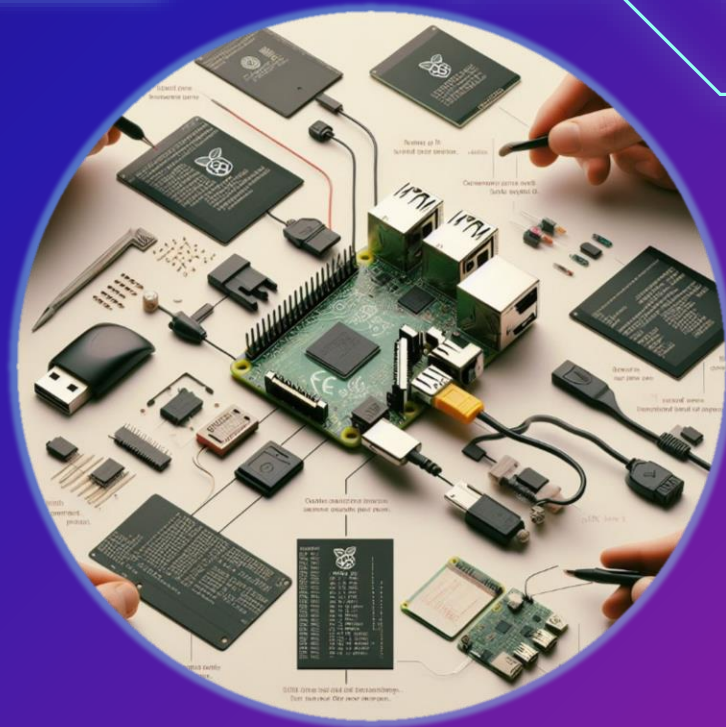


دومین دوره‌ی گروه کاربران لینوکس تعبیه شده E-LUG

موضوع
درس‌هایی از Android

ارائه دهنده
عبدالرحمن امانی

28 فروردین ماه 1403



#!/inTheNameOf/God

Who I am

AbdoRahman Amani

- A Software engineer.
- Start Embedded journey with Nokia-sysmbian Smart phones
 - Then Android era.
 - Continued with RPi in university.
 - Lots of Embedded project as freelancer.
 - Back to smart phones as security researcher.





TABLE OF CONTENTS

01

Security

How we protect
sensitive data.

How android does it.

02

Update

Every software needs
update ?



PROBLEMS



SECURITY

Protect Sensitive Data
Against
Unauthorized access



UPDATE

Delivering updates in more
secure and efficient way



01 SECURITY

Embedded systems have become an integral part of various industries. These compact computing systems play a crucial role in modern technology, but they also pose unique security challenges.

I want to protect my Data !

There are always a sensitive data

Lists like this :

- Authentication Tokens
- Business valuable data
- En/Decryption keys
- Personal data
- And more ...

That needs to be protected.



Common Solutions



External Storage

A NOR, NAND or SD/MMC flash that your program can access it securly



External Chip

Use another IC along with your main SoC to store, generate or protect your data



Encryption

Encrypt data using one of common solutions or combined with each other



Android's Solution



Full Disk Encryption

Fully Encrypt partitions that contains important data
Like trueCrypt or bitLocker



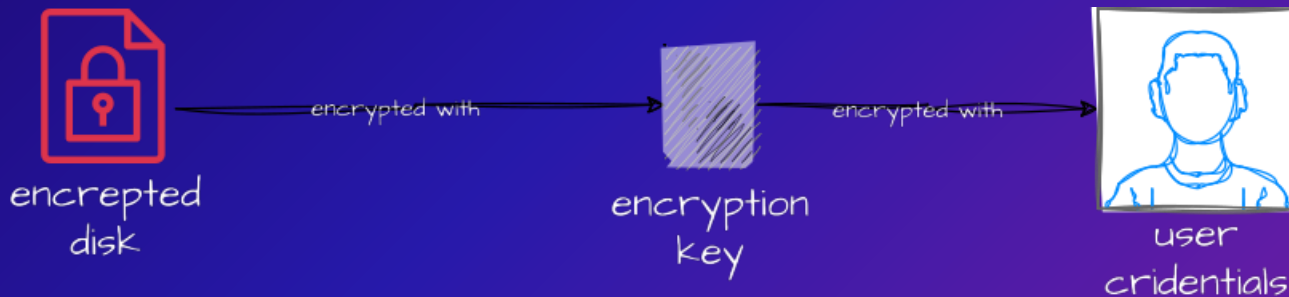
File Based Encryption

Using fscrypt to encrypt
file names and their
content and metadata

Android's Solution



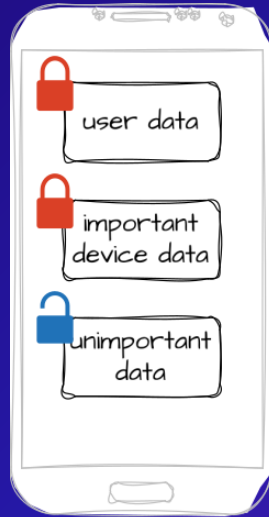
Full Disk Encryption



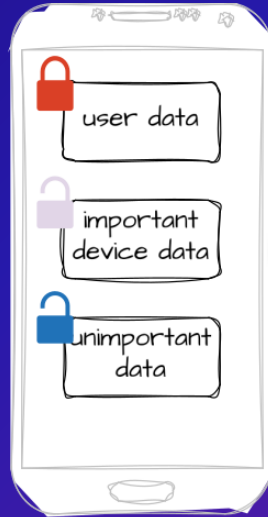
Android's Solution



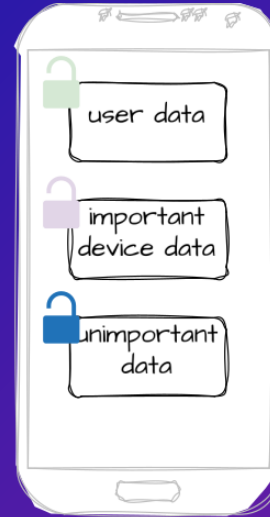
File Based Encryption



off



On
locked



On
user authenticated

Android's Solution

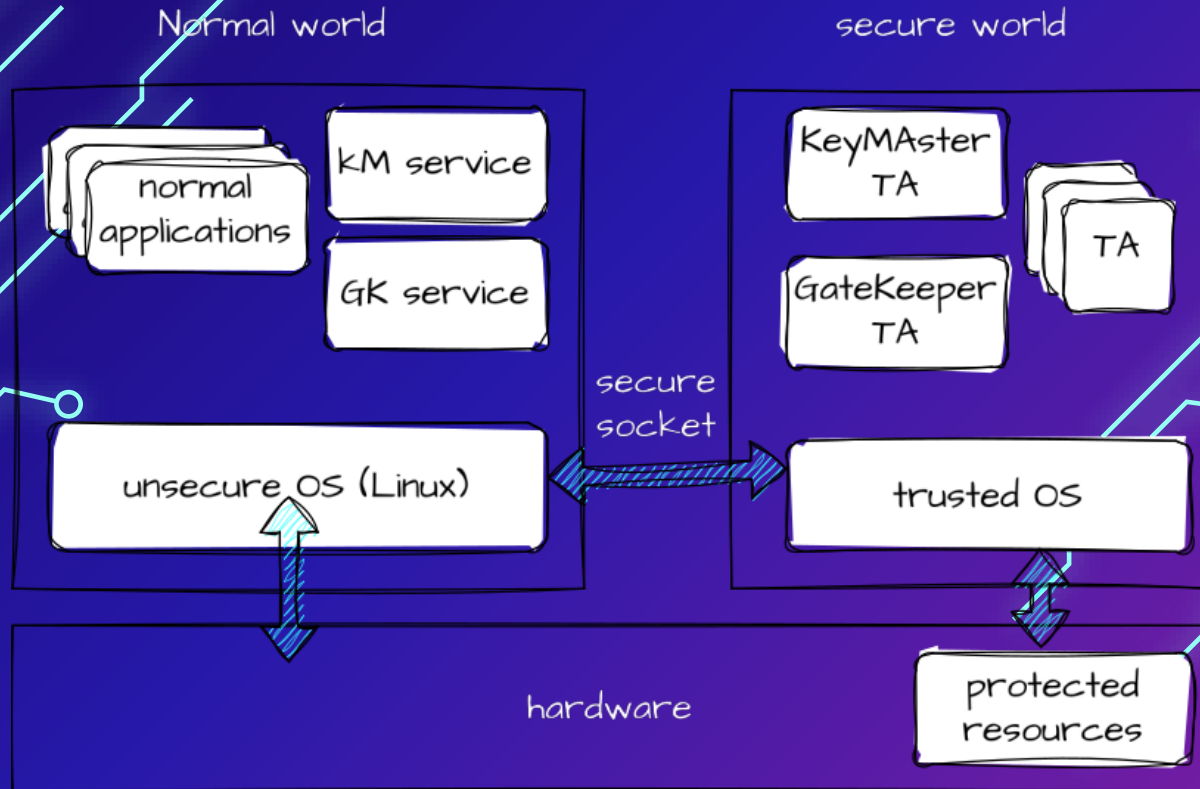


File Based Encryption

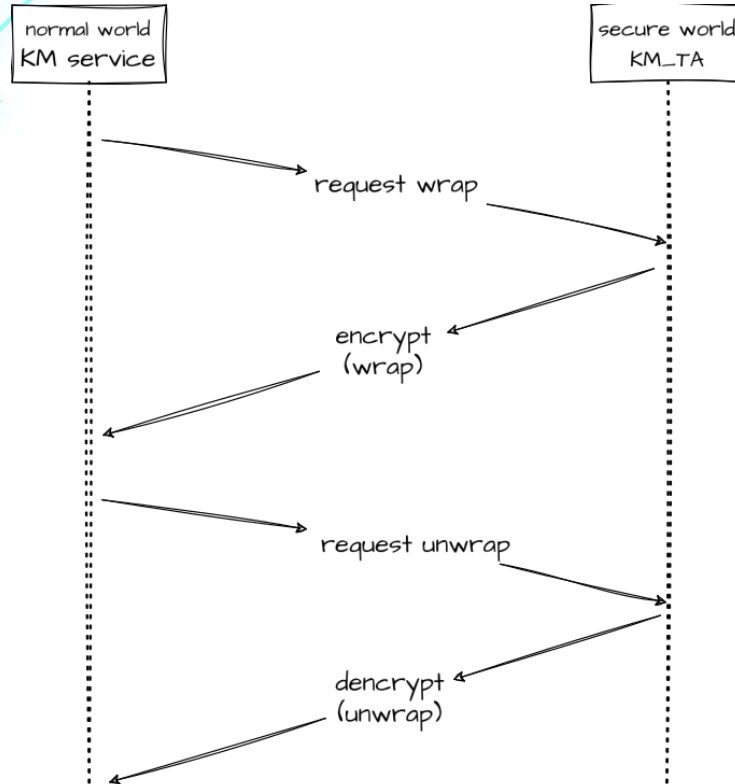
- *TEE*
- *KeyMaster*

Trusted Execution Environment

Trusted Execution Environment



KeyMaster



Try it your self



Get into your Phone

- *Android Debug Bridg*
- *Root access*

```
~/workspace/doc/presentations/E-LUG/me adb shell
m32:/ $ su
m32:/ # ls /data
DownFilters  app-asec      attribution   data          fota          local
adb          app-ephemeral backup        debuglogger   gsi           log
aee_exp      app-lib       bootchart    drm           ia            lost+found
anr          app-private   cache        dumpsys       incremental   mdl
apex         app-staging   core         duraspeed     keyfota       mdlog
app          app_fonts    dalvik-cache enc_user      knox          media
m32:/ # ls /data/data
+OR@PCAAAAwauME3odSXWQafqKnsBusJXJ8zFBEPcdxG6rEu6CRHhQ8FKHTbMLvNCYlq@dRlcSK
+mNDdBAAAAgohgYonIZ4b3jBt07j9FV9zuUETGpRG86QA5MuwjUChD
,0o2BBAAAAABSAX6aGJtqfm@1MT3wJ2phmwWpGrKngCE9eUUF2i9nD
,4HPEAAAAA27IOQZCA9bpAzVmUuHKf+iJli0o9hMayIbQ01q2JB,B
,BHL2DAAAAAw9hsRRU8Kr+gi0ekRS9Ukxy+s1fbtkuFD,s,MosIb1VC
,DMPBDAAAAAw7,Nuweb3,V7b6ex1BIu+J9h,SaUWvuiHsQr8DxwXnA
,L1+wAAAAAQsf4vkG1rr4BL0K,QM81JFNgwTIgbs3WTTMDZJJZnrqbAFKKGD37HddKSijUso5M
,RxsTCAAAAAXLJzh4EFSt26u149Tf7aDu5nV04rufB,WKYaNYty+AtRWJVvqhZ9dyVJ0MYE169A
,bHRQBAAAAgLB0Az6cwtX4TP9hnu3gBk0cWih8SZdwuKXLDu8wdTTC
,cvA7DAAAAQsf4vkG1rr4BL0K,QM81J6mtAiYHUfwf2E22oq2k46ZdPvWItnnCnf+T4z84,pME
,wSzoAAAAAQsf4vkG1rr4BL0K,QM81JKKyQ0EB0ws5j7egF29aD131L08znY5mXx,s6gGy86LA
,xTqlCAAAAQCDSW4nivEpe2ugfMz5RTgRURiyCEQVvwzHASbapfyZD
05I,pCAAAAAY3IC05pmqXTENERDzFX+a4CVKav0ZXex0ZknidzhRD
15tWwCAAAAgmK08Afs,ambkw+JHtFRTUQ9CJJjEz0pjAMVvAGQZSjC
228DgBAAAAALHTF7DUGasohNvLguLZ8veWMcww+lmLDrnUANBp6uDD
2L3KTBAAAAACv1JLtraPbkcw5q5,ELA+J9h,SaUWvuiHsQr8DxwXnA
2b8FMCAAAQ00memS1zkQvvcQeoyAMZo
```

Try it your self



Get into your Phone

```
zGjn3CAAAAwEUIYqLyDAfxtdBwojYw5Mr5aScj2JdZBB8pqcyG4ymA
zHQW1DAAAWE1+LlvYC23tI,+SLp88L6J9h,SaUWvuiHsQr8DxwXnA
zHiy9CAAAAQoJsVqxKZDoARvHF1ntY,5Jm87,Zv18CBMTG7N0Nma3NRUGIVeTIE0FyrclFCLkaL
zKu9NAAAAAwaumE3odSXWQAfQKnsBusJgLzzDzz@ZizmEhdauYF52+d2oLvKf0Jiy8LPrBWghMN
zmSXVBAAAAwWaYUC0vnUAwiqLEN28MBw0omzW+FS6jPVsgYUgw2SC
m32:/ # locksettings verify --old "1234"
Lock credential verified successfully
```

```
m32:/ # ls /data/data
```

android	com.samsung.android.app.settings.bixby
android.auto_generated_rro_product__	com.samsung.android.app.sharelive
android.auto_generated_rro_vendor__	com.samsung.android.app.simplesharing
android.autoinstalls.config.samsung	com.samsung.android.app.smartcapture
be.mygod.vpnhotspot	com.samsung.android.app.soundpicker
com.android.backupconfirm	com.samsung.android.app.spag
com.android.bips	com.samsung.android.app.taskedge
com.android.bluetooth	com.samsung.android.app.telephonyui
com.android.bluetoothmidiservice	com.samsung.android.app.updatecenter
com.android.bookmarkprovider	com.samsung.android.app.watchmanagerstub
com.android.calllogbackup	com.samsung.android.appseparation
com.android.carrierconfig	com.samsung.android.ardrawing
com.android.carrierdefaultapp	com.samsung.android.aremoji
com.android.certinstaller	com.samsung.android.aremojieditor
com.android.chrome	com.samsung.android.arzone
com.android.companiondevicemanager	com.samsung.android.authfw
com.android.cts.ctsshim	com.samsung.android.aware.service

USE CASES



In an Embedded Project

- *Smart Home*
- *Software defined vehicle*
- *Crypto wallet*
- ...

Some Idea



Use TEE for your Embedded Project

- *OP-TEE*
 - *opensource TEE designed for Arm Cortex-A cores using the TrustZone technology*
- *Linux TEE framework*
 - *Registration of TEE drivers*
 - *Managing shared memory between Linux and the TEE*
 - *Providing a generic API to the TEE*



02 UPDATE

What happens if your mission-critical control computer or retail kiosk gets an update and then fails?



Common UPDATE problems

- Crash after update

- High bandwidth consumption



common Solution



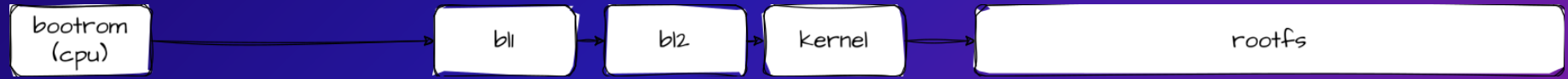
Immutable Linux

- OSTree
 - LG WebOS
- Transactional-update
 - openSUSE MicroOS
 - BTRFS snapshots

Android's Solution



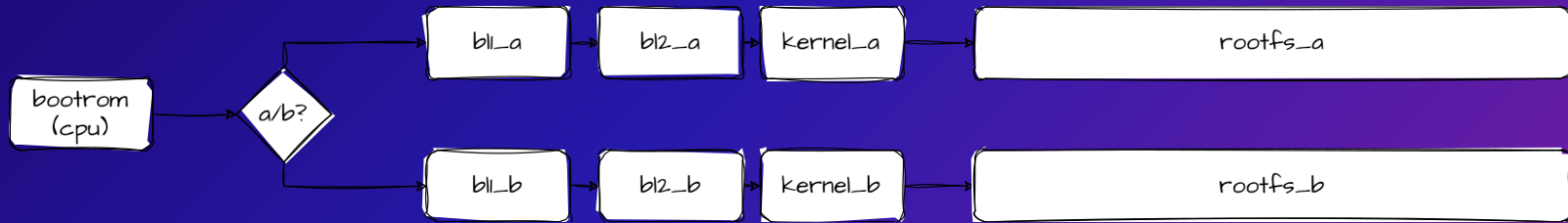
The old boot-chain



Android's Solution



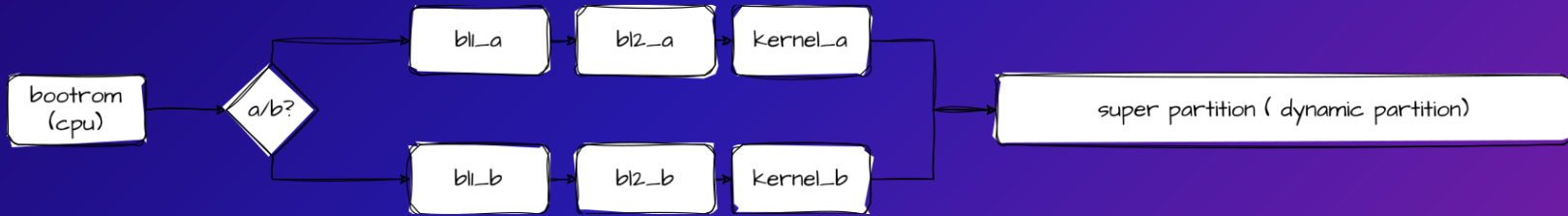
Securing update: the A/B solution



Android's Solution



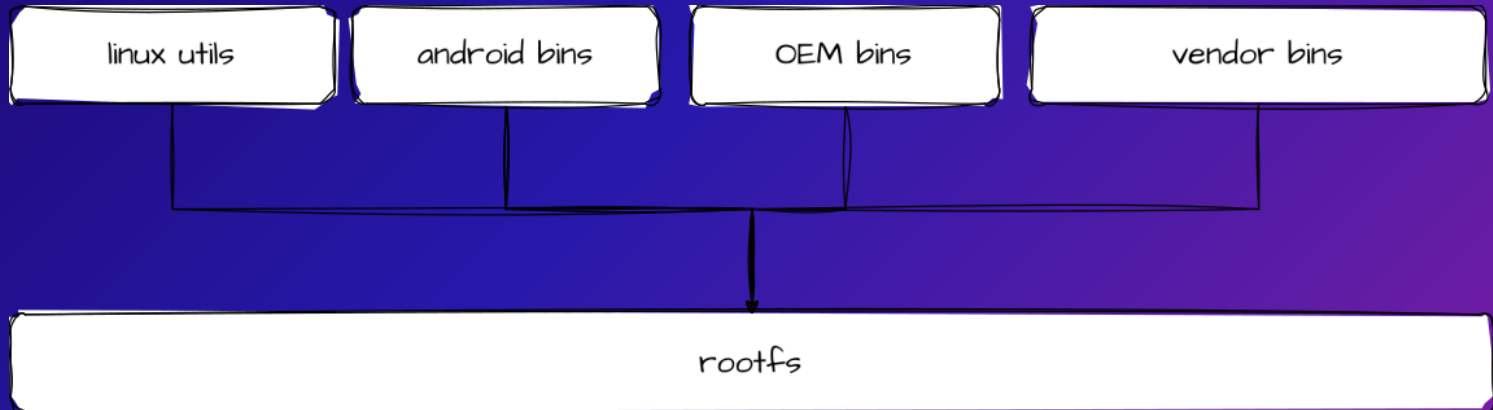
Reducing update size: **Dynamic partitions**



Android's Solution



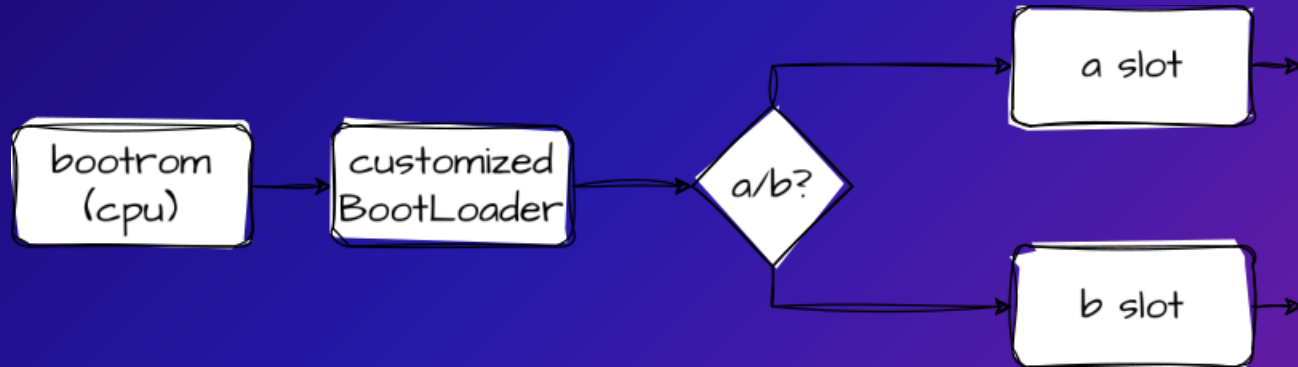
Reducing update size: Dynamic partitions



Try it your self



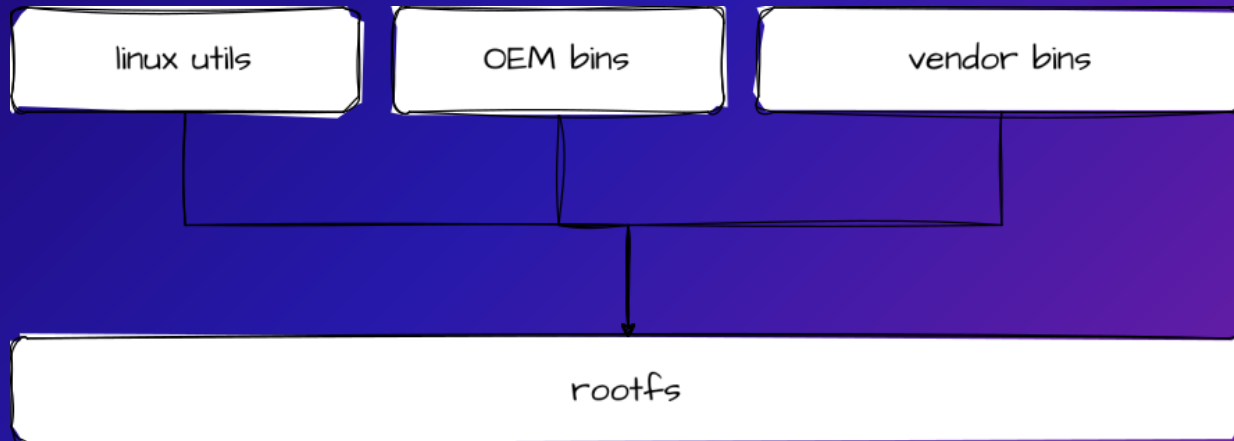
Customize your bootloader



Try it your self



Config you build system



با تشکر



ما را در شبکه های اجتماعی دنبال کنید:

