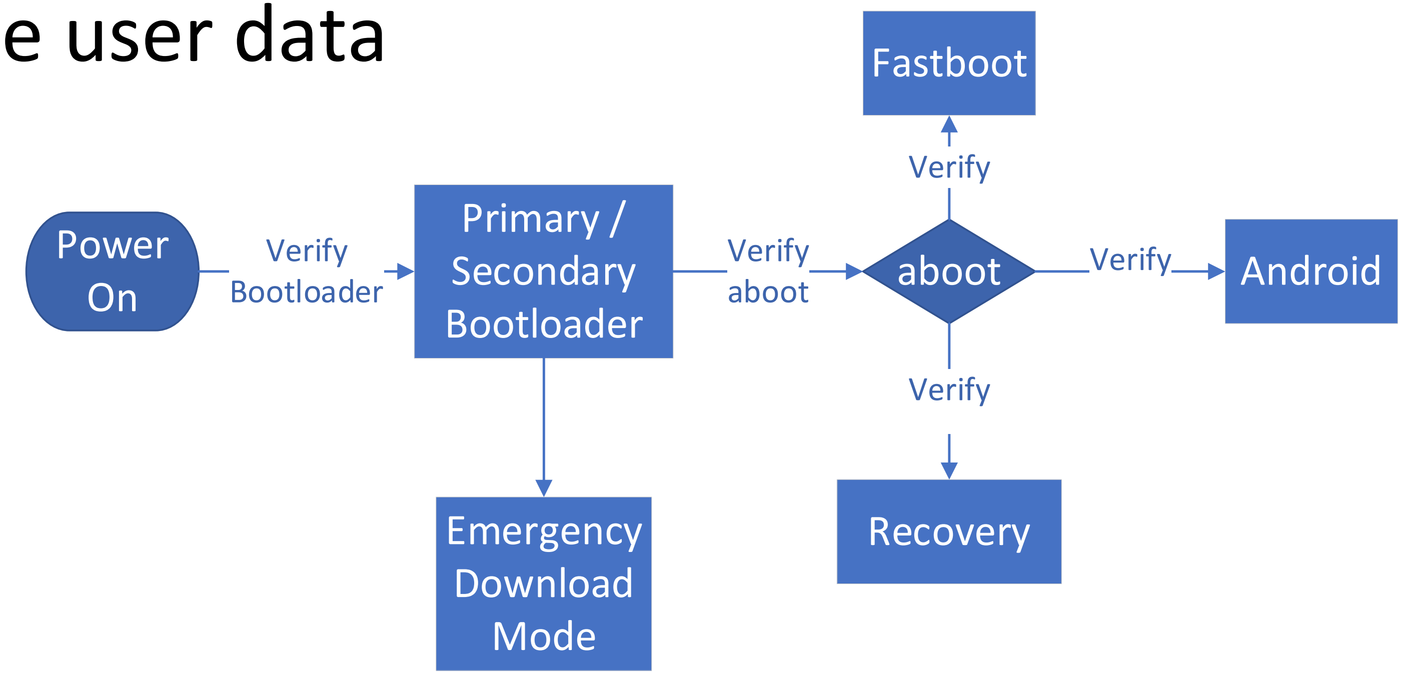
- Emergency Download mode
- Three modes of boot up
- Secure boot
- Unlock bootloader



End Goal: Access User Data (AUD)

- Complex problem to solve
- Unlock bootloader will wipe user data
- Boot images are verified
  - No Custom ROM
- Android > 6 ~= encrypted

user data



RSAConference2019
Asia Pacific & Japan

Xiaomi Android smartphone powered by Qualcomm Snapdragon pre-msm8994

Attacking surfaces

Attacking surfaces – s.s.h.

- Emergency Download Mode (EDL)
- Recovery
- Fastboot

System

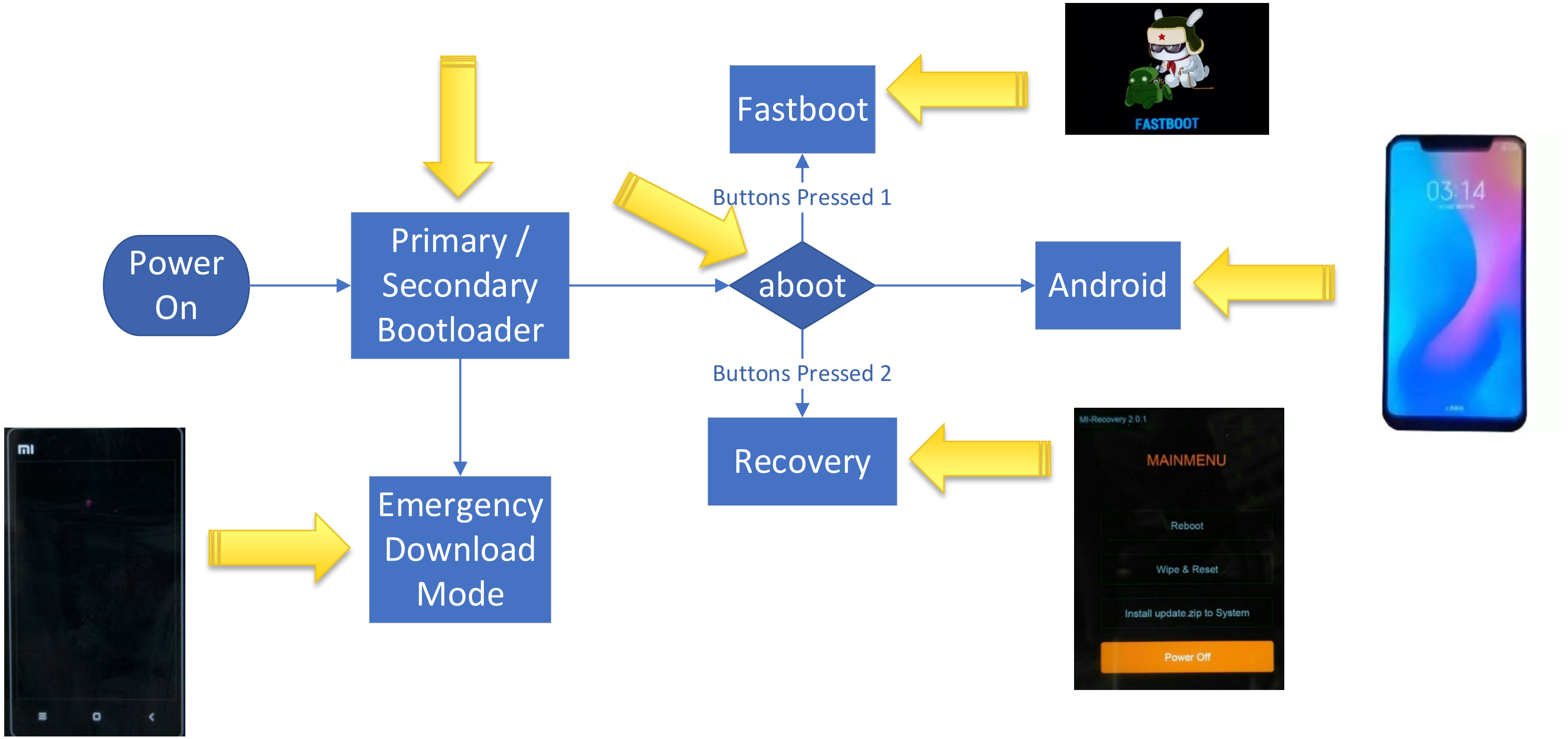
- Bootloader
- aboot
- Android

Software

- Chip-off
- JTAG
- ISP (In-System Programming)

Hardware

Attack surfaces



Power On

Primary / Secondary Bootloader

aboot

Buttons Pressed 1

Fastboot

Android

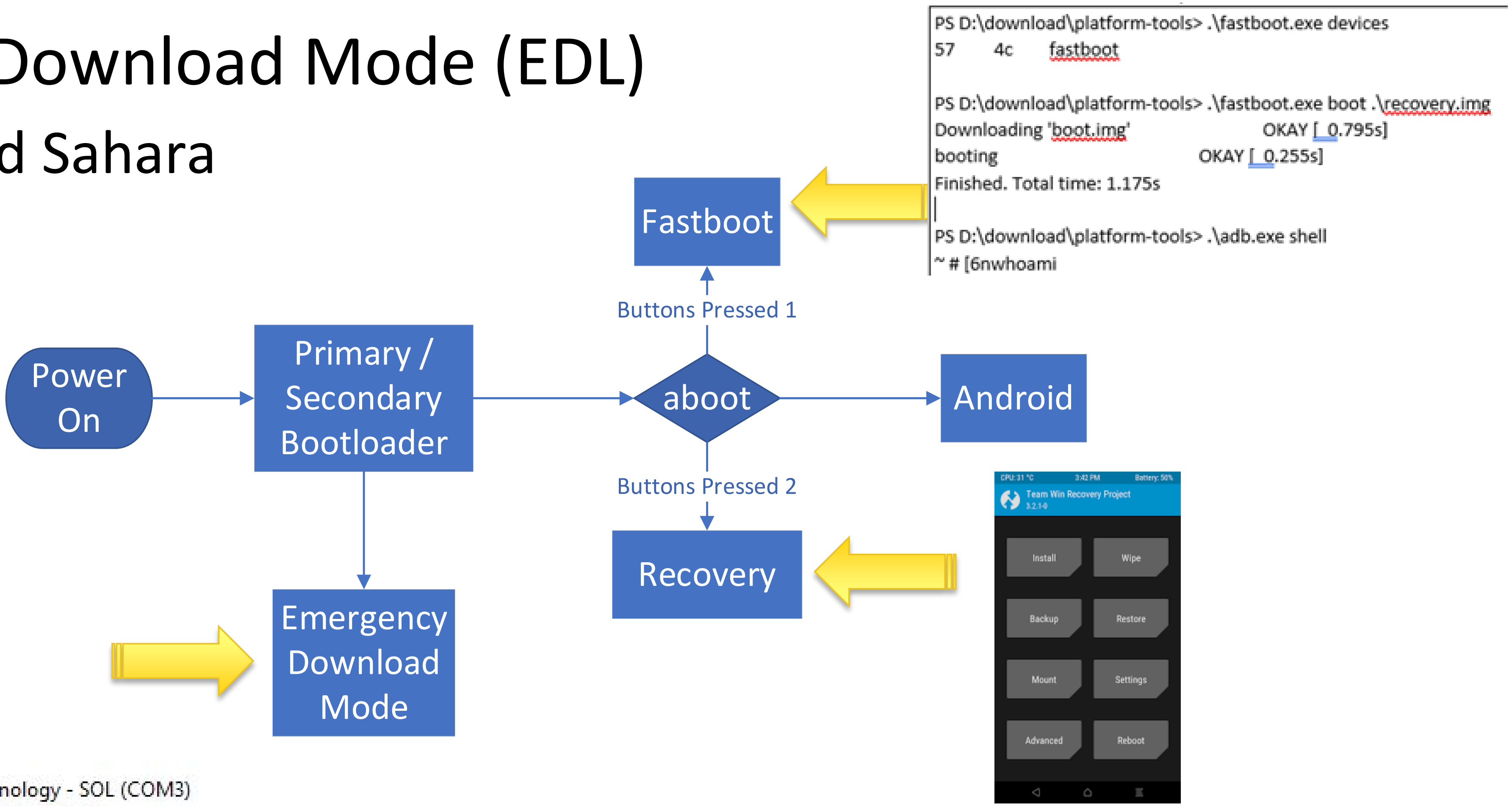
Buttons Pressed 2

Recovery

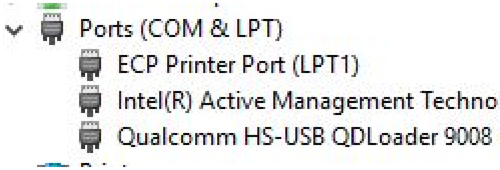
Emergency Download Mode

System attack surface

- Emergency Download Mode (EDL)
  - Firehose and Sahara
- Recovery
- Fastboot



```
PS D:\download\platform-tools> .\fastboot.exe devices
57      4c      fastboot

PS D:\download\platform-tools> .\fastboot.exe boot .\recovery.img
Downloading 'boot.img'                      OKAY [  0.795s]
booting                                 OKAY [  0.255s]
Finished. Total time: 1.175s
|
PS D:\download\platform-tools> .\adb.exe shell
~ # [6nwhoami
```

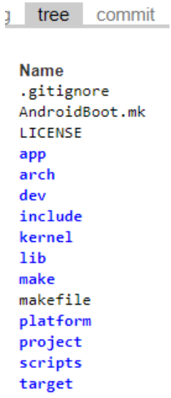


```
⌄ Ports (COM & LPT)
    ECP Printer Port (LPT1)
    Intel(R) Active Management Technology - SOL (COM3)
    Qualcomm HS-USB QDLoader 9008 (COM14)
```

https://twrp.me/

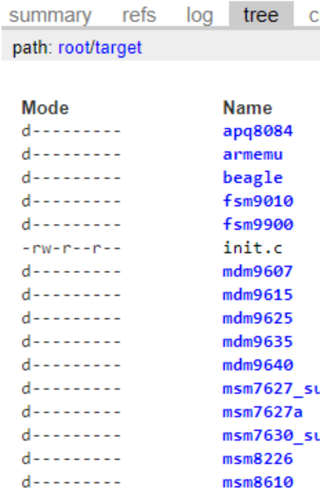
Software attack surface

- Bootloader, aboot and Android



g tree commit

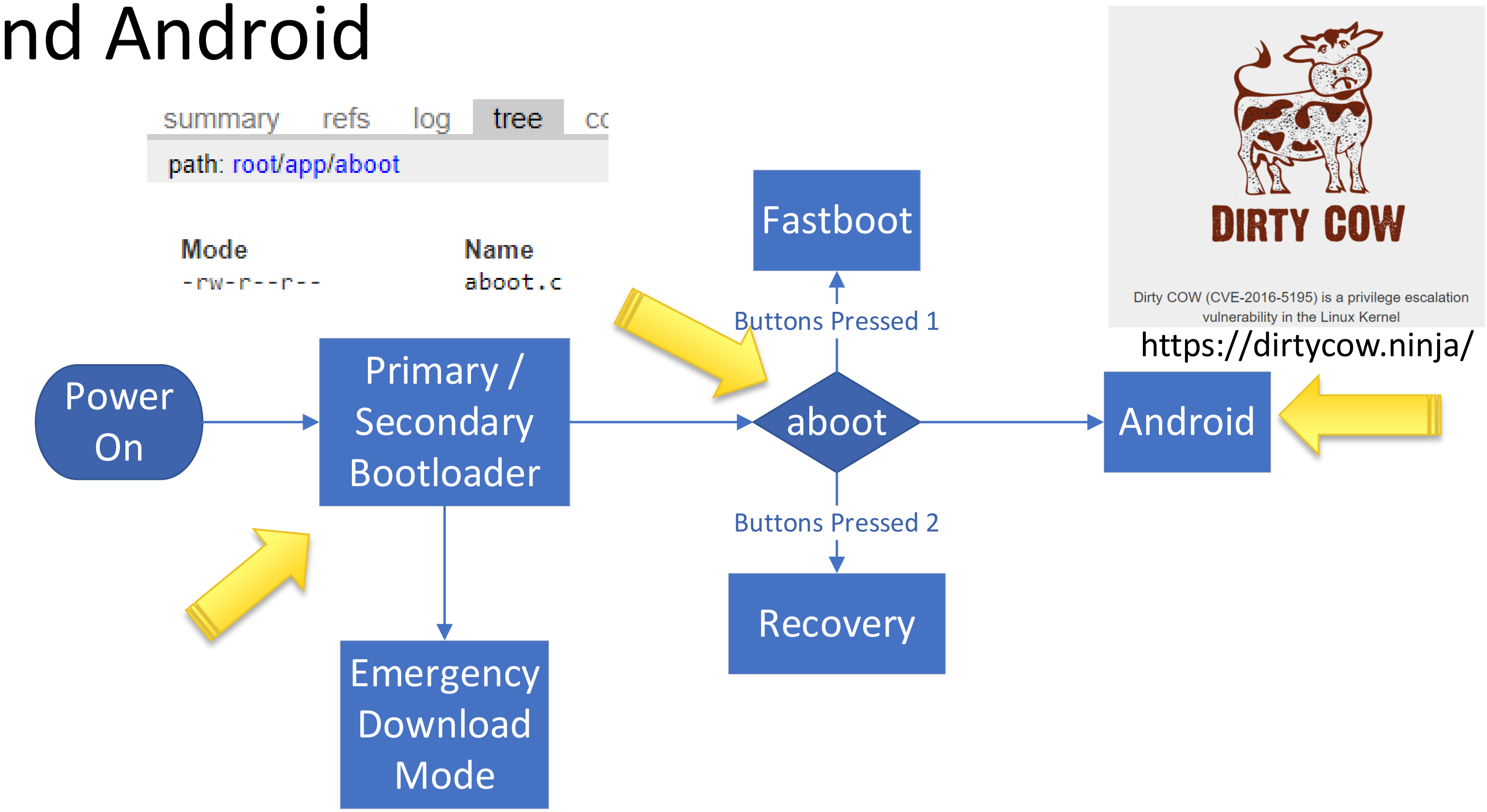
Name
.gitignore
AndroidBoot.mk
LICENSE
app
arch
dev
include
kernel
lib
make
makefile
platform
project
scripts
target



summary refs log tree c

path: root/target

Mode	Name
d---------	apq8084
d---------	armemu
d---------	beagle
d---------	fsm9010
d---------	fsm9900
-rw-r--r--	init.c
d---------	mdm9607
d---------	mdm9615
d---------	mdm9625
d---------	mdm9635
d---------	mdm9640
d---------	msm7627_su
d---------	msm7627a
d---------	msm7630_su
d---------	msm8226
d---------	msm8610



summary refs log tree cc

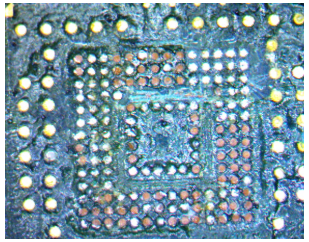
path: root/app/aboot

Mode	Name
-rw-r--r--	aboot.c

Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

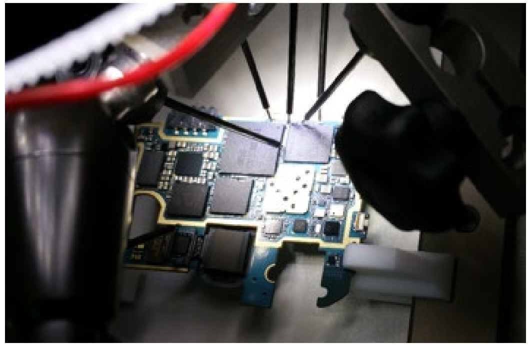
https://dirtycow.ninja/

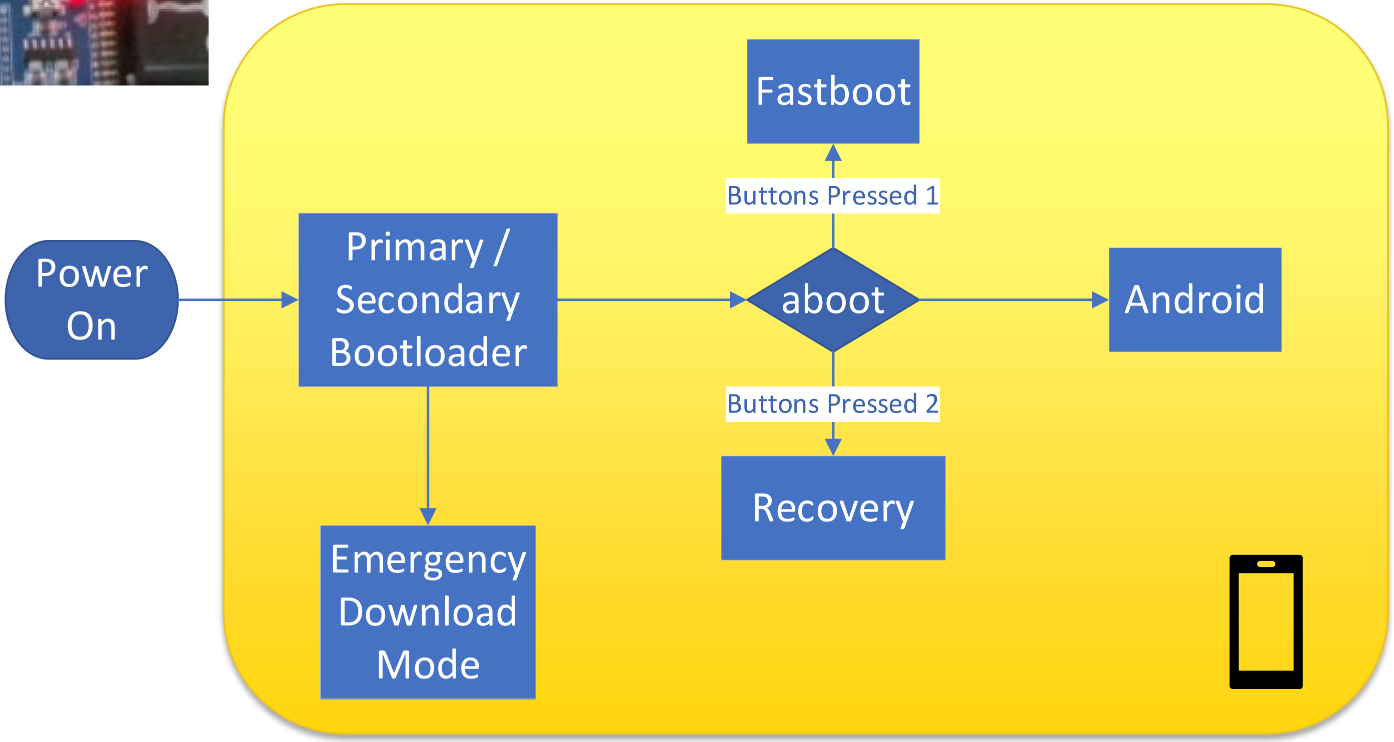
Hardware attack surface



- Chip-off
- JTAG

- ISP
  - In-System Programming





Power On

Primary / Secondary Bootloader

Emergency Download Mode

aboot

Buttons Pressed 1

Fastboot

Buttons Pressed 2

Recovery

Android

RSAConference2019 Asia Pacific & Japan

Xiaomi Android smartphone powered by Qualcomm Snapdragon pre-msm8994

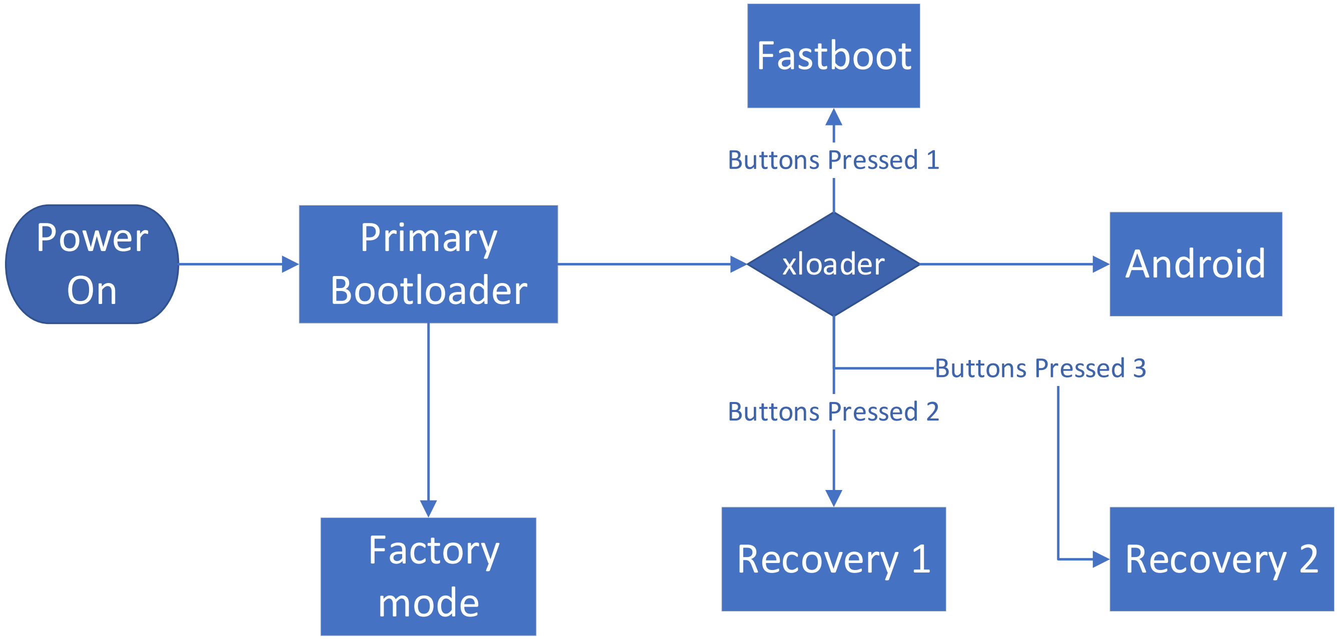
Demo – XiaoMi Android smartphone powered by Qualcomm Snapdragon pre-msm8994 era with Full Disk Encryption with user password

Introduction to Kirin

Overview of Android boot process

Kirin boot process for Huawei phone in a Nutshell

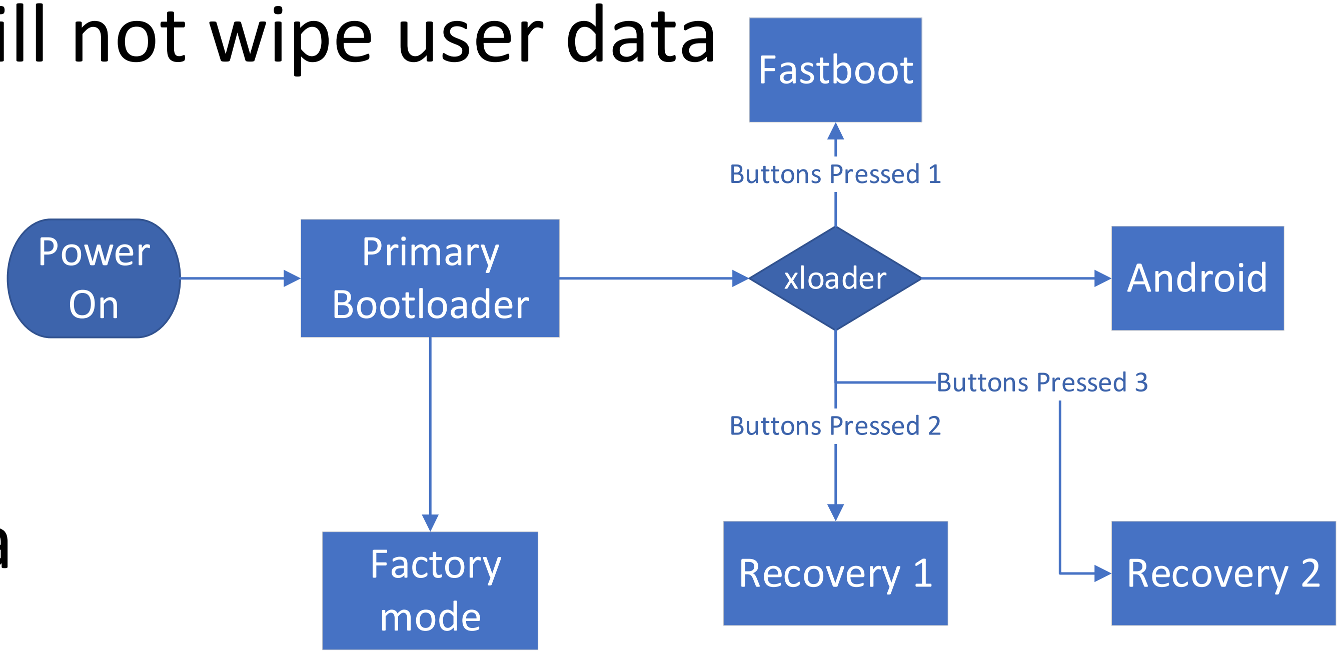
- Factory mode
- Four modes of boot up
- Secure boot
- Unlock bootloader (Ceased unlock service)
  - User unlock
    - Unlock bootloader
  - Full bootloader unlock
    - Full changes to all partitions



End Goal: Access User Data (AUD)

- Complex problem to solve
- Unlock bootloader will/will not wipe user data
- Boot images are verified
  - No Custom ROM
- Android > 6 ~= encrypted

user data



RSAConference2019
Asia Pacific & Japan

Huawei Android smartphone powered by Kirin pre-970

Attacking surfaces

Attacking surfaces – s.s.h.

- Factory mode
- Recovery 1 and 2
- Fastboot

System

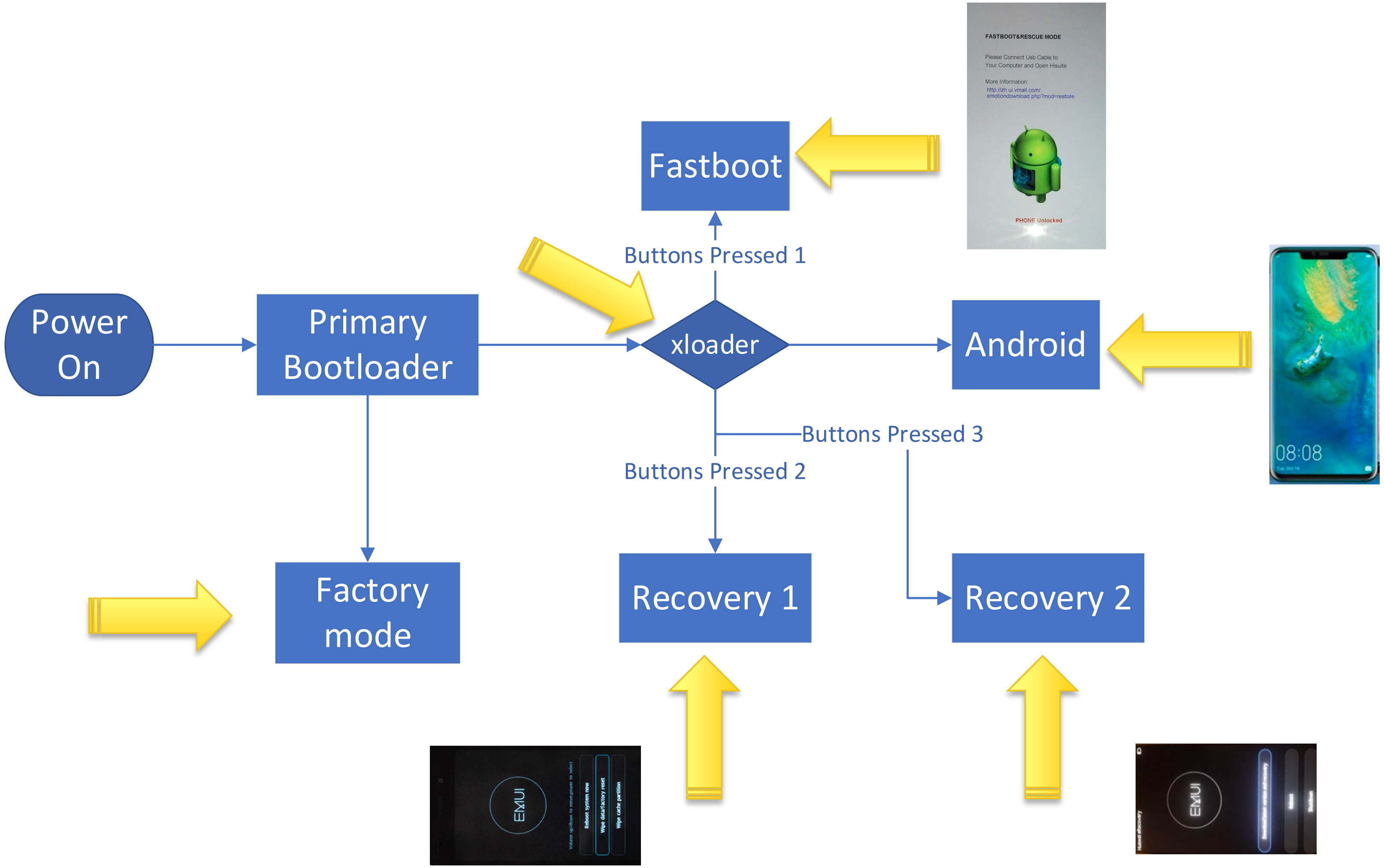
- xloader
- Android
- Manufacture mode

Software

- Chip-off
- JTAG
- ISP (In-System Programming)

Hardware

Attack surfaces



FASTBOOT&RESCUE MODE

Please Connect Usb Cable to
Your Computer and Open Hisuite

More Information:
http://zh.ui.vmall.com/
emotiondownload.php?mod=restore

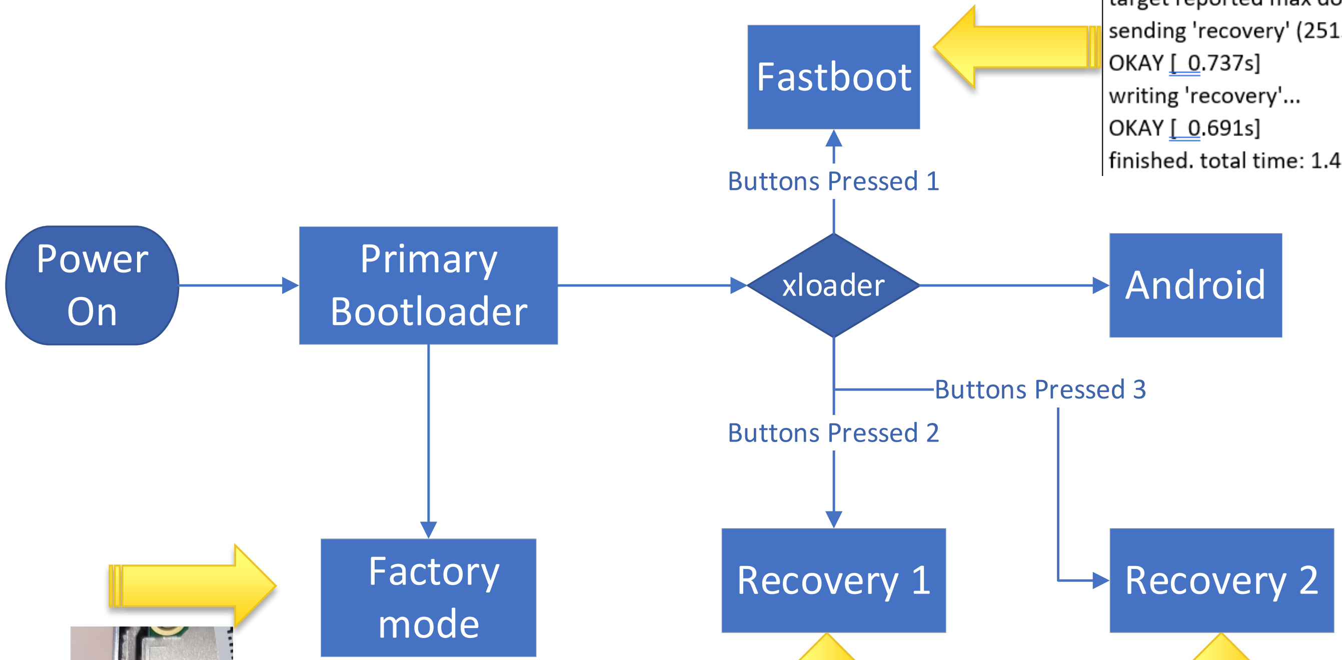
PHONE Unlocked

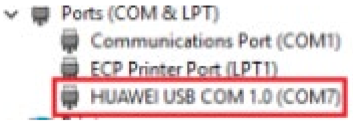
Volume up/down to move,power to select

Attack surfaces

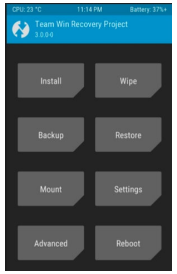
- Factory mode
- Recovery 1 and 2
- Fastboot
  - No fastboot boot

```
fastboot.exe flash recovery .\recoveryp.img
target reported max download size of 471859200 bytes
sending 'recovery' (25152 KB)...
OKAY [ 0.737s]
writing 'recovery'...
OKAY [ 0.691s]
finished. total time: 1.432s
```





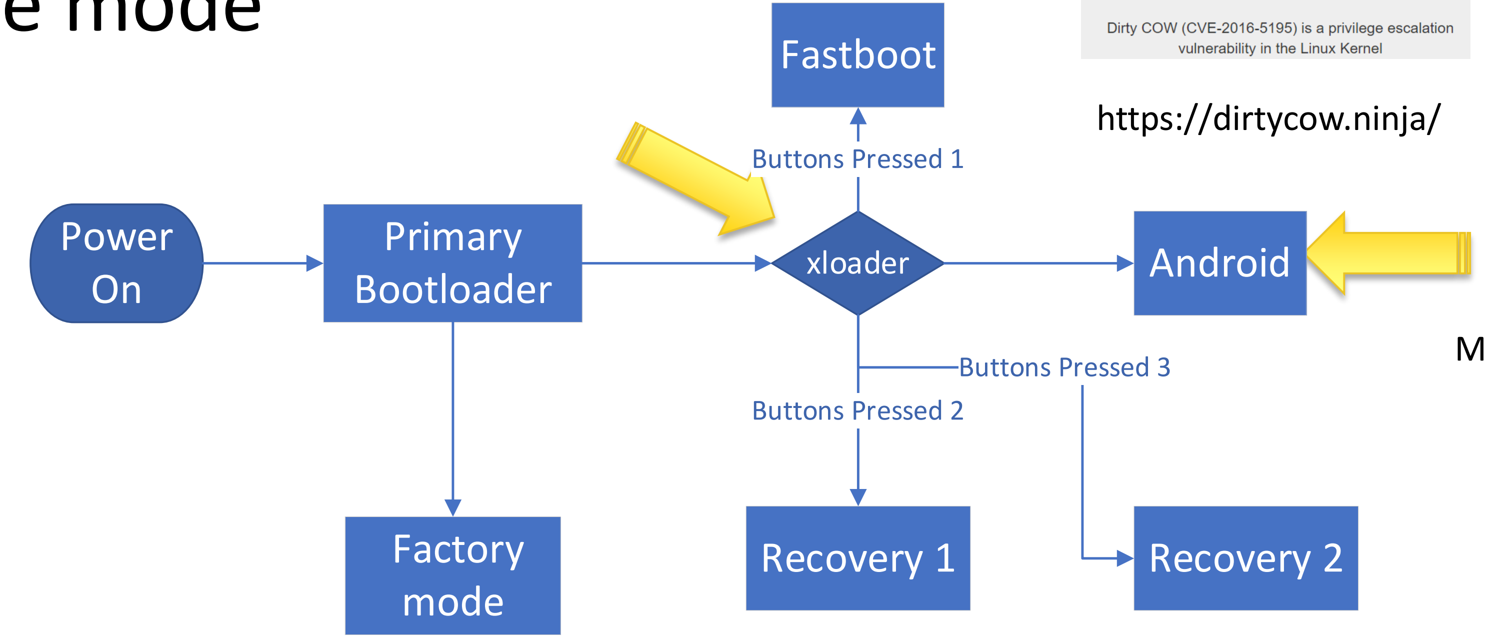
Ports (COM & LPT)
Communications Port (COM1)
ECP Printer Port (LPT1)
HUAWEI USB COM 1.0 (COM7)



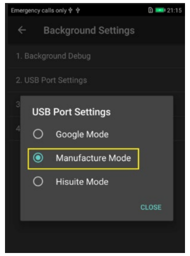
Software attack surface

- xloader
- Android
- Manufacture mode

Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel



https://dirtycow.ninja/


Emergency calls only 21:15

Background Settings

1. Background Debug

2. USB Port Settings

USB Port Settings

○ Google Mode

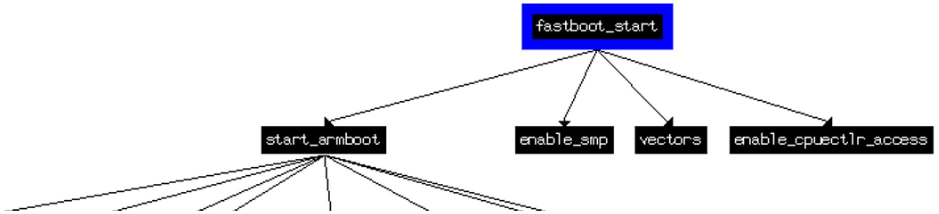
● Manufacture Mode

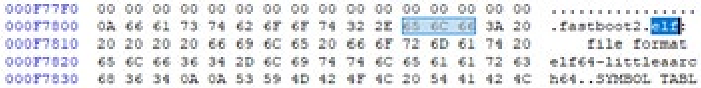
○ Hisuite Mode

CLOSE

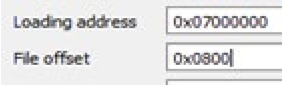
Manufacture mode

Reversing Fastboot



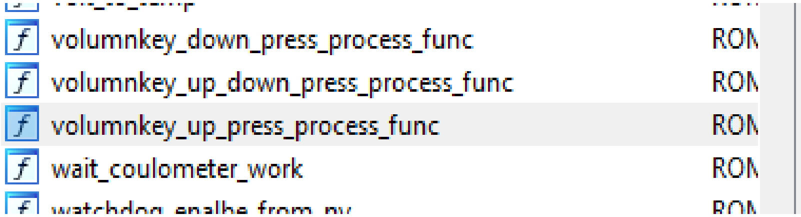


```
000F77F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000F7800  0A 66 61 73 74 62 6F 6F 74 32 2E 65 6C 66 3A 20  .fastboot2.elf: 
000F7810  20 20 20 20 66 69 6C 65 20 66 6F 72 6D 61 74 20      file format 
000F7820  65 6C 66 36 34 2D 6C 69 74 74 6C 65 61 61 72 63  elf64-littleaarc
000F7830  68 36 34 0A 0A 53 59 4D 42 4F 4C 20 54 41 42 4C  h64..SYMBOL TABL
```

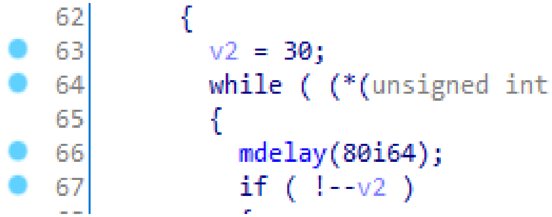


Loading address 0x07000000

File offset 0x0800

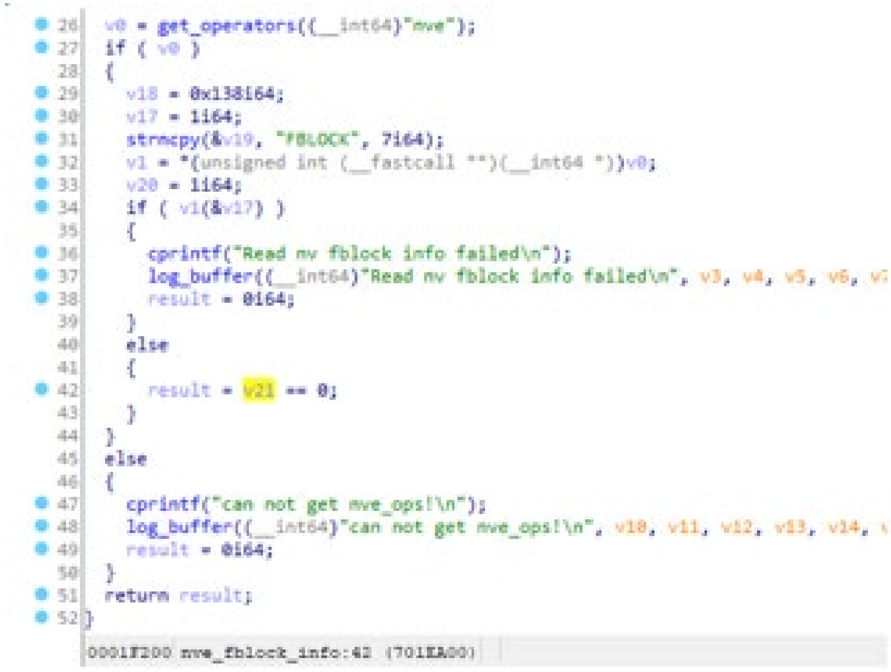


volumnkey_down_press_process_func	ROM
volumnkey_up_down_press_process_func	ROM
volumnkey_up_press_process_func	ROM
wait_coulometer_work	ROM
watchdog_enalbe_from_nv	ROM

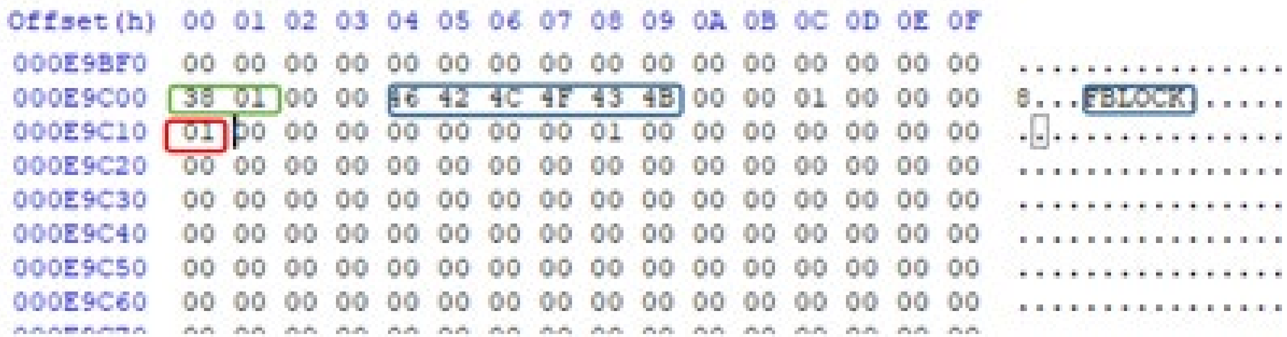


```
{
  v2 = 30;
  while ( (*(unsigned int
  {
    mdelay(80i64);
    if ( !--v2 )
```

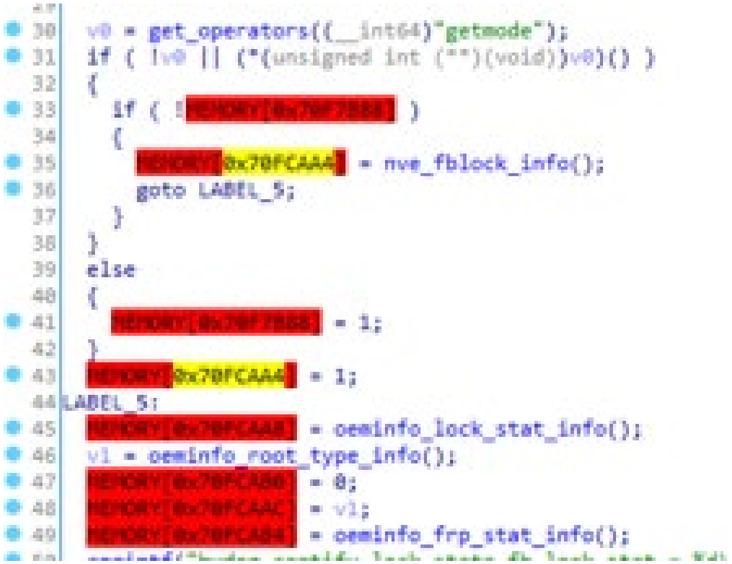
Permanent FB bootloader unlock



```
  v0 = get_operators((__int64)"nve");
  if ( v0 )
  {
    v18 = 0x138i64;
    v17 = 1i64;
    strncpy(&v19, "FBLOCK", 7i64);
    v1 = *(unsigned int (__fastcall **)(__int64 *))v0;
    v20 = 1i64;
    if ( v1(&v17) )
    {
      cprintf("Read nv fblock info failed\n");
      log_buffer((__int64)"Read nv fblock info failed\n", v3, v4, v5, v6, v7
      result = 0i64;
    }
    else
    {
      result = v21 == 0;
    }
  }
  else
  {
    cprintf("can not get nve_ops!\n");
    log_buffer((__int64)"can not get nve_ops!\n", v10, v11, v12, v13, v14, v
    result = 0i64;
  }
  return result;
}
0001F200 nve_fblock_info:42 (701EA00)
```



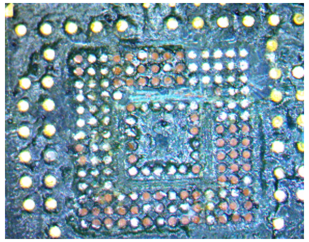
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

000E9BF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000E9C00  38 01 00 00 46 42 4C 4F 43 4B 00 00 01 00 00 00  8...FBLOCK......
000E9C10  01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000E9C20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000E9C30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000E9C40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000E9C50  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000E9C60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

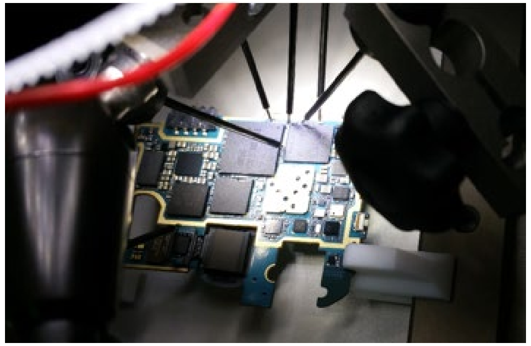


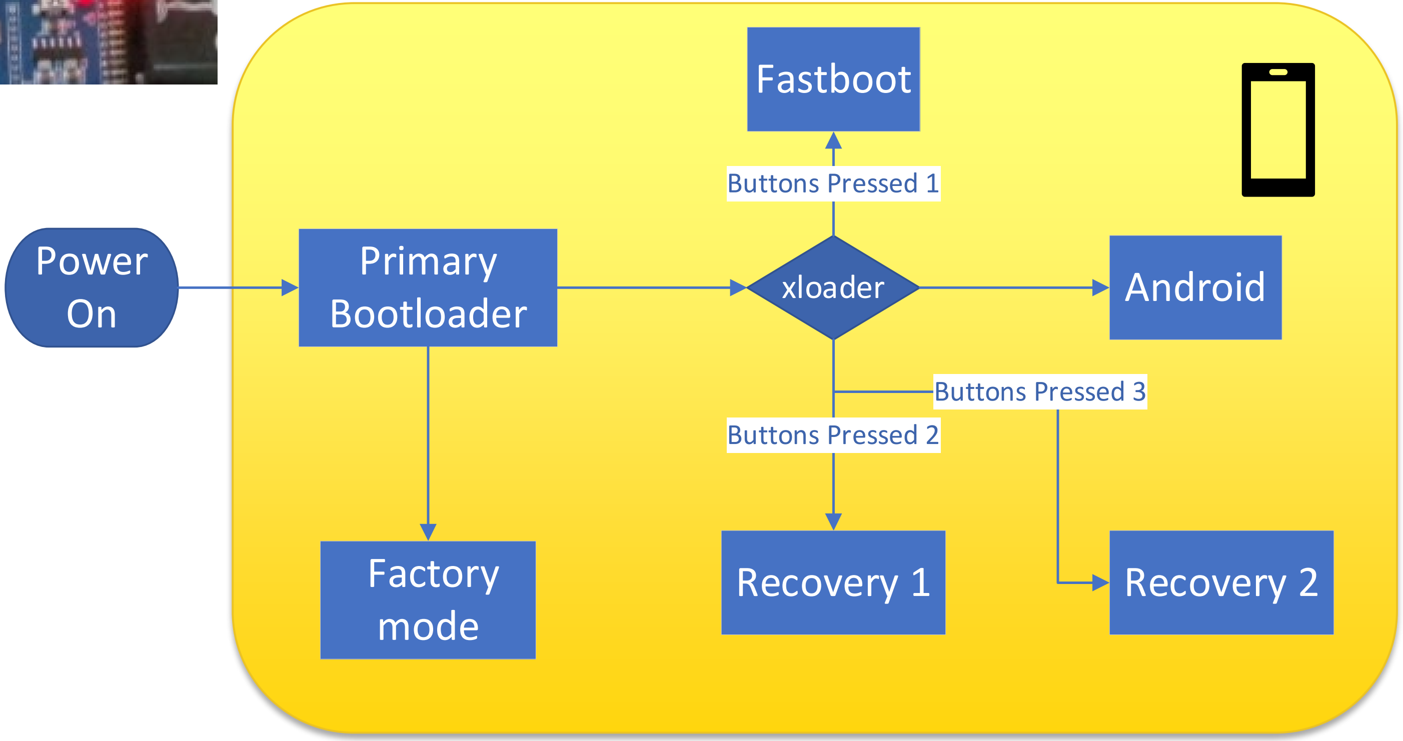
```
  v0 = get_operators((__int64)"getmode");
  if ( !v0 || (*(unsigned int (**)(void))v0)() )
  {
    if ( !MEMORY[0x70F7888] )
    {
      MEMORY[0x70FCAA4] = nve_fblock_info();
      goto LABEL_5;
    }
  }
  else
  {
    MEMORY[0x70F7888] = 1;
  }
  MEMORY[0x70FCAA4] = 1;
LABEL_5:
  MEMORY[0x70FCAA8] = oeminfo_lock_stat_info();
  v1 = oeminfo_root_type_info();
  MEMORY[0x70FCAB0] = 0;
  MEMORY[0x70FCAAC] = v1;
  MEMORY[0x70FCAB4] = oeminfo_frp_stat_info();
```

Hardware attack surface

- Chip-off
- JTAG
- ISP
  - In-System Programming







RSAConference2019
Asia Pacific & Japan

Huawei Android smartphone powered by Kirin pre-970

Demo - Huawei Android smartphone powered by P8 Lite ALE-L21 with Full Disk Encryption - Bootloop

Apply What You Have Learned Today

- Identify the types of mobile phones in your organization
  - Their Android, Kernel, security patches versions
- Remediation actions could be
  - Baseline all the mobile phones
  - Apply security patches to the mobile phones
  - Perform a vulnerability testing of the mobile phones
  - Remain the pristine state of the bootloader

RSA®Conference2019
Asia Pacific & Japan

Thank You