

Anti Evil Maid for modern AMD UEFI-based platform

Qubes OS and 3mdeb minisummit 2020





Michał Żygowski



- Introduction
- Evil Maid attacks
- Anti Evil Maid
- Qubes OS Anti-Evil-Maid
- Qubes OS Anti-Evil-Maid status
- Enabling AEM in Qubes OS for AMD platform
- Enabling AEM in Qubes OS for TPM2
- Demo
- Q&A



Michał Żygowski
Firmware Engineer

-  [@miczyg](https://twitter.com/_miczyg)
-  michal.zygowski@3mdeb.com
-  linkedin.com/in/miczyg
-  facebook.com/miczyg1395
- Braswell SoC, PC Engines and Protectli maintainer in coreboot
- interested in:
 - advanced hardware and firmware features
 - coreboot
 - security solutions



Short recap:

- burn Evil Maid USB stick
- boot target machine from the prepared stick
- injecting key loggers, password sniffers
- wait machine owner launches the machine and types password
- boot again from Evil Maid stick
- retrieve password saved by key-logger or password sniffer on the disk
- enjoy a new laptop/PC

1st phase take about 2 minutes (first boot of Evil Maid USB and malicious software installation). 2nd phase also may take about 2 minutes.

Very high reward ("ownership" of a new PC) at a cost of single USB stick and some amount of time.

Source: <http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html>

Protection by ensuring the state of the platform.

If we can trust the hardware and software we use, can we feel safe?

How to determine if the state of the platform is trusted and hardware/firmware/software has not been tampered?

Trusted Execution / Trusted Computing:

- TPM module by TCG
- Intel TXT
- AMD Secure Launch with SKINIT

Short recap from Qubes OS minisummit 2019...

Intel TXT

- TPM required
- BIOS ACM and SINIT ACM required
- implementation: tboot
- BIOS needs to enable VT-x, VT-d, load BIOS ACM
- many GETSEC sub-instructions called leaf functions

AMD Secure Launch

- TPM required
- no blobs required
- implementation: Trenchboot (WIP)
- BIOS needs to enable SVM
- Only 1 SKINIT instruction

```
sudo qubes-dom0-update anti-evil-maid
```

Additional protection:

- multi-factor with AEM USB boot device and TOTP
- using 2 AEM USB sticks in case one could be stolen
- using non-default SRK password
- using additional secret key file for LUKS on AEM USB

Attack still not prevented:

- attacker can sniff passwords, keystrokes and access AEM USB stick
- fake motherboard injection with radio link
- successful measurement bypass by buggy CRTM implementations in BIOS
- buggy BIOS updates leading to BIOS compromise
- SMM attacks leading to Intel TXT compromise (can be prevented by STM)

<https://www.qubes-os.org/doc/anti-evil-maid/>

<https://github.com/QubesOS/qubes-antievilmaid/blob/master/anti-evil-maid/README>

Qubes minisummit 2019 AEM status:

- only for Intel silicon
- not supported on UEFI installations
- TPM 1.2 only

Current AEM status:

- not only for Intel but also for AMD silicon thanks to TrenchBoot
- can be supported by UEFI installations on AMD (not tested yet on Qubes OS)
- also available for TPM 2.0 - WIP (available at <https://github.com/3mdeb/qubes-antievilmoid-amd>)

The installation comes down to a few simple steps:

1. Use [qubes-builder](#) to build necessary packages:
 - [landing-zone](#)
 - [custom GRUB2](#) with TrenchBoot support
 - [Anti Evil Maid for AMD with TPM 2.0 support](#)
2. Install *tpm2-tools* and *tpm2-abrmd* with *qubes-dom-update*.
3. Copy the built packages to Dom0 and install them with dnf.
4. Install the anti-evil-maid as described in [AEM README](#) (WIP)
5. Test the installation by booting the Qubes OS with AEM entry. (WIP)

Most of these packages are still work in progress, contributions welcome. GRUB2 support still awaits for upstream contributions. TPM 2.0 may not work well yet. Kudos to my colleague from 3mdeb - Krystian Hebel - for help in developing the multiboot support for Secure Launch

Challenges and differences:

- Huge specifications consuming time to get familiar with
- Software stack different than TPM 1.2 and not compatible
- Specification is written in very technical way and hard to understand
- TPM 2.0 is based on contexts
- Different approach to sealing/unsealing data

Demo time...

- landing-zone Qubes package:
https://github.com/3mdeb/qubes-landing-zone/tree/lz_support
- landing-zone code:
<https://github.com/3mdeb/landing-zone/tree/multiboot2>
- GRUB2 Qubes package:
https://github.com/3mdeb/qubes-grub2/tree/trenchboot_support
- GRUB2 code:
https://github.com/3mdeb/grub2/tree/trenchboot_mb2
- Anti Evil Maid for AMD with TPM 2.0 support:
https://github.com/3mdeb/qubes-antievilmoid-amd/tree/aem_amd

Q&A



Thank you