TrenchBoot Anti Evil Maid: Roadmap, Challenges, and Advancements

Qubes OS Summit 2023

Maciej Pijanowski

3MDEB

whoami

Maciej Pijanowski
Engineering Manager

- @macpijan
- maciej.pijanowski@3mdeb.com
- linkedin.com/in/maciej-pijanowski-9868ab120

- over 7 years in 3mdeb
- Open-source contributor
- Interested in:
  - build systems (e.g., Yocto)
  - embedded, OSS, OSF
  - firmware/OS security

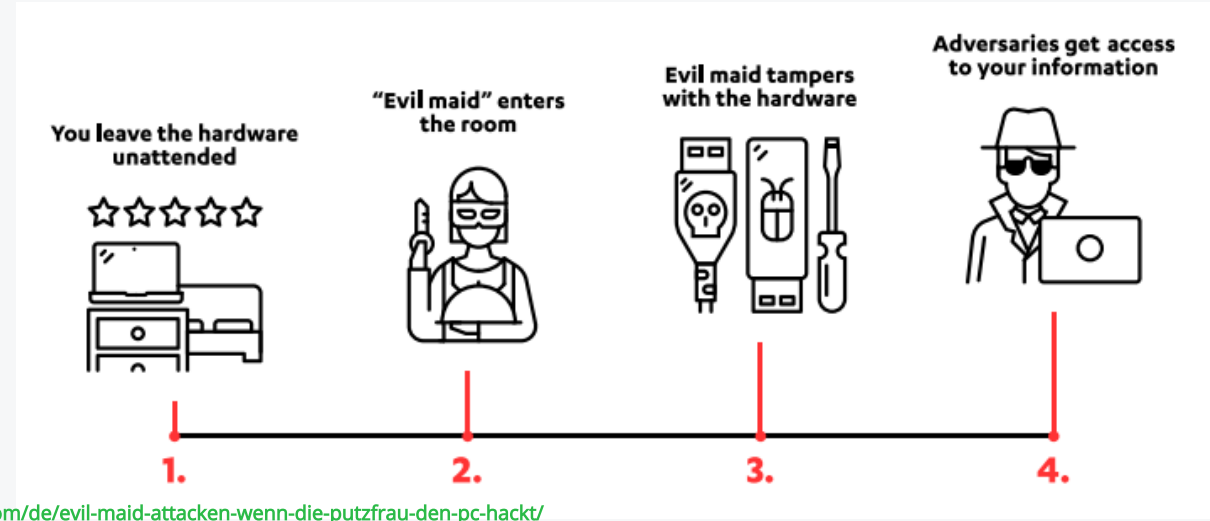
Agenda

- AEM in QubesOS
- TrenchBoot
- Project plan
- Challenges
- Current Status
- Q&A

- Focus and plan and current state
- Short overview of the AEM and TrenchBoot
- Already presented last year in the QubesOS summit
  - TrenchBoot - the only AEM-way to boot Qubes OS
  - https://www.youtube.com/watch?v=A9GrlQsQc7Q&t=17441s

Qubes OS Anti Evil Maid

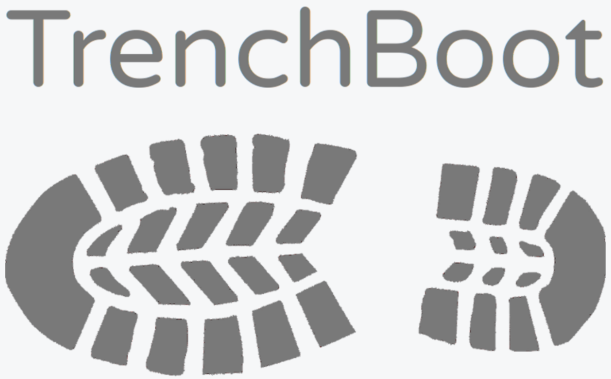
- A set of software packages and utilities
  - https://github.com/QubesOS/qubes-antievilmaid
- The goal to protect against Evil Maid attacks
- Requires **TPM**
- Requires **Dynamic Root of Trust for Measurement (DRTM)**
  - technology from silicon vendor
  - needs to be present in hardware and supported by the firmware



https://blog.f-secure.com/de/evil-maid-attacken-wenn-die-putzfrau-den-pc-hackt/

TrenchBoot is a framework that allows individuals and projects to build security engines to perform launch integrity actions for their systems.

- Uses DRTM as well
- The goal is to replace current solution in AEM (tboot) with TrenchBoot

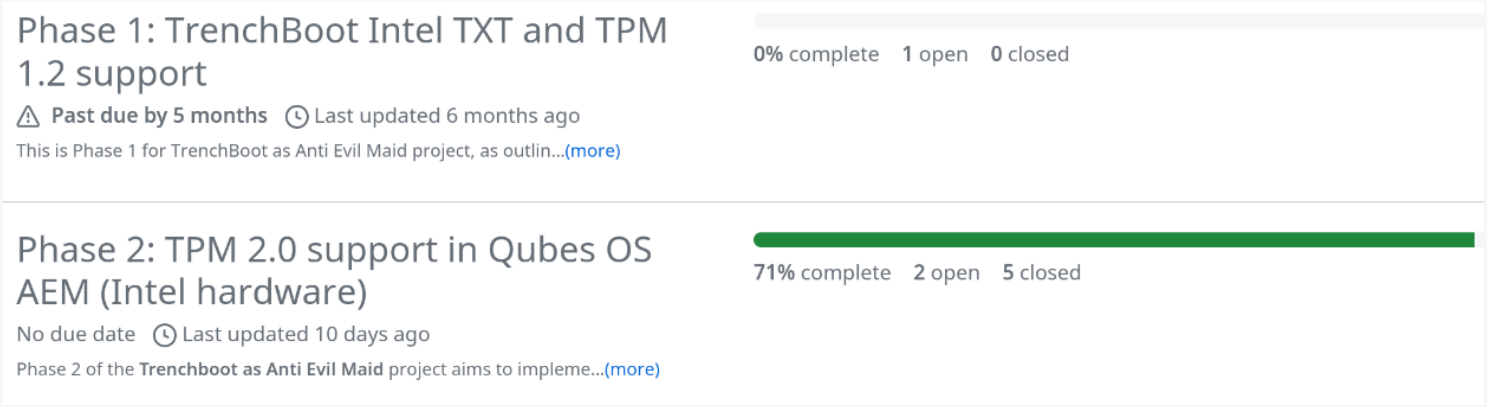


- https://trenchboot.org/

TrenchBoot components

- Secure Kernel Loader (SKL)
  - Secure Loader for AMD Secure Startup
  - https://github.com/TrenchBoot/secure-kernel-loader
- GRUB
  - https://github.com/TrenchBoot/grub
- Xen
  - https://github.com/TrenchBoot/xen
- Linux
  - https://github.com/TrenchBoot/linux

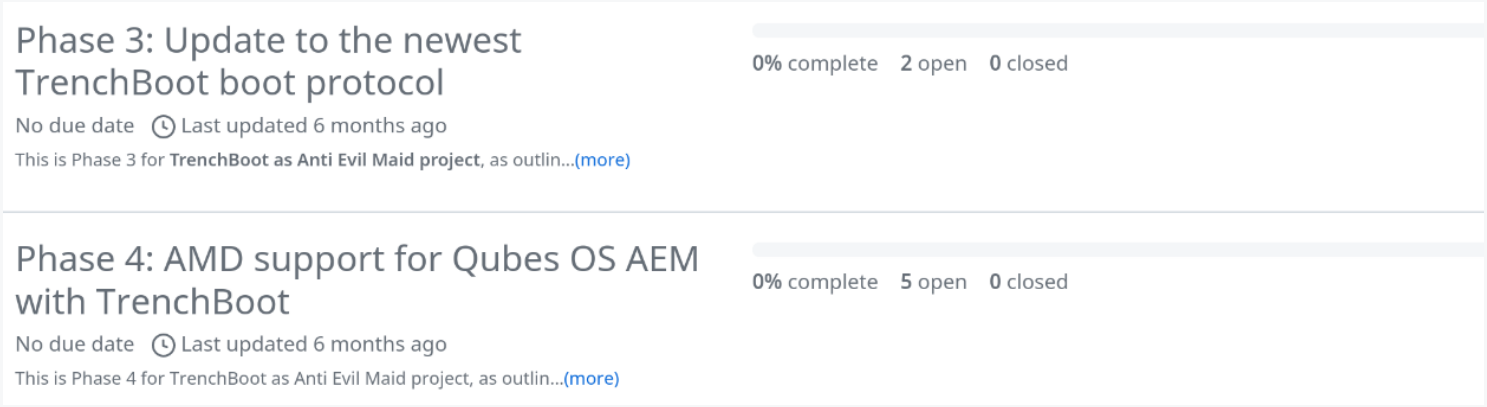
Project Plan



nlnet FOUNDATION

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

Project Plan



nlnet FOUNDATION

- Phase 5
  - UEFI support, scope to be precised
  - No GH milestone

Project Plan

Phase 3

- Specification
  - https://trenchboot.org/specifications/Secure_Launch/
  - Currently, it is focused on booting Linux only
  - We need to extend specification with Xen boot flow
- Adjust our GRUB patches to the latest version of boot protocol

Phase 4

- Integrate AMD Secure Startup support in AEM
- We expect more changes to the specification to support AMD

Challenges

Building and installing QubesOS packages

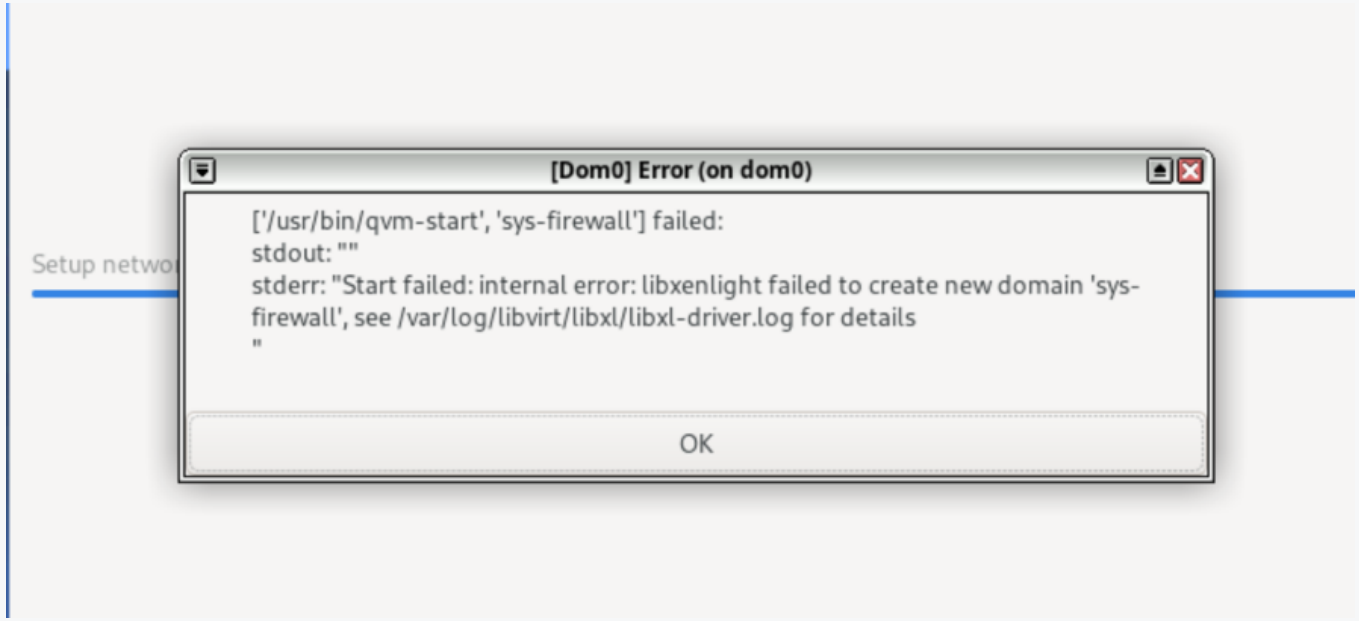
- It is not trivial to ramp-up non-QubesOS developers
- Building GRUB/Xen with custom TrenchBoot changes
  - Creating patches from TrenchBoot changes
  - Applying them on top of the QubesOS GRUB/Xen patches
- AEM/TB packages need to be installed into dom0
  - copying to dom0 is hard
  - https://www.qubes-os.org/doc/how-to-copy-from-dom0/#copying-to-dom0
- Some dev notes
  - https://gist.github.com/krystian-hebel/4359297e4ca3d9e9e3da01f9695d0e27

Reproducing OpenQA setup on VM

- Reproducing https://openqa.qubes-os.org/ would be useful
- Testing changes from TrenchBoot repository, before pushing to QubesOS
- Added some documentation on basic OpenQA setup
  - https://github.com/QubesOS/openqa-tests-qubesos/pull/21/files
- Faced several problems, discussing with Marek in the Matrix chat
- Could not get the full QubesOS installation test (in VM) to work
- Latest problem

```
libxl_device.c:1200:device_backend_callback: Domain 4:unable to add device with path /local/domain/2/backend/vif/4/0
libxl_create.c:2000:domcreate_attach_devices: Domain 4:unable to add vif devices
libxl_device.c:1200:device_backend_callback: Domain 4:unable to remove device with path /local/domain/2/backend/vif/4/0
libxl_domain.c:1589:devices_destroy_cb: Domain 4:libxl__devices_destroy failed
```

Reproducing OpenQA setup on VM



Challenges

Reproducing OpenQA setup on real hardware

- We have some HW in lab hooked-up with PiKVM
- Wanted to run QubesOS OpenQA test (especially AEM) on these
- Wanted to retain the functionality of the PiKVM
- QubesOS setup uses OpenQA worker installed directly on the RPI
  - The `/dev/video` is exposed directly to the worker
- Not trivial to make the video stream work over network
- OpenQA can accept VNC, but requires RAW or ZRLE encoding
- PiKVM exposes VNC, but supports TightJPEG and H.264 encoding

Challenges

Hardware selection for P2 (legacy boot, Intel, TPM2.0)

- Legacy boot support (such as proper CSM support in UEFI firmware)
- TPM2.0 discrete module
- TXT supported by the CPU
- TXT supported by the PCH
  - if platform has vPro sticker, there is a good chance of compatibility
- TXT supported by the firmware
- ACM provided in the firmware
  - if not, we can still load it from GRUB
- **Physical serial port** - for GRUB/Xen development
  - BIOS serial console redirection is a plus

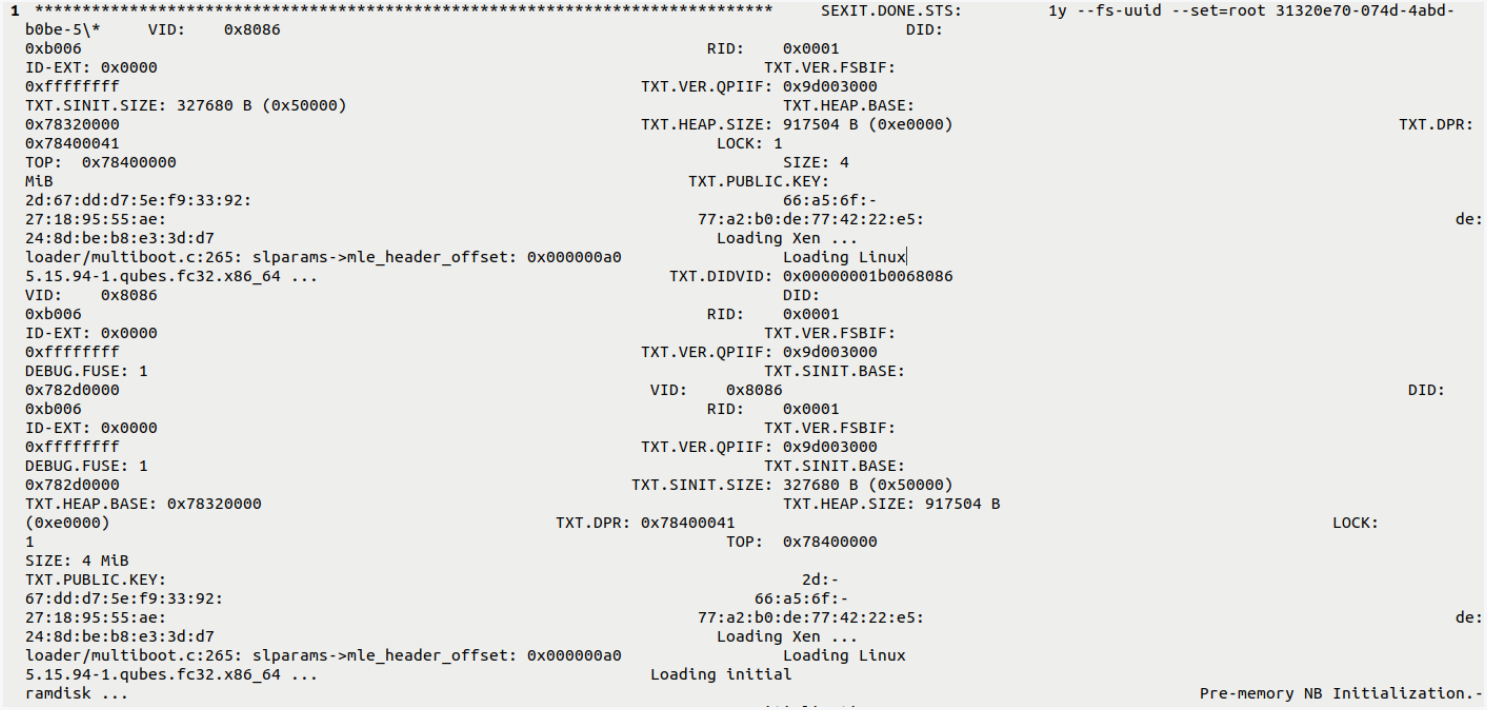
Challenges

Hardware selection for P2 (legacy boot, Intel, TPM2.0)

- Supermicro X11SSH-F
  - 8th Gen Intel server board
- Long boot time
- Poor BMC experience in general
  - Partial (or not working) Redfish implementation
  - Cannot automate BIOS actions (as changing boot devices)
- Serial (both SoL and from physical port) always goes through BMC
  - The output was malformed, we could not get reliable logs from Xen
- More details
  - https://github.com/TrenchBoot/trenchboot-issues/issues/16#issuecomment-1693399379

Challenges

Hardware selection for P2 (legacy boot, Intel, TPM2.0)



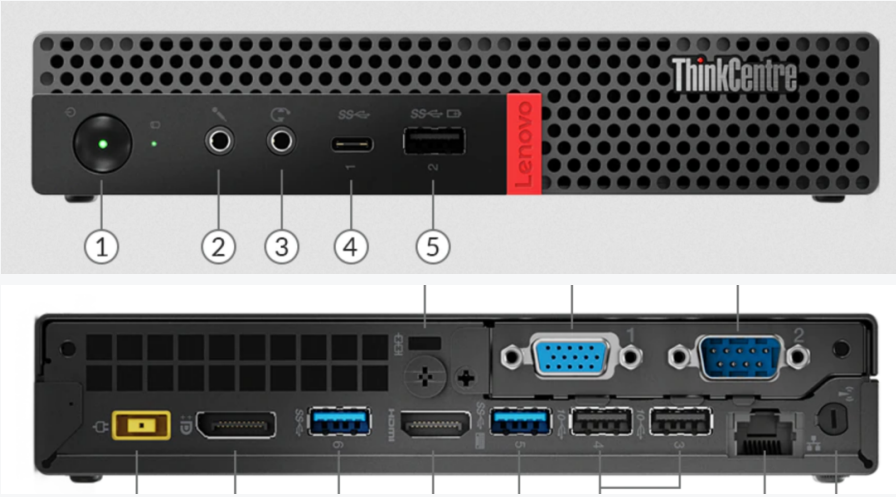
Challenges

Hardware selection for P2 (legacy boot, Intel, TPM2.0)

- No TXT support in AMI BIOS
- No TXT support in current Dasharo releases
  - They are UEFI-only anyway, no CSM
  - https://github.com/Dasharo/dasharo-issues/issues/94#issuecomment-1296210422
- We made some dev-build with TXT support and SeaBIOS payload
  - Xen does not boot in legacy mode
  - Not investigated further yet

Hardware selection for P2 (legacy boot, Intel, TPM2.0)

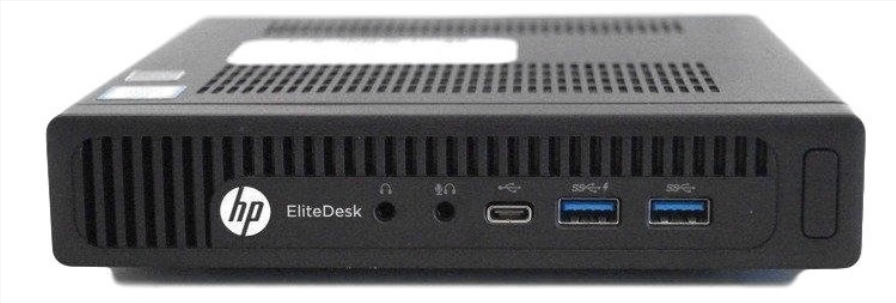
- Lenovo ThinkCentre M920q (M920 Tiny)
  - i5-8500T (vPro), TPM2.0
  - Some lower models have TXT support in CPU, but not in PCH 🤯
  - No ACM in the firmware image (despite BIOS option is there)
  - ACM exits with undocumented error: `0xC00014A1`



Challenges

Hardware selection for P2 (legacy boot, Intel, TPM2.0)

- HP Elite Desk 800 G2
  - i5-6500T (vPro)
  - TPM1.2 upgradable to TPM2.0
  - (Almost) a success
  - AMT came locked and there was no way to reset password
  - No graphical output from BIOS via PiKVM (tried various EDIDs) 😕
  - Some USB ports do not work (could be issue of this particular unit)
  - Gave up on automation, implementing with hardware on a desk



Current Status

Phase 1

- Intel, legacy boot, TPM1.2, TrenchBoot
- Released January 2023
- Blog posts
  - https://www.qubes-os.org/news/2023/01/31/trenchboot-aem-for-qubes-os/
  - https://blog.3mdeb.com/2023/2023-01-31-trenchboot-aem-for-qubesos/
- MRs still pending review to be merged in QubesOS
  - https://github.com/QubesOS/qubes-grub2/pull/13
  - https://github.com/QubesOS/qubes-vmm-xen/pull/160

Current Status

Phase 1

- Hardware used for testing
  - Dell OptiPlex 9010 SFF (Intel Ivybridge, TPM 1.2)
  - Dev-build of Dasharo with TXT and SeaBios

Current Status

Phase 2

- The main development is finalized 🏁
- We are working on integration and testing

Current status

Phase 2

Extend the AEM scripts to detect TPM version on the platform

- GitHub task
  - https://github.com/TrenchBoot/trenchboot-issues/issues/14
- Contributions
  - https://github.com/QubesOS/qubes-antievilmaid/pull/45

Integrate TPM 2.0 software stack into Qubes OS Dom0

- GitHub task
  - https://github.com/TrenchBoot/trenchboot-issues/issues/13
- Contributions
  - https://github.com/QubesOS/qubes-builder-rpm/pull/124
  - https://github.com/QubesOS/qubes-antievilmaid/pull/46

Current status

Phase 2

Extend the AEM scripts to use appropriate software stack for TPM 2.0

- GitHub task
  - https://github.com/TrenchBoot/trenchboot-issues/issues/15
- Contributions
  - https://github.com/QubesOS/qubes-antievilmaid/pull/43
  - https://github.com/QubesOS/qubes-antievilmaid/pull/47
  - https://github.com/QubesOS/qubes-tpm-extra/pull/7
  - https://github.com/QubesOS/qubes-trousers-changer/pull/6
  - https://github.com/QubesOS/qubes-antievilmaid/pull/42
  - https://github.com/QubesOS/openqa-tests-qubesos/pull/23

Phase 2

OpenQA test for AEM

- Example run
  - https://openqa.qubes-os.org/tests/80924#
- PR
  - https://github.com/QubesOS/openqa-tests-qubesos/pull/22

Phase 2

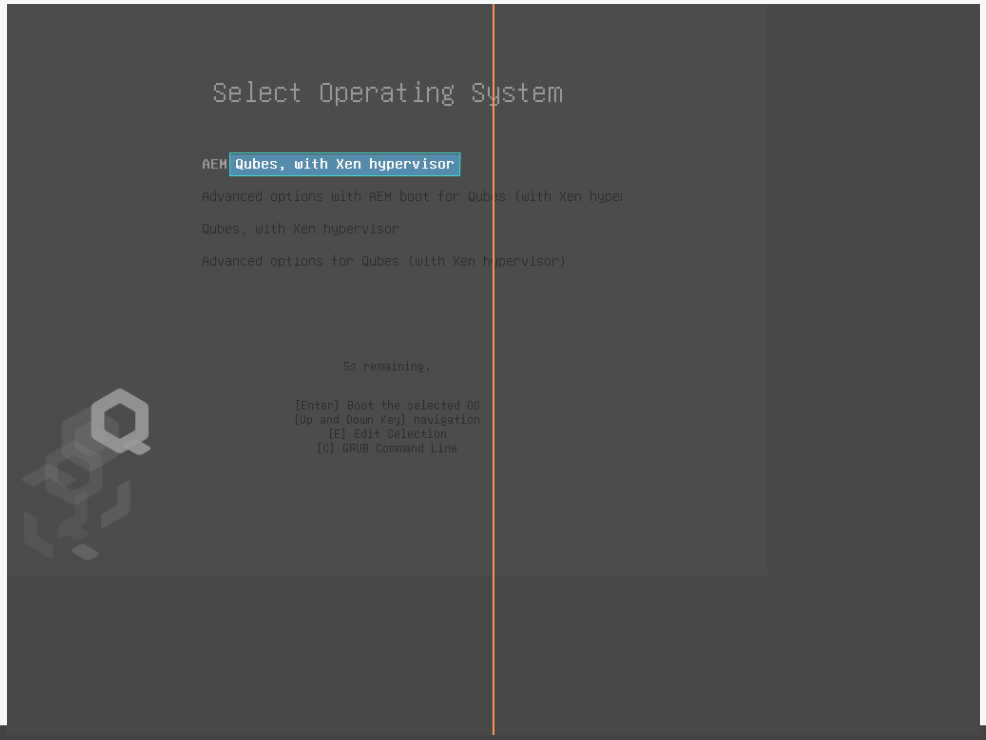
OpenQA test for AEM

Test	x86_64
aem-tpm1	●
aem-tpm1-mfa	●
aem-tpm1-srk	●
aem-tpm1-srk-mfa	●
aem-tpm2	●
aem-tpm2-mfa	●
aem-tpm2-srk	●
aem-tpm2-srk-mfa	●
system_tests_update_encrypted	●

Current status

Phase 2

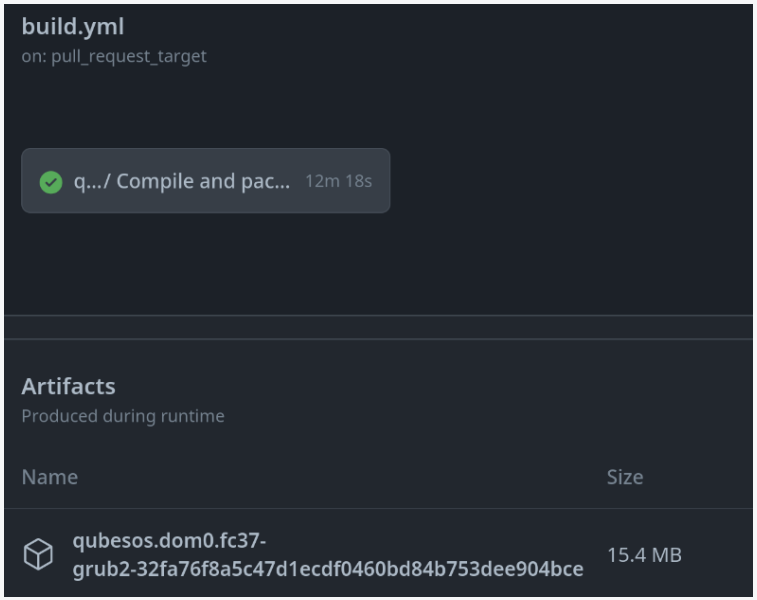
OpenQA test for AEM



Phase 2

CI for GRUB TB packages

- https://github.com/TrenchBoot/grub/pull/9

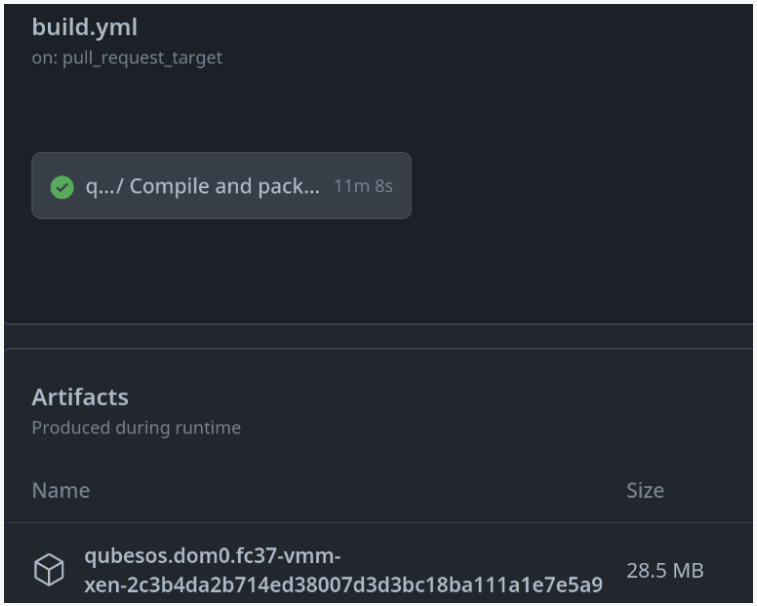


Current status

Phase 2

CI for Xen TB packages

- https://github.com/TrenchBoot/xen/pull/5



Next steps

- P2
  - Integration
  - Demo/blog post
  - Upstream to QubesOS repositories
- P3
  - Adjust to the most recent TB boot protocol

Contact us

We are open to cooperate and discuss

- contact@3mdeb.com
- facebook.com/3mdeb
- @3mdeb_com
- linkedin.com/company/3mdeb
- https://3mdeb.com
- Book a call
- Sign up for the newsletter

Feel free to contact us if you believe we can help you in any way. We are always open to cooperate and discuss.

3MDEB

Q&A