Trustworthy 2020 Platforms

TPM.dev Mini Conference 2020

Piotr Król

3MDEB

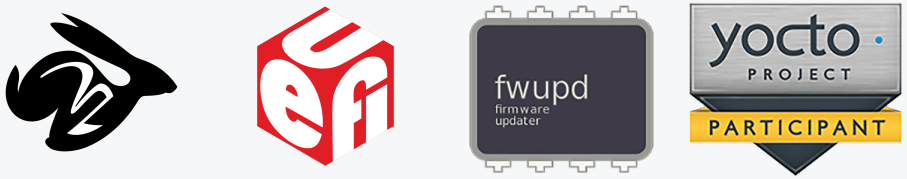
whoami

Piotr Król
3mdeb Founder

- coreboot contributor and maintainer
- Conference speaker and organizer
- Trainer for military, government and industrial organizations
- Former Intel BIOS SW Engineer
- 12yrs in business
- 6yrs in Open Source Firmware
- C-level positions in

3MDEB LPN PLANT VITRO

Who we are ?



- coreboot licensed service providers since 2016
- coreboot project leadership participants
- UEFI Adopters since 2018
- Official consultants for Linux Foundation fwupd/LVFS project
- Yocto Participants and Embedded Linux experts
- Open Source Firmware enthusiasts and evangelists

Problem statement

There is no reference platform, which seamlessly leverage OSS stack, that can be used for building secure and trusted environment on low-SWaP devices

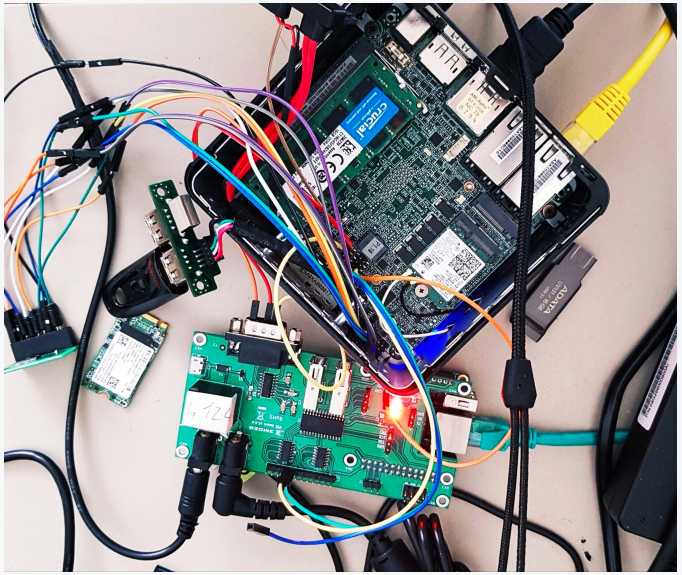
- **Who should care?**
  - remote and home office builders
  - homelabbers (`r/Homelab`)
  - IoT makers
  - FinTech
  - DevOps building CI/CD labs
- **What are the goals?**
  - Setup modern AMD hardware with TPM 2.0
  - Setup and provision: safeboot, TrenchBoot and Yocto/OE with Xen and sample VM
  - Discuss OEM challenges

low-SWaP - low Size, Weight and Power, military term and one of the goals of tactical computing

Hardware

- **ASRock 4x4 BOX-R1000V (AMD Ryzen R1505G, 16GB DDR4) - 279.99USD**
- AMD Radeon Vega 3 Graphics
- Extensible: M.2 Key-E and Key M slots, SATA connectors
- DRAM: Max. 32GB, ECC support
- TPM over LPC

Development setup



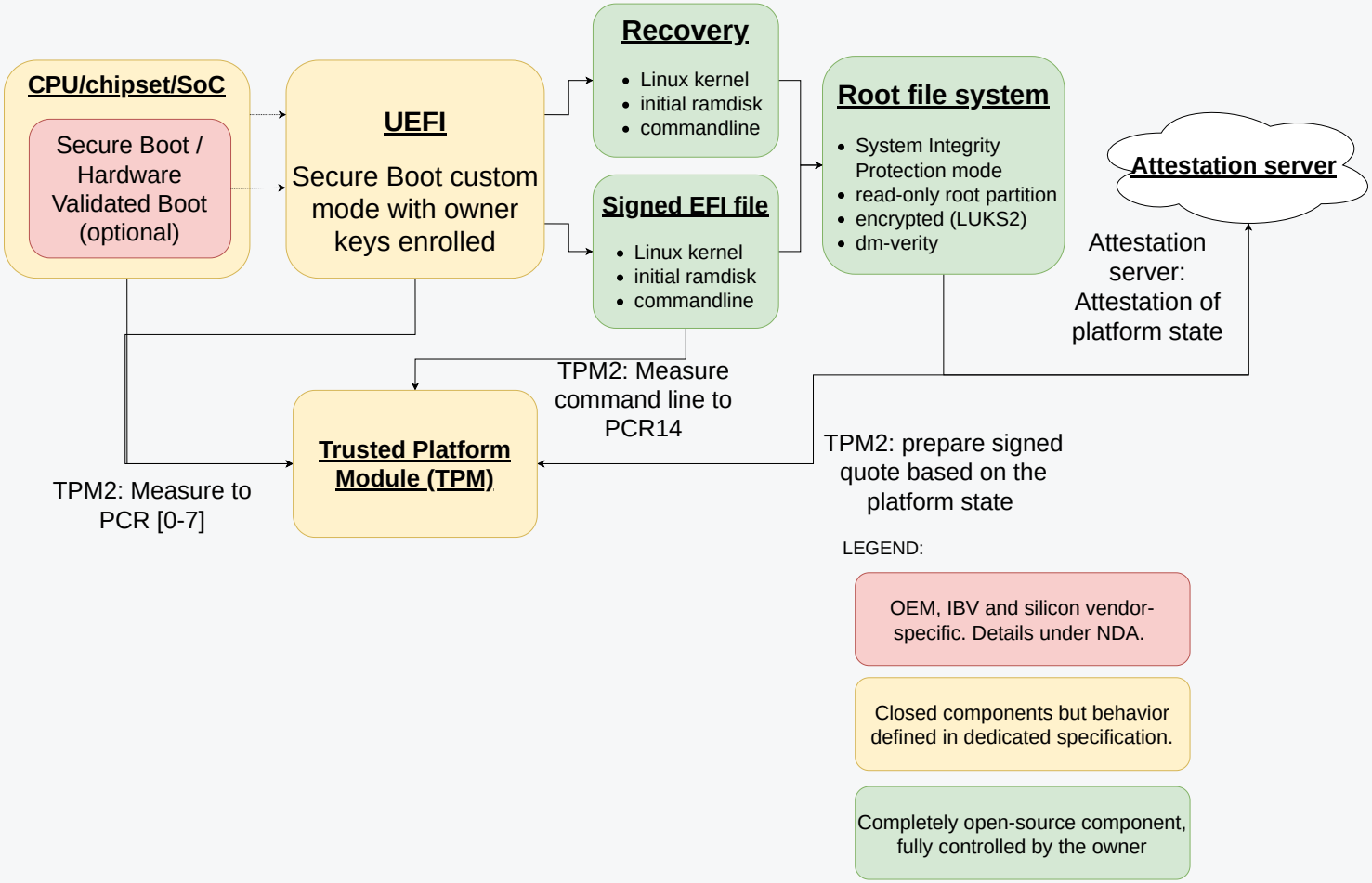
- ASRock 4x4 BOX-R1000V setup for remote development
- **TPM: PC Engines TPM2 module Infineon SLB9665**
- 3mdeb Remote Testing Environment - OSHW certified remote access and test automation tool

Why AMD?

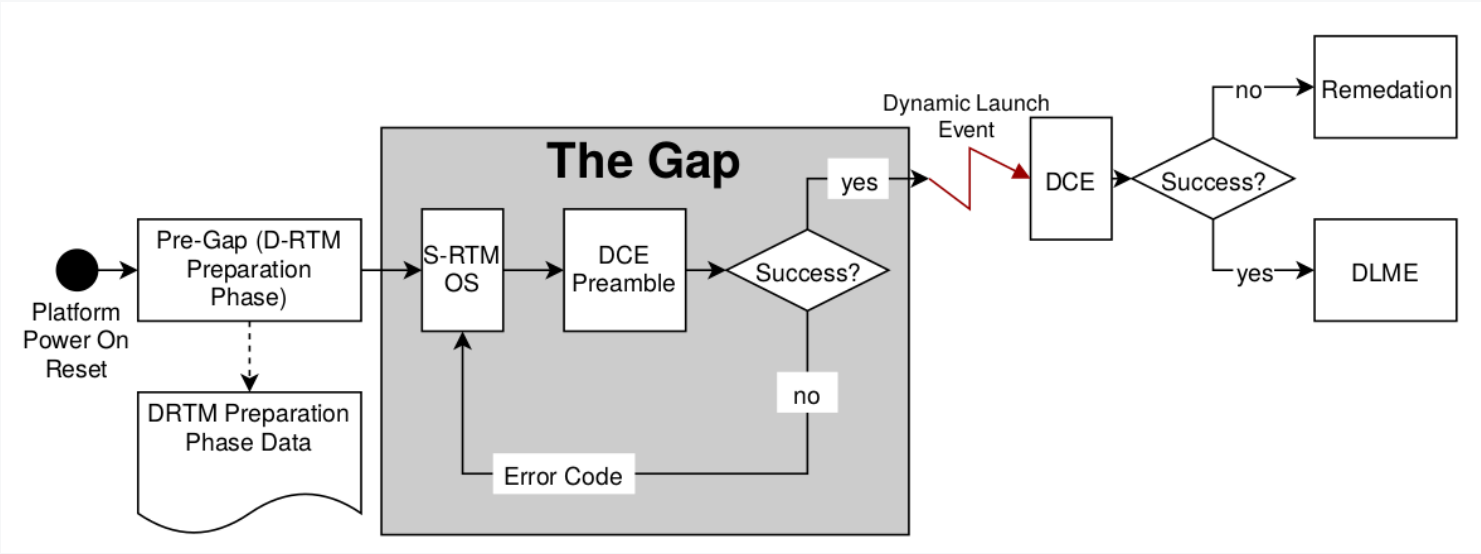
- Wide range of low-SWaP devices
- Cost efficiency
- Support for SKINIT DRTM instruction in both Ryzen and Epyc
  - Intel provide TXT only in higher-end SKUs (workstations, servers) not suitable for low-SWaP
  - There are no plans for TXT support in low-end SKUs
- Fully open-source DRTM implementation through TrenchBoot project
  - No ACM BIOS and ACM SINIT like in Intel - closed source components with questionable distribution model
- Hardware Validated Boot - AMD version of Boot Guard
- New attractive models coming like ASRock 4X4 BOX-4300U with Ryzen 4000U-Series

- Project initiated by Trammel Hudson in 2020
- GPLv2-licensed set of scripts to improve security of Linux boot process with UEFI Secure Boot and TPM support
- Why? Because process of leveraging standard platform security features is too complex for users and administrators.
- Goals
    - Booting only code that is authorized by the system owner
    - Streamlining the encrypted disk boot process
    - Reducing the attack surface
    - Protecting the runtime system integrity
    - Proving to remote systems that the local machine is safe

safeboot website: https://safeboot.dev/



TCG D-RTM

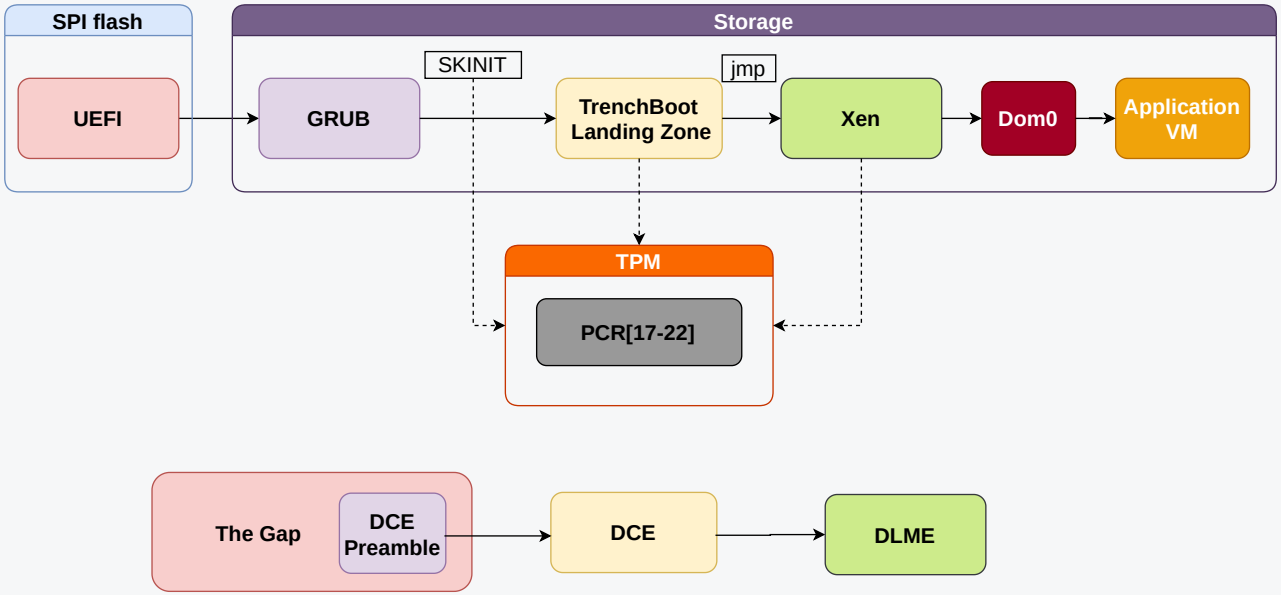


- DRTM start when Dynamic Launch event call executes
- DL Event controls PCRs 17-22, those are initialized with value -1
- DL Event change PCRs value to 0 and immediately extends with DCE hash
- Any attempt to reset TPM will set PCR[17] to -1 (TPM reset attack immunity)

TCG D-RTM Architecture v1.0.0

TrenchBoot for AMD

- TrenchBoot is s a framework that allows individuals and projects to build security engines to perform launch integrity actions for their systems.
- TrenchBoot Landing Zone is GPLv2-licensed implementation of AMD-V Secure Loader

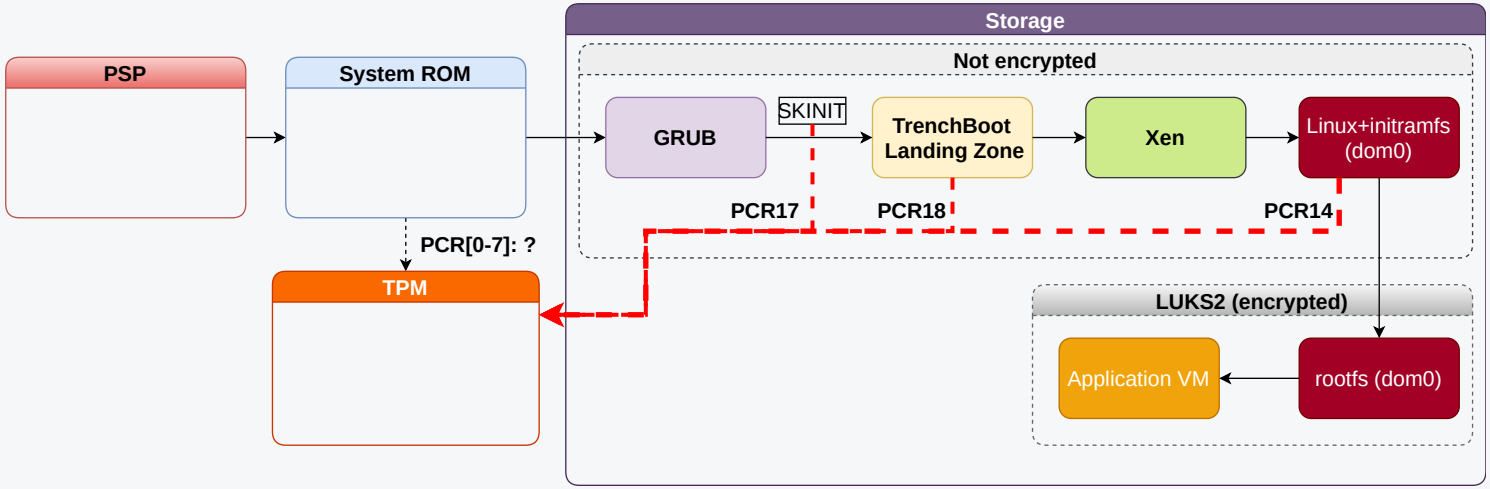


TrenchBoot: http://trenchboot.org/

- Produce ready to use, minimal system image with tools to provision security features
  - `safeboot` deployment simplification in embedded environment
  - TrenchBoot integration through `meta-trenchboot`
- `tpm2-tools` integration
  - `meta-measured` delivers most recent version of TPM tools
- Xen
  - supported through `meta-virtualization`
- Reliable update mechanism with flexible policies though `swupdate`
- Following demo was built fully with OE/Yocto

Yocto: https://www.yoctoproject.org

System architecture

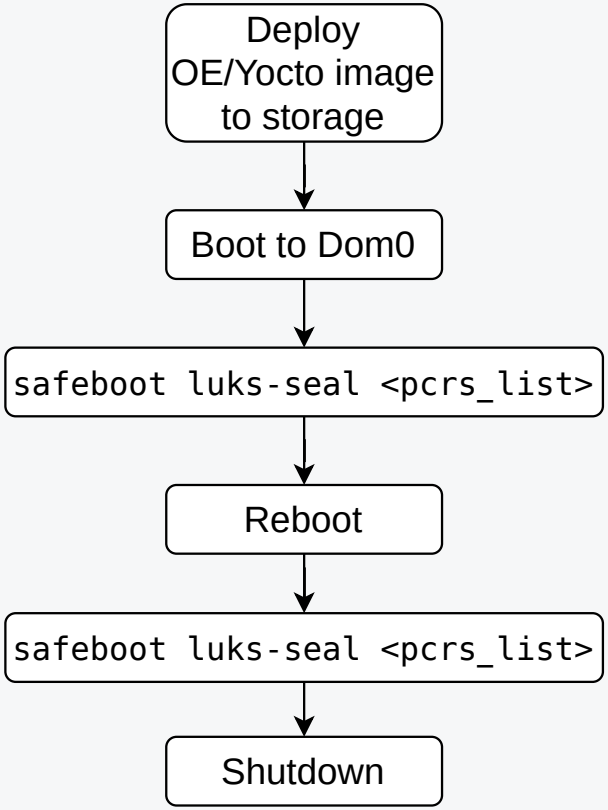


- **PCR[0-7]** - we have no knowledge what is exactly measured, event log readability would be discussed later
- **PCR14** - safeboot boot mode to avoid key access by recovery boot path and repeated key access attack
- **PCR17** - TrenchBoot Landing Zone, Xen kernel, Dom0 kernel and initramfs
- **PCR18** - multiboot2 MBI (MultiBoot Info) structure containing all kernel's command line parameters as well as kernel location passed to LZ

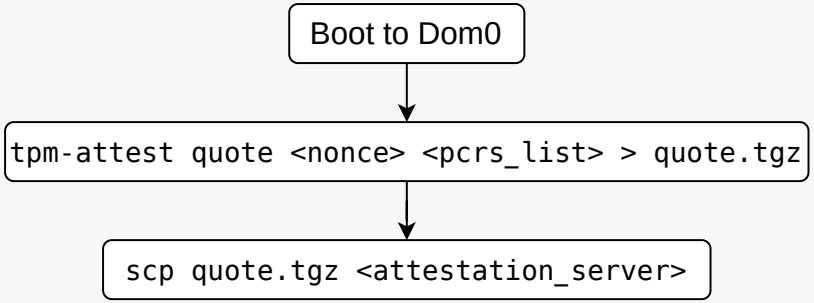
System architecture

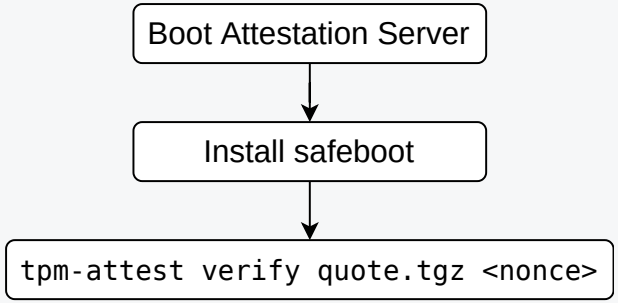
- Very similar architecture was presented by 3mdeb Firmware Engineer Michał Żygowski on Virtual Xen Development Summit 2020
- What was improved?
  - This is first time we show UEFI based platform - previously OSF based on coreboot
  - Everything is built with OE/Yocto - previously Ubuntu 18.04 LTS
  - Storage is sealed to both SRTM and DRTM PCRs - previously just DRTM

System provisioning

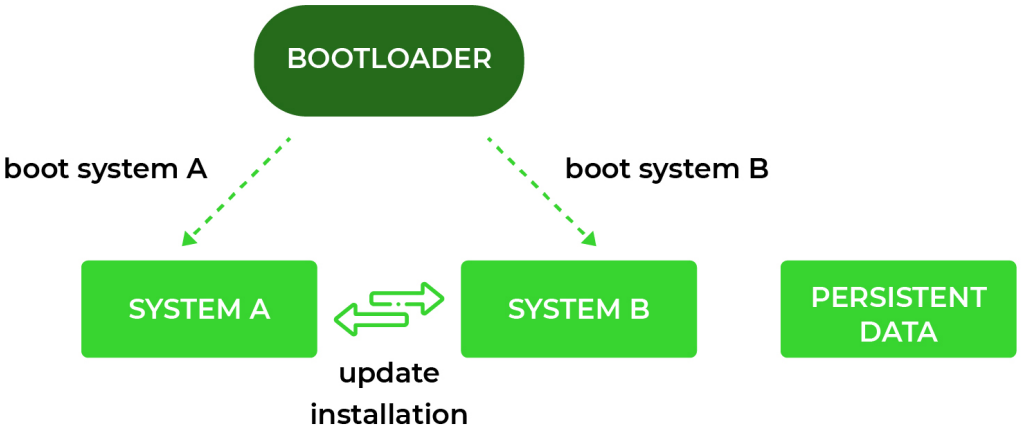


System attestation

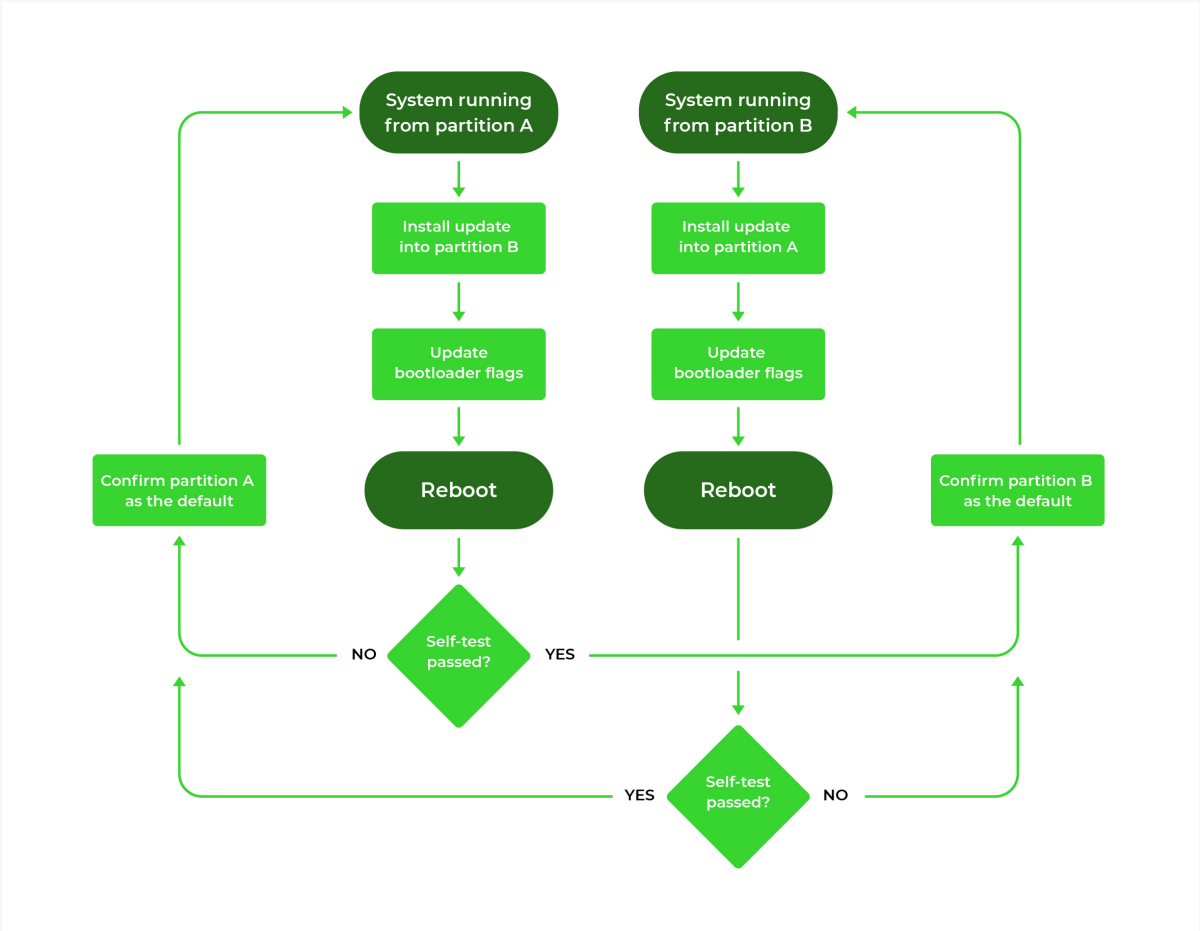




System updates



System updates



Challenges

- Firmware stack capabilities are not clearly presented and there are no guides how to leverage its features
  - AMI Aptio Setup Utility has no associated guides for given options, this is probably responsibility of OEM or whoever did the modifications of AMI Aptio to match platform needs
  - User manuals provided by OEMs are simplified and not cleat especially in security area
- fTPM implementation supports only CRB (*Command Response Buffer*) interface not compliant to PC Profile
  - there are no information what interface we dealing with, but it seem to match TPM2.0 Mobile Common Profile, which supports only locality 0, but DRTM needs locality 4
  - this force us to use dTPM over LPC connector

Challenges

- Readability of TPM event log is questionable

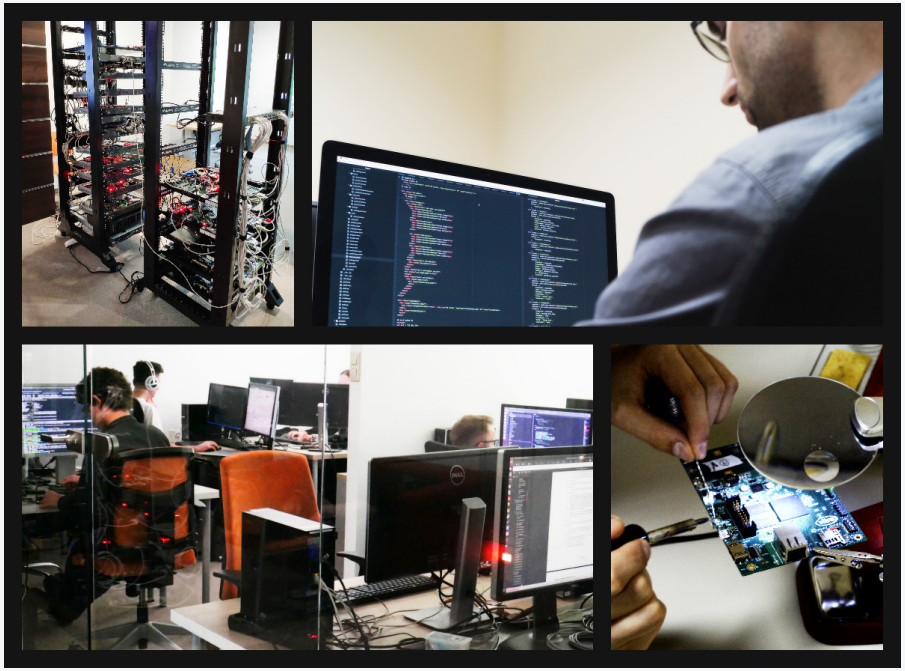
```
- EventNum: 93
    PCRIndex: 8
    EventType: EV_IPL
    DigestCount: 2
    Digests:
      - AlgorithmId: sha1
        Digest: 6aa335e23eaeb621685265253abc82e4ddedbc69
      - AlgorithmId: sha256
        Digest: 9db6a39db69e6087eebaf2e519d9d1cb2939cd7657912ea32fdcd50f72de0301
    EventSize: 156
    Event: 677275625f636d643a20736561726368202d2d6e6f2d666c6f707079202d2d66732d75756964202d2d736
5743d726f6f74202d2d68696e742d62696f733d6864302c67707432202d2d68696e742d6566693d6864302c677074322
02d2d68696e742d626172656d6574616c3d61686369302c677074322062633636383363332d663261332d343035652d6
23963382d623432303435656161626353300
```

- Clear information if hardware security features are enabled and provisioned
  - to realize if HVB (*Hardware Validated Boot*) is enabled it is required to know PSP Directory structure and extract it from update binary or SPI image
  - no official info how to use, provision and confirm it works

Future ideas

- Use UEFI boot
  - ExitBootServices before SKINIT call
  - Enable EFI64b in Xen
- Use UEFI Secure Boot to validate LZ and Xen
- Safeboot requires LVM partitioning, but Yocto cannot produce an LVM partitioned image. One has to configure LVM on runtime.
- OSHW TPM 2.0 with interposer that simplify connection with various pinouts

Marketing pitch

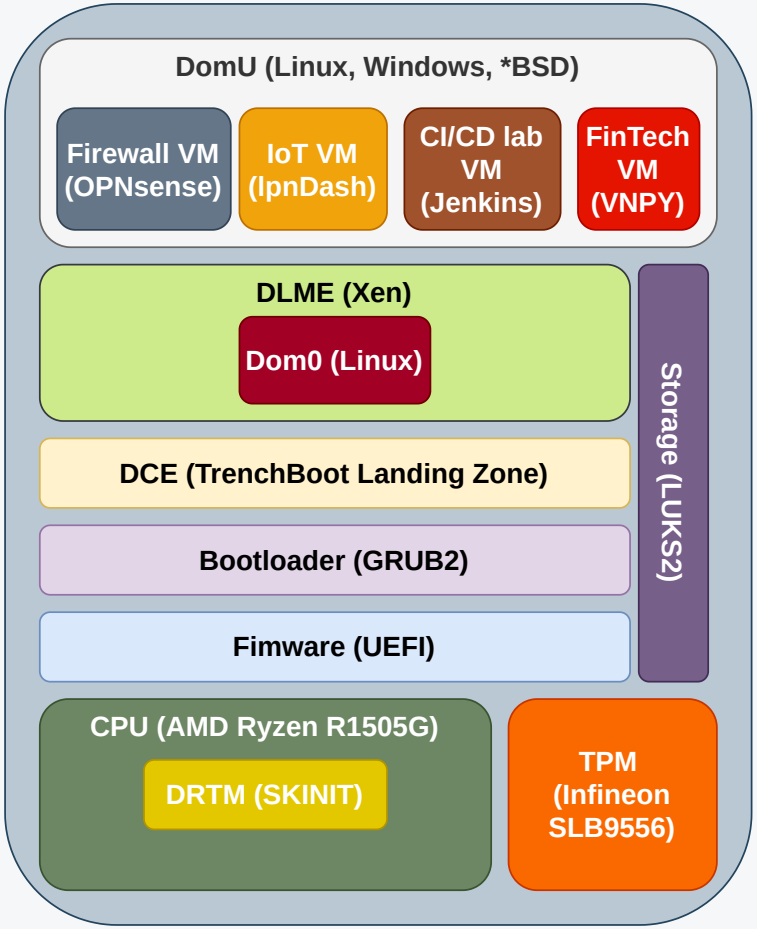


- We provide customized, trustworthy and updatable images for IoT, Edge Computing, Digital Signage, Kiosk and FinTech customers.
- Feel free to contact us through email `contact@3mdeb.com` or our website https://3mdeb.com

3MDEB

Q&A

Backup



Backup