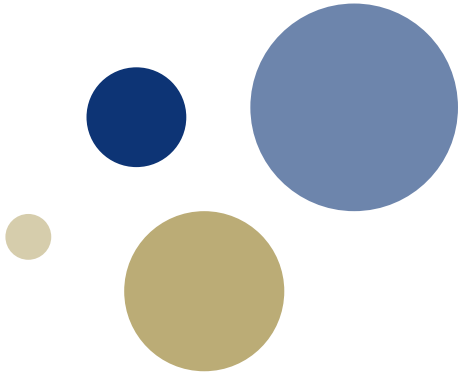
Norwegian University of
Science and Technology



Mandatory security vs. Digital Forensics

Finse Winter School 2018
Gunnar Alendal

Motivation

- Digital forensic needs data
- COTS mandatory security protects data
- Digital forensic needs to adapt

Mobile security - then

- device encryption ⇒ no
- screen lock ⇒ no
- secruity ⇒ no/low
- complexity ⇒ low

- digital forensics ⇒ ad-hoc, case driven
  - “Can you fix anything for this device by end of the day?”

Mobile security - now

- device encryption ⇒ mandatory
- screen lock ⇒ opt out
- security ⇒ in all layers
- complexity ⇒ high
  - OS, flash (UFS / eMMC), modem, Wifi, camera, usb, sdcard, NFC, Bluetooth, GPS, sensors, fingerprint reader, iris scanner, face recognition, peripheral connections, …

- digital forensics ⇒ complex and resource demanding

Mobile security - data protection

- Encryption of user data
  - HW AES
  - Keys tied to user credentials (screen lock)
    - Max. tries
    - Automatic wiping
    - Remote wiping
  - Keys tied to HW
    - Only *this* phone can decrypt user data
    - chip-off hard

Mobile security - phone protection 1

- Theft protection
  - Remote wipe
  - Remote track
  - Remote lock
  - Factory Reset Protection (FRP)
    - prevent reuse
    - prevent installation of custom firmware

Mobile security - phone protection 2

- Integrity protection
  - All running code signed by vendor
    - Custom firmware wipes user data
  - apps are sandboxed
  - user is not *root*
  - Secure Boot
    - Signature chain from boot to OS (Android / iOS)

Mobile security - Enterprise

- Device lock down
  - Password policy
  - Bunch of security policies
  - no *non-OTA* updates
- Common Criteria (CC) mode
- Mobile Device Manager (MDM) mode

Mandatory security vs. Digital Forensics

- Is this game over?
- What security measurements needs to be bypassed?
  - Some?
  - All?
- How to approach this?

Mandatory security vs. Digital Forensics

- Security vulnerabilities?
- Pwn2Own contest 2017:
  - 11 vulnerabilities chained to get *root* (Samsung Galaxy S8)
- LE has possible advantages
  - Time (wait for vulnerability)
  - Resources (money and people)
  - Police authority

Bypassing security mechanisms

- Bigger attack surface ⇒ higher prob. of vulnerability

- Example attack surfaces on mobile phones:
  - Network ⇒ wifi, modem, ..
  - Physical interfaces ⇒ usb, sim, sdcard, jack, ..
  - Vendor proprietary ⇒ Firmware update protocol (usb), ..

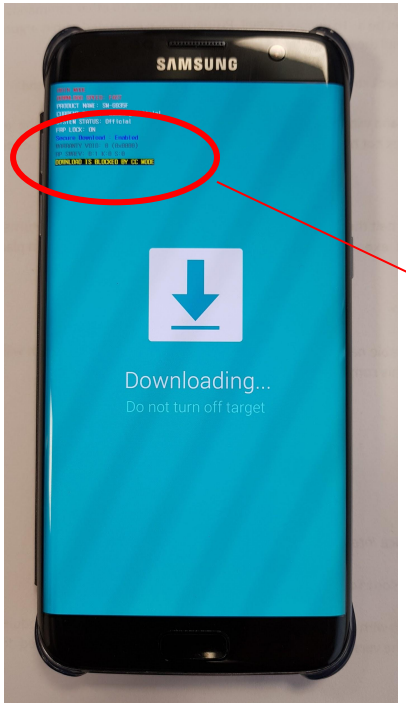
Example: *one* layer

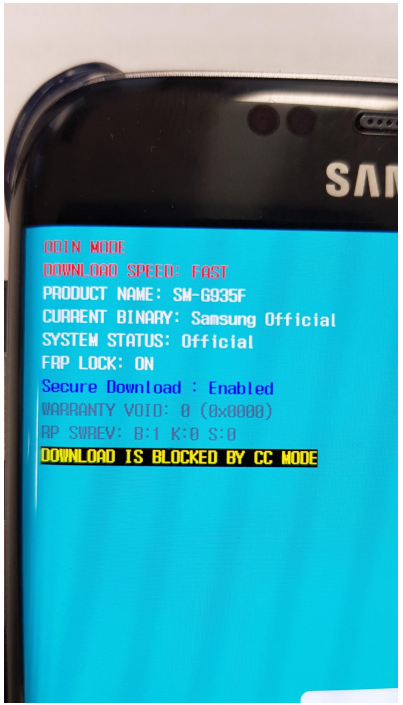
- CC mode
  - Enterprise lock down of employee phones
  - Blocks non-OTA firmware updates

Firmware update / ODIN mode (non-OTA)

- Vendor proprietary
- Physical access to device (USB)
- User (attacker) install unsigned/signed FW
- Increase attack surface

Blocked Firmware update mode / ODIN (SM-G935F)





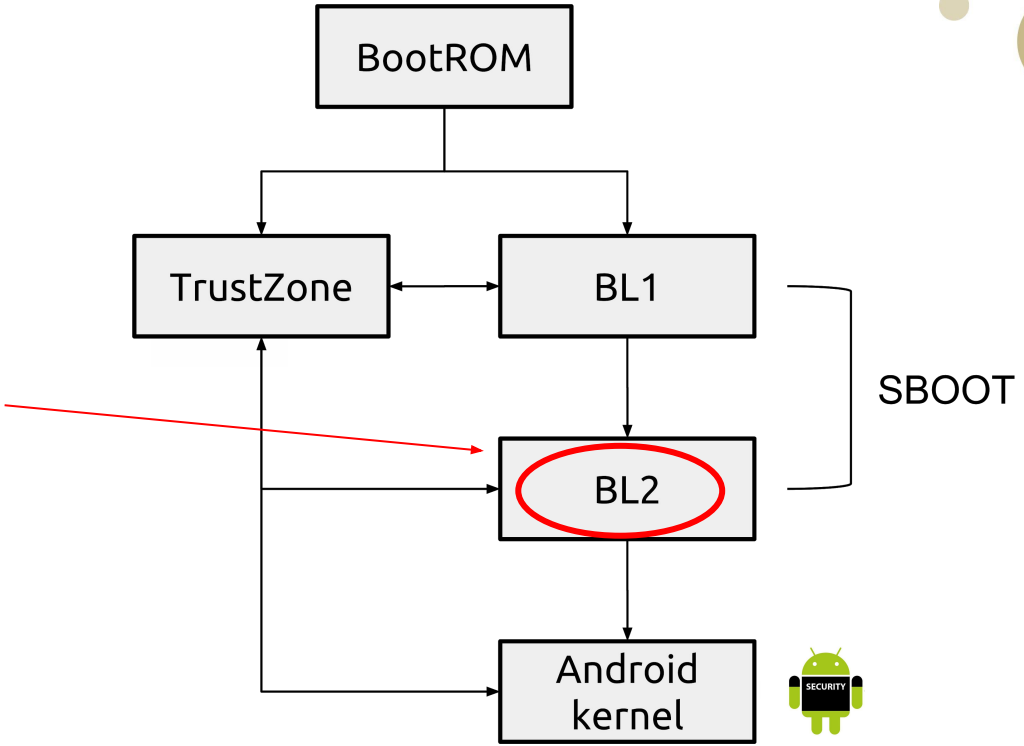
CC mode / MDM mode - questions

- How does phone knows when to block *ODIN mode*?
- Can we disable this, to regain access to *ODIN mode*?

Samsung Secure Boot model (Exynos SoC)

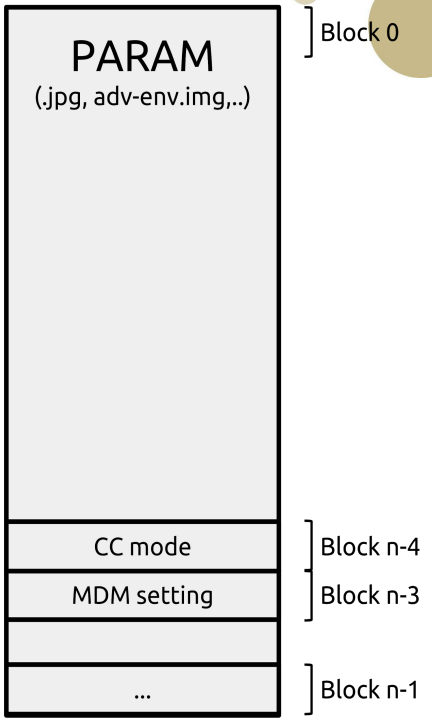
SBOOT/BL2 functionality:

- Signature check kernel
- eFUSE reading/setting
- RPMB
- ...
- Load and boot Android kernel
- firmware update mode / ODIN
- CC mode
- MDM mode



CC mode / MDM mode - SBOOT knowledge

- CC and MDM mode settings stored in a logical partition, PARAM
- SBOOT parses PARAM
- CC mode setting is encrypted with *white box* AES
  - Key embedded in algorithm
- MDM setting stored in clear text



Example summary

- ODIN mode can be re-enabled
- We demonstrated three possible approaches
  - Trigger error condition ⇒ Error handling vulnerability
  - Low level access to flash ⇒ Modify PARAM partition
  - Modify execution flow through vulnerability ⇒ Break code trust

Mandatory security vs. Digital Forensics

- Examples of security vulnerabilities
  - Logical error ⇒ Trigger error condition
  - Design flaws ⇒ Broken assumptions (chip-off / *chip-on*)
  - Program flow error (“buffer overflow”) ⇒ Exploitation
  - Hidden secrets ⇒ Debug functionality (aka. “backdoors”)

Mandatory security vs. Digital Forensics

- Digital forensic needs?
  - More focus on security in COTS products
  - More reverse engineering efforts
  - More weaponization of known/unknown vulnerabilities

- Exploitation development cycle needed?
  - Identify
  - Surveillance
  - Develop
  - Acquire data

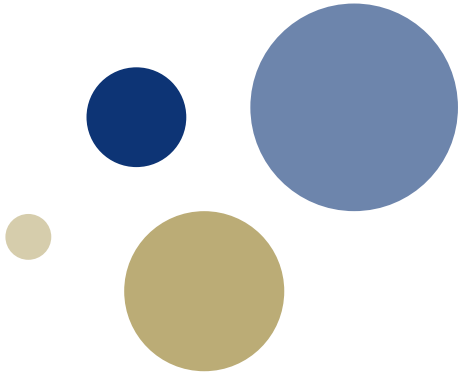
Mandatory security vs. Digital Forensics

- Which direction is best for mankind?
  - LE backdoors <==> All cops are good?
  - Keep current “develop/exploit/patch” cycle?

- Is hacking COTS security “for good” OK?

NTNU

Norwegian University of Science and Technology



Q&A

Gunnar Alendal