👋 Dasharo User Group #9 🎉 and Developers vPub 0xD 🍻

Introduction to deguard

whoami

- Filip Lewiński
- Junior Firmware Engineer @ 3mdeb

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

Agenda

- What is Intel Boot Guard? + demo #1
- What does it mean for coreboot?
- What is deguard?
- How can I use it?
- Demo #2 - deguarded T480 running coreboot
- Discussion

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

What is Intel Boot Guard?

Intel Boot Guard is a security feature that ensures only trusted firmware runs when a computer starts.

- OEM Public Key and Boot Guard Policy are fused into the platform
- Field Programmable Fuses
- The firmware (Initial Boot Block - IBB) is signed by the manufacturer.
- Intel ME makes sure the CPU checks this signature before execution.
- Introduced with the 4th generation of Intel CPUs (Haswell)

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

Demo #1 - BootGuarded T480

Finding out if you have Boot Guard enabled

```
$ sudo rdmsr 0x13a
( ... )  ⟵ non-zero output
```

Any **non-zero** value in the 0x13a Model Specific Register means Boot Guard is enabled.

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

What does it mean for coreboot?

In theory, Intel Boot Guard makes coreboot development impossible on a given platform. This is why coreboot has *largely* revolved around pre-Haswell boards.

In practice, there have been already a few exceptions:

- Buying unfused platforms from hardware vendors in bulk
  - NovaCustom
  - Protectli
- Some large OEMs choose not to / fail to fuse their platforms
  - Felix Singer's BootGuard status
  - Successful coreboot port example: ThinkCentre M700/M900 Tiny
- Using leaked IBG OEM keys to sign a coreboot binary
  - Popular in the WinRaid and CSDN BIOS modding communities

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

Deguard

Deguard is a tool written by Mate Kukri that bypasses Intel BootGuard on Skylake, Kaby Lake, and some Coffee Lake platforms.

What does it do?

- It exploits CVE-2017-5705 in vulnerable ME 11.x firmware.
- It downgrades ME via SPI flash overwrite
- It modifies BootGuard fuses in SRAM allowing execution of unsigned firmware.
- Works out of the box on the Lenovo T480 and Dell OptiPlex 3050
- Can be used to bypass BootGuard on other ME 11.x platforms, using a provided script to generate the required metadata.

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

Deguard

coreboot ports enabled by deguard

- Thinkpad T480(s) WIP
- Dell OptiPlex 3050 Merged

How can I use it?

- Read the SPI flash
- Extract your platform-specific ME settings with `generatedelta.py` OR use already contributed settings if your board is supported
- Obtain a donor ME 11.6.0 image
- Patch the donor image with your settings and fake FPFs with `finalimage.py`
- Pack it into your flash image with `ifdtool` and flash it back onto the platform *(spoiler: that's what I'm doing with the T480 right now)*
- Open a PR adding your platform's ME settings

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

How can I contribute and use it?

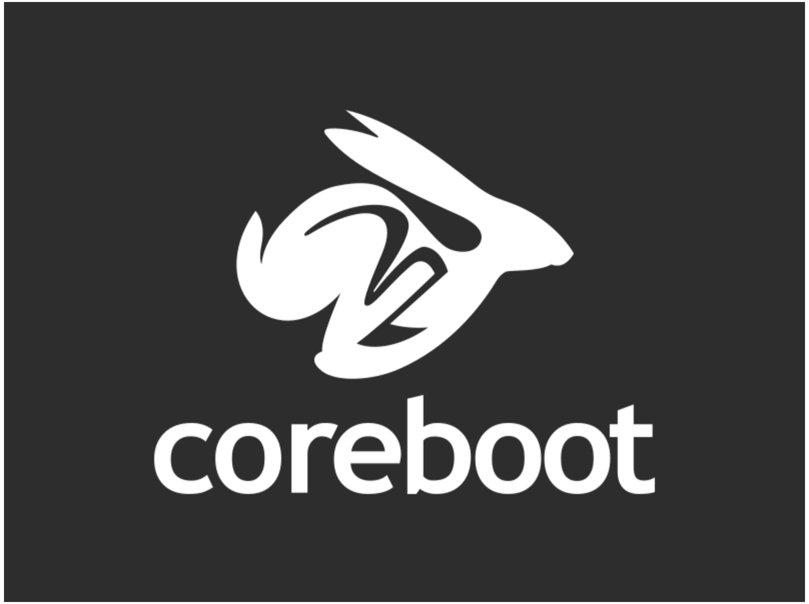
Potential issues

There's been two issues so far suggesting that the `generatedelta.py` script has trouble handling different platforms due to hardcoded offsets and being tailored for the T480

- Invalid checksum assert generating delta for T460s (ME 11.8.xxx)
- Deguarding an Optiplex 5050

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

Demo #2 - deguarded T480, running coreboot



© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

Discussion

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.

Discussion

Question 1

Do you consider a deguarded platform compromised/flawed in terms of security? How would you rank

- a deguarded platform
- one that's never had bootguard support
- one whose private IBG keys had been leaked

Question 2

Have you tried to do it, do you have platforms you'd really like to see ported?

© 2025 3mdeb Sp. z o.o. Licensed under the CC BY-SA 4.0.