BUS
ONLY
ONLY

sigfox

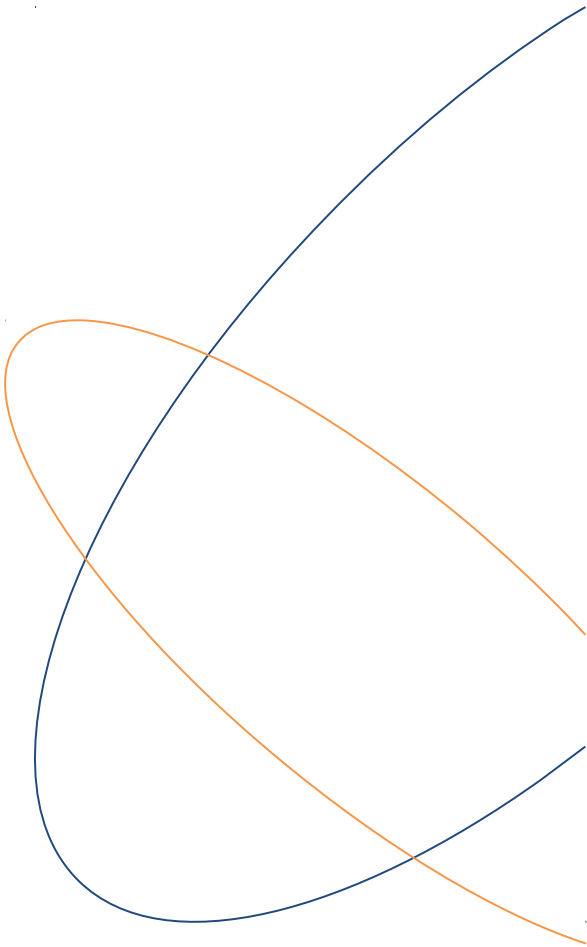
Measured boot: How to link the operating system to the platform integrity

Capitole du libre – 17/11/2018

sigfox

Plan

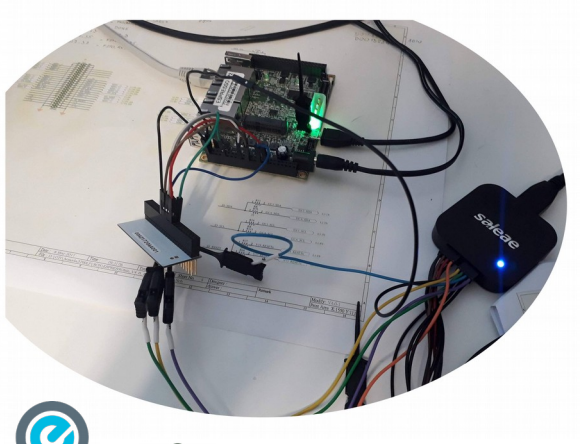
1) Measure boot overview
2) Trusted Platform Module overview
3) Measured boot in practice
4) Open source tools for implementation
5) Questions?



sigfox

Speaker presentation

- A Sigfox employee for more than three years
- My main activities:
  - New platform integration
  - Build system
  - Board support packages
  - Core system features
- Free software enthusiast
- Contributor in my free time



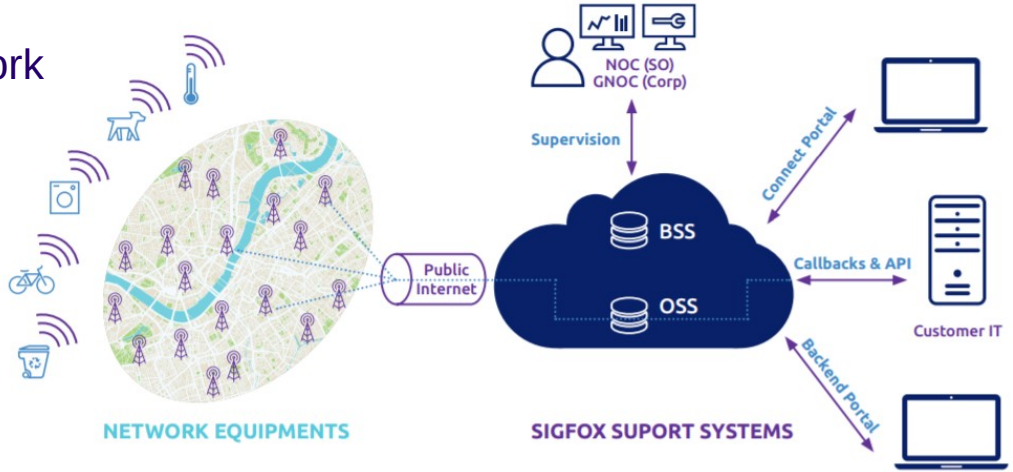
openembedded

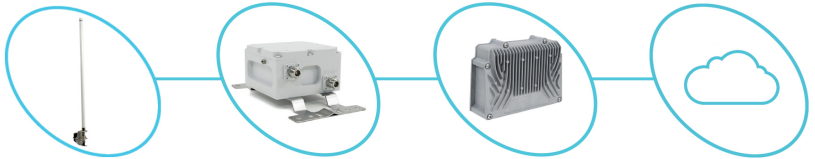
yocto PROJECT

sigfox

Sigfox presentation

- A global Low Power Wide Area network
  - Low cost
  - Low power
  - Several thousand of base stations
  - +50 countries
- Offer data and cloud services
  - Geo-location
  - Etc.
- Contribute to open sources





sigfox

What is a Sigfox base station ?

Access point which receive messages from devices to send them to our cloud.

- Hardware
  - CPU X86-64 / ARMv7 / ARMv8
  - RAM >= 1GBytes
  - Watchdog
  - SSD / eMMC / NAND >= 1GBytes
  - RADIO USB / SPI
  - Ethernet
  - 4G
  - TPM
- Software
  - Connectivity management
  - Data management
  - Hardware management
  - Identity management
  - Monitoring
  - Software Defined Radio
  - Time management

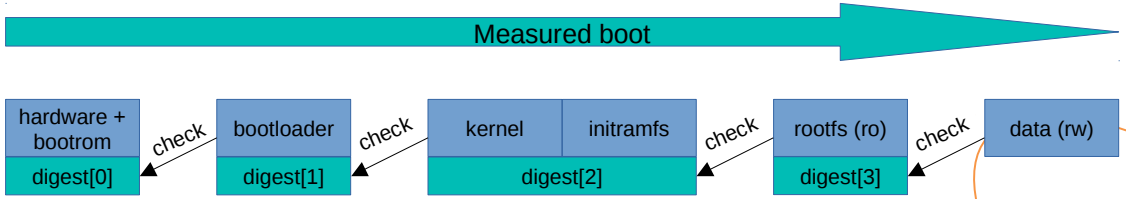
sigfox

1

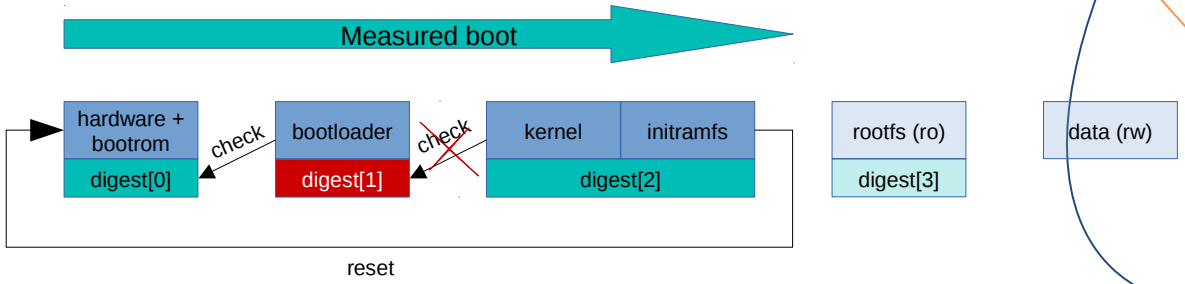
Measured boot overview

sigfox

Measured boot: definition

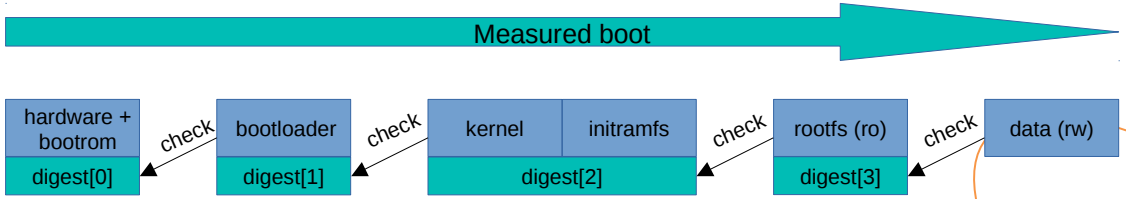


Measured boot chain of trust which prevents the boot stage execution when the system state (from previous stage) is not expected.

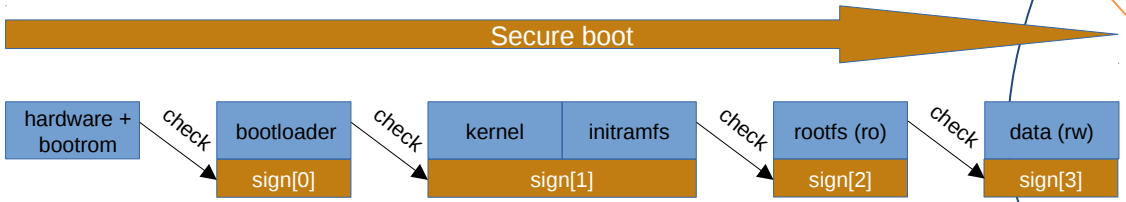


sigfox

Measured boot: difference with secure boot



Measured boot chain of trust which prevents the boot stage execution when the system state (from previous stage) is not expected.



Secure boot chain of trust which prevent the next boot stage execution when the signature is invalid.

sigfox

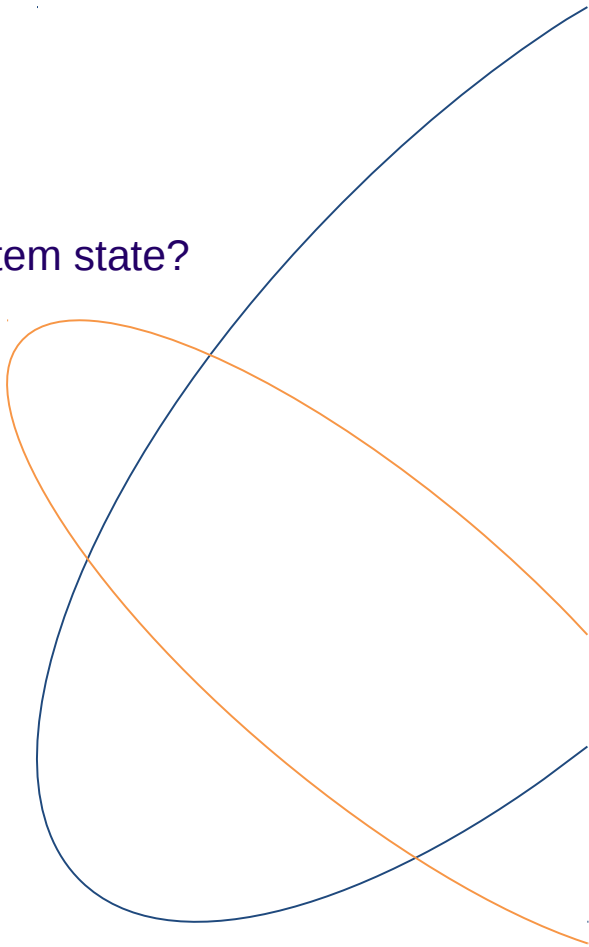
Measured boot: how to

How to guarantee the integrity of the representation of the system state?

This requires to use a trusted environment:

- to execute cryptography operations
- to store data representing the current stage integrity
- to read data representing previous stages integrity

=> The solution use a Trusted Platform Module (TPM)



2

Trusted Platform Module overview

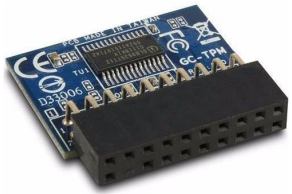
sigfox

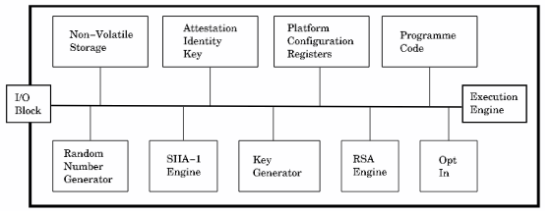
Trusted Platform Module

Trusted Platform Module (TPM, also known as ISO/IEC 11889) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

Each TPM chip contains two unique RSA keys from a persistent memory which cannot be accessed by software, cannot be cannot changed or extracted from the chip:

- The Endorsement Key (EK)
- The Storage Root Key (SRK)



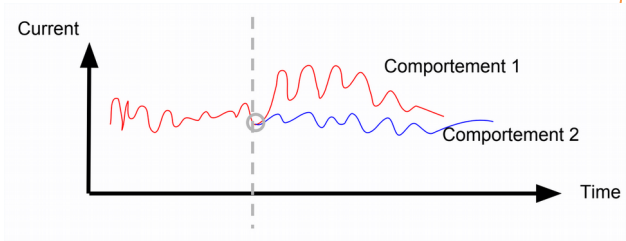


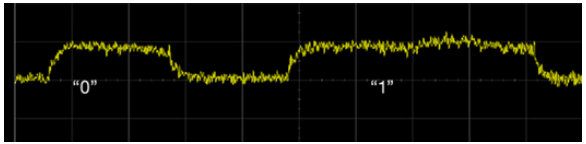
sigfox

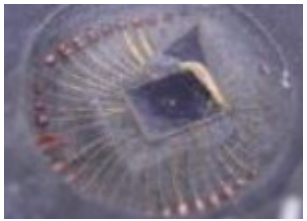
TPM hardware protections

It is protected against physical attacks:

- Brute force
- Side-channel
- Fault injection
- Imaging techniques
- Etc.





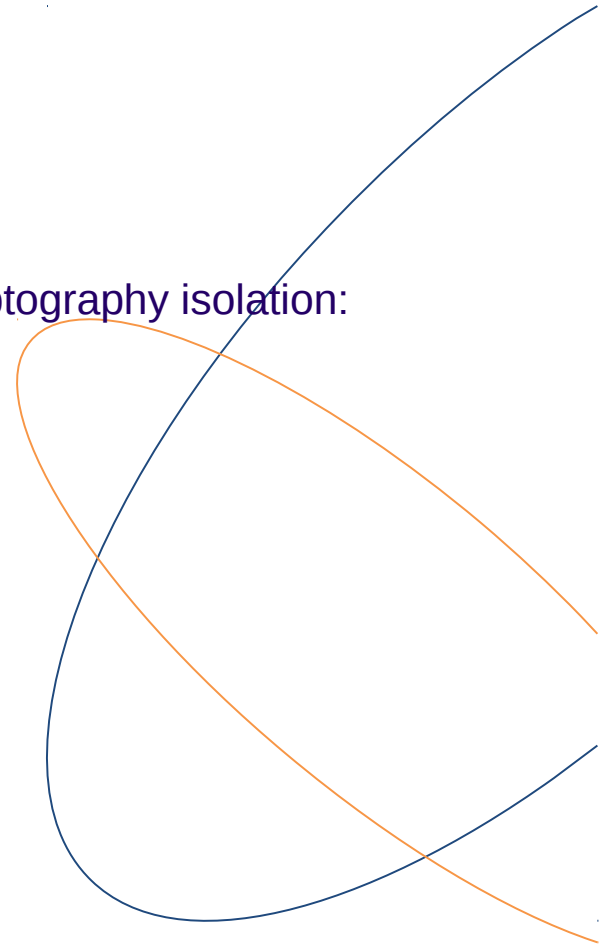


sigfox

TPM Cryptography features

Warning! TPM is not a cryptography accelerator but offer cryptography isolation:

- To add/remove keys (keys can not extracted)
- To generate random number
- To generate RSA key
- To hash
- To encrypt/decrypt signature

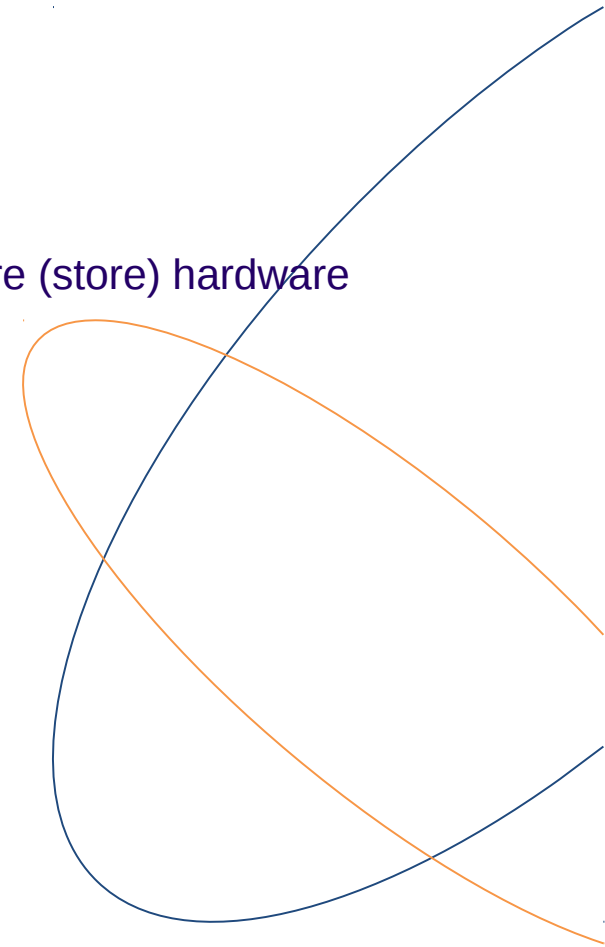


sigfox

TPM Platform Configuration Registers

- Platform Configuration Registers (PCR) used to measure (store) hardware and software states representing the system integrity.
- 24 banks containing SHA256 (or SHA1) hashes

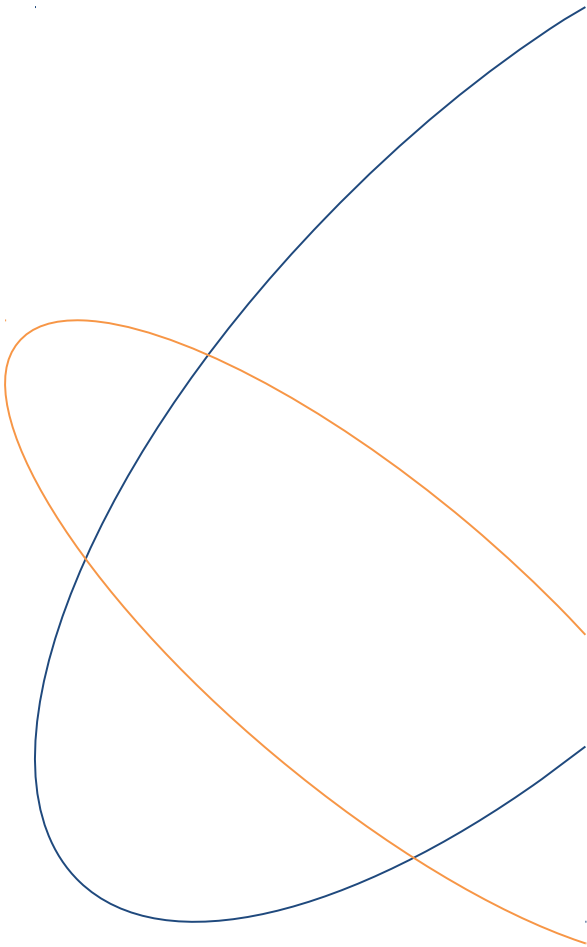
```
PCR_00: 3d 45 8c fe 55 cc 03 ea 1f 42 3f 15 62 be ec
PCR_01: c6 91 c0 ef b4 b4 0e f8 f9 5b 3b 95 a8 2f f4
…
PCR_23: 64 7c 9a 36 3b 5c 94 38 81 de 68 78 9c 00
```



sigfox

TPM PCR UEFI conventions

PCR Number	Convention
0	BIOS
1	BIOS Configuration
2	Option ROMs
3	Option ROMs Configuration
4	MBR (master boot record)
5	MBR Configuration
6	State transitions and wake events
7	Platform manufacturer specific measurements
8-15	Static operating system
16	Debug
23	Application support



sigfox

TPM PCR Operations

- These PCRs can then be read to report their state.
- PCRs can also be used in an extended authorization policy to restrict the use of other objects by:
  - hmac
  - password
  - Policy
- Can be accessed through a resource manager (kernel or userspace)

TPM PCR extend

The PCR update calculation, called an “extend”, is a one-way hash so that measurements can’t be removed.

Formula to measure the platform integrity:

PCR[N] = HASHalg(PCR[N] || ArgumentOfExtend)

Example:

PCR_10: 64 7c 9a 36 3b 5c 94 38 81 de 68 78 9c 00

tpm_extend 10 5fd4be8028d48249a594d18d8e6e

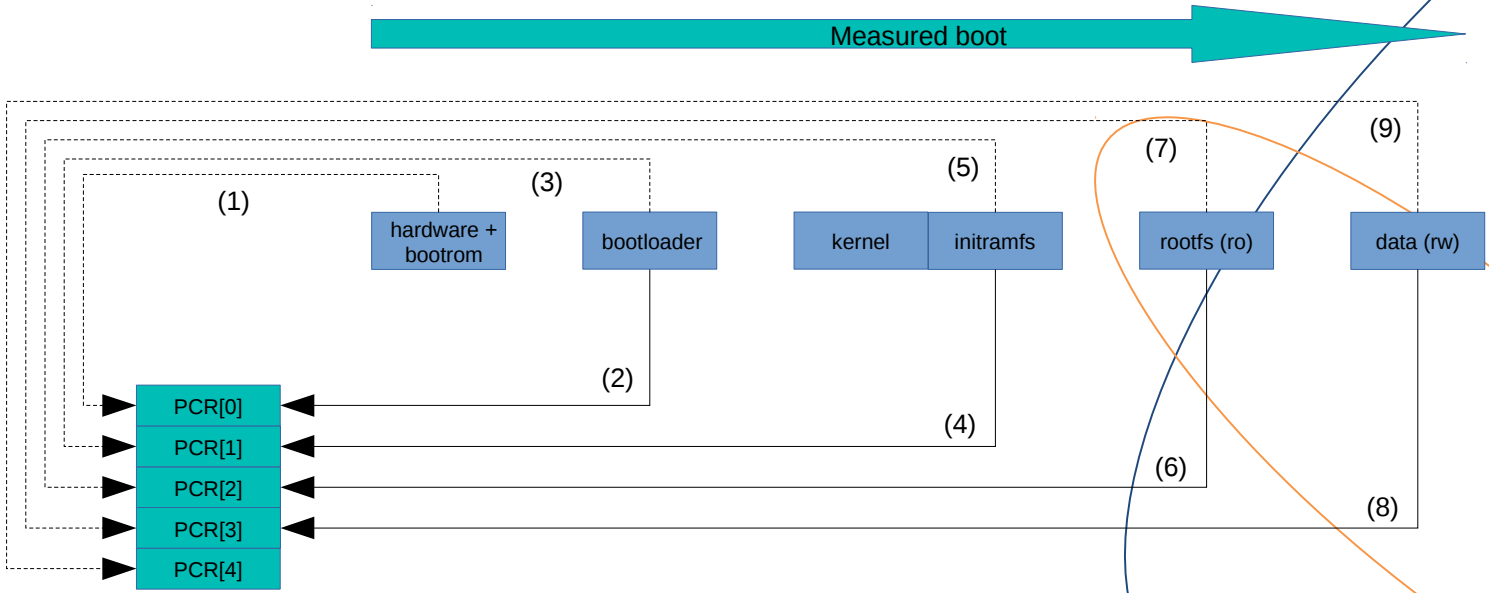
PCR_10: 21 31 10 06 a2 b7 dc 68 f4 7f 04 db fd e2 8f

3

Measured boot in practice

sigfox

Measured boot using TPM



sigfox

Measured boot variants

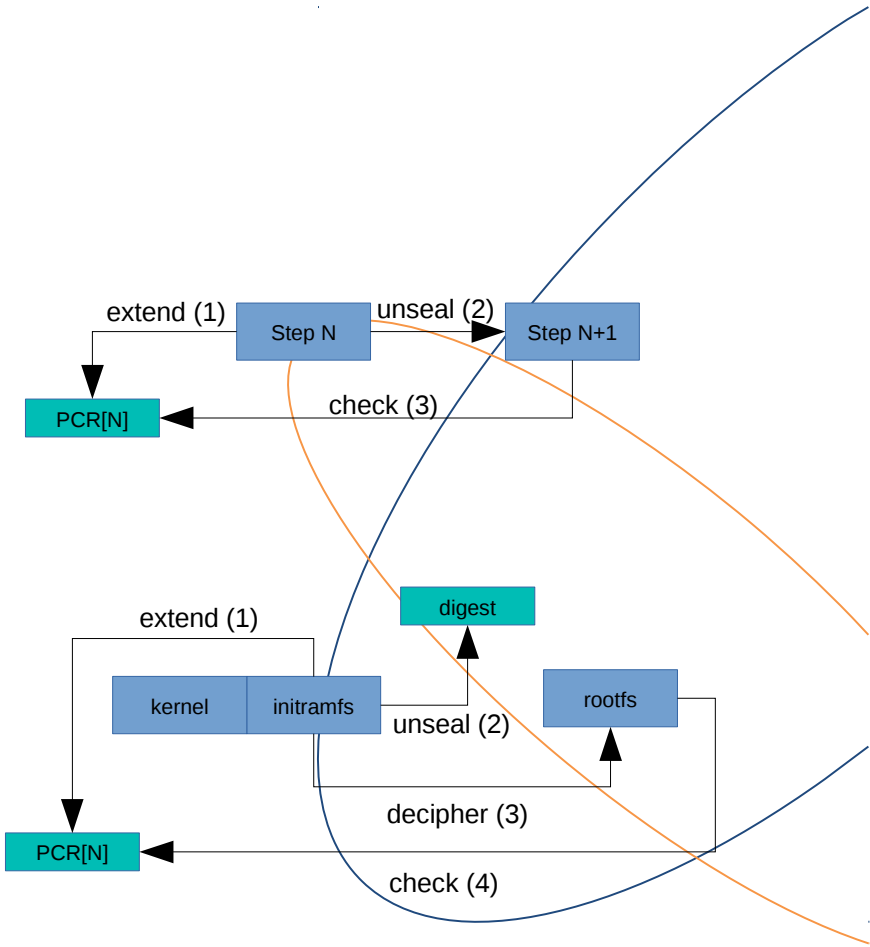
There are some variants:

- to unseal all boot stages

  (unseal = decipher data using the TPM bind key and platform integrity)

- to unseal the cryptsetup key file and to use this deciphered key file to decipher the rootfs

- Etc.



sigfox

Measured boot issue

Is it possible to build a complete chain of trust using only the measured boot?

Currently, it is very difficult because all boot stages must be capable to extend and read PCRs (or can be patched):

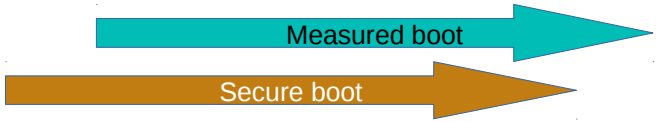
- bootROM: have rarely this support and can not be patched. So it is necessary to use another method to build a chain of trust.
- bootloader: some have the support or can be patches.
- kernel: have the support but require to use an initramfs to bootstrap the real rootfs.
- rootfs: have the support

Measured boot issue

There are two available solutions:

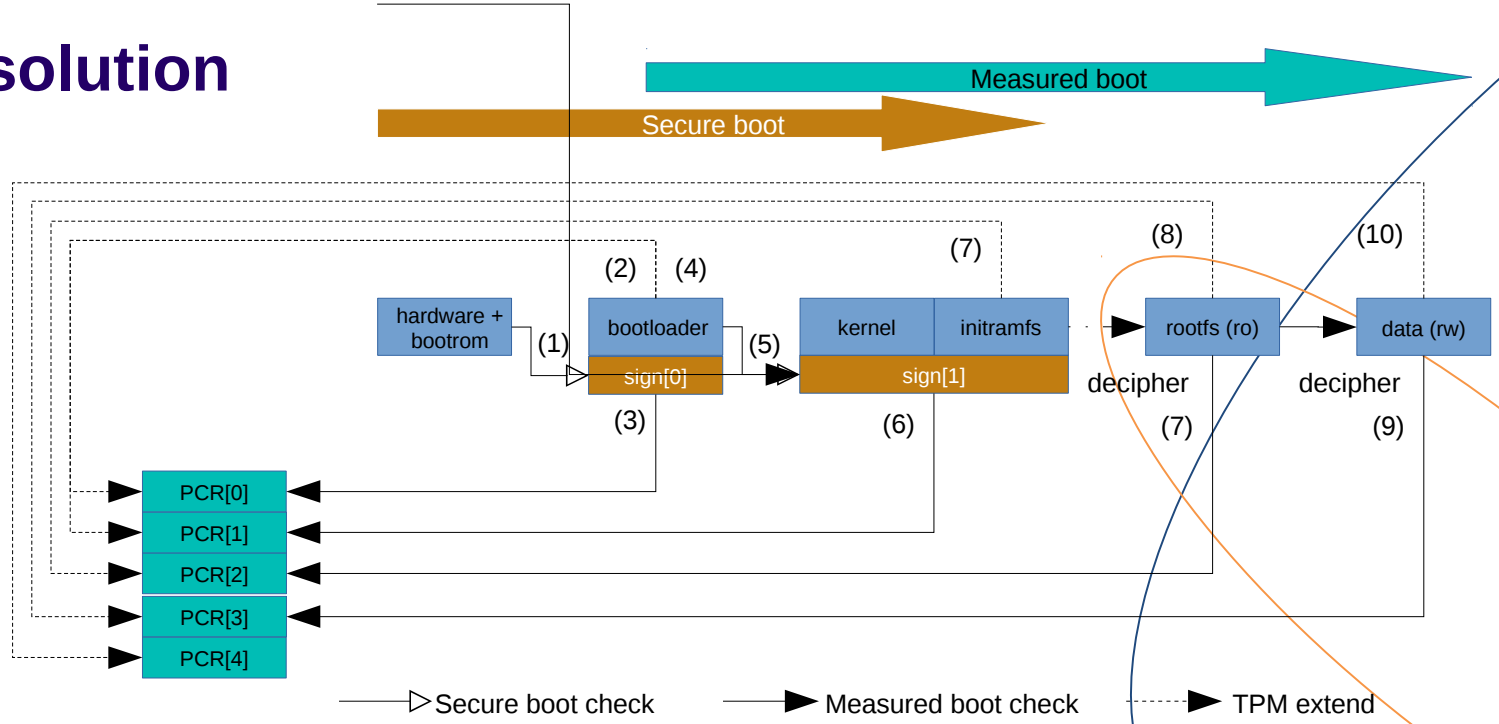
1- Use the secure boot solution provided by the manufacturer in order to have a root of trust for the measurement, that means the last stage from secure boot measure all hardware parts, the previous boot steps and the next step.

2 - Use the measured boot to harden the a full secure boot trust of chain, to prevent secure boot limitation, against bootkit (and filesystems).



sigfox

A solution



Here, in first, the bootloader extends the PCR[0] with the digest of hardware integrity, checks the value and extends the PCR[1]...

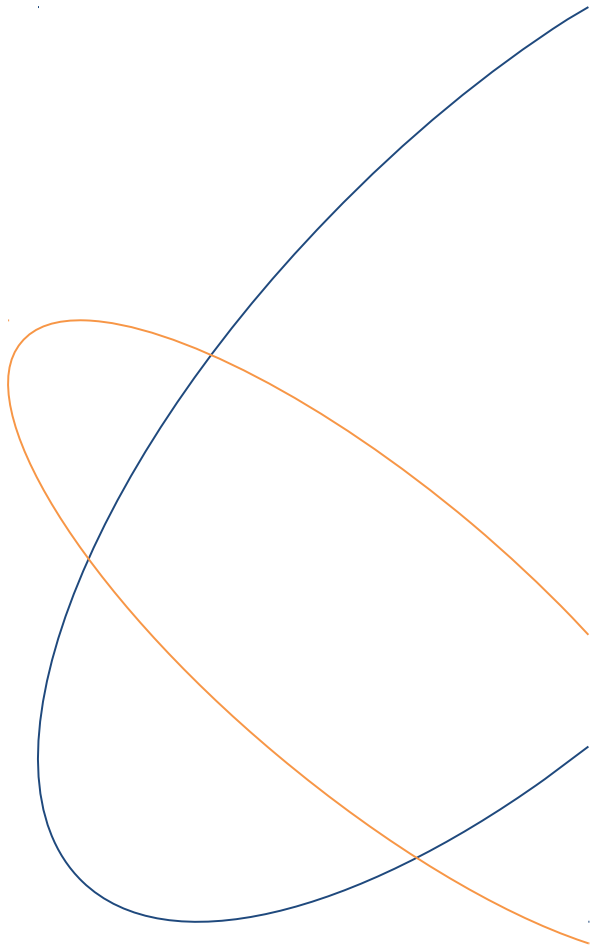
sigfox

4

Open sources tools for implementation

Available tools

- UEFI Bios
  - Core Root of trust for measurement (CRTM)
- Bootloader
  - TrustedGrub
  - U-boot
- Kernel: TPM_TIS, IMA/EVB
- Userspace
  - TPM2-tools
  - Trousers
- Etc.



sigfox

References

- TCG TPM2 Software Stack and Embedded Linux : https://elinux.org/images/6/6e/ELC2017_TPM2-and-TSS_Tricca.pdf
- TPM2 Software Stack (TSS2) : https://events.linuxfoundation.org/wp-content/uploads/2017/11/Getting-Started-with-the-TPM2-Software-Stack-TSS2-Philip-Tricca-Intel-1.pdf

5

Questions?

sigfox

Thank you!

sigfox