AMD TrenchBoot support in GRUB2

GRUB mini-summit 2020

Piotr Król

3MDEB

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

Kudos

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

Goal

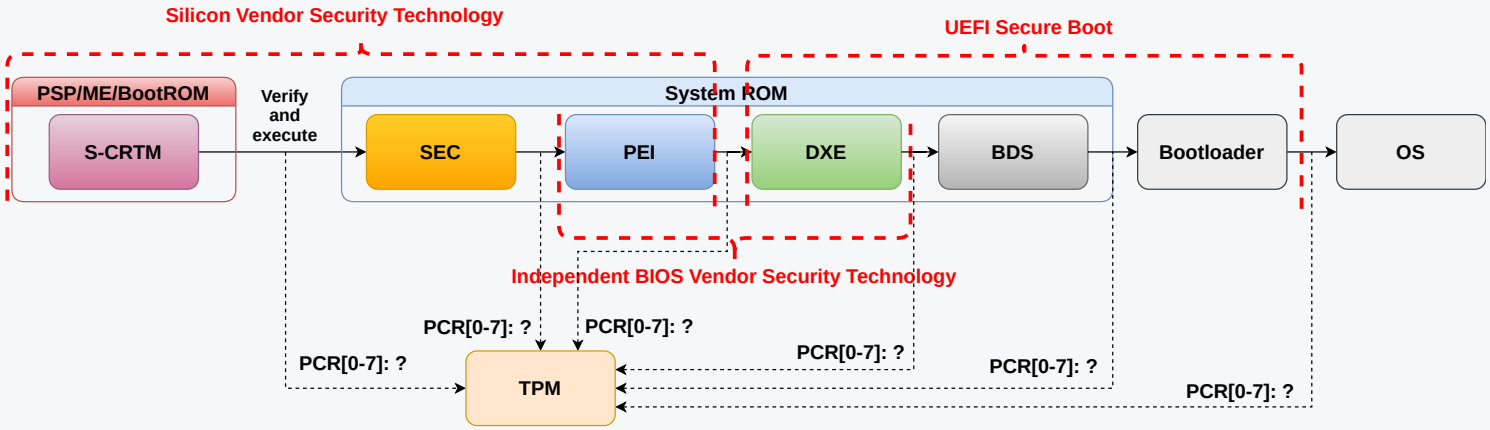
Practical demonstration of TrenchBoot integration leveraging GRUB2 on AMD-based platforms

- Difference between S-CRTM and D-RTM
- GRUB2 role in TrenchBoot
- Feature-rich system architecture that leverages GRUB2 and TrenchBoot
- Dasharo Firewall firmware, GRUB2 and OE/Yocto
- System features
- Demo

S-CRTM

- **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

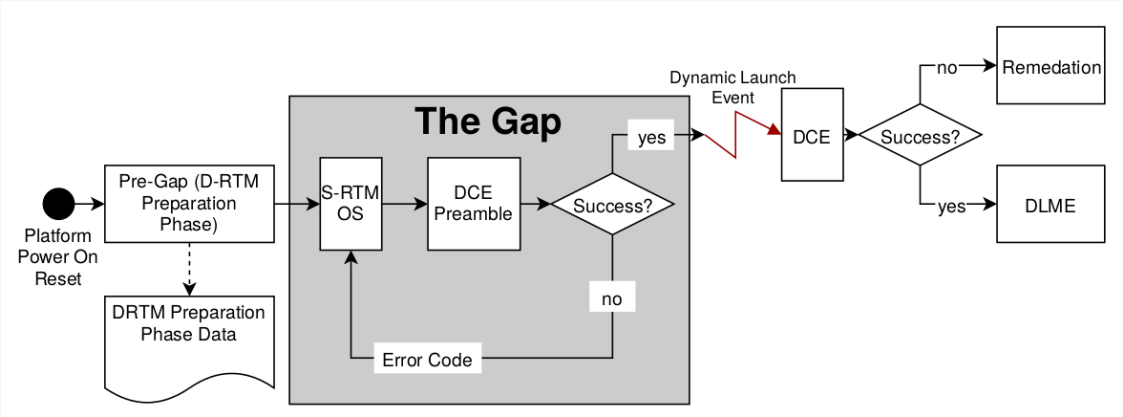


- Diagram shows were S-CRTM starts and how it looks in the context of UEFI-based firmware boot process
- **PCR[0-7]** - we have no knowledge what is exactly measured, event log readability would be discussed later
  - those PCRs are mentioned as an example, since despite TCG spec every vendor seems to interpret the usage of particular PCRs differently
- There is no standardization around TPM event log creation

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

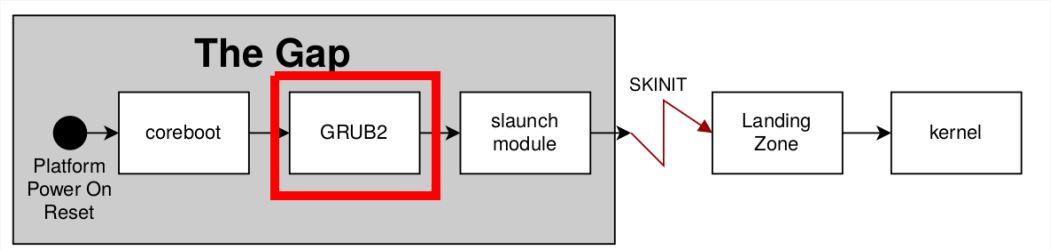
Alex Matrosov 2017: BETRAYING THE BIOS: WHERE THE GUARDIANS OF THE BIOS ARE FAILING



- 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

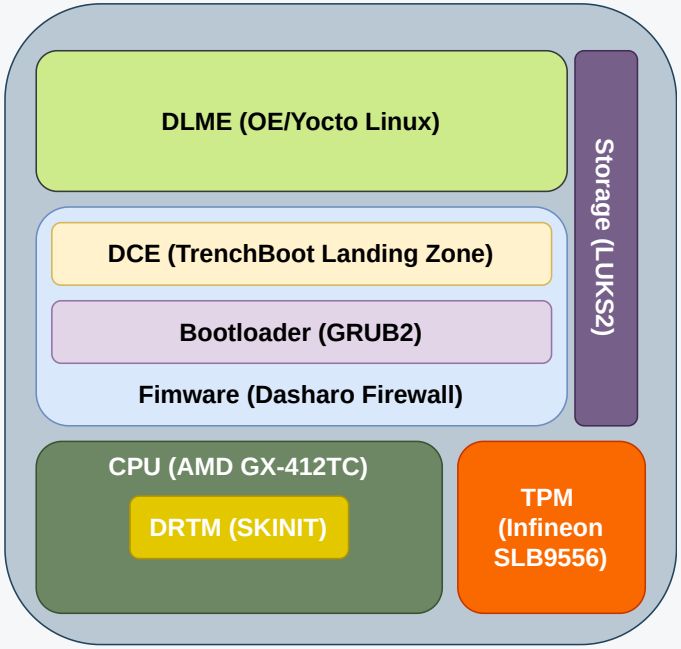
GRUB2 role in TrenchBoot



- 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

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

System architecture diagrams



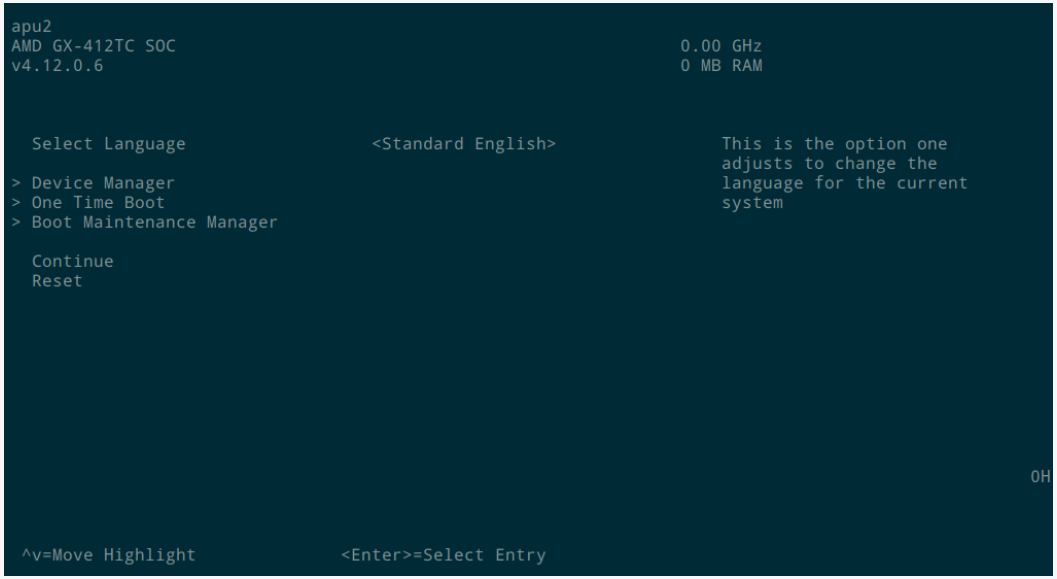
- Legacy boot path
- OE/Yocto builds full disk image
- Dasharo Firewall consist of coreboot+GRUB2+TrenchBoot Landing Zone
    - coreboot builds SPI binary

Dasharo Firewall (Swiss Gambit)

DASHARO
FIREWALL

- Dasharo is a family of BIOS firmware products based on Open Source components
- Dasharo Firewall has 2 flavours
  - Legacy boot path: coreboot+GRUB2+TrenchBoot LZ
  - UEFI boot path: coreboot+TianoCore/UEFI
- Hardware Compatibility List
  - PC Engines apu2/3/4/6
  - Protectli FW2/4/6
  - any other platform that supports coreboot
- coreboot v4.12
  - Verified Boot
  - Recovery partition with minimal Linux in SPI
  - Optional: S-CRTM with read-only bootblock using Adesto SPI features

Dasharo Firewall (Swiss Gambit)



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

- GRUB2 v2.05 with recent TrenchBoot patches for AMD
- Legacy build path
  - integrated in SPI binary
  - built using coreboot build system
- UEFI build path
  - stored on disk
  - built using OE/Yocto
- Config for UEFI looks as follows:

- Produce ready to use, minimal system image with tools to provision security features
- TrenchBoot Landing Zone v0.3.0 (meta-trenchboot)
- Linux v5.5 with TrenchBoot patches (meta-trenchboot)
- tpm2-tools 5.0-rc0 (meta-measured)
- safeboot with D-RTM patches for UEFI Secure Boot provisioning
- update using SWUpdate (meta-swupdate)

System Features

- Deployment
  - HTTPS over iPXE using https://boot.3mdeb.com
  - for firmware
  - for OE/Yocto image
- Provisioning (UEFI)
  - safeboot scripts
- Boot
  - Legacy and UEFI boot path
  - Verified boot with S-CRTM in read-only boot block
  - UEFI Secure Boot support
- Dasharo firmware update
  - regular tools: gpg and flashrom
  - LVFS/fwupd
- OE/Yocto system update
  - encrypted and signed updates
  - dual image update using SWUpdate
  - power-fail safe

System Features

- Self-decrypting rootfs through LUKS2 and TPM2.0 secret unsealing
- Recovery
  - SPI built-in minimal Linux kernel with basic tools for flashing and signatures verification
- Attestation
  - Attestation of S-RTM and D-RTM PCRs
  - TPM Event Log support (Legacy)
- Maintenance
  - public regression test results
  - public CI/CD with validated and signed artifacts

DASHARO FIREWALL

Boot and Event Log Demo

- Legacy TrenchBoot boot flow: https://asciinema.org/a/371576?size=big&speed=0.5
- UEFI TrenchBoot boot flow: https://asciinema.org/a/371870?size=big&speed=0.5
- UEFI TrenchBoot provisioning: https://asciinema.org/a/371872?size=big&speed=0.5

Contact us

We provide customized, trustworthy and updatable images for Firewalls and Office Workstations

We are professional training providers in mentioned technologies

Feel free to contact us through email or our websites

https://3mdeb.com/contact

https://training.3mdeb.com

Q&A