



“
Waarom open-source op firmware-niveau
belangrijk is.
”



Introductie

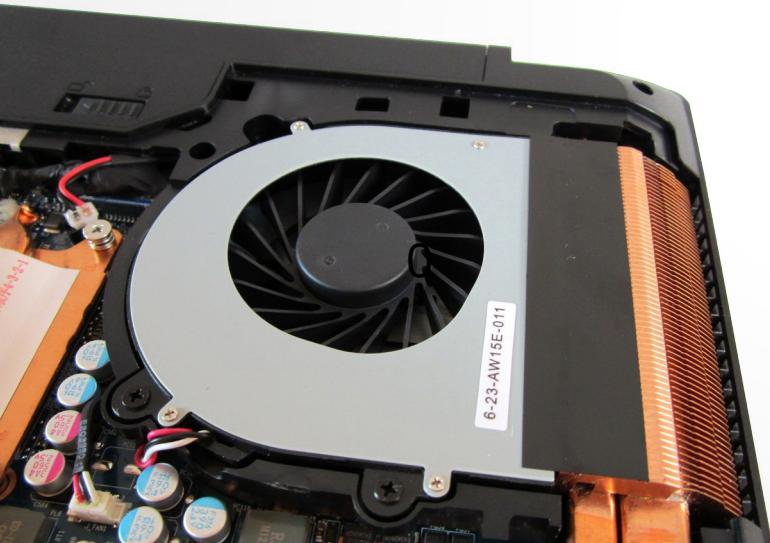
- Wessel klein Snakenborg
- Kindheid
- Opgericht in 2015 (toen nog SnaakSystems)
- 2018 → NovaCustom
- Op maat gemaakt:
 - Laptops
 - Mini PCs
 - Smartphones
- CPU, GPU, werkgeheugen, opslag ...
- Eigen lasergravures
- Dasharo coreboot firmware
- Windows en GNU/Linux (of beide)
- Qubes OS-gecertificeerde modellen
- Focus op privacy en beveiliging
- Right to repair en duurzaamheid
- <https://novacustom.com/nl>



Anekdote



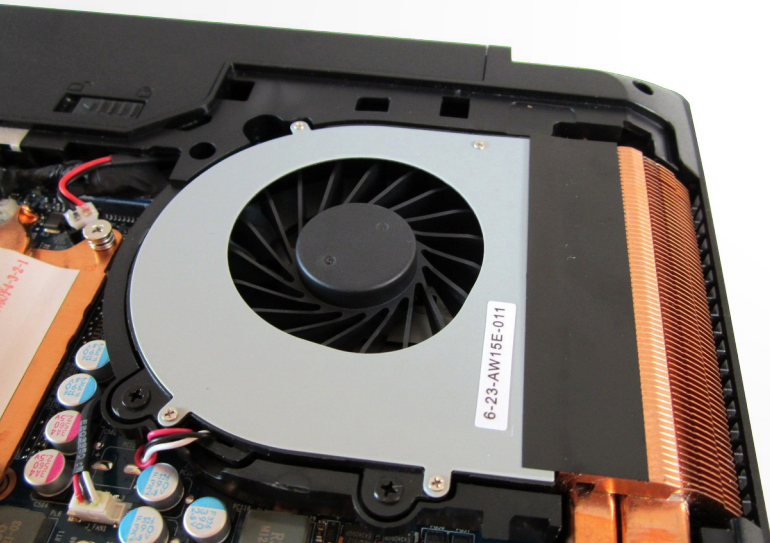
- Hoe het begon in 2021?
- Niet vanwege beveiliging
- Een irritante ventilator ...
 - Geen controle
- Zoektocht: manieren om dit te beïnvloeden
 - Bij de wortel aanpakken



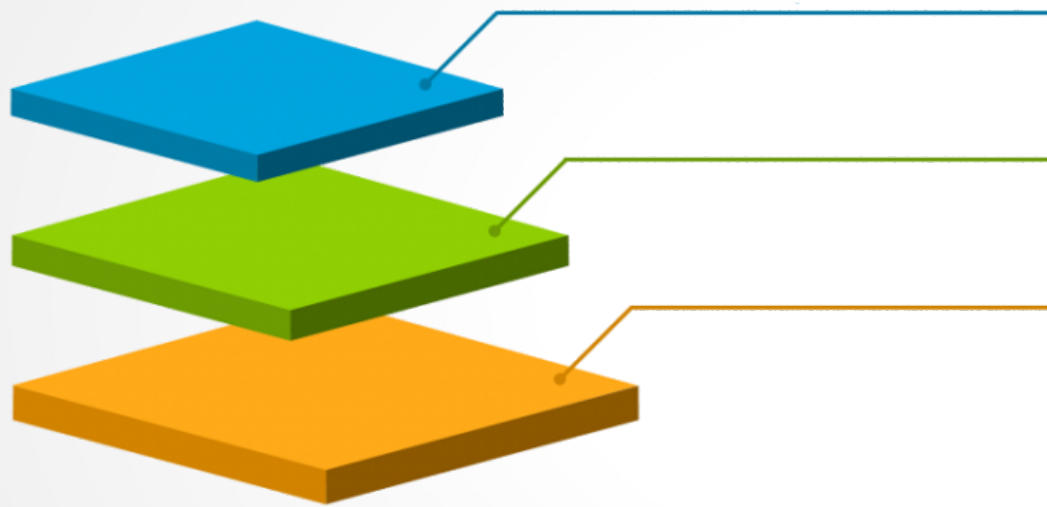
Anekdote



- Dasharo (3mdeb)
 - Open firmware
- Verbetering van klanttevredenheid
- Onverwachte bijkomende voordelen:
 - Betere gebruikservaring (energiebeleid, enz.)
 - Betere platformbeveiliging
- Basis geweest voor open firmware
 - Controle terug



Wat is firmware?



Hardware

Bijvoorbeeld: Ventilator

- Applications
Bijvoorbeeld: GNOME of Firefox
- Besturingssysteem (incl. kernel)
Bijvoorbeeld: Ubuntu of Mint
- Firmware
Bijvoorbeeld: AML, Insyde of coreboot



Wat is firmware?

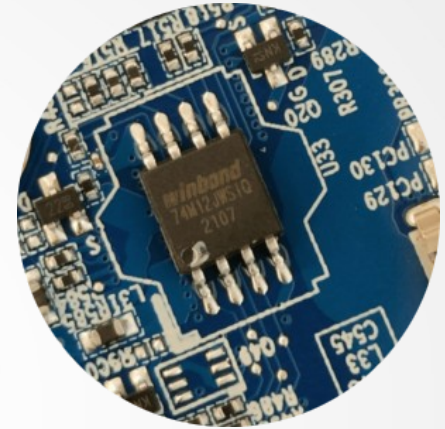
De firmware stuurt de hardware aan.

Het heeft directe toegang tot hardwarecomponenten.



Gevaren onveilige firmware

- Firmware rootkits
- Malware die zich in firmware nestelt
- OS opnieuw installeren heeft geen zin
- Keyloggers
- Backdoors
- Schadelijke of ongewenste software
- Verborgen voor virusscanners e.d.
- Volledige controle
- Vermijdt detectie en is persistent
- Geavanceerd (laag infectiegevaar)
- Installatie vaak gepaard met fysieke manipulatie
- Als het misgaat, gaat het goed mis



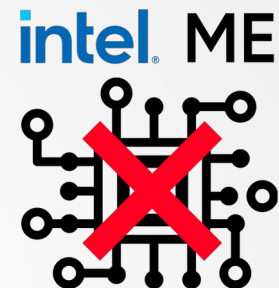
Voorbeelden van bekende rootkits

- LogoFAIL
 - Injectie van schadelijke code
 - Kwetsbaarheid in bepaalde UEFI applicaties
- Thunderstrike
 - Firmware-injectie via de Thunderbolt-poort
- Lenovo Superfish
 - Installatie van ongewenste software
 - Kwetsbaarheid die werd uitgebuit



Intel Management Engine (ME)

- Een subcomputer binnen de computer
- Zelfs als de computer uit staat
- Eigen processor, werkgeheugen, etc.
- Draait op Minix
- Gebruikt voor remote management
- Niet nodig voor de meesten
- Veel complottheorieën
- Closed source: niet verifieerbaar
- Attack surface
- Uitschakelen vaak niet mogelijk



De oplossing: coreboot

- Alternatieve open source firmware-implementatie
 - Alternatief voor o.a. Insyde en American Megatrends
- Open-source = transparant
- Verbeterde gebruikerservaring
 - Snel opstarten
 - Geen irritant ventilatorbeleid
- Verbeterde beveiliging
 - BIOS schrijfbeveiliging
 - Intel ME uitschakelen (HAP + HECI)



Laten we coreboot installeren.

We vervangen Insyde firmware door coreboot.



Vergelijking: Beveiliging



- ✓ UEFI Secure Boot
- ✓ TPM 2.0 Support
- ✓ Wachtwoord firmware-instellingen
- ! Intel Boot Guard (gelekte private keys)
- ✗ Measured boot
- ✗ Verified boot
- ✗ BIOS boot medium lock
- ✗ Early boot DMA protection
- ✗ SMM BIOS write protection
- ✗ USB stack-opties
- ✗ Intel ME disabling (HECI + HAP)



- UEFI Secure Boot ✓
- TPM 2.0 Support ✓
- Wachtwoord firmware-instellingen ✓
- Optioneel:* Intel Boot Guard ✓
- Measured boot ✓
- Verified boot ✓
- BIOS boot medium lock ✓
- Early boot DMA protection ✓
- SMM BIOS write protection ✓
- USB stack-opties ✓
- Intel ME disabling (HECI + HAP) ✓

Vergelijking: Gebruikerservaring



- ✓ Accudrempelwaarden (*instelbaar*)
- ✗ Oververhittingspreventie (*90 °C*)
- ✗ Irritant luid ventilatorbeleid
- ✗ Toetsenbordverlichting benodigt driver
- ✗ Fn lock hotkey
- ✗ ACPI driver



- (*standaard*) Accudrempelwaarden ✓
- (*80 °C*) Oververhittingspreventie ✓
- Stil ventilatorbeleid ✓
- Toetsenbordverlichting OS onafhankelijk ✓
- Fn lock hotkey ✓
- ACPI driver ✓

Vergelijking: Transparantie



- ✗ Open source
- ✗ Openness score
- ✗ Documentatie voor herstellen
- ✗ Building-handleiding
- ✗ Eenvoudige firmware-updates



- Open source ✓
- Openness score ✓
- Documentatie voor herstellen ✓
- Building-handleiding ✓
- Eenvoudige firmware-updates ✓

Vergelijking: Compatibiliteit



- ✓ Ondersteunt Windows 11
- ✗ Ondersteunt GNU/Linux
- ✗ Ondersteunt LVFS/fwupd
- ✗ Ondersteunt Qubes OS
- ✗ Heads firmware-variant



- Ondersteunt Windows 11 ✓
- Ondersteunt GNU/Linux ✓
- Ondersteunt LVFS/fwupd ✓
- Ondersteunt Qubes OS ✓
- Heads firmware-variant ✓

Dasharo ACPI driver

- Communicatie tussen besturingssysteem en firmware
- Energie-optimalisatie
- Temperaturen
- Ventilatorsnelheid
- Feedback op Fn toetsen
- Power management
- Accudrempelwaarden
- Niet meer naar UEFI firmware-instellingen



Dasharo TrustRoot: Intel Boot Guard

- Beveiligingsfunctie
- Controversieel
- Vendor lock-in effect
- E-fuse
- Eén keer
- Gesigneerde firmware
- Of start helemaal niet op
- Beschermt tegen rootkits
- Fysieke manipulatie van de firmware
- Optioneel
- Eigen sleutels



Oplossing? Niet altijd louter techniek

En wat als een aanvaller het moederbord vervangt?

Dan heb je niks aan technische oplossingen als deze.



Tamper-evident-schroeven en -verpakking

- Glittersubstantie op de schroeven
 - Creëert een 3D-glitterpatroon
- E-mail met foto's van de schroeven (optioneel)
 - Via Proton Mail
 - PGP-gesigneerd
- Anti-tamper tape
 - Laat een *OPENED* print achter
 - Plastic beschermhoes
 - Alle verzenddozen
- Security seals (optioneel)



Let op het glitterpatroon



UEFI Capsule Updates en fwupd



- Tot op heden:
 - BIOS flash bescherming uitschakelen
 - UEFI Secure Boot uitschakelen
- Dasharo Tools Suite (DTS)
- Hoeft niet meer
- Fwupd/LVFS-ondersteuning voor firmware updates vanuit het OS
 - Alleen voor Linux



Dasharo coreboot is geïnstalleerd.

Laten we het NLLGG-opstartlogo integreren!



Schaamteloze productpromotie



V54 Serie

14 inch F-HD+/2.8K
Ultra 5 / Ultra 7 CPU
NVIDIA optioneel
Tot 96 GB geheugen
Tot 2× 4 = 8 TB opslag
Dasharo coreboot
Vanaf 1420 EUR



V56 Serie

16 inch F-HD+/Q-HD+
Ultra 5 / Ultra 7 CPU
NVIDIA optioneel
Tot 96 GB geheugen
Tot 2× 4 = 8 TB opslag
Dasharo coreboot
Vanaf 1460 EUR



NUC Box

Ultra 5 / Ultra 7 CPU
Tot 96 GB geheugen
Tot 4 TB opslag
Dasharo coreboot
Vanaf 830 EUR



SHIFTphone 8.1

6.67 inch AMOLED
Qualcomm QCM6490
Hardware kill switches
12 GB geheugen
Tot 512 GB opslag
IodéOS (geen Google)
Vanaf 870 EUR

Repareerbaarheid



- **Beschikbaarheid gegarandeerd voor ten minste 7 jaar.**



Repareerbaarheid

Vervangingsinstructies

🕒 20 min

🕒 Gemiddeld

Benodigdheden:

- Een zachte ondergrond - *Gebruik bijvoorbeeld een handdoek*
- Een bakje om de schroeven in te bewaren - *Zorg dat je de schroeven niet kwijtraakt*
- [Schroevendraaier](#)
- [Spudger](#) (of een vergelijkbaar plastic hulpmiddel)
- [Koelpasta met een spatel](#)
- [Metaalreiniger](#)
- [Vochtige doekjes](#)
- [Microvezel schoonmaakdoek](#)



Stap 1: Verwijder de schroeven

Leg de laptop ondersteboven op een zachte ondergrond.

Dit voorkomt krassen op de schermklep van de laptop. Verwijder vervolgens alle schroeven met de schroevendraaier.



Stap 2: Verwijder de onderkant

Pak de spudger en plaats deze tussen de onderkant en het scharnier.

Druk voorzichtig tegen het scharnier. Doe dit aan beide kanten. Je kunt nu voorzichtig de onderkant volledig verwijderen.



Stap 3: Ontkoppel de accu



V54 Series: How to replace the power LED daughterboard

57 views • 3 months ago



NUC Box: how to replace the fan

43 views • 8 days ago



Belangrijkste conclusie



**Open source firmware vergroot
transparantie, beveiliging en keuzevrijheid.**

Coreboot maakt dit mogelijk.





NovaCustom

Bedankt voor jullie aandacht!



<https://novacustom.com>