Open and Secure System Firmware and Architecture

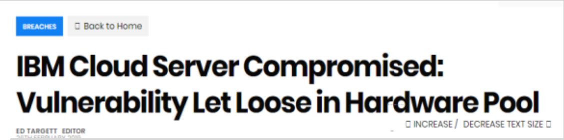
Todd Takken
Todd Rosedahl
Sandhya Koteshwara
Yutaka Sugawara
IBM

Outline

- Motivation
    - Security problems
    - Lack of openness
- OpenBMC
- LibreBMC
- Secure vs. measured boot
- Platform Root of Trust Architecture
- Firmware Attestation, SPDM, Keylime
- Platform progression
    - x86 server with OpenBMC, (partially) open platform firmware.
    - FPGA-based Root of Trust card
    - RoT algorithm functions
- IBM’s Long-term vision

Copyright IBM 2022

Motivation: Security problems

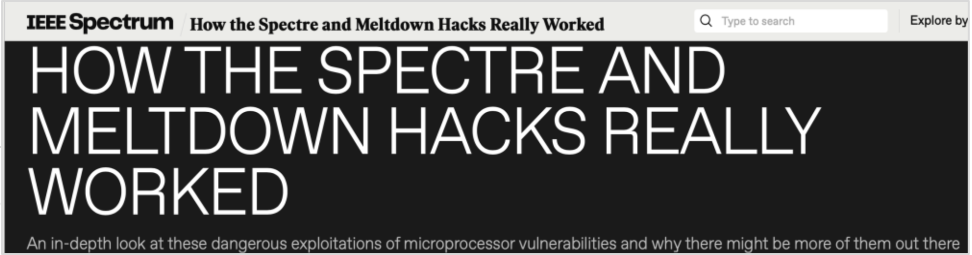


BREACHES □ Back to Home

IBM Cloud Server Compromised: Vulnerability Let Loose in Hardware Pool

ED TARGETT EDITOR

□ INCREASE / DECREASE TEXT SIZE □



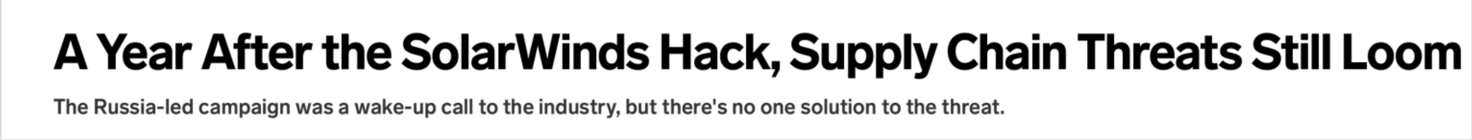
IEEE Spectrum How the Spectre and Meltdown Hacks Really Worked

Type to search

Explore by

HOW THE SPECTRE AND MELTDOWN HACKS REALLY WORKED

An in-depth look at these dangerous exploitations of microprocessor vulnerabilities and why there might be more of them out there

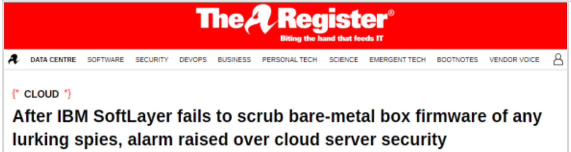


WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

LILY HAY NEWMAN SECURITY 12.08.2021 06:23 PM

A Year After the SolarWinds Hack, Supply Chain Threats Still Loom

The Russia-led campaign was a wake-up call to the industry, but there's no one solution to the threat.

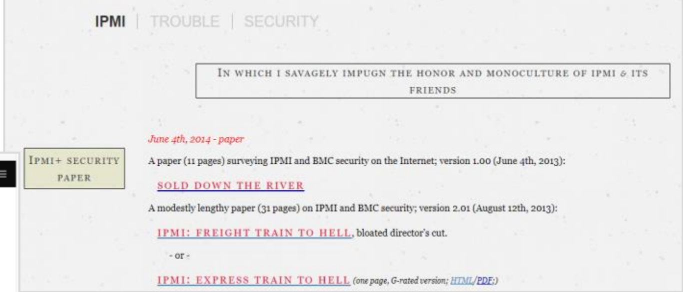


The Register® Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES VENDOR VOICE

{* CLOUD *}

After IBM SoftLayer fails to scrub bare-metal box firmware of any lurking spies, alarm raised over cloud server security



IPMI | TROUBLE | SECURITY

IN WHICH I SAVAGELY IMPUGN THE HONOR AND MONOCULTURE OF IPMI & ITS FRIENDS

IPMI+ SECURITY PAPER

June 4th, 2014 - paper

A paper (11 pages) surveying IPMI and BMC security on the Internet; version 1.00 (June 4th, 2013):

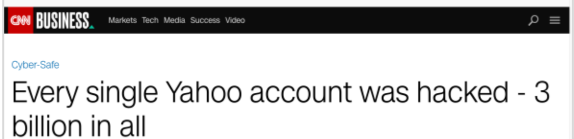
SOLD DOWN THE RIVER

A modestly lengthy paper (31 pages) on IPMI and BMC security; version 2.01 (August 12th, 2013):

IPMI: FREIGHT TRAIN TO HELL, bloated director's cut.

- or -

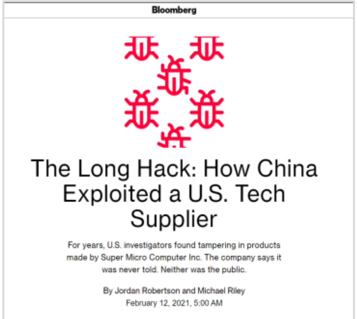
IPMI: EXPRESS TRAIN TO HELL *(one page, G-rated version; HTML/PDF;)*



CNN BUSINESS Markets Tech Media Success Video

Cyber-Safe

Every single Yahoo account was hacked - 3 billion in all

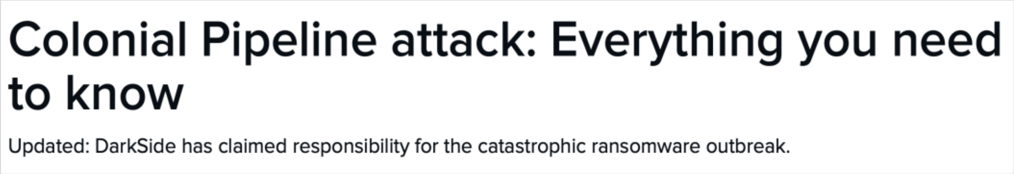


Bloomberg

The Long Hack: How China Exploited a U.S. Tech Supplier

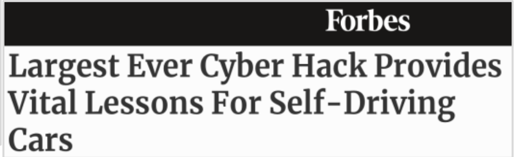
For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it was never told. Neither was the public.

By Jordan Robertson and Michael Riley
February 12, 2021, 5:00 AM



Colonial Pipeline attack: Everything you need to know

Updated: DarkSide has claimed responsibility for the catastrophic ransomware outbreak.



Forbes

Largest Ever Cyber Hack Provides Vital Lessons For Self-Driving Cars

Motivation: Current Solutions Are Not Open

- Many solutions are NOT open:
  - Some low-cost, discrete RoT and BMC chips, available only with proprietary firmware
- Processor firmware (x86, ARM, etc) needs to be open
  - Need fully open firmware/software to be secure
  - End customer needs to be able to see/validate the firmware
- All firmware must be developed in the open, not just opened up after the fact
- Long term IBM Research vision:
  - All open, All DC-SCM, All LibreBMC, 1 Solution across IBM.

- Join us to solve these problems together!

Copyright IBM 2022

OpenBMC

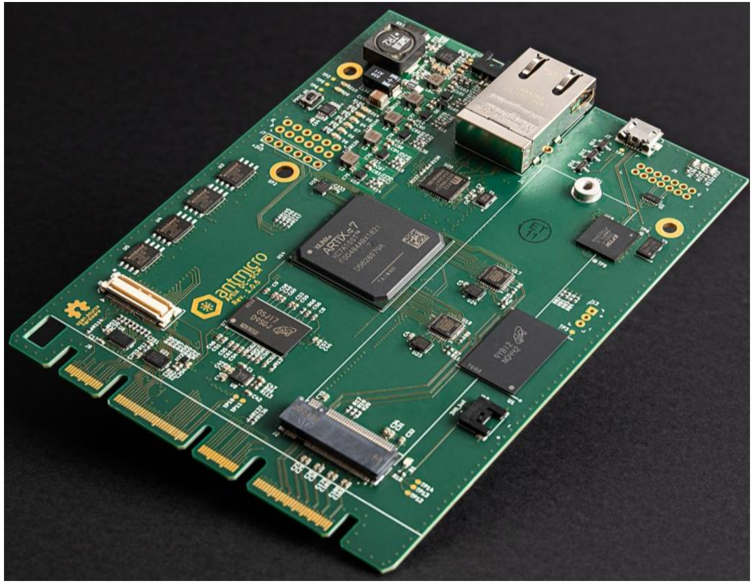
- An Open-Source Baseboard Management Controller firmware stack
  - Contributed to and supported by many large companies (IBM, Google, Intel, Meta, etc)
  - Robust and secure designs utilizing the best designers in the industry
- Provides simplified management of:
  - Environment
  - Inventory
  - Sensors and event logs
- Provides an embedded Linux stack
  - Linux Kernel 4.10, Yocto 2.2.2, python, SSH
- Applications communicate via D-Bus
- External communication via Redfish or IPMI

- Currently runs on POWER platforms:
  - P8 -- Barreleye, S822LC
  - P9 -- Zaius, Barreleye, Romulus, and AC922
  - **P10 – S1022, S1024**
  - Supports AST2400/AST2500/AST2600 BMC processors

Copyright IBM 2022

LibreBMC with a DC-SCM card – an open HW/SW BMC solution

- Connects and boots an IBM AC922
  - Replaces the existing BMC card
- BMC is an FPGA
  - Open ISA (POWER ISA)
  - Open Core (microwatt)
  - Open Peripherals with Lite-X
  - OpenBMC firmware
- Uses the DC-SCM/DC-SCI standards
- Complete Openness for enhanced security – allows HW security patches in the field.

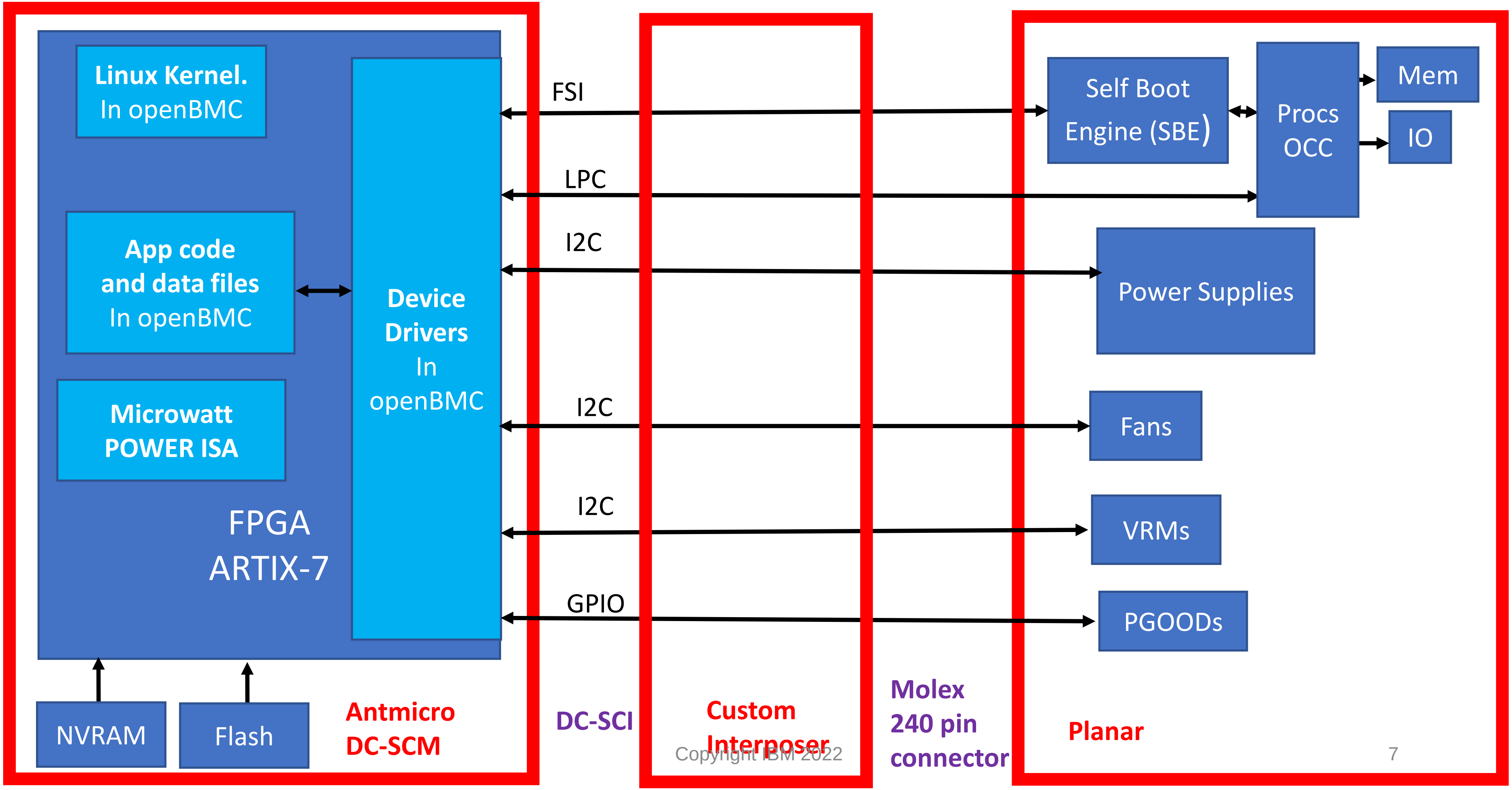


LibreBMC: https://git.openpower.foundation/librebmc/librebmc

Demo Video: https://www.youtube.com/watch?v=YYNegXDsRoU

Copyright IBM 2022

LibreBMC Architecture–IBM AC922–Antmicro DC-SCM



Copyright IBM 2022

LibreBMC -- Software details/Status

- **AC922 boots and is fully operational using OpenBMC**
- Linux kernel running on microwatt
- Bit banging kernel drivers (I2C, FSI)
- Fan controllers via I2C
- LPC:
  - Host console – 16550 UART
  - Host firmware via LPC FW/IPMI BT
- See the Demo at: https://www.youtube.com/watch?v=YYNegXDsRoU
- See the instructions at: https://git.openpower.foundation/librebmc/librebmc

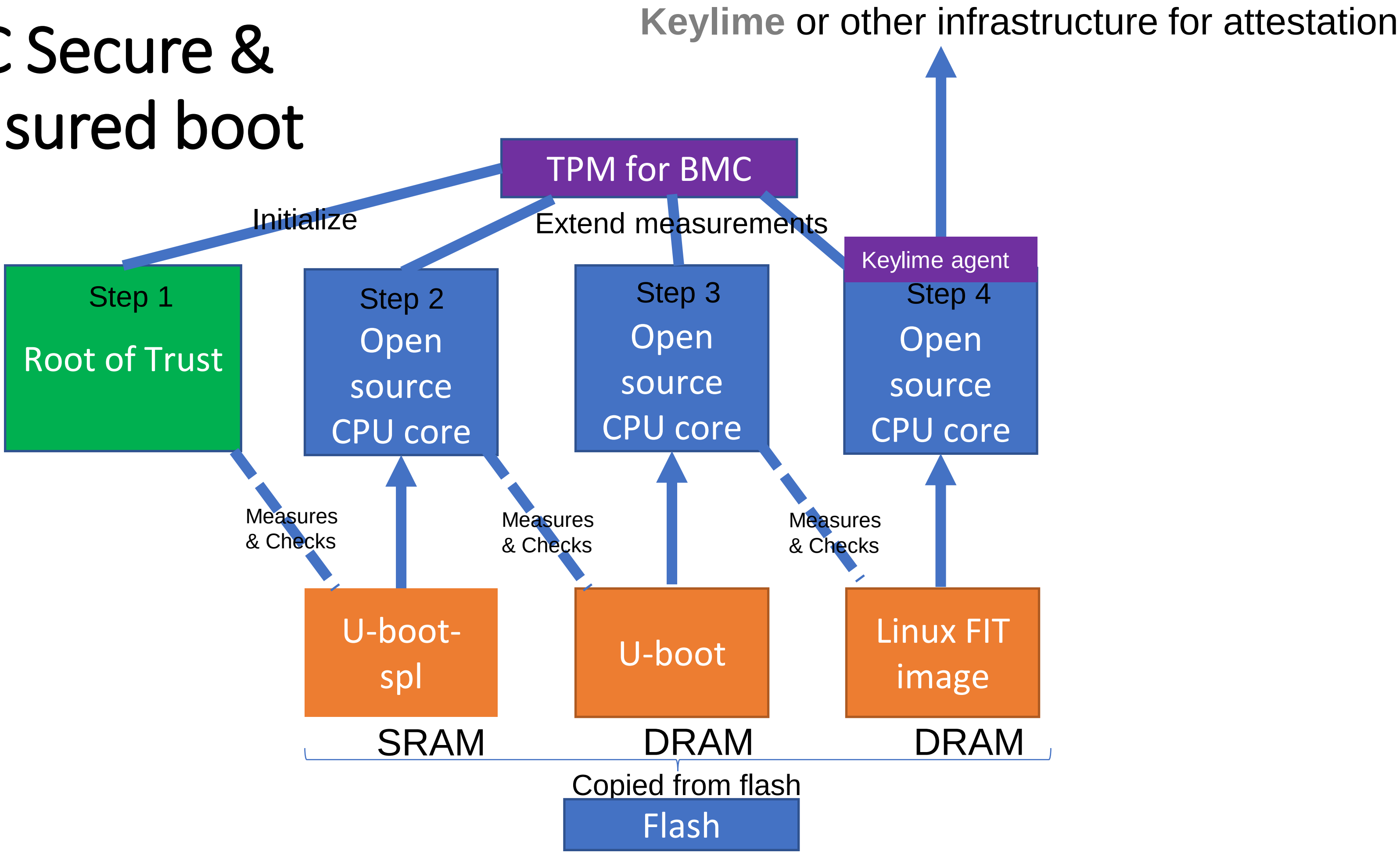
Copyright IBM 2022

Secure boot and Measured boot

- Secure Boot is active:
  - measures firmware images for provenance (encrypted signature of originator) and integrity (hash checking) before the image is loaded.
  - If it fails, it invokes a recovery procedure.
- Measured Boot is passive:
  - measurements and logs are taken while the software goes through the boot stages
  - digests of the measurements are stored in the TPM for purposes of authenticating the boot log.
- Measured Boot is also more expansive than secure boot:
  - Can also cover configuration parameters, peripherals, etc.
- The salient features of Measured Boot are:
  - "root of trust" -- the TPM device must be initialized by secure, preferably immutable, code early in the boot process
  - "chain of trust" -- each booted software component is measured before it runs and individual measurements are authenticated by the TPM device

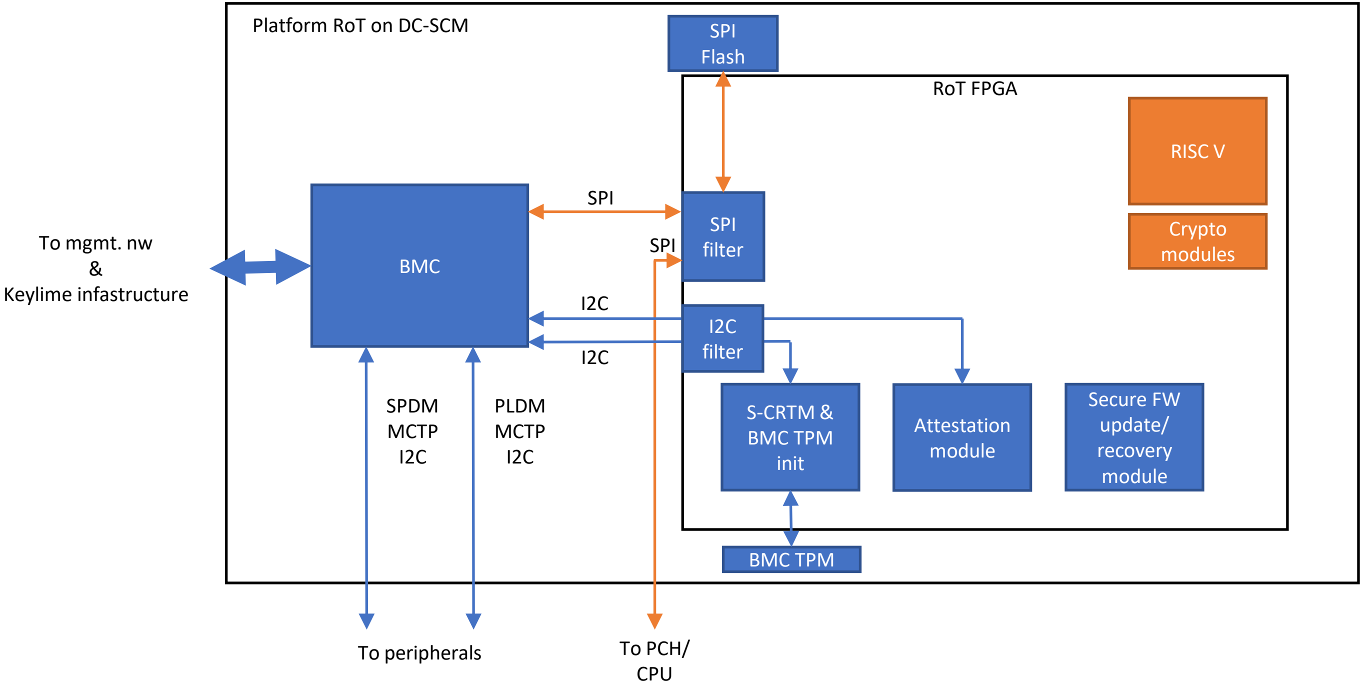
Copyright IBM 2022

BMC Secure & Measured boot



Copyright IBM 2022

Platform RoT architecture

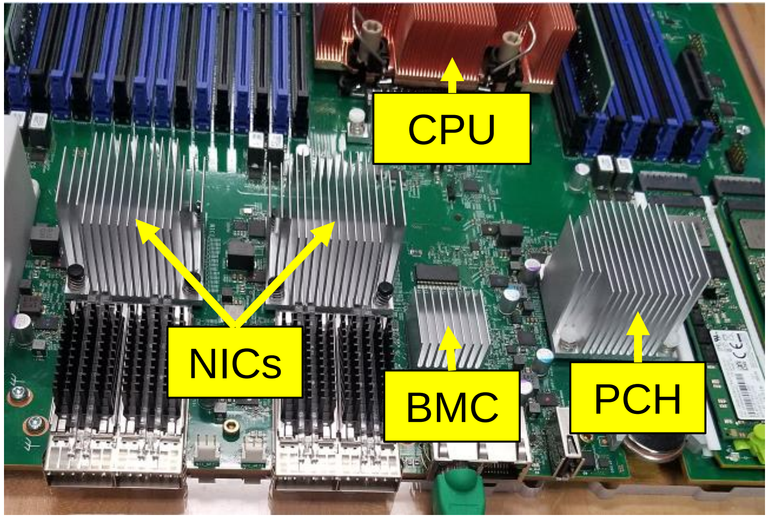


- Platform RoT = BMC + RoT FPGA
- Performs functions such as SPI filter, Attestation, Secure FW Update/Recovery, TPM initialization etc.
- Attestation of peripherals using SPDM (Security Protocol and Data Model)
- Satisfies NIST PFR 800-193 guidelines for the platform
- Complete solution and based on open-source design (hardware and software)

Copyright IBM 2022

IBM SBP1 - x86 Server with OpenBMC

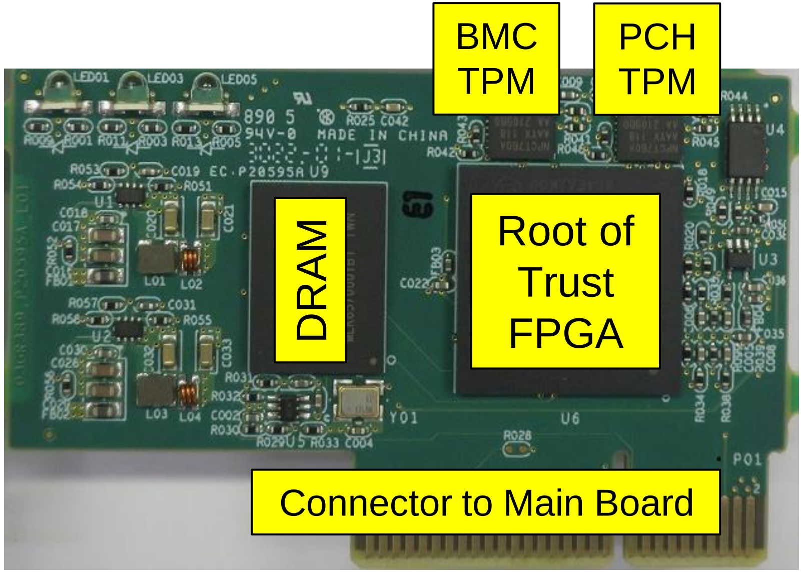
- IBM's Secure Boot Platform
  - Four Sapphire Rapids processors
  - Baseboard Management Controller (BMC)
    - Aspeed AST2600 BMC chip
    - OpenBMC, fully uploaded to the community
    - BMC controls power sequencing and clocking
  - Open platform firmware configuration
    - Intel Platform Control Hub (PCH) chip
    - Intel Firmware Support Package (FSP)
    - Coreboot open-source bootloader
  - System in laboratory bring-up now

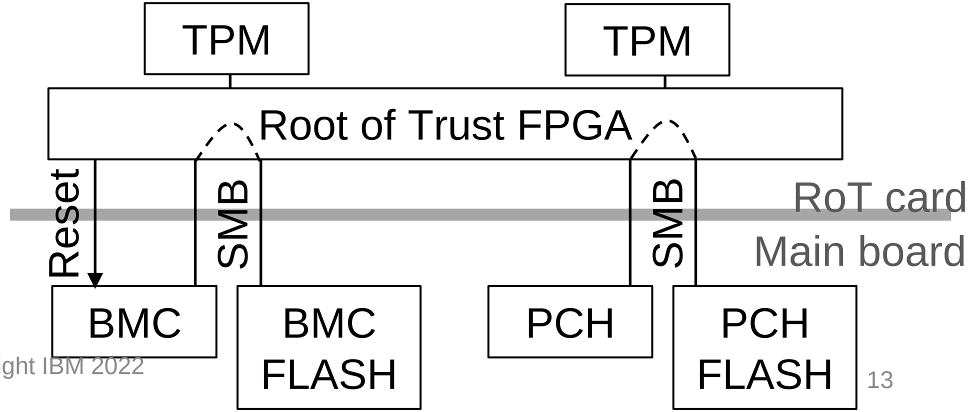


Copyright IBM 2022

Root of Trust Card for SBP1

- Add Root of Trust (RoT) features to open firmware platform
  - RoT in programmable FPGA
    - Boots first
    - controls busses to FLASH
    - Takes BMC out of reset
    - Manages TPM access

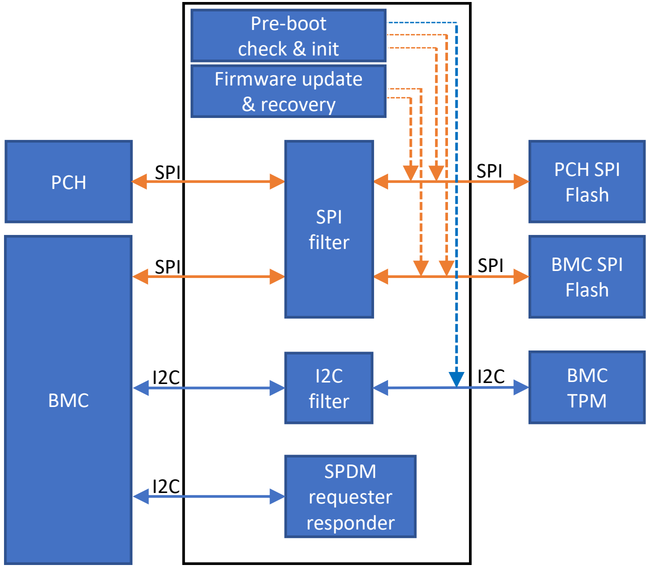




Copyright IBM 2022

Root of Trust Functions

- Pre-boot check/initialization for BMC/PCH secure & measured boot
  - Cryptographically verify the first stage BMC/PCH boot code
  - Initialize BMC/PCH TPMs for subsequent measured boot
- BMC/PCH firmware update & recovery
  - Update firmware in SPI FLASH, and
  - Recover SPI FLASH contents when all images are corrupted
  - Images downloaded from control plane with cryptographic checks
- SPI FLASH protection filter
  - Block bad command opcodes, illegal write addresses, and wear-out attacks
- I2C TPM protection filter
  - Address protection, write protection, command-length limits
- SPDM for pre-boot device attestation
  - SPDM master: At power-on/reset: RoT attests BMC before it boots
  - SPDM responder: after BMC boots and becomes SPDM master



Copyright IBM 2022

IBM Research’s Long-Term Vision

- IBM’s vision for an open Secure Control Module (SCM)
  - Open card hardware based on the DC-SCM standard
  - Open chip hardware, FPGA-based, for Root of Trust and BMC
  - OpenBMC firmware
  - Root of Trust features in open firmware
- Open means truly open!
  - Not just visible/inspectable but open under an Apache License, Version 2.0

Copyright IBM 2022

Join the Action

- LibreBMC: https://openpower.foundation/groups/librebmc/
    - The forum and all information is free and completely open to all
    - We meet every other week. One European time slot(10am Central) and one Australian (5pm Central)
        - Agendas and recordings are made public
    - Buy your own AC922: https://www-store.shop.ibm.com/shops/ips/product/server-18335-model-gth
- DC-SCM link: https://www.opencompute.org/wiki/Hardware_Management/Hardware_Management_Module
- Lite-X link: https://github.com/enjoy-digital/litex
- Open POWER ISA link: https://openpowerfoundation.org/tag/power-isa/
- Microwatt link: https://en.wikipedia.org/wiki/OpenPOWER_Microwatt
- OpenBMC: https://github.com/openbmc

Copyright IBM 2022

Thank you!

© 2022 International Business Machines Corporation IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT, SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. Client examples are presented as illustrations of how those clients have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. Not all offerings are available in every country in which IBM operates. Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.