EFI + Intel TXT and TPM + Xen/Linux

How to make it work

Daniel Kiper
Software Developer, GRUB2 upstream maintainer

July 11th, 2017

tboot + Xen – Current State, Do we care?

- tboot is started by a bootloader, e.g. GRUB2, which is not measured,
- tboot passes control to Xen via the Multiboot protocol,
- Xen has to be started with the Multiboot2 protocol which can pass pointers to EFI_HANDLE and EFI_SYSTEM_TABLE,
- tboot would need to shutdown EFI boot services in order to enter Safer Mode Extensions (SMX) CPU mode (due to hangs?),
- Xen uses the EFI boot services to get information about the platform and pre-configures some hardware,
- tboot uses the shared page to pass some information about the platform, however, it lacks the pointers to EFI stuff including the EFI runtime services,
- Xen has to have access to the EFI runtime services to pass them to dom0; if they are not available, then e.g. the efibootmgr does not work.

tboot.efi – Current State

- tboot.efi will load Xen, kernel, etc. directly using the load/exec UEFI calls,
- There is no plan to support full blown bootloaders (do we care?); this is due some concerns related to switching between Sx power states.

EFI TBOOT – WIP/POC/Research Project

- https://github.com/rossphilipson/efi-tboot
- EFI TBOOT is based directly off of the TBOOT (around version 1.9.5).
- *The main approach as represented by the code in the master branch launches Xen are an EFI bootloader using boot services. It uses a callback from Xen to TBOOT to return control to TBOOT to do the measured launch. A callback from TBOOT to Xen is used to return control to Xen which does EBS.*
- *The plan-b approach as represented by the code in the plan-b branch does all the setup work itself (loading modules, getting graphics information, loading configs) that Xen would normally do. TBOOT does EBS, then does the measured launch and then transfers control to Xen via a special exported entry point.*

GRUB2 UEFI TPM support - WIP

- https://mjg59.dreamwidth.org/37656.html
- https://projects.sirrix.com/trac/trustedgrub/
- http://lists.gnu.org/archive/html/grub-devel/2017-06/msg00022.html
- Some copyright issues with the BIOS code from the trusted-grub blocks relevant patches for the BIOS.

Safe Harbor Statement

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Integrated Cloud

Applications & Platform Services


ORACLE®