Anti Evil Maid

(Anti) Evil Maid for Intel and AMD

Michał Żygowski

3MDEB

Introduction

Michał Żygowski
Firmware Engineer

- @_miczyg_
- michal.zygowski@3mdeb.com
- linkedin.com/in/miczyg
- facebook.com/miczyg1395

- PC Engines platforms maintainer
- interested in:
  - advanced hardware and firmware features
  - coreboot

Evil Maid attacks

Evil Maid attacks

Short recap:

- burn Evil Maid SUB 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

Evil Maid attacks

How should we protect ourselves?

TrueCrypt Developer: Given the scope of our product, how the user ensures physical security is not our problem. Anyway, to answer your question (as a side note), you could use e.g. a proper safety case with a proper lock (or, when you cannot have it with you, store it in a good strongbox).

Joanna Rutkowska: If I could arrange for a proper lock or an impenetrable strongbox, then why in the world should I need encryption?

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

Anti Evil Maid

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

AMD vs Intel

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

Can we trust hardware features silicon vendors provide?

Qubes OS Anti-Evil-Maid

```
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

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

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

Qubes OS Anti-Evil Maid

Current AEM status:

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

Ani-Evil Maid in UEFI

On PSEC2018 Lengyel and Karrigan presents AEM with UEFI and Xen.

SRTM:

- shim verification and measurement
- shim measures and verifies Xen
- Xen loads Dom0, shim verifies and measures Dom0 kernel and initrd
- GRUB-like configs to pass boot parameters, also measured
- rootfs read-only, can't properly measure accessed files in multi-core systems

DRTM:

- tboot loaded from Xen EFI, measured by shim
- second copy of Xen measured and verified by shim
- build multiboot struct in Xen EFI to point to second Xen EFI copy
- launch tboot using multiboot struct

Sounds like an entanglement... Still no AMD support.

https://www.platformsecuritysummit.com/2018/speaker/kerrigan/PSEC2018-Anti-Evil-Maid-UEFI-Xen-Brendan-Kerrigan.pdf

Bonus

Evil maid attacking You in the Sims

Q&A