NovaCustom

Heads Firmware Introduction and Future Plans

 :  + Heads

Content

- Dasharo Entry Subscription (Heads):
  - Advantage 1: Minimalistic design
  - Advantage 2: Integrity verification of the BIOS, kernel and boot process
  - Advantage 3: Native integration with Qubes OS
  - Costs
- Intel Boot Guard?
- Firmware update procedure
- Roadmap: plans for this year

#1/3: Minimalistic (compared to EDK-II)

- Reduced attack surface:
  - Smaller code means fewer potential backdoors
  - Improved feasibility to review and audit

+

Heads

#2/3: Integrity verification of key components

- Enhance security
- Key components verified:
  - BIOS/UEFI firmware: the firmware responsible for booting and initialising
  - Kernel: Core of the OS that manages system resources and essential services
  - Bootloader: The software responsible for loading the OS kernel into the memory (usually GRUB 2)
- How?
  - Measured boot: creating cryptographic hashes for each component
  - TPM hardware to securely store and attest to the integrity of the measurements
- Very early state

+

Heads

• #3/3: Native integration with Qubes OS

- Chain of trust
- Hardware based integrity check (TPM)
- Solid base, solid OS

+

Heads

QUBES OS

• Dasharo Entry subscription costs

- 60 EUR/year (+ VAT)
- Choose 1, 2 or 3 year(s) when purchasing
- To be renewed after expiry of subscription
- Not automatically continued
- Non-renewal means no further updates and support

+

Heads

• Intel Boot Guard (?)

- Protecting processor and firmware from unauthorised modifications
- Signed with digital signatures
- Great extra protection layer, BUT:
  - Keys are in hands of the manufacturer (normally)
  - Leak of keys (like MSI) could happen
  - Disallows end-users to modify firmware

  - What if we can give the keys to the end-user?
  -- Legal problems

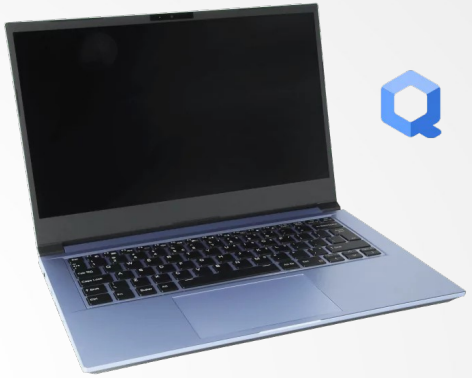
- CPU fusing (?)

Firmware update procedure

- Fwupd – update firmware within the OS (or trigger it)
- Flashrom: problem with EC firmware
- Not stored in main SPI flash
- Dasharo Tools Suite (DTS)
- Alternative update solution

Qubes OS certified

- NV41 Series
- Only NC-model for Entry subscription (Heads)
- Suspend (S3)



BE ACTIVE! LET'S SOLVE TOGETHER!

https://github.com/Dasharo/dasharo-issues/issues

Near future plans

2023:

- Dasharo Entry (Heads)
- Better update accessibility
- Bug resolves
- New firmware features:
  - UEFI setup password
  - SMM BIOS write protection
  - Early boot DMA protection
  - Network stack enable/disable
  - USB Stack enable/disable
- Physical anti-tamper solution

2024:

- 14th Gen Meteor Lake:
  - DDR5 and PCI 5
  - Dasharo for all models we offer
- New firmware features:
  - FlexiCharger (?)
  - Microphone + camera firmware switch (?)
  - WiFi + BT module switch (?)
  - Intel Boot Guard (???)

What firmware feature do you want?

Time for questions and further discussions.