

# DRTM as a modern Root of Trust in OSF





Linux Secure Launch - TrenchBoot Summit 2021

Michał Żygowski





Michał Żygowski  
*Firmware Engineer*

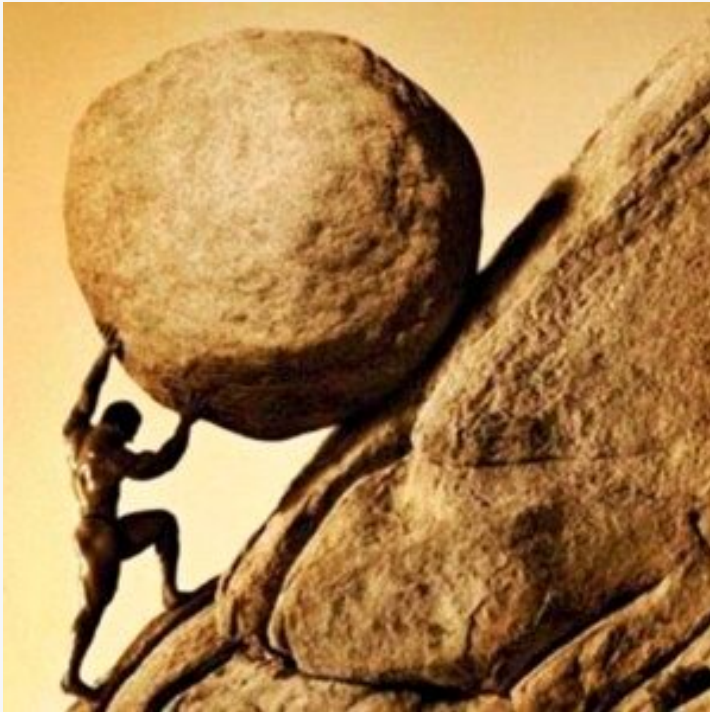
-  [@\\_miczyg\\_](https://twitter.com/_miczyg_)
-  [michal.zygowski@3mdeb.com](mailto:michal.zygowski@3mdeb.com)
-  [linkedin.com/in/miczyg](https://linkedin.com/in/miczyg)
-  [facebook.com/miczyg1395](https://facebook.com/miczyg1395)
- Braswell SoC, PC Engines and Protectli maintainer in coreboot
- OpenPOWER System Software Workgroup chair
- 4 years in Open Source Firmware
- interested in advanced hardware and firmware security features



- coreboot licensed service providers since 2016 and leadership participants
- UEFI Adopters since 2018
- Yocto Participants and Embedded Linux experts since 2019
- Official consultants for Linux Foundation fwupd/LVFS project
- IBM OpenPOWER Foundation members

- SRTM vs DRTM
- DRTM for AMD
- DRTM on Asus KGPE-D16
- Demo TrenchBoot
- DRTM for Intel
- DRTM on Dell OptiPlex 9010
- Demo Trusted Boot
- Demo TrenchBoot
- Intel TXT coreboot configuration
- Summary

## SRTM



## DRTM



Sources:

[https://twitter.com/Szyf\\_/photo](https://twitter.com/Szyf_/photo)

<https://userscontent2.emaze.com/images/229a72d7-5345-48c5-bc2e-7d1210a051b6/981a371ae2051b72d7901a00b94e9575.jpg>

- implemented with an SVM (Secure Virtual Machine) instruction called SKINIT
- SKINIT instruction takes a 64KB Secure Loader Block (SLB) address in the EAX architectural register of the register
- everything is well documented in the AMD Architecture's Programmer Manual (except the bits to disable SLB protection on Zen+ CPUs)

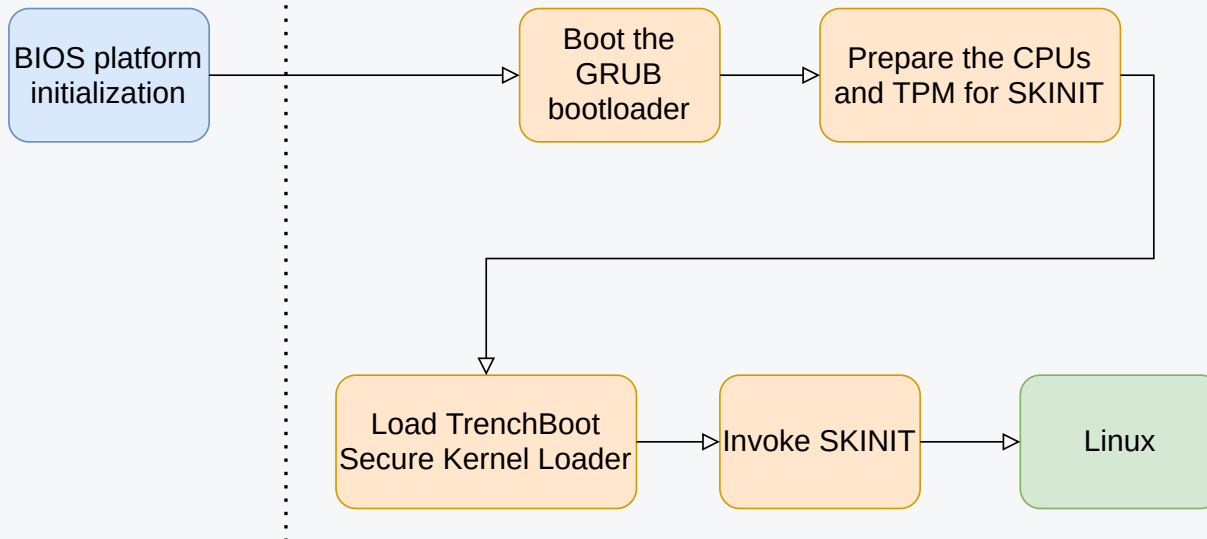
## 15.27 Secure Startup with SKINIT

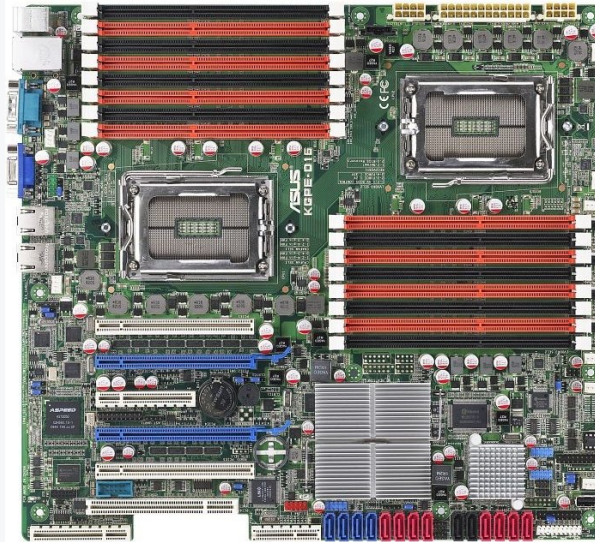
The SKINIT instruction is one of the keys to creating a “root of trust” starting with an initially untrusted operating mode. SKINIT reinitializes the processor to establish a secure execution environment for a software component called the secure loader (SL) and starts execution of the SL in a way that cannot be tampered with. SKINIT also copies the secure loader executable image to an external device, such as a Trusted Platform Module (TPM) for verification using unique bus transactions that preclude SKINIT operation from being emulated by software in a way that the TPM could not readily detect. (Detailed operation is described in Section 15.27.4.)

### 15.27.1 Secure Loader

A secure loader (SL) typically initializes SVM hardware mechanisms and related data structures, and initiates execution of a trusted piece of software such as a VMM (referred to as a Security Kernel, or SK, in this document), after first having validated the identity of that software.

## Measured Launch Environment





- KGPE-16 - Dual AMD G34 socket server/workstation board from Asus release in 2010
- FSF RYE certified hardware with open source firmware implementation in coreboot and libreboot(<https://libreboot.org/>)
- Good and quite cheap hardware to test TrenchBoot SKL on a server platform



- Currently dropped from coreboot master branch, but thanks to [Immunefi](#) the platform is undergoing revival process
- 3mdeb will manage binary releases under [Dasharo](#) trademark providing validated and signed deliverables that can be used out of the box by end users.

```
sha256:
0 : 0xD27CC12614B5F4FF85ED109495E320FB1E5495EB28D507E952D51091E7AE2A72
1 : 0x60B02C95C26DF87DE2FB5FCCF230AF23B586200BAB02E6BFEEA20FE95FCD0656
2 : 0xAC77E45C34605983A4F801E7957B31572BE7EF7639CD4F8DC69F36DC66F4C5B7
3 : 0xD27CC12614B5F4FF85ED109495E320FB1E5495EB28D507E952D51091E7AE2A72
4 : 0xEEA509AA8A7554B7B4040C44A580660923246633B3593D0547D4FD52841971E0
5 : 0xD27CC12614B5F4FF85ED109495E320FB1E5495EB28D507E952D51091E7AE2A72
6 : 0xD27CC12614B5F4FF85ED109495E320FB1E5495EB28D507E952D51091E7AE2A72
7 : 0xD27CC12614B5F4FF85ED109495E320FB1E5495EB28D507E952D51091E7AE2A72
8 : 0x00000000000000000000000000000000000000000000000000000000000000
9 : 0x00000000000000000000000000000000000000000000000000000000000000
10: 0x00000000000000000000000000000000000000000000000000000000000000
11: 0x00000000000000000000000000000000000000000000000000000000000000
12: 0x00000000000000000000000000000000000000000000000000000000000000
13: 0x00000000000000000000000000000000000000000000000000000000000000
14: 0x00000000000000000000000000000000000000000000000000000000000000
15: 0x00000000000000000000000000000000000000000000000000000000000000
16: 0x00000000000000000000000000000000000000000000000000000000000000
17: 0x0FDC626300E69E2A937878DFB688242A2B95CB8ABF4F1BE1CA66A8A3E17C73EB
18: 0xA2EE2E471E1E82F7F6957647ED5D7EAD14C86D9563859AC7D58447EB25FB566B
19: 0x00000000000000000000000000000000000000000000000000000000000000
20: 0x00000000000000000000000000000000000000000000000000000000000000
21: 0x00000000000000000000000000000000000000000000000000000000000000
22: 0x00000000000000000000000000000000000000000000000000000000000000
23: 0x00000000000000000000000000000000000000000000000000000000000000
```

- At the time of platform release, only TPM 1.2 was supported
- but with open source firmware we can make TPM 2.0 possible
- LPC TPM 1.2 and TPM 2.0 are compatible from the SKINIT perspective





- it occurs the platform support code in coreboot 4.11 branch has issues with TPM cycles decoding
- hopefully we can fix that with the Dasharo firmware
- for those interested in AMD DRTM here is the recording of SKINIT on PC Engines apu2: <https://asciinema.org/a/371576?cols=96&rows=24>

- implemented with a set of SMX (Safer Mode Extensions) instructions called GETSEC
- GETSEC uses Authenticated Code Module (ACM), binary blobs signed by Intel to initialize Intel Trusted Execution Technology, in short TXT (Intel DRTM technology)
- [initial coreboot implementation](#) done by 9elements and tested on OCP Wedge100s and Facebook Watson

### 5.23 SAFER MODE EXTENSIONS

The behavior of the GETSEC instruction leaves of the Safer Mode Extensions (SMX) are summarized below:

GETSEC[CAPABILITIES] Returns the available leaf functions of the GETSEC instruction.

GETSEC[ENTERACCS] Loads an authenticated code chipset module and enters authenticated code execution mode.

GETSEC[EXITAC] Exits authenticated code execution mode.

GETSEC[SENDER] Establishes a Measured Launched Environment (MLE) which has its dynamic root of trust anchored to a chipset supporting Intel Trusted Execution Technology.

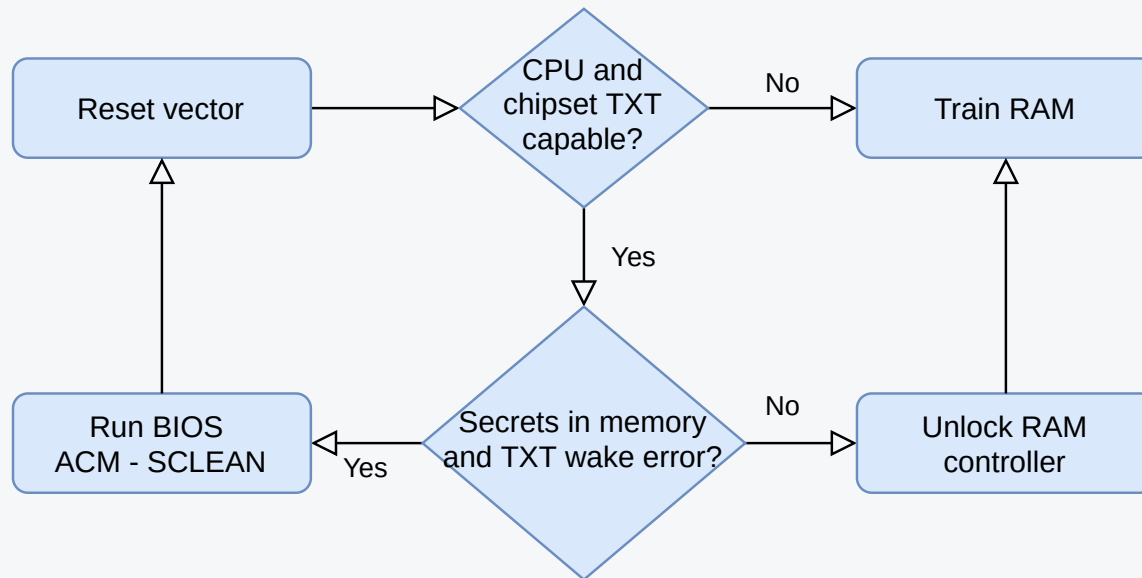
GETSEC[SEXIT] Exits the MLE.

GETSEC[PARAMETERS] Returns SMX related parameter information.

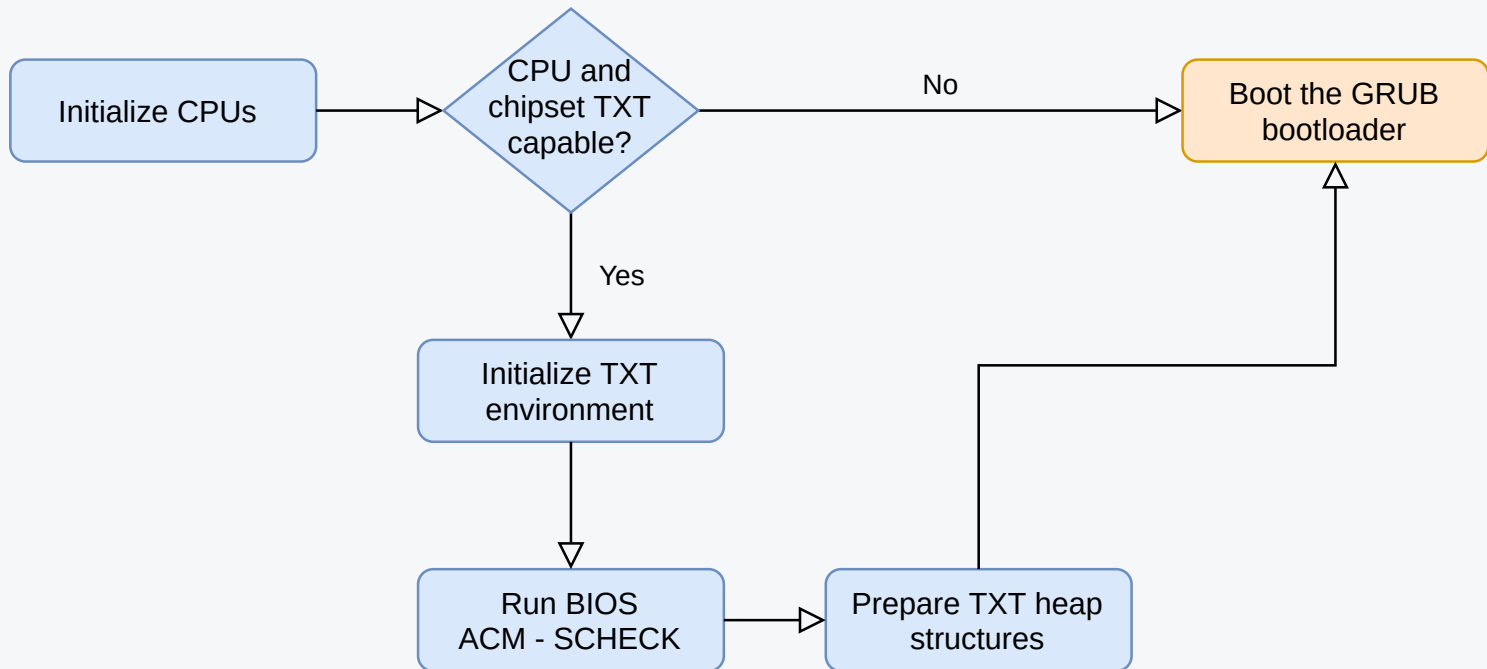
GETSEC[SMCTRL] SMX mode control.

GETSEC[WAKEUP] Wakes up sleeping logical processors inside an MLE.

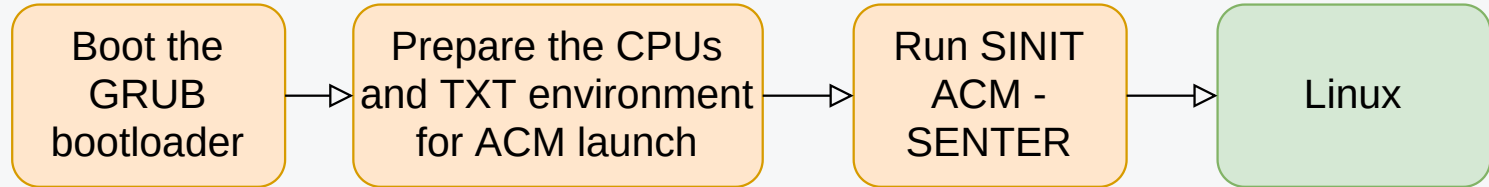
# Pre-RAM firmware phase



# RAM firmware phase



# Measured Launch Environment





- Dell OptiPlex 7010/9010 - a workstation with 3rd generation Intel Core processors and Intel Q77 TXT-capable chipset
- Also needs TXT capable CPU to use Intel TXT, that is only high-end i5 and i7 processors have the TXT capability
- Cheap workstation for home and office use with coreboot open source firmware ported by 3mdeb



- coreboot-based Dasharo firmware for this machine will also be released as validated and signed binary with 3mdeb support for ends users
- 3rd generation processors have fully open silicon initialization in coreboot
- we are bound to TPM1.2 because the ACMs do not support TPM 2.0

```
PCR-00: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-01: B4 B3 AA 80 78 80 DC 8A BC 20 52 FC 13 95 D0 9E 6D C1 1C 0A
PCR-02: B9 9F AF 15 56 33 08 51 EF D9 06 70 95 6D 77 D1 16 C5 0B 92
PCR-03: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-04: A8 19 CD 80 A7 2B 41 BB C4 D1 5D 7A AA 76 21 9E AD 5B AC 2A
PCR-05: 78 0B 90 3A 54 01 58 F1 9E BD 22 59 FE F1 B5 E9 63 A4 56 5E
PCR-06: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-07: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-08: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-09: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-10: 47 A2 45 F0 A2 B5 DC 2F FE 44 6C C5 4E 99 EF C5 B7 50 73 47
PCR-11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-13: F3 F4 F6 8D B9 D6 FF 5F 48 27 6A E3 9A 13 9E 50 80 B9 63 84
PCR-14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-17: 42 77 A9 88 AB 57 6D 37 CC BF 95 F2 B1 90 A3 84 74 9D AB B6
PCR-18: B2 AB 91 13 FC 65 67 75 47 15 C0 2D 04 5F 5C 1C 57 83 5C 9B
PCR-19: BB 9F 7D 22 2F 3A D0 4D 9D 01 75 16 01 DA EE C2 67 64 58 74
PCR-20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-21: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-22: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-23: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
# dmidecode 3.1
Getting SMBIOS data from sysfs.
SMBIOS 3.0 present.

Handle 0x0000, DMI type 0, 26 bytes
BIOS Information
    Vendor: coreboot
    Version: TXT test
    Release Date: 11/15/2021
    ROM Size: 12288 kB
    Characteristics:
        PCI is supported
        PC Card (PCMCIA) is supported
        BIOS is upgradeable
        Selectable boot is supported
        ACPI is supported
        Targeted content distribution is supported
    BIOS Revision: 4.15
    Firmware Revision: 0.0
```

```

TB00T:                Type: 0x501
TB00T:                Digest: c3 43 84 97 fd a8 27 be 3b 32 1c 53 09 a2 04 f0 c9 e5 39 43
TB00T:                Data: 0 bytes
TB00T:                Event:
TB00T:                PCRIndex: 18
TB00T:                Type: 0x501
TB00T:                Digest: e3 8c 63 b6 38 16 15 fc b4 d1 70 44 af b7 19 73 32 c8 9b 6b
TB00T:                Data: 0 bytes
TB00T:                Event:
TB00T:                PCRIndex: 19
TB00T:                Type: 0x501
TB00T:                Digest: 52 ef 7e 88 5f 7d 8c 9c 46 e3 a2 bc f6 44 44 dd da 03 f3 d7
TB00T:                Data: 0 bytes
TB00T:                Event:
TB00T:                PCRIndex: 19
TB00T:                Type: 0x501
TB00T:                Digest: 59 9b 3a 56 bf 71 22 3c b1 57 3e 4d 05 d6 ec 11 ad d7 15 90
TB00T:                Data: 0 bytes
TB00T: creation or verification of S3 measurements failed.
TB00T: tboot_shared data:
TB00T:   version: 6
TB00T:   log_addr: 0x00060000
TB00T:   shutdown_entry: 0x000041b0
TB00T:   shutdown_type: 0
TB00T:   tboot_base: 0x00804000
TB00T:   tboot_size: 0x2c4a40
TB00T:   num_in_wfs: 7
TB00T:   flags: 0x00000000
TB00T:   ap_wake_addr: 0x00000000
TB00T:   ap_wake_trigger: 0
TB00T: no LCP module found
TB00T: kernel is ELF format
TB00T: 0x67a000 bytes copied from 0x186000 to 0x2a82000
TB00T: transferring control to kernel @0x100000...
TB00T: VMXOFF done for cpu 1
TB00T: cpu 1 waking up, SIPI vector=8f000
TB00T: VMXOFF done for cpu 2
TB00T: cpu 2 waking up, SIPI vector=8f000
TB00T: VMXOFF done for cpu 3
TB00T: cpu 3 waking up, SIPI vector=8f000
TB00T: VMXOFF done for cpu 4
TB00T: cpu 4 waking up, SIPI vector=8f000
TB00T: VMXOFF done for cpu 5
TB00T: cpu 5 waking up, SIPI vector=8f000
TB00T: VMXOFF done for cpu 6
TB00T: cpu 6 waking up, SIPI vector=8f000
TB00T: VMXOFF done for cpu 7
TB00T: cpu 7 waking up, SIPI vector=8f000

```



<https://asciinema.org/a/449387?cols=96&rows=24>



- GRUB with TrenchBoot slaunch module does not support TPM 1.2 for Intel TXT yet

```
/home/miczyg/Projects/coreboot/.config - coreboot configuration

Security

Verified Boot (vboot) --->
Trusted Platform Module --->
Memory initialization --->
[*] Intel TXT support (legacy)
    (IVB_BIOSAC_PRODUCTION.BIN) BIOS ACM file
    (3rd_gen_i5_i7_SINIT_67.BIN) SINIT ACM file
[ ] Test BIOS ACM calling code with NOP function (NEW)
[*] Enable verbose logging
[ ] Enable STM
    Boot media protection mechanism (to lock boot media sections) --->
[ ] Boot media only writable in SMM

F1 Help F2 SymInfo F3 Help 2 F4 ShowAll F5 Back F6 Save F7 Load F8 SymSearch F9 Exit
```

<https://asciinema.org/a/449501>

AMD	Intel
no blobs required	BIOS and SINIT ACM blobs required, the former requires NDA, distribution of the latter is under clickthrough EULA
BIOS doesn't need to do any DRTM initialization	complex BIOS initialization of Intel TXT
possible to use any TPM family	TPM family support dependent on the ACMs
SKINIT available on all processors since introduction of the instruction	Intel TXT available only on high-end i5 and i7 CPUs and most Xeon CPUs

## Wishlist:

- reproducible binary builds of all Intel-signed ACMs, with read-only source code available outside Intel)

Tested devices	TPM family	Test result	Notes
Intel Tiger Lake client	TPM 2.0	PASS	UEFI firmware
Intel Kaby Lake server	TPM 2.0	PASS	UEFI firmware
Intel Skylake sever	TPM 2.0	PASS	UEFI firmware
PC Engines APU2 platform series (AMD family 16h models 30h-3fh embedded)	TPM 2.0	PASS	coreboot firmware
PC Engines APU2 platform series (AMD family 16h models 30h-3fh embedded)	TPM 1.2	PASS	coreboot firmware
Asus KGPE-D16 (AMD Opteron family 15h models 00h-0fh server)	TPM 2.0	FAIL	coreboot firmware TPM issue
Supermicro M11SDV-8CT (AMD EPYC 3000 Snowy Owl server)	TPM 2.0	PASS	legacy boot
Supermicro M11SDV-8CT (AMD EPYC 3000 Snowy Owl server)	TPM 2.0	FAIL	UEFI boot
Dell OptiPlex 9010 (Intel Ivybridge workstation)	TPM 1.2	FAIL	TPM 1.2 not yet supported in GRUB slaunch

- DRTM simplifies establishing the Root of Trust for Measurement and is order of magnitude less complex than SRTM (at least on AMD)
- TrenchBoot allows to integrate DRTM secure launch to any Intel machine with TPM 2.0 and proper BIOS support and any AMD machine (with discrete TPM, AMD fTPM is known to not work due to lack of localities)
- TPM 1.2 support for Intel TXT is still underway
- Ideal solution when you do not trust the BIOS
- Can be troublesome in UEFI environments due to the presence of Runtime Services and System Management Mode (although it can be containerized to restrict the SMM privileges)