Morello Board
booting procedure with capabilities passing

Dept. of Computer Science and Technology
Univ. of Cambridge
(Jan 2023)
carlos.molina@cl.cam.ac.uk

Legend:
MCC: Motherboard Configuration Controller
AP: Application Processor
PCC: Platform Configuration Controller
SCP: System Control Processor
MCP: Manageability Control Processor
IOFPGA:

```
                    ┌─────────────────┐
                    │     power       │
                    │  switched on    │
                    └─────────────────┘
                             │
                             ▼
```

MCC executes initial setup:
a) enables UART and power
b) takes PCC out of reset

MCC
a) enables PCC
b) loads IOFPGA image from SD card

SCP and MCP run their code:
a) SCP sets up SoC

AP executes its firmware code
a) ARM trusted firmware runs with boot time capabilities: data access and instruction fetch allowed across full addr space and all cap tags are cleared in memory
b) Control is transferred to UEFI bootloader which is verified and will act as root of trust in this secure boot.
c) caps under monotonicity principle are passed from firmware to bootloader.

bootloader is executed:
a) initiates memory map
b) initiates drivers

bootloader looks for a device (USB stick, SATA disk, remote device, etc.) with a boot sector.

boot manager
a) executes all (three) boot stages to load the kernel.
a) caps are passed (from stage to stage) to the kernel.

kernel creates user proc and passes caps:
a) caps passed are restricted (eg, access only to specific range of mem addr

user proc executes
a) user proc might pass caps to functions and other user processes.
b) kernel clears all caps when user proc terminates.