gapfruit

Trusted boot with the Genode OS Framework

Alice Domage, Software Engineer

About Gapfruit

2012: R&D of real-world products with microkernel and capability-based security

2017: Roll-out military-grade notebook (HW/SW co-design)

2018: Founding of Gapfruit AG in Switzerland

2020: TEE for transactional workloads in the finance industry

2022: Partnership with Bechtle and Device Insight (and others) for the IIoT sector

2024: Funding by Innosuisse SIP

bechtle

DEVICE INSIGHT

GENODE

axiros Lasting Advantage

securosys

codit

Innovation project supported by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

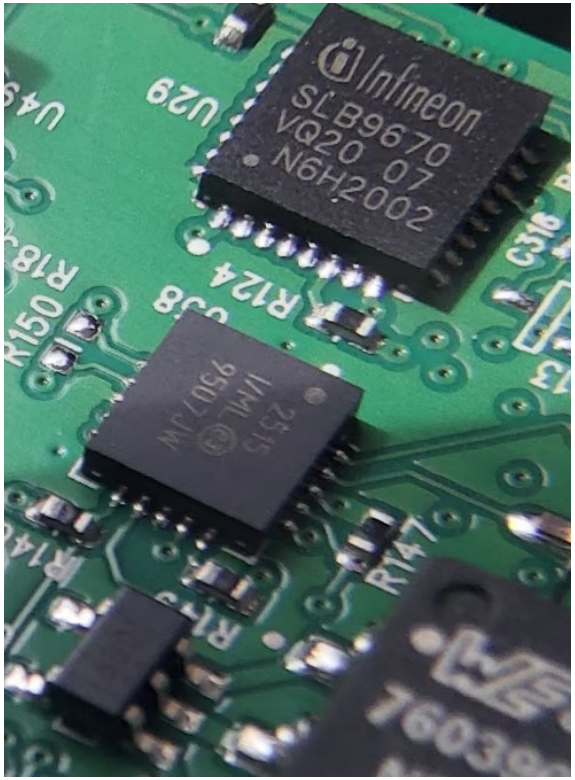
Innosuisse – Swiss Innovation Agency

Private Key Infrastructure (PKI) at Gapfruit

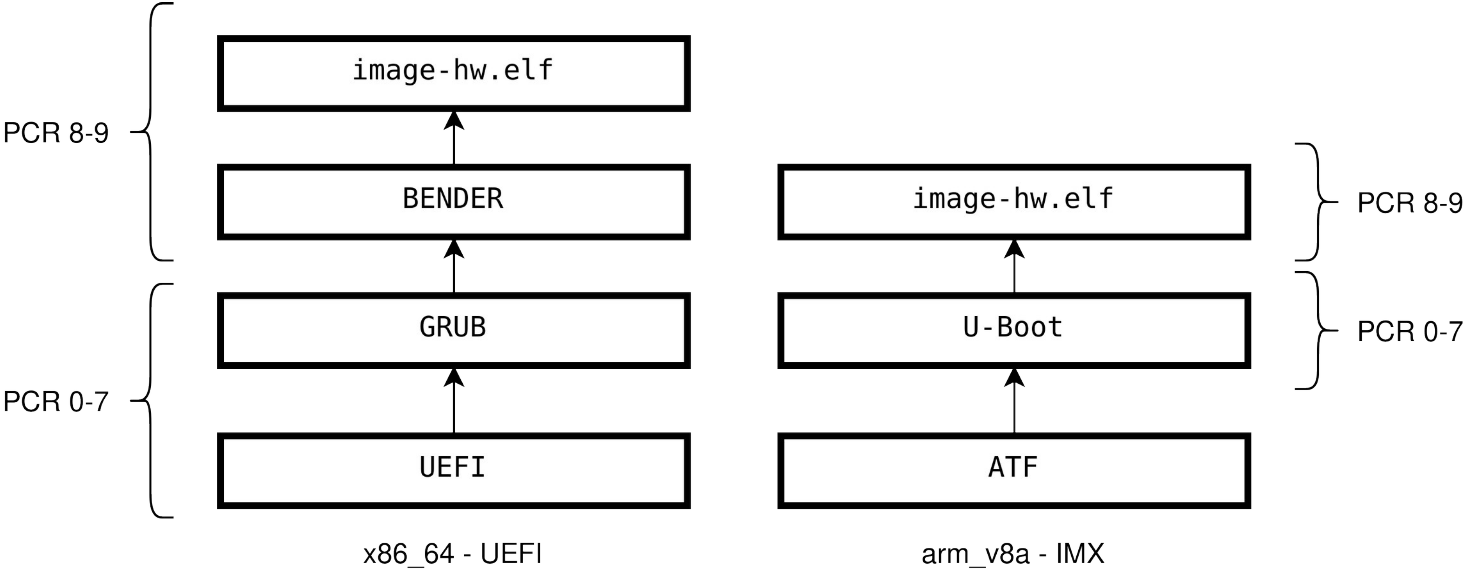
- Access to the cloud with Zero touch provisioning
- Protect the key that provide access to the Cloud
- Trusted Computing base record the bootchain environment in PCRs
- TPM is used to sign a short lived certificate that legacy apps use to access the cloud

TPM Stack: Design Goals

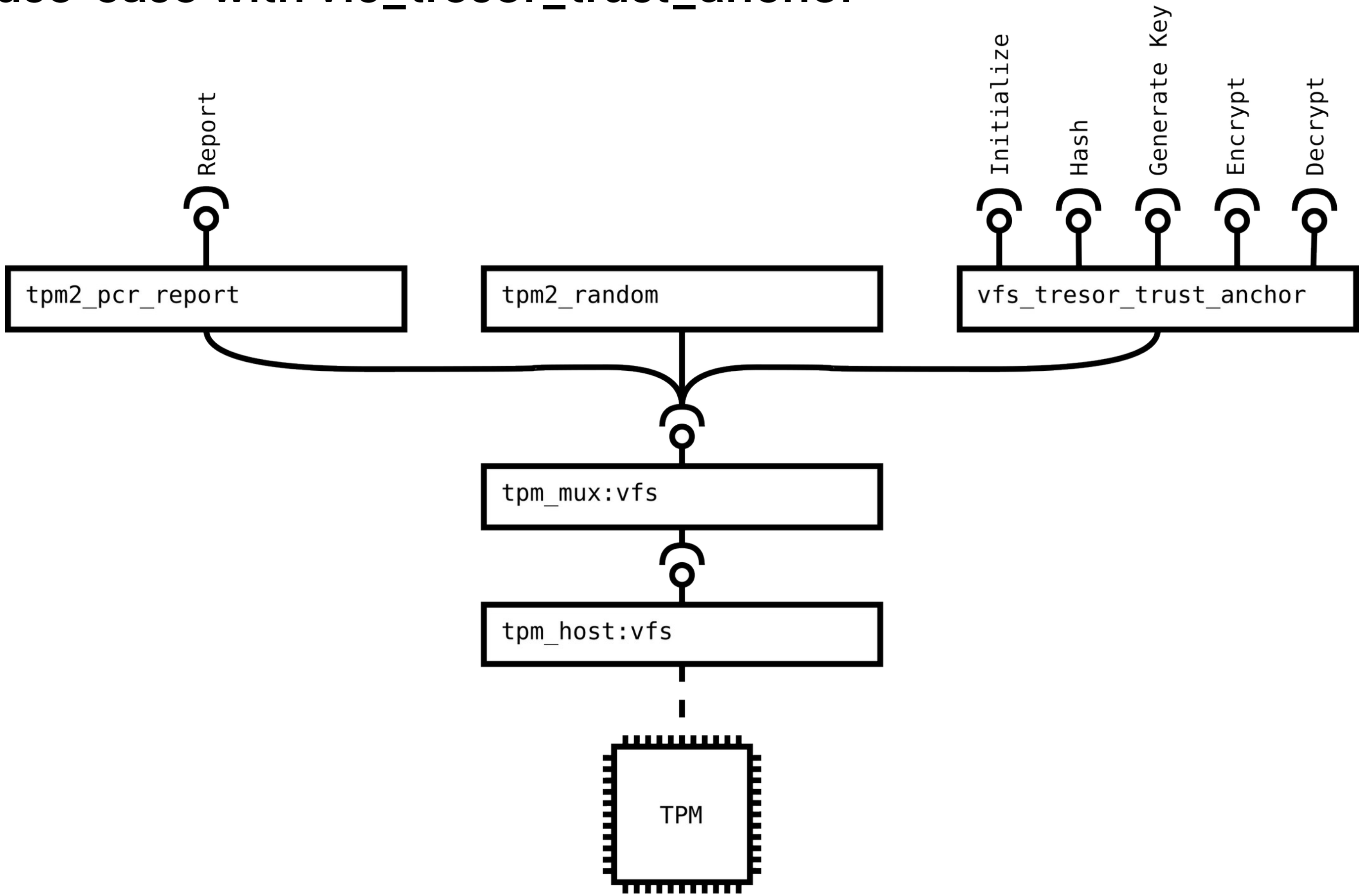
- Composability and separation of concerns
- Minimal Trusted Computing Base
- Benefit from existing libraries
- Integration of measured boot with non-brittle PCRs
- Updates with rollback prevention
- Use TPM for authentication and integration to PKI
- Compatibility with legacy POSIX applications



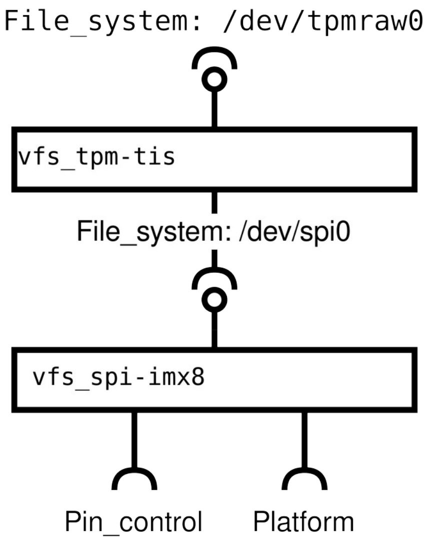
TPM Stack: measured boot & Platform Configuration Registers (PCR)



TPM Stack: use-case with vfs_tresor_trust_anchor



TPM stack: supported hardware



File_system: /dev/tpmraw0

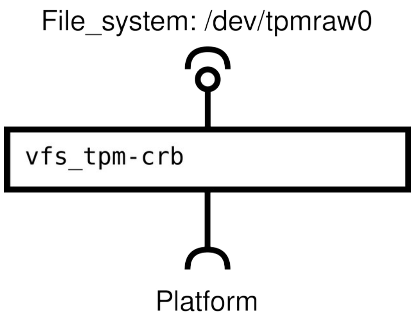
vfs_tpm-tis

File_system: /dev/spi0

vfs_spi-imx8

Pin_control

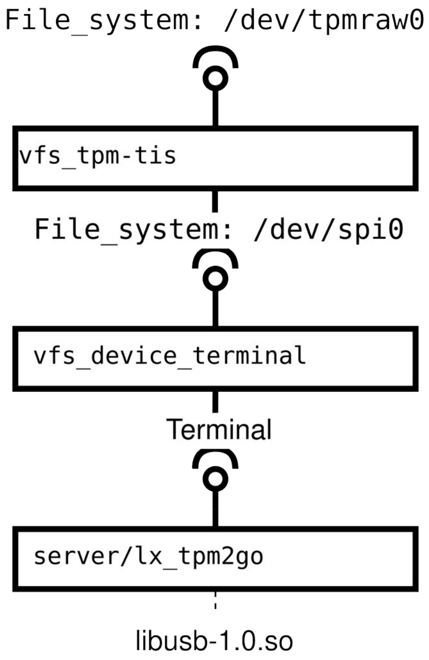
Platform



File_system: /dev/tpmraw0

vfs_tpm-crb

Platform



File_system: /dev/tpmraw0

vfs_tpm-tis

File_system: /dev/spi0

vfs_device_terminal

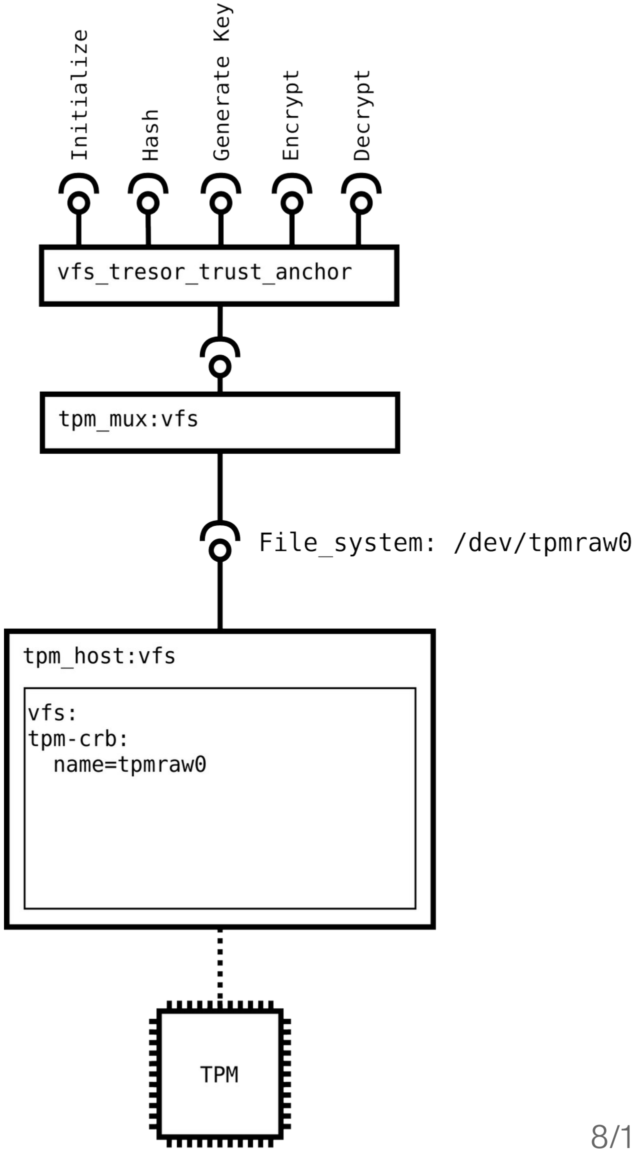
Terminal

server/lx_tpm2go

libusb-1.0.so

TPM Stack: TPM Driver

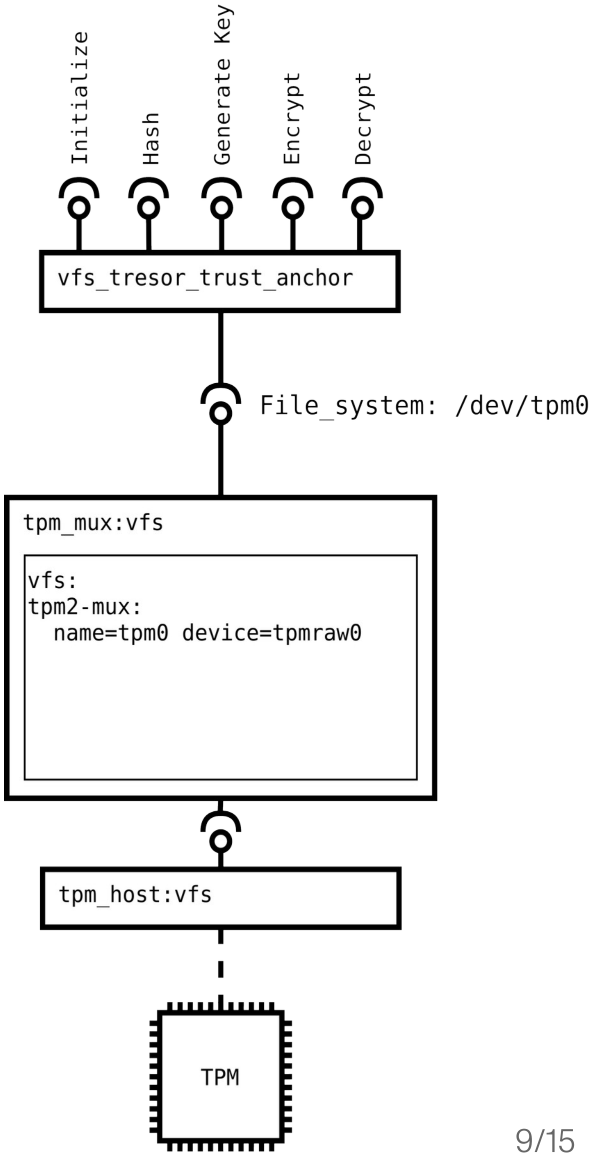
- **tpm-tis** VFS plugin that adapts TPM commands to SPI Bus
- Drivers:
  - CRB driver for fTPM (x86_64-hw)
  - SPI driver for dTPM (i.MX8-hw) + tpm_tis
  - lx_tpm2go driver for tpm2go (linux-linux) + tpm_tis



```
vfs:
tpm-crb:
  name=tpmraw0
```

TPM Stack: TPM Multiplexer

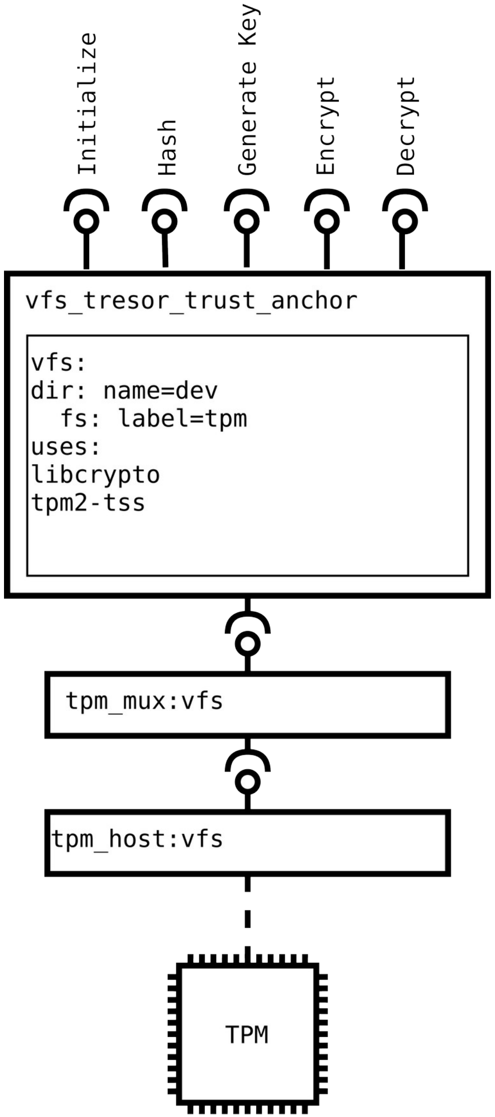
- The **tpm2-tss** client expects a **/dev/tpm0** device
- The **tpm_mux** provides this file as VFS plugin
- It multiplexes commands
- It load/unload objects to **managed limited resources**
- **tpm2-abrmd** from linux world is too complex for our use-case
- **tpm_mux** a simple vfs-pluging keeping the TCB small



```
vfs:
tpm2-mux:
  name=tpm0 device=tpmraw0
```

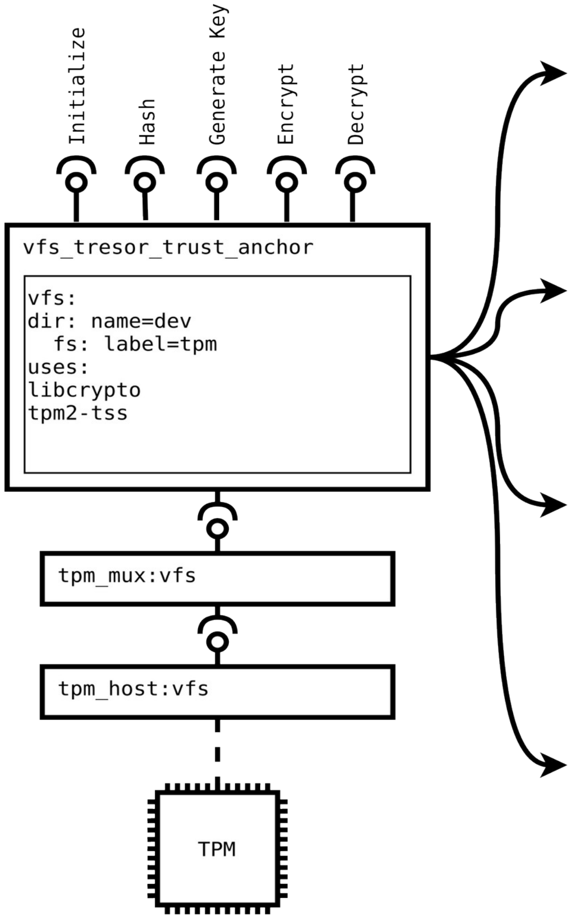
TPM Stack: vfs_tresor_trust_anchor

- File system pluging:
  - Generate the CBE secret key
  - Seal/Unseal the secret key on persistant FS
- Uses **tpm2-tss** that expect a **/dev/tpm0** file
- Use HMAC Session for **paramater encryption**
- Use Policy Session for PCR and passphrase **authorization**



```
vfs:
dir: name=dev
  fs: label=tpm
uses:
libcrypto
tpm2-tss
```

TPM Stack: vfs_tresor_trust_anchor tpm2-tss call overview



```
vfs:
dir: name=dev
  fs: label=tpm
uses:
libcrypto
tpm2-tss
```

Esys_PolicyPCR()
Esys_NV_DefineSpace()*
Esys_PolicyGetDigest()
Esys_NV_Write()

`ctor`

Esys_GetRandom()* -> Secret_key

`Job::GENERATE`

Esys_PolicyPCR()
Esys_PolicyAuthorizeNV()
Esys_PolicyPassword()
Esys_Create()* -> Wrapped_secret_key

`Job::INIT`

Esys_Load()
Esys_PolicyPCR()
Esys_PolicyAuthorizeNV()
Esys_PolicyPassword()
Esys_Unseal()* -> Secret_key

`Job::UNLOCK`

*use paramater encryption/decryption

vfs_tresor_trust_anchor: work in progress

- No input GUI to provide the OWNER hierachy password
- No input GUI to provide the NV space auth_value, **randomly generated** value instead, therefor PCR Policy digest can not be changed
- no mechanisme to update the PCR policy digest in the NV space when the **system is updated**
- **tpm2-tss** depends on **libc**

vfs_tresor_trust_anchor challenge: **tpm2-tss** depends on **libc**

Current Mitigation

- *libc_vfs* alternativ to *vfs*
- Initialize a secondary vfs for libc, so libc can be used
- Wrapp calls to *tpm2-tss* with *with_libc()*

Solution

- TPM Command Transmission Interface (aka tcti) for genode
- Create minimal libc for tpm2-tss without relying on vfs

Lessons Learned

- TPM’s are hard
- Painkillers vs. vitamins
- Using tpm2-tss and upgrading Openssl brings challenges when used in VFS
- Using a vfs pluging design organizes the complexity of trust_anchors and TPM access

Questions

Alice Domage, Software Engineer

https://gapfruit.com

LinkedIn: https://linkedin.com/in/alice-domage

Mastodon: @alicedomage@infosec.exchange

Github: https://github.com/a-dmg