Linux Plumbers Conference 2019

Contribution ID: **284** Type: **not specified**

Secure and Trusted boot in OpenBMC

Wednesday, 11 September 2019 15:00 (20 minutes)

The OpenBMC project has brought modern Linux to the firmware in your new server. A missing piece of this is ensuring the firmware is the image you expect it to be running.

The next generation of BMC hardware will allow a hardware root of trust to secure the boot chain. This talk will present the a proposed design for trusted boot in OpenBMC.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary author: STANLEY, Joel (IBM)

Presenter: STANLEY, Joel (IBM)

Session Classification: System Boot and Security MC