

Challenges and Status of Enabling TrenchBoot in Xen Hypervisor





Xen Project Summit 2024

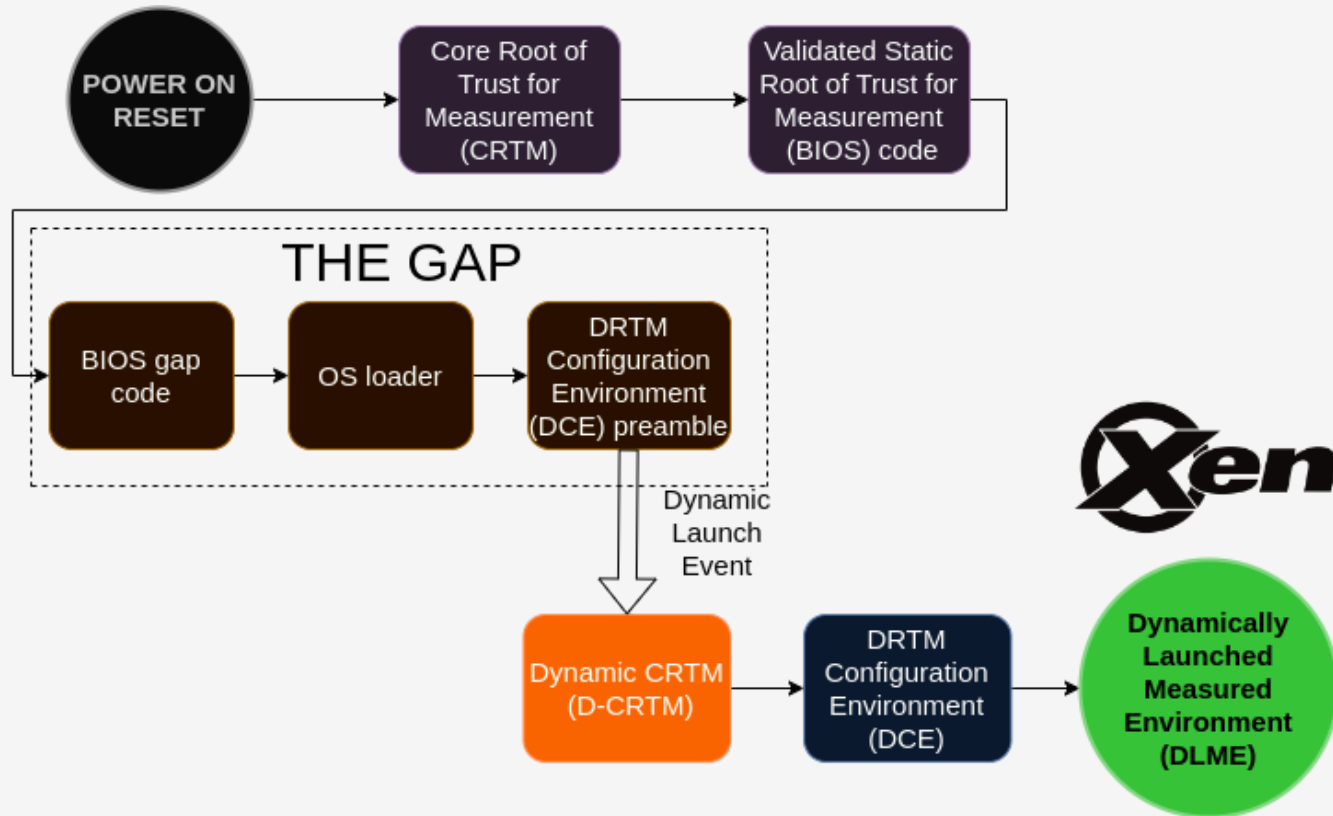
Michał Żygowski



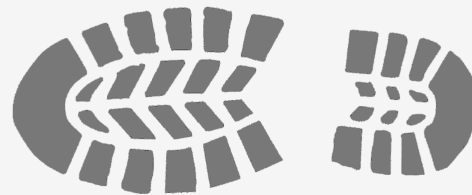


Michał Żygowski
Firmware Engineer

-  [@miczyg_](#)
-  michal.zygowski@3mdeb.com
-  [linkedin.com/in/miczyg](https://www.linkedin.com/in/miczyg)
-  [facebook.com/miczyg1395](https://www.facebook.com/miczyg1395)
- Braswell SoC, PC Engines, Protectli
MSI MS-7D25/MS-7E06 maintainer
in coreboot
- dedicated to the open-source
firmware since 2017
- interested in advanced hardware
and firmware security features



TrenchBoot



- [TrenchBoot Mailing List](#)
- The #OSFW-Trenchboot channel on [Matrix](#)
 - Bridged with #trenchboot channel on [OSFW Slack](#)
- Twitter [@TrenchBoot](#)

TrustedBoot

- TrustedBoot (tboot) supports only Intel TXT
- Is an exokernel and Xen (or any other kernel) has to be aware of its presence
- Supports Linux and multiboot protocols
- Requires a couple of lines to be added to GRUB menu configuration file

TrenchBoot

- Aims for unified approach supporting AMD, Intel and ARM processors
- The goal is to implement a native support for D-RTM to let Xen have full control without any exokernels
- Potential to boot with any protocol/bootloader
- Needs just 1 or 2 lines to be added to perform DRTM launch



- Qubes OS Anti Evil Maid (AEM) is a set of software packages and utilities to aid against [Evil Maid attacks](#)
- Leverages DRTM and TPM to seal secrets, which are used by the owner to confirm whether the device has been tampered with or not
- Initially only Intel TXT and TPM1.2 with tboot was supported using legacy BIOS boot mode, now TrenchBoot replaces tboot, extending the support to TPM2.0 and AMD SKINIT

7 Open ✓ 3 Closed Sort ▾	
<p>Phase 4: AMD support for Qubes OS AEM with TrenchBoot</p> <p>Closed 2 weeks ago ⌚ Last updated 13 days ago</p> <p>This is Phase 4 for TrenchBoot as Anti Evil Maid project, as outlin...(more)</p>	<p>100% complete 0 open 6 closed</p> <p>Edit Reopen Delete</p>
<p>Phase 3: Update to the newest TrenchBoot boot protocol</p> <p>Closed on Jan 17 ⌚ Last updated 5 months ago</p> <p>This is Phase 3 for TrenchBoot as Anti Evil Maid project, as outlin...(more)</p>	<p>100% complete 0 open 2 closed</p> <p>Edit Reopen Delete</p>
<p>Phase 2: TPM 2.0 support in Qubes OS AEM (Intel hardware)</p> <p>Closed on Dec 27, 2023 ⌚ Last updated 5 months ago</p> <p>Phase 2 of the Trenchboot as Anti Evil Maid project aims to impleme...(more)</p>	<p>100% complete 0 open 7 closed</p> <p>Edit Reopen Delete</p>



- <https://github.com/TrenchBoot/trenchboot-issues/milestones>

Phase 2: TPM 2.0 support in Qubes OS AEM (Intel hardware)

Closed on Dec 27, 2023 100% complete

Phase 2 of the **Trenchboot as Anti Evil Maid** project aims to implement support for TPM 2.0 modules in Xen, including the ability to measure Dom0 kernel and initial ram disk before execution, log Dom0 kernel and initial ram disk hashes to the TPM event log, and bring up parallel CPU cores for DRTM launch. Additionally, the project will integrate the TPM 2.0 software stack into Qubes OS Dom0, extending AEM scripts to detect the TPM version on the platform and use the appropriate software stack for TPM 2.0.

The more detailed scope of this phase can be found at docs.dasharo.com.

[Show less](#) ^


<input type="checkbox"/> <input checked="" type="radio"/> 0 Open <input checked="" type="checkbox"/> 7 Closed	
<input type="checkbox"/> <input checked="" type="radio"/> Test TPM 2.0 support on Intel hardware with legacy boot mode and Update Qubes OS AEM documentation P: default T: feature request W: done	7
#16 by BeataZdunczyk was closed on Nov 15, 2023	
<input type="checkbox"/> <input checked="" type="radio"/> Implement parallel CPU cores bring-up for DRTM launch P: default T: feature request W: done	5
#12 by BeataZdunczyk was closed on Oct 18, 2023	
<input type="checkbox"/> <input checked="" type="radio"/> Support for TPM 2.0 module in Xen P: default T: feature request W: done	7
#10 by BeataZdunczyk was closed on Sep 26, 2023	
<input type="checkbox"/> <input checked="" type="radio"/> Support for TPM 2.0 event log in Xen P: default T: feature request W: done	9
#11 by BeataZdunczyk was closed on Sep 26, 2023	
<input type="checkbox"/> <input checked="" type="radio"/> Extend the AEM scripts to use appropriate software stack for TPM 2.0 P: default T: feature request W: done	14
#15 by BeataZdunczyk was closed on Aug 30, 2023	
<input type="checkbox"/> <input checked="" type="radio"/> Integrate TPM 2.0 software stack into Qubes OS Dom0 P: default T: feature request W: done	12
#13 by BeataZdunczyk was closed on Jun 28, 2023	
<input type="checkbox"/> <input checked="" type="radio"/> Extend the AEM scripts to detect TPM version on the platform P: default T: feature request W: done	11
#14 by BeataZdunczyk was closed on May 31, 2023	

Phase 3: Update to the newest TrenchBoot boot protocol

Closed on Jan 17 100% complete

This is Phase 3 for TrenchBoot as Anti Evil Maid project, as outlined in the documentation: and <https://docs.dasharo.com/projects/trenchboot-aem-v2/>.

This phase aims to update the TrenchBoot support in Qubes OS AEM to align with the newest TrenchBoot boot protocol upstreamed to Linux kernel and GRUB. This involves code rebasing onto the most recent work i...
[Show more](#) ▾

☐ 🔄 0 Open ✓ 2 Closed	
<input type="checkbox"/> ✓ Retest the solution on Intel hardware with TPM 1.2 and TPM 2.0 using legacy boot mode P: default	 3
T: feature request W: done #18 by BeataZdunczyk was closed on Jan 12	
<input type="checkbox"/> ✓ Code rebase onto the most recent work implementing Secure Launch protocol being upstreamed to Linux and GRUB P: default T: feature request W: done	6
#17 by BeataZdunczyk was closed on Jan 12	







Phase 4: AMD support for Qubes OS AEM with TrenchBoot

Closed 2 weeks ago 100% complete

This is Phase 4 for TrenchBoot as Anti Evil Maid project, as outlined in the documentation: and <https://docs.dasharo.com/projects/trenchboot-aem-v2/>. Phase 4 of the TrenchBoot AEM project aims to add support for AMD hardware with TrenchBoot on Qubes OS AEM. This phase consists of the following scope:

1. Updating the Secure Kernel Loader package support for ...

[Show more](#) ▾

<input type="checkbox"/> <input checked="" type="radio"/> 0 Open <input checked="" type="checkbox"/> 6 Closed	
<input type="checkbox"/> <input checked="" type="radio"/> TrenchBoot Secure Kernel Loader (SKL) improvements for AMD server CPUs with multiple nodes P: default T: feature request W: done #20 by BeataZdunczyk was closed 2 weeks ago	 2
<input type="checkbox"/> <input checked="" type="radio"/> AMD hardware selection P: default T: task W: in progress #24 by BeataZdunczyk was closed 2 weeks ago 5 of 8 tasks	 20
<input type="checkbox"/> <input checked="" type="radio"/> Test TrenchBoot support on AMD hardware with TPM 2.0 and TPM 1.2 with legacy boot mode P: default T: feature request W: done #23 by BeataZdunczyk was closed 2 weeks ago	 2
<input type="checkbox"/> <input checked="" type="radio"/> Update TrenchBoot boot protocol for AMD in Secure Kernel Loader P: default T: feature request W: done #22 by BeataZdunczyk was closed on Apr 19	 6
<input type="checkbox"/> <input checked="" type="radio"/> Update the Secure Kernel Loader package support for QubesOS P: default T: feature request W: done #19 by BeataZdunczyk was closed on Apr 19 6 of 7 tasks	 5
<input checked="" type="checkbox"/> <input checked="" type="radio"/> Update TrenchBoot boot protocol for AMD in GRUB2 A: amd C: grub2 P: default T: feature request W: done #21 by BeataZdunczyk was closed on Apr 19	 7

It is relatively easy to get a hardware which supports DRTM:

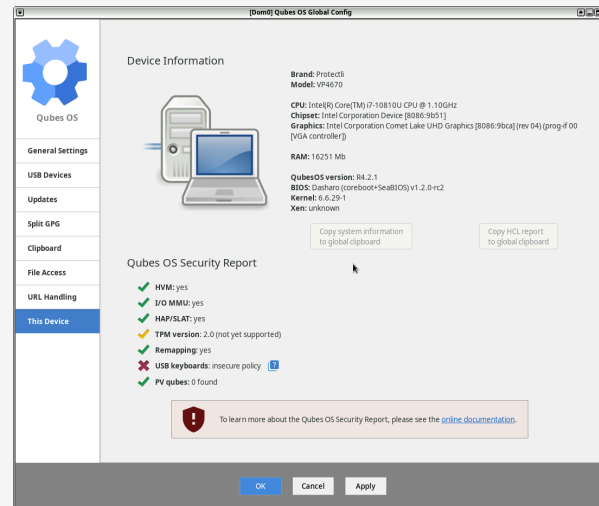
- Intel-based tested and known to work:
 - Protectli VP4670 (open-source-firmware supported)
 - Dell OptiPlex 7010/9010 (open-source-firmware supported)
 - HP EliteDesk 800 G2 Desktop Mini

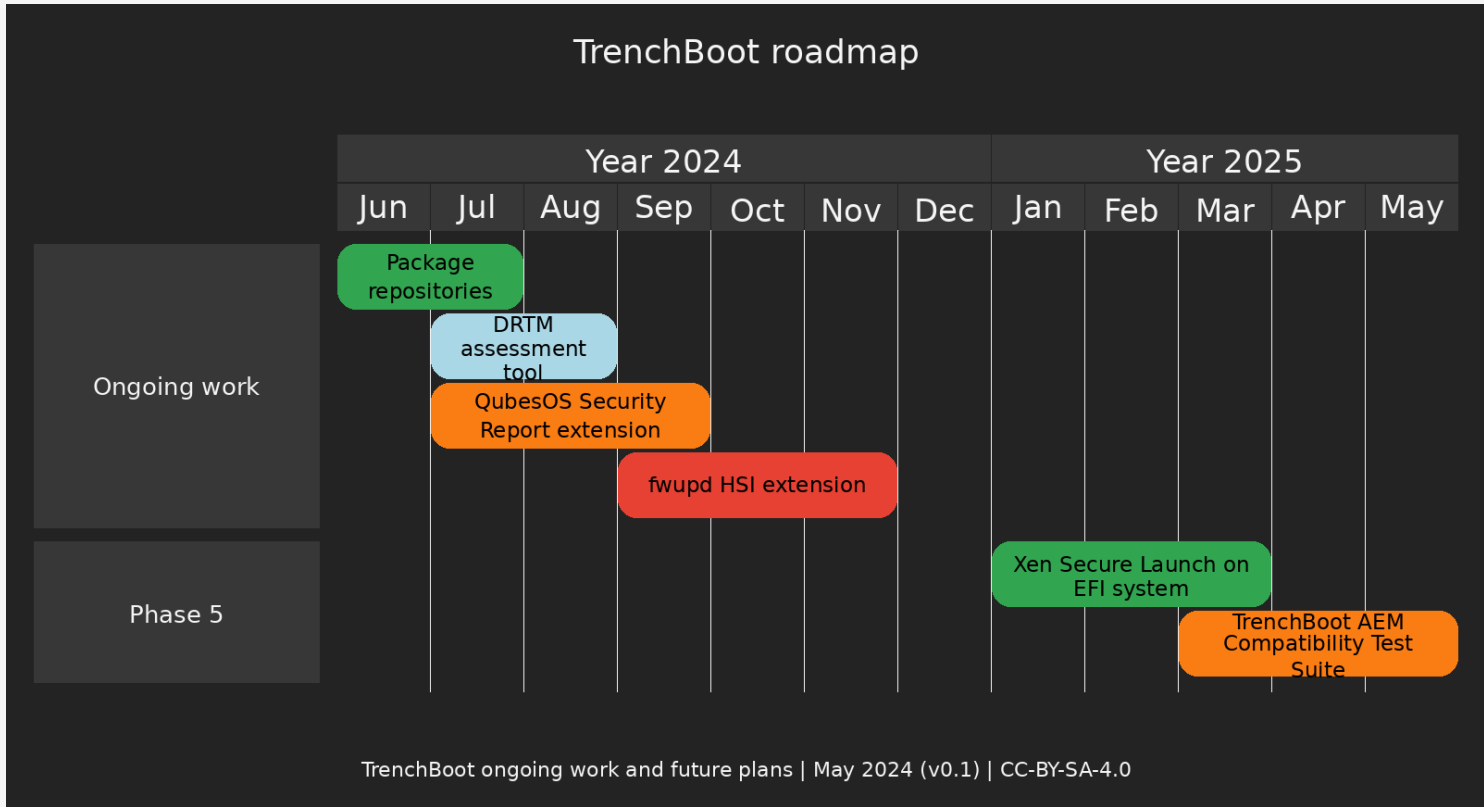


- AMD-based tested and known to work:
 - Terminal HP T630



- Provide package repositories for other major distros (Debian, Ubuntu Fedora)
- Prepare tools for assessing the readiness of the system and BIOS to perform Dynamic Launch
- Adding DRTM Ready indicator to the system security reports: Qubes OS Security Report, [fwupd HSI](#)





More details about Secure Launch on trenchboot.org

Q&A