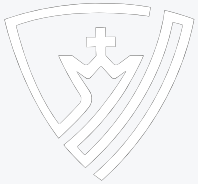
class: center, middle, intro

Tymoteusz Burak



Tymoteusz Burak

- *Junior Embedded Systems Developer*
- 1 year an 3mdeb
- Integration of functionalities into Zarhus OS
- tymoteusz.burak@3mdeb.com
- linkedin.com/in/tymoteusz-burak-a108252a0

Agenda

- Reminder: What is DCU?
- What we envisioned
- Current Status
- The problem
- Our solution
- What does this mean to Dasharo users
- Example Scenario
- Q&A

Reminder: What is DCU?

The Dasharo Configuration Utility is a tool designed to configure Dasharo firmware binary images.

Until now there was support for

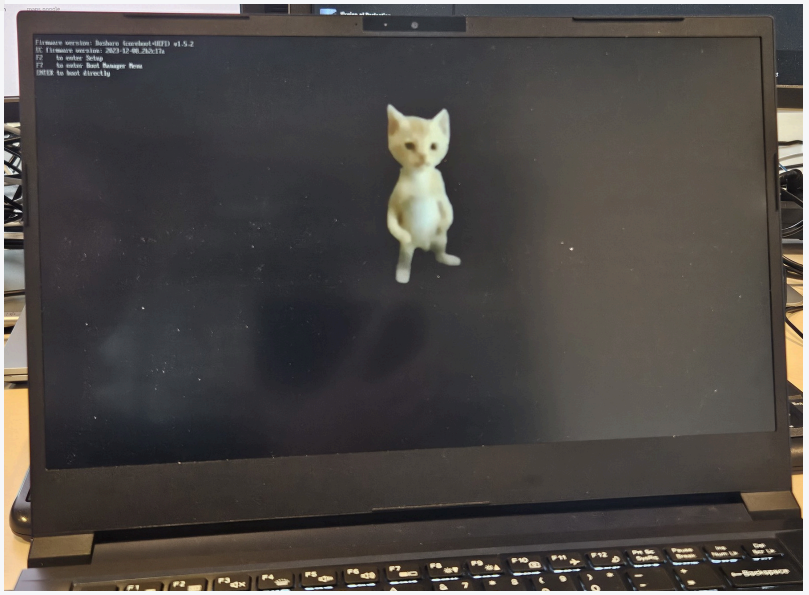
- Customizing the boot logo
- Setting unique UUIDs or Serial Numbers in SMBIOS tables

Reminder: What is DCU?

The Dasharo Configuration Utility is a tool designed to configure Dasharo firmware binary images.

```
$ ./dcuc logo coreboot.rom -l bootsplash.bmp
```

.center[



]

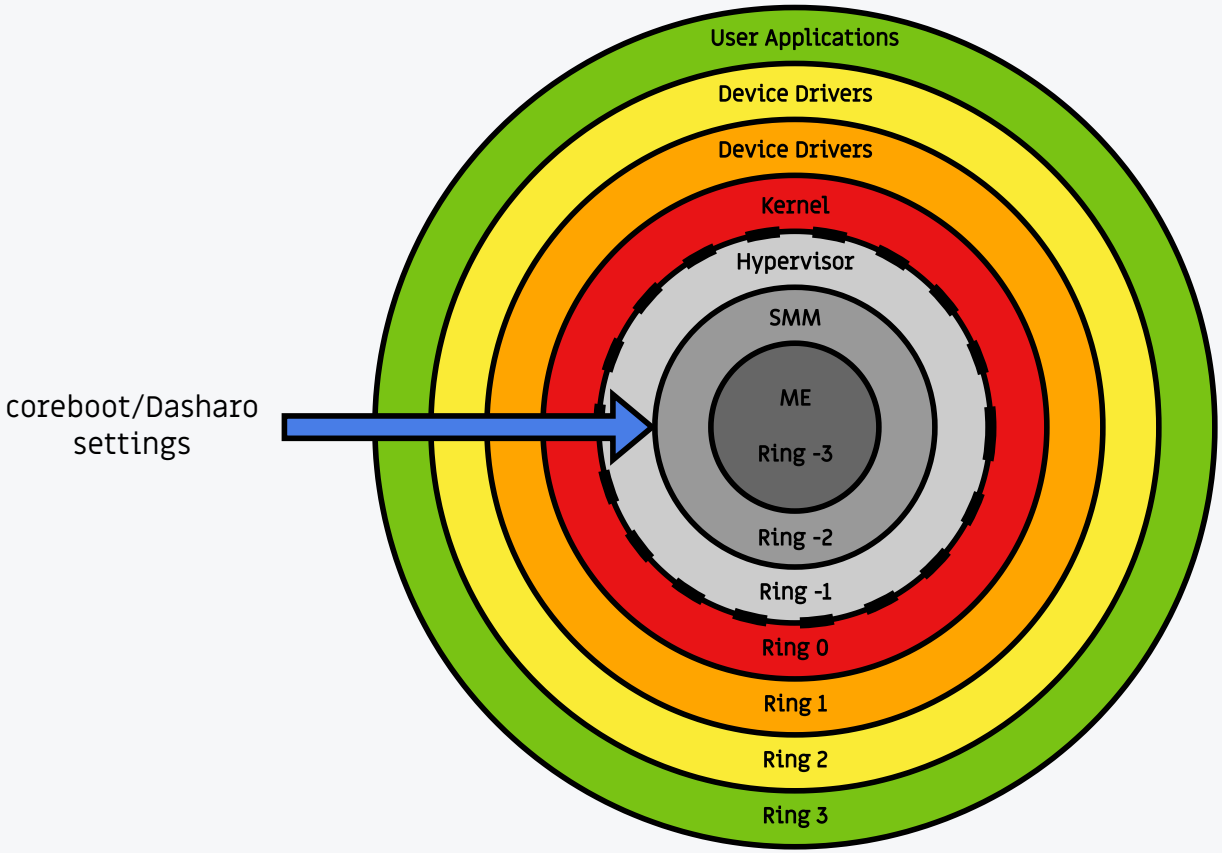
What we envisioned

- Custom Configuration Profiles
- Sane Defaults Verification
- Data Migration Tools
- Enterprise Security Features
- Chipsec and HSI Checks Integration
- Integration with Commercial Tools like Binarly

Current Status

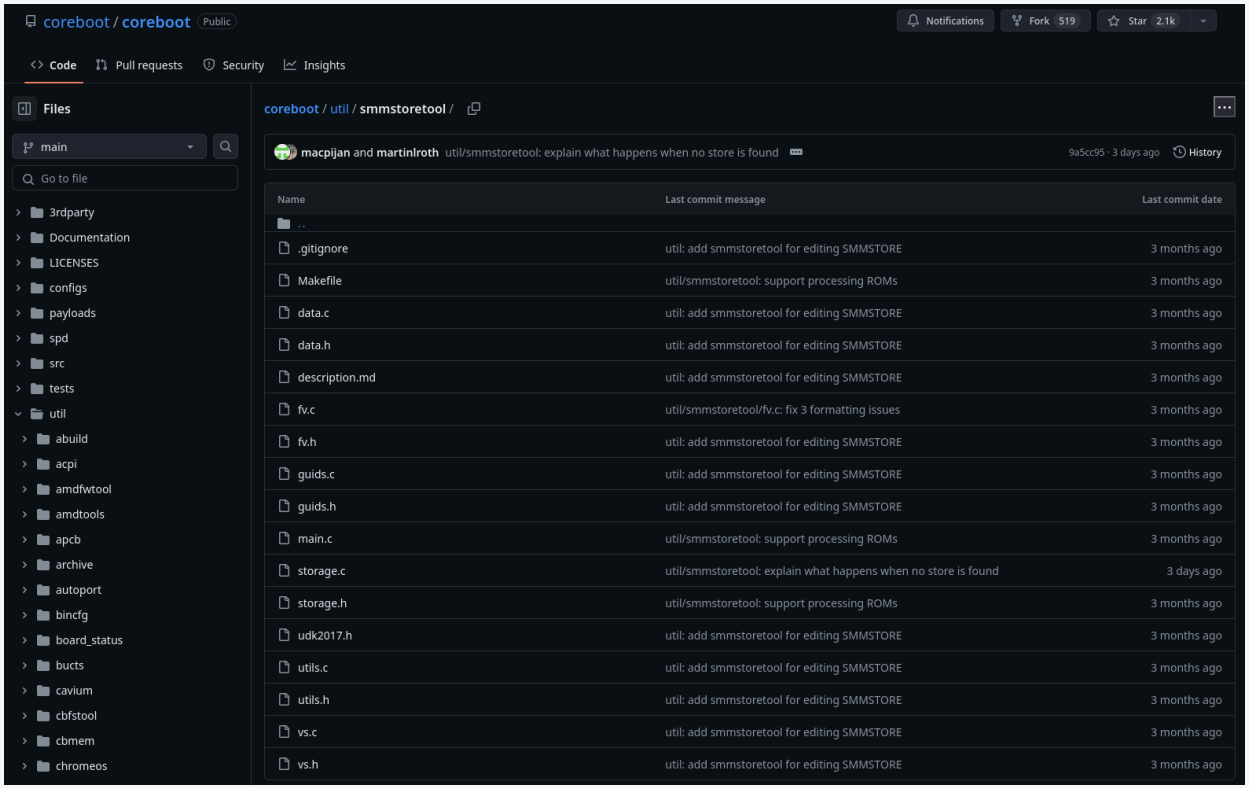
- ~~Custom Configuration Profiles~~
- ~~Sane Defaults Verification~~
- ~~Data Migration Tools~~
- ~~Enterprise Security Features~~
- ~~Chipsec and HSI Checks Integration~~
- ~~Integration with Commercial Tools like Binarly~~

The problem



Our solution

smmstoretool



What does this mean to Dasharo users

- Get a list of settings in a binary:

```
$ ./dcuc variable --list coreboot.rom
Settings in coreboot.rom:
NAME        VALUE            ACCEPTED VALUES
MeMode      Enabled          Enabled / Disabled (Soft) / Disabled (HAP)
```

- Change a setting:

```
$ ./dcuc variable coreboot.rom --set "MeMode" --value "Disabled (Soft)"
```

```
$ ./dcuc variable --list coreboot.rom
Settings in coreboot.rom:
NAME        VALUE            ACCEPTED VALUES
MeMode      Disabled (Soft)  Enabled / Disabled (Soft) / Disabled (HAP)
```

What does this mean to Dasharo users

- **Get a list of settings supported by this tool:**

```
$ ./dcuc variable --list-supported coreboot.rom
Settings that can be modified using this tool:
NAME                        ACCEPTED VALUES
LockBios                    Disabled / Enabled
NetworkBoot                 Disabled / Enabled
UsbDriverStack              Disabled / Enabled
SmmBwp                      Disabled / Enabled
Ps2Controller               Disabled / Enabled
BootManagerEnabled          Disabled / Enabled
PCIeResizeableBarsEnabled   Disabled / Enabled
EnableCamera                Disabled / Enabled
EnableWifiBt                Disabled / Enabled
SerialRedirection           Disabled / Enabled
SerialRedirection2          Disabled / Enabled
MeMode                      Enabled / Disabled (Soft) / Disabled (HAP)
FanCurveOption              Silent / Performance
CpuThrottlingThreshold      0-255 (Actual supported values may vary)
```

Example Scenario

Example Scenario

```
$ git clone https://github.com/Dasharo/dcu.git
$ cd dcu
```

Example Scenario

```
$ ./dcuc variable --list-supported msi_ms7d25_v1.1.3_ddr4.rom
Settings that can be modified using this tool:
NAME                          ACCEPTED VALUES
LockBios                    Disabled / Enabled
NetworkBoot                 Disabled / Enabled
UsbDriverStack              Disabled / Enabled
SmmBwp                      Disabled / Enabled
Ps2Controller               Disabled / Enabled
BootManagerEnabled          Disabled / Enabled
PCIeResizeableBarsEnabled   Disabled / Enabled
EnableCamera                Disabled / Enabled
EnableWifiBt                Disabled / Enabled
SerialRedirection           Disabled / Enabled
SerialRedirection2          Disabled / Enabled
MeMode                      Enabled / Disabled (Soft) / Disabled (HAP)
FanCurveOption              Silent / Performance
CpuThrottlingThreshold      0-255 (Actual supported values may vary)
```

Example Scenario

```
$ ./dcuc variable --list msi_ms7d25_v1.1.3_ddr4.rom
Settings in msi_ms7d25_v1.1.3_ddr4.rom:
No firmware volume header present
No valid firmware volume was found
Failed to find variable store in "msi_ms7d25_v1.1.3_ddr4.rom"
NAME                          VALUE                         ACCEPTED VALUES
```

Example Scenario

```
$ ./dcuc variable msi_ms7d25_v1.1.3_ddr4.rom --set "SerialRedirection" --value "Enabled"
No firmware volume header present
No valid firmware volume was found

The variable store has not been found in the ROM image
and is about to be initialized. This situation is normal
for a release image, as the variable store is usually
initialized on the first boot of the platform.

Successfully created variable store in "msi_ms7d25_v1.1.3_ddr4.rom"
Successfully set variable SerialRedirection in the variable store.
```

Example Scenario

Q&A