TrenchBoot DRTM features for AMD platforms

Open Source Firmware 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

Kudos

- NLNet
- Daniel P. Smith (Apertus Solutions)
- Andrew Cooper (Citrix)
- Amazing 3mdeb Embedded Firmware Team, especially:
  - Michał Żygowski
  - Krystian Hebel
  - Norbert Kamiński

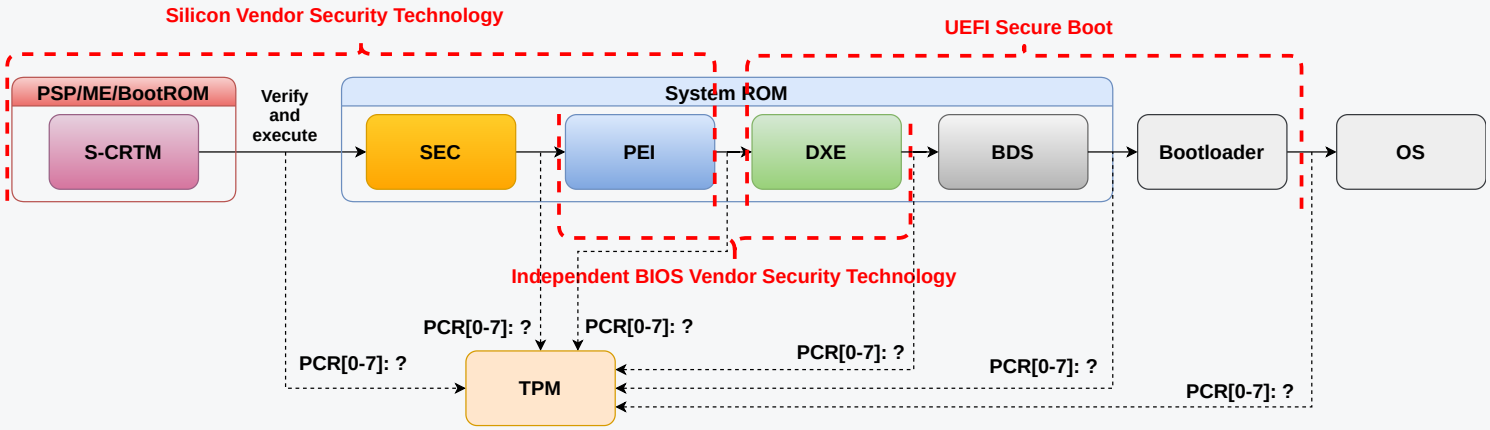
Goal

Explain how TrenchBoot features can be leveraged on AMD-based platforms

- S-CRTM is challenging
- What is TrenchBoot and how it work
- What is Dasharo and how we use it to deploy TrenchBoot
- What operation improvements, security features and use cases modern OSF can provide for you

- **S-CRTM (*Static-Code Root of Trust for Measurement*)**
  - initial measurement established by static code component (e.g. SoC BootROM, read-only bootblock)
  - this code is typically not updatable
- Commercial use cases (Silicon Vendor Security Technologies):
  - Intel Boot Guard, AMD HVB, NXP HAB
  - Intel/IBV/UEFI Secure Boot
  - Microsoft BitLocker
- Open source use cases: coreboot+TrustedGRUB2, Dasharo+LUKS2
- Problems
  - requires reboot to reestablish trust
  - requires NDA with SV and skilled personnel to perform task
  - most hardware vendors do not implement it correctly
  - not standardized measurement information (event log)
  - over 20 keys involved (~5 just for Intel Boot Guard)
- Without correct S-CRTM further measurements have no value

S-CRTM

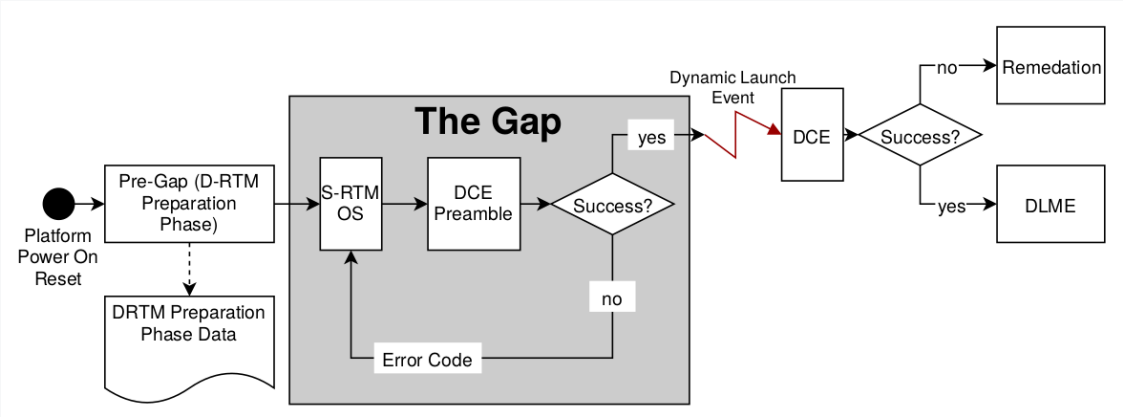


- Diagram shows were S-CRTM starts and how it looks in the context of UEFI-based firmware boot process
- **PCR[0-7]** - we have no knowledge what is exactly measured and where
  - despite TCG specs describe PCRs usage IBVs do not comply with standard
  - event log readability is questionable

Intel Boot Guard

Vendor Name	ME Access	EC Access	CPU Debugging (DCI)	Boot Guard	Forced Boot Guard ACM	Boot Guard FPF	BIOS Guard
ASUS VivoMini	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
MSI Cubi2	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
Gigabyte Brix	Read/Write Enabled	Read/Write Enabled	Enabled	Measured Verified	Enabled (FPF not set)	Not Set	Disabled
Dell	Disabled	Disabled	Enabled	Measured Verified	Enabled	Enabled	Enabled
Lenovo ThinkCentre	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
HP Elitedesk	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
Intel NUC	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
Apple	Read Enabled	Disabled	Disabled	Not Supported	Not Supported	Not Supported	Not Supported

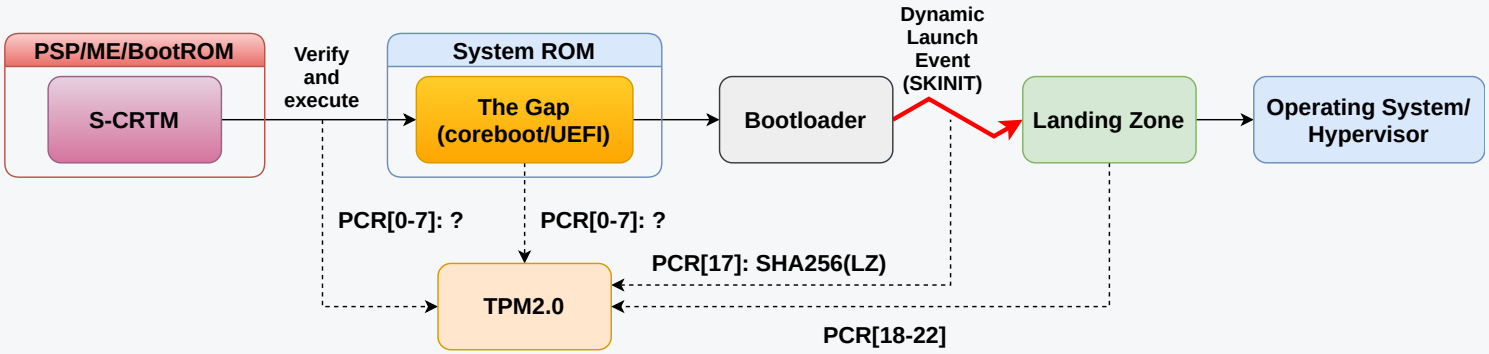
Alex Matrosov 2017: BETRAYING THE BIOS: WHERE THE GUARDIANS OF THE BIOS ARE FAILING



- Leverage open source **D-RTM (*Dynamic Root of Trust for Measurement*)** implementation
- Let's forget about S-CRTM complexity and NDAs with SV
- Solves measured/verified boot continuation problem for legacy systems
  - it was solved before by no longer maintained TrustedGRUB2
  - INT 1Ah BIOS interface support in bootloader is required
  - with TrenchBoot no INT 1Ah interface nor TrustedGRUB2 is needed

Non-UEFI-aware measured boot using coreboot, GRUB and TPM2.0:https://3mdeb.com/events/#Linux-Plumbers-Conference-2019

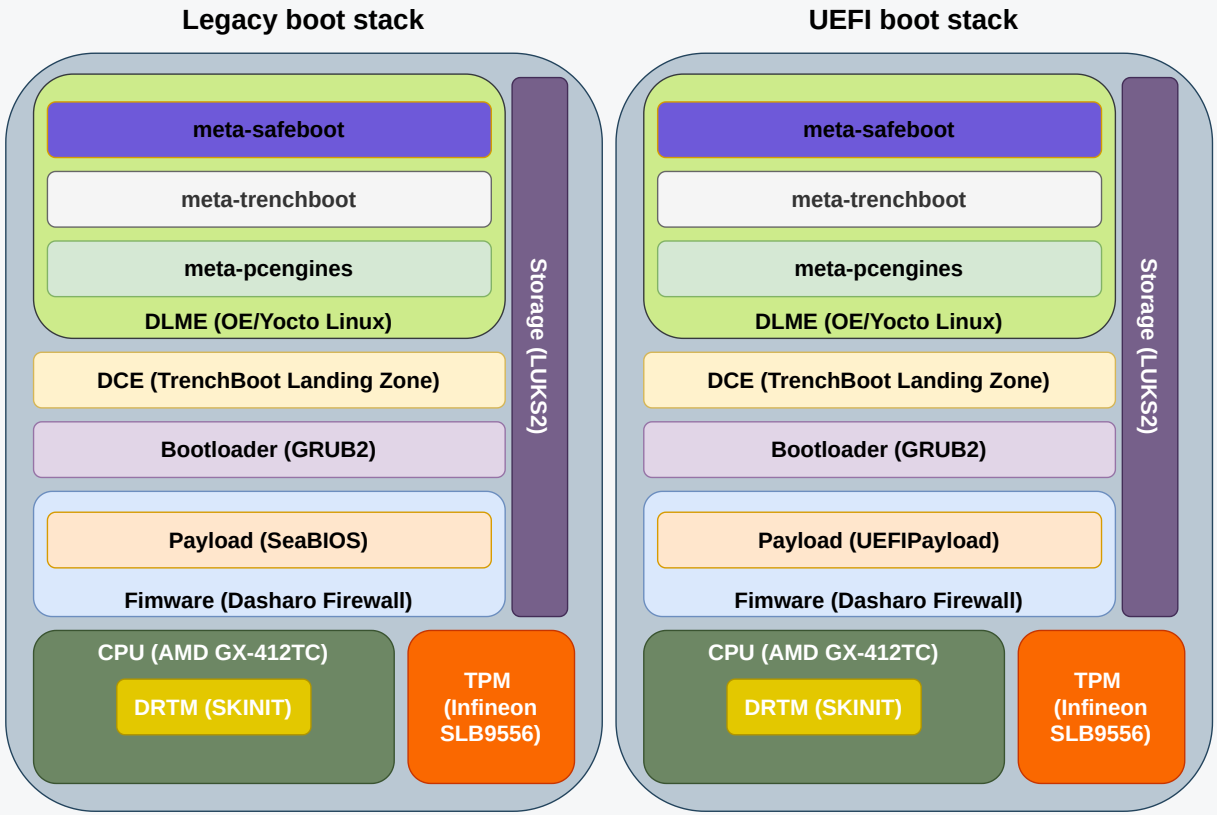
TrenchBoot components



- Bootloaders
  - GRUB2
  - iPXE
- Operating systems
  - NixOS
  - OE/Yocto (`meta-trenchboot`)
- Hypervisors
  - Xen

https://blog.3mdeb.com/tags/trenchboot/

System architecture diagrams



- Alternative DLME would be Xen built using OE/Yocto with OPNSense in VM

DASHARO

Dasharo is a set of productized services, Open Core, and SaaS products which help to provide scalable, modular, easy to combine Open Source BIOS, UEFI, and Firmware solutions.

TrenchBoot is integrated and maintained but Dasharo components in various BIOS and firmware solutions

DASHARO
FIREWALL

- Firewall-targeted ecosystem for coreboot-based solutions which support TrenchBoot for AMD and Intel platforms
- Reference Platform: PC Engines apu2
- Hardware Compatibility List: Protectli FW2/4/6, PC Engines apu2/3/4/6
- Binaries available here: https://boot.3mdeb.com/OSFC2020/

Legacy boot stack

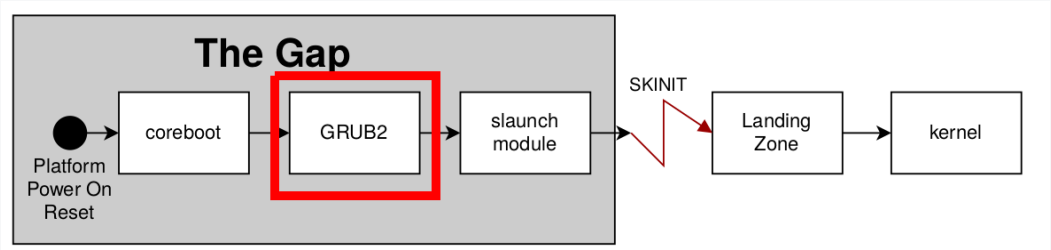
- Verified and Measured Boot
- Fast boot
- Network boot (iPXE)
- TPM Menu

UEFI boot stack

- UEFI Secure Boot
- Setup menu
- Boot order manager
- Network boot (iPXE)
- TPM and OPAL Menu

AMD Landing Zone (LZ) status

- Open Source implementation of of AMD Secure Loader Block (SLB)
- LZ supports coreboot and UEFI-based firmware
- LZ supports TPM1.2 (SHA1) and TPM2.0 (SHA256)
- LZ CI/CD and validation infrastructure was added
- TPM Event Log support
- Multiboot2 support
- IOMMU support - more about that at the end of presentation



- Reference bootloader for TrenchBoot implementation
- Short history of AMD patches
  - Dec 2019: the first version of working AMD patches
  - May 2020: the first version of working Intel TXT patches
  - Nov 2020: second version of AMD patches
- GRUB2 with patches supporting AMD were tested on PC Engines apu2:
  - coreboot+GRUB2 Payload and coreboot+UEFI Payload
  - SPI and SSD storage

```
39      changed, 4168 insertions(+), 184 deletions(-)
```

https://lists.gnu.org/archive/html/grub-devel/2020-11/msg00050.html

- As part of TrenchBoot project iPXE support was developed
- Main purpose was to simplify TrenchBoot testing and development cycle
- It can be easily checked if your AMD platform supports D-RTM, just go to iPXE shell

```
module https://boot.3mdeb.com/tb/lz_header.bin
kernel https://boot.3mdeb.com/tb/bzImage console=ttyS0,115200
initrd https://boot.3mdeb.com/tb/test_initramfs.cpio
boot
```

- HTTP(S) support depending on features built-in iPXE

https://blog.3mdeb.com/2020/2020-06-01-ipxe_lz_support/

Operating Systems

- OE/Yocto produce ready to use, minimal system image with updates and tools to provision security features
- meta-trenchboot
  - TrenchBoot Landing Zone
  - Linux v5.5 with TrenchBoot patches
  - tpm2-tools
- meta-safeboot - with D-RTM patches for UEFI Secure Boot provisioning
- meta-swupdate - layer for image-based system update using SWUpdate
- NixOS - Linux distro with focus on being reproducible, declarative and reliable

https://github.com/3mdeb/meta-trenchboot

System Features

- **Deployment** - use HTTPS network boot to safely deploy firmware and operating system of your choice
- **Provisioning** - use safeboot to leverage UEFI Secure Boot and TPM sealing for disk encryption key
- **Boot** - use various boot stacks and its security features depending on your needs
- **Firmware update** - leverage LVFS/fwupd public/on-premise infrastructure or use manual method
- **System update** - leverage OE/Yocto SWUpdate for reliable OS/hypervisor update
- **Recovery** - recover from system and firmware failure through minimal Linux booted from SPI flash
- **Attestation** - attest locally or remotely selected set of PCRs
- **Maintenance** - apply best practices to firmware maintenance

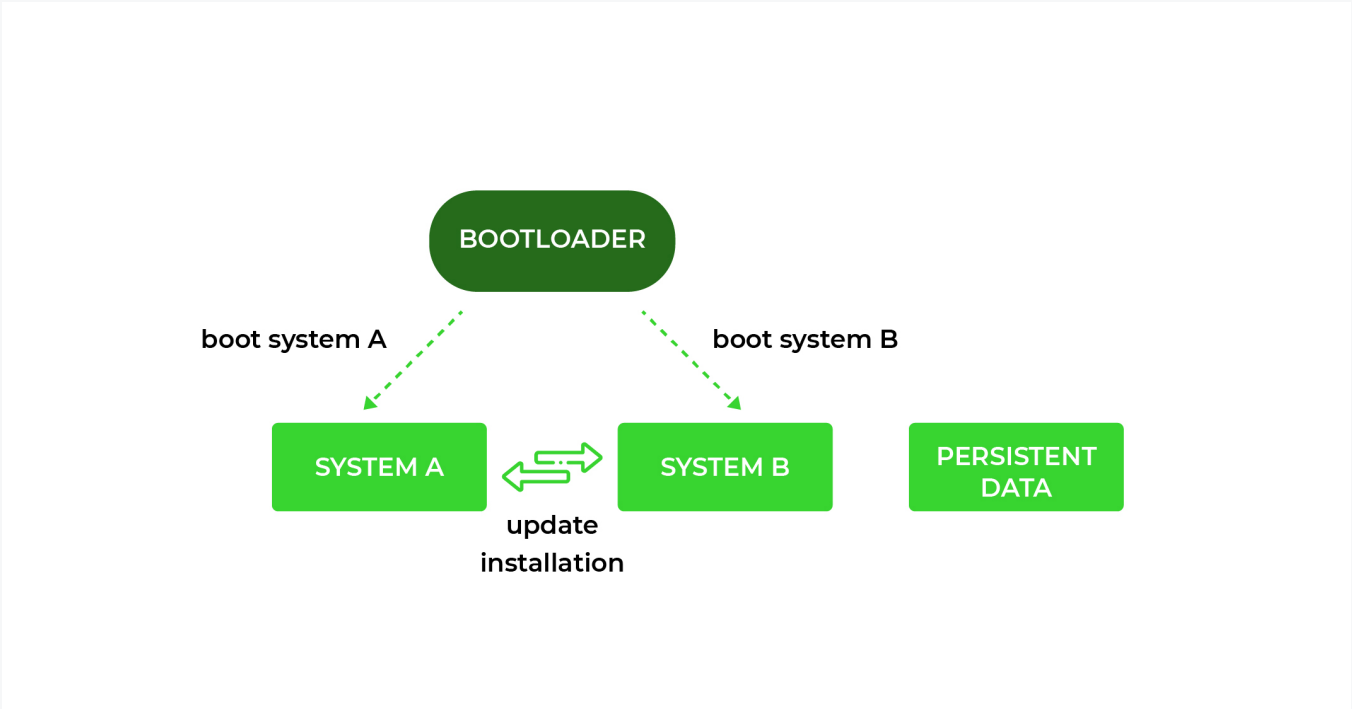
Dasharo Deployment and Provisioning

- Basic use case
  - HTTPS over iPXE using https://boot.3mdeb.com
  - `flashrom` for firmware
  - `bmaptool` for OE/Yocto image
- Dasharo Firewall deployment demo
  - https://asciinema.org/a/374149?cols=100&rows=30&size=big
- safeboot provisioning demo
  - https://asciinema.org/a/374153?cols=100&rows=30&size=big
- Future plans with leveraging TrenchBoot
  - trusted deployment and provisioning
  - trusted diagnostics tools

Dasharo Boot

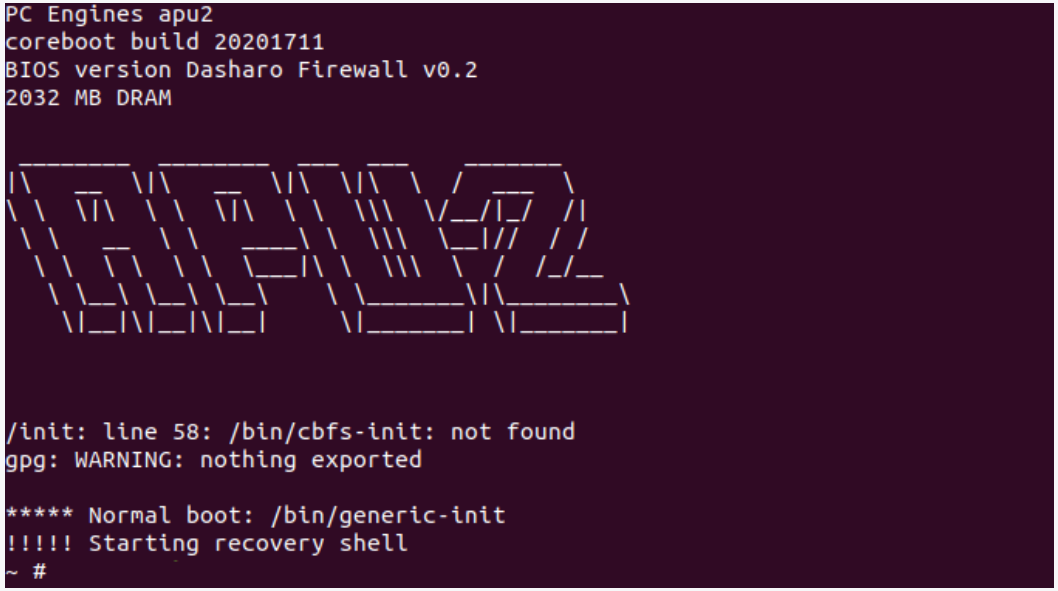
- Legacy and UEFI boot path
- Verified boot with S-CRTM in read-only boot block
- UEFI Secure Boot support
- Demo: https://asciinema.org/a/374153?cols=100&rows=30&size=big

Dasharo OS/hypervisor update



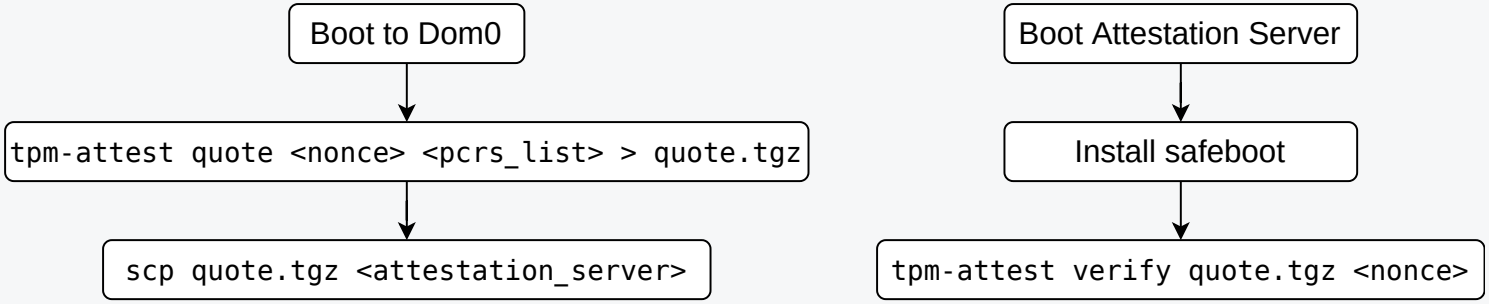
- encrypted and signed updates
- dual image update using SWUpdate
- power-fail safe

Recovery



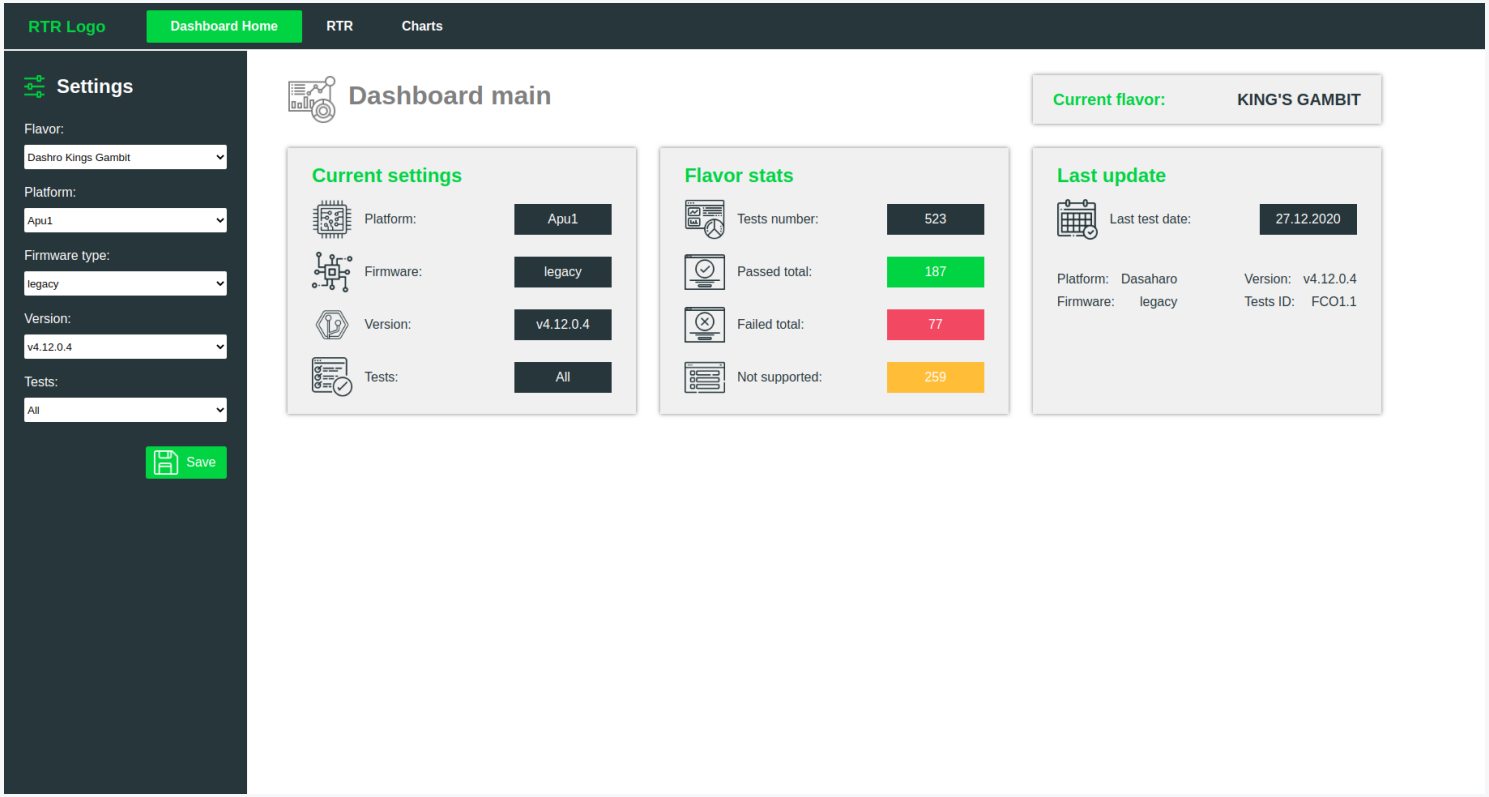
- SPI built-in minimal Heads-based Linux kernel with basic tools for flashing and signatures verification
- UEFI: https://asciinema.org/a/374014?cols=100&rows=30&size=big
- Legacy: https://asciinema.org/a/374012?cols=100&rows=30&size=big

Attestation



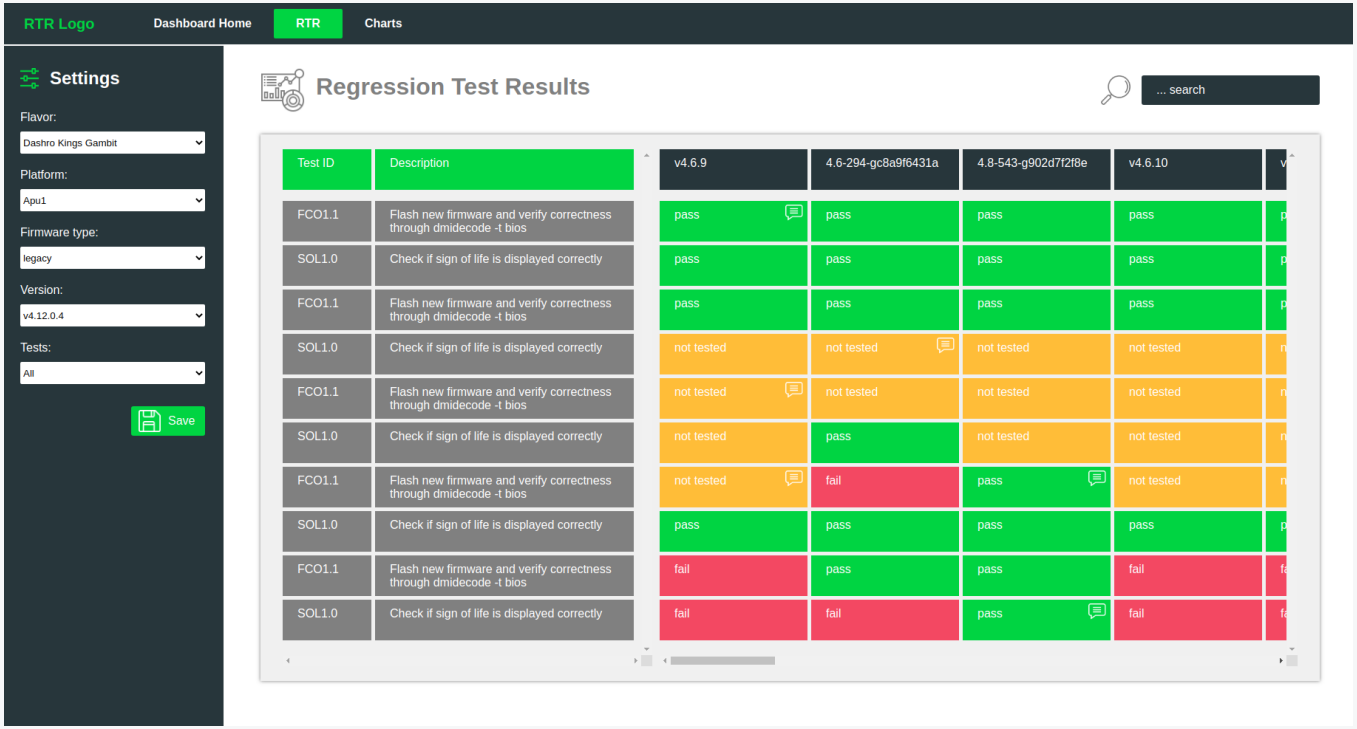
- Attestation of S-RTM and D-RTM PCRs
- Dasharo Attestation Server (WIP)
- TPM Event Log support for Legacy and UEFI (WIP)
- Demo: https://asciinema.org/a/374172?cols=100&rows=30&size=big

Dasharo Maintanance



- BIOS and Firmware Releases/Validation/Maintenance as a Service

Dashro Maintanance



- Over 150 unique test cases validating various Dasharo generic and customer specific features

Challanges

- **DMA protection** - because of AMD SoC issues there is no guarantee that IOMMU would be safely initialized, unless we know it was not used before SKINIT
  - modern CPU families may challenge 64k LZ size limit in light of IOMMU support requirements
  - IOMMU will complicate Late Launch scenario for TrenchBoot
- **SMM Supervisor** - there is need for protection against attacks from SMI, AMD recently developed that solution for Microsoft Secured-core PC
- **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 Mobile CRB specification
  - this force us to use dTPM
- **ARM, OpenPOWER and RISC-V support**

Contact us

DASHARO

Dasharo is under heavy development
If you are interested about Dasharo and TrenchBoot related products
Feel free to contact us through email `contact@3mdeb.com` or our websites
https://3mdeb.com/contact
https://dasharo.com

3MDEB

Q&A