

3mdeb Contribution Review

TrenchBoot Developer Forum 2021

Piotr Król and Michał Żygowski





Piotr Król
3mdeb Founder

- OSS contributor
- Conference speaker and organizer
- Former Intel BIOS SW Engineer
- 12yrs in business
- 6yrs in Open Source Firmware
- C-level positions in





















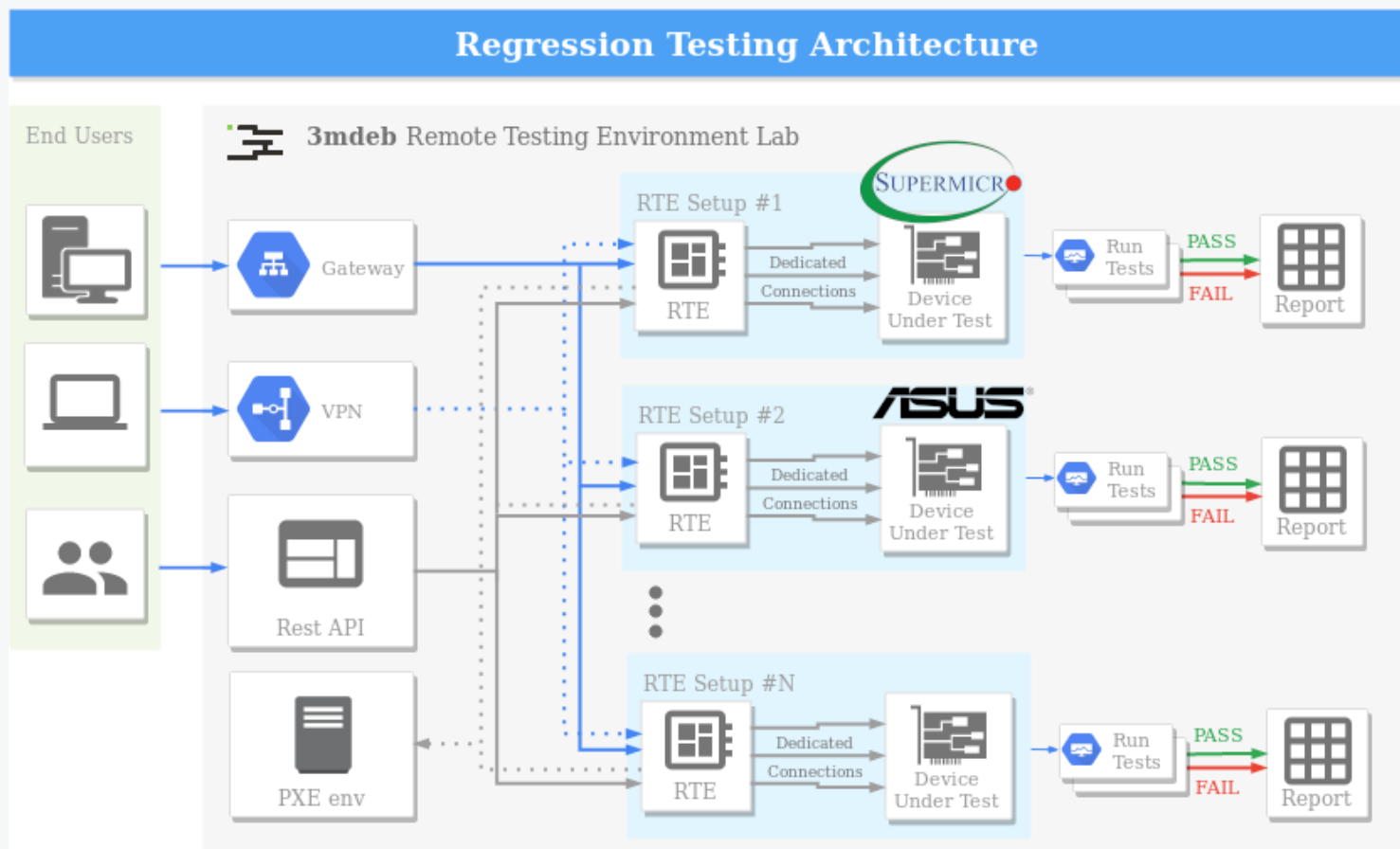


- coreboot licensed service providers since 2016
- coreboot project leadership participants
- UEFI Adopters since 2018
- Official consultants for Linux Foundation fwupd/LVFS project
- Yocto Participants and Embedded Linux experts
- Open Source Firmware enthusiasts and evangelists

Following contribution would be impossible without

- TrenchBoot community members
 - Daniel S.
 - Rich
 - Andrew
 - Daniel K.
 - Ross
 - Christopher
- 3mdeb Team
 - Krystian
 - Michał
 - Norbert
 - Maciej
 - Test Automation Team
- NLNet Foundation

TrenchBoot-related contribution from 3mdeb			
User Space	<div> CHARRA</div>	<div> safeboot</div>	<div> Robot Framework</div>
Operating System	<div> NixOS</div>	<div> yocto PROJECT</div>	<div> debian</div>
Kernel and Hypervisor	<div> Linux</div>	<div> Xen</div>	<div> TrenchBoot Landing Zone</div>
Payloads and Bootloaders	<div> iPXE</div>	<div> GRUB2</div>	
Firmware	<div> coreboot</div>	<div> UEFI</div>	
Hardware	<div> apu2</div>	<div> KGPE-D16</div>	<div> M11SDV-8CT-LN4F</div>
	<div> 4X4 BOX-R1000V</div>		
<div></div>			



coreboot

- [ACPI D-RTM Resource Table](#) - TCG-compliant ACPI table for D-RTM resources
- [D-RTM Event Log](#) - event log entries and tools to parse gathered data
- [AMD IOMMU support](#) - support for AMD IOMMU ACPI table (PC Engines apu2, ASUS KGPE-D16)
- [WIP: Intel Ivy Bridge BIOS ACM support](#) - support for Intel TXT on Dell OptiPlex 7010/9010 platforms

UEFI

- For ASRock and Supermicro stock UEFI firmware was used

iPXE

- [Support for starting TrenchBoot Landing Zone](#)
It boots Linux kernel with TrenchBoot patches as well as Xen through Multiboot2 support

GRUB2

- [D-RTM Event Log](#)
Allows exposing event log to OS for remote attestation simplification and debugging purposes
- AMD SKINIT core implementation [\[1\]](#) [\[2\]](#) [\[3\]](#)
Core functionality that allows SKINIT instruction execution

Linux

- [Support for AMD Secure Launch in 5.8 kernel](#)
Co-developed with Ross

Xen hypervisor

- [Xen early driver](#)
Minimal code to boot Xen through SKINIT and LZ
Merged in upstream

Merged in upstream:

- [SHA256 support](#) - port of SHA256 implementation from Linux kernel
- [Variable data separation](#) - keep hash values independent of memory layout
- [Basic support for forward sealing](#) - script that calculate expected PCRs values

Awaiting review:

- [Multiboot2 support](#) - allows boot Multiboot2 compliant binary using AMD Secure Startup
- [D-RTM Event Log](#) - as discussed before, this features had to be implemented across the stack
- [Early IOMMU support](#) - very basic support for DMA attacks protection cannot be merged for now due to a bug in DEV

TODO

- Resolving existing issues - 5 open, but not everything is publicly reported
- IOMMU DMA protection (cannot be implemented in a secure way due to hardware bug in DEV which blocks IOMMU from reading configuration created inside SLB) - awaits mitigation
- Configurable builds
- Refactoring LZ binary layout
- CI/CD infrastructure improvements
- PE header for UEFI Secure Boot purposes

NixOS

- [Support for Trenchboot in the Nixpkgs](#)
- [Preconfigured Nix repo](#)
- [Trenchboot CI for Nix](#)

Yocto

- [meta-trenchboot layer](#)
- [WIC plugin for legacy TrenchBoot boot partition](#)
- [WIC plugin for UEFI TrenchBoot boot partition](#)
- [meta-trenchboot CI](#)

Debian

- [Debian package for Landing Zone](#)
- [Debian package GRUB](#)
- [Debian package for Linux Kernel](#)

- [safeboot support](#)

Automatic disc decryption based on secret sealed to values of PCR17 and PCR18

Attestation and verification of TPM quote with D-RTM PCRs

- [Remote attestation using Fraunhofer CHARRA](#)

Verification of TPM Quote signature generated by CHARRA attester

- ~2400 Engineering Hours over almost 2 years
- 11 projects received TrenchBoot-related contribution
- 10 conferences presentations promoting TrenchBoot
 - <https://3mdeb.com/events/>
- 16 blog posts
 - <https://blog.3mdeb.com/tags/trenchboot/>

If you looking for experts in area of firmware, Yocto, NixOS, Debian, CHARRA and other mentioned software components feel free to contact us: <https://3mdeb.com/contact/>

contact@3mdeb.com



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. It offers the components that are needed to develop and maintain a high quality, and modular firmware, for the stability and security of your platform.

Ultimate goal is to leverage all TrenchBoot related features through Dasharo ecosystem

Most notable candidates

- Dasharo Provisioning, Deployment and Recovery Server
- Dasharo Debugging Server
- Dasharo Attestation Server
- Secure firmware update through fwupd/LVFS in DLME
- Offline attestation
- Application specific solutions using Linux and *BSD
 - D-RTM PCRs based disk encryption/decryption
 - System updates

- #trenchboot channel on OSFW Slack: <https://slack.osfw.dev>
- Mailing List: <https://groups.google.com/g/trenchboot-devel>
- Website: <https://trenchboot.org/>

Q&A