

TPM support in GRUB2 for legacy boot mode





GRUB2 and 3mdeb minisummit 2019

Michał Żygowski





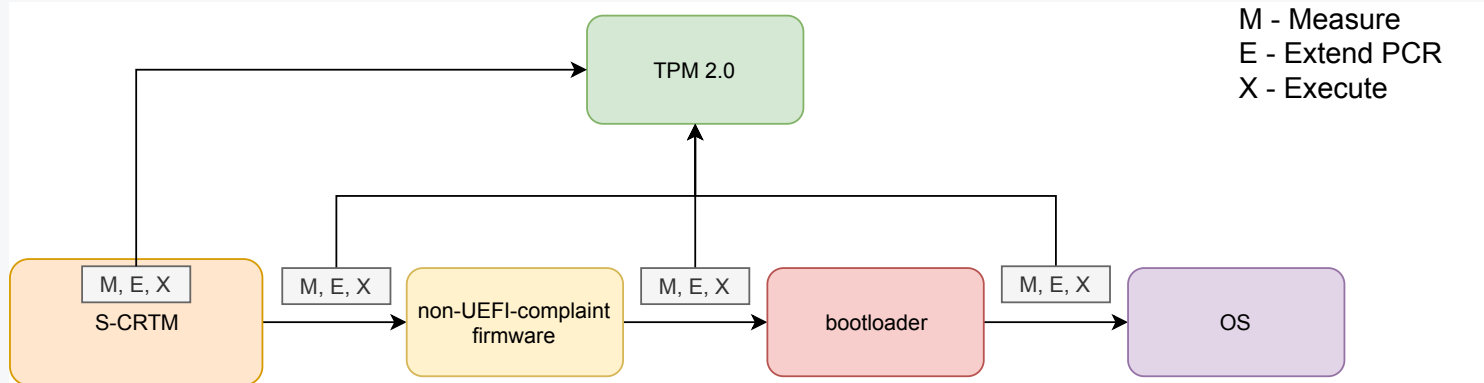
Michał Żygowski
Firmware Engineer

-  @_miczyg_
-  michal.zygowski@3mdeb.com
-  linkedin.com/in/miczyg
-  facebook.com/miczyg1395
- PC Engines platforms maintainer
- interested in:
 - advanced hardware and firmware features
 - coreboot
 - security solutions

- boot process integrity works for UEFI-compliant systems
- there are boot firmware implementations that are natively non-UEFI-compliant
 - coreboot/libreboot/oreboot
 - U-Boot
 - LinuxBoot
 - SeaBIOS
 - Legacy BIOS/UEFI CSM
 - skiboot
- existing solutions
 - petitboot - measured kexec to Linux
 - TrustedGRUB2 - use INT 1Ah, only TPM 1.2 implementation, not widely adopted
- other effort
 - HardenedBSD Call for Participations to unify and collaborate on security issues

<https://twitter.com/HardenedBSD/status/1170040875075985408>

- Chromebooks users who want to repurpose the device
- Users of previously mentioned firmware stacks
- All distros supporting non-UEFI/legacy boot
- Cloud providers using QEMU with SeaBIOS (?)
 - Xen
 - Proxmox



- **S-CRTM** - Static Code/Core Root of Trust for Measurement
- **bootloader** - GRUB/GRUB2, SeaBIOS
- **OS** - Linux, BSD, L4 based OSes, multiboot, ReactOS

- coreboot
 - can M,E,X since it was proven through Vboot implementation
 - finally measures payload and jumps to it
 - question is if payload can take that further?
- GRUB2
 - depends what and how it boots (bootloader in SPI vs HDD/SSD/eMMC)
 - there is no support for measured boot for MBR based boot
- SeaBIOS
 - supports TPM 1.2 and 2.0
 - already measures MBR
 - expose INT 1Ah interface
 - TrustedGRUB2 seem to be the only user

- Use API INT 1Ah from **TCG PC Client Specific Implementation Specification for Conventional BIOS**
- Supports only TPM 1.2
- INT 1Ah (...) allows the caller of the interface to have direct access to a limited set of TSS functions and a pass-through to the TPM.
- TrustedGRUB2 can leverage previously installed interface, the only known BIOS implementation that do it is SeaBIOS
- Topic was extensively discussed here: <https://github.com/Rohde-Schwarz/TrustedGRUB2/issues/23>

- exposes INT 1Ah to the next bootloader as in **TCG PC Client Specific Implementation Specification for Conventional BIOS**
- same API for both TPM 1.2 and 2.0
- currently no option to differentiate between TPM 1.2 and 2.0 when using INT 1Ah
- no SHA256 implementation for TPM2 SHA256 banks, SHA1 is padded with zeros and extended

GRUB2:

- rewrite MBR assembly code to measure the diskboot.img which loads GRUB kernel (size restrictions of MBR)
- rewrite diskboot.img to measure the rest of GRUB
- GRUB kernel needs to measure the modules
- implement TPM driver to measure the grub.cfg , kernel (possibly with commandline) and initrd
- optional commands and parameters measuring in the GRUB shell

SeaBIOS:

- return different values of TCG version in INT 1Ah call for TPM 1.2 and 2.0 detection
- possibly add SHA256 for extending TPM 2.0 SHA256 bank PCRs

.travis.yml	53	++
Changelog.md	54	++
README.md	294	++++++++++
grub-core/Makefile.am	3	+
grub-core/Makefile.core.def	9	+
grub-core/boot/i386/pc/boot.S	364	+++++++-----
grub-core/boot/i386/pc/diskboot.S	97	++++
grub-core/disk/cryptodisk.c	32	+-
grub-core/disk/luks.c	432	+++++++++++-----
grub-core/kern/dl.c	34	+-
grub-core/kern/i386/pc/tpm/tpm_kern.c	433	+++++++++++++++
grub-core/kern/main.c	2	+-
grub-core/kern/sha1.c	446	+++++++++++++++
grub-core/kern/tpm.c	37	++
grub-core/loader/i386/linux.c	68	++-
grub-core/loader/i386/pc/chainloader.c	10	+
grub-core/loader/i386/pc/linux.c	69	++-
grub-core/loader/i386/pc/ntldr.c	9	+
grub-core/loader/linux.c	8	+
grub-core/loader/multiboot.c	13	+
grub-core/normal/main.c	6	+-
grub-core/script/execute.c	51	++
grub-core/tpm/i386/pc/tpm.c	966	+++++++++++++

include/grub/err.h	4 +-
include/grub/file.h	1 +
include/grub/i386/pc/boot.h	4 +
include/grub/i386/pc/tpm.h	89 +++
include/grub/sha1.h	40 ++
include/grub/tpm.h	64 +++
runSonarQubeAnalysis.sh	41 ++
sonar-project.properties	16 +
util/mkimage.c	17 +

TOTAL: 32 files changed, 3407 insertions(+), 359 deletions(-)

Statistical diff made on master branch of TrustedGRUB2 which is supposed to base on 2.02 tag of GRUB2.

- Does adoption of INT 1Ah still make sense in light of expanding kexec based solutions?
- Why GRUB2 still has not adopted any TPM implementation for legacy boot mode?
- Can GRUB2 rely on TPM?

- We doubt that Legacy BIOS/UEFI CSM with INT 1Ah exist
- Both solutions would require implementation in bootloader for cases where bootloader is included in firmware (e.g. coreboot)

Q&A