Contribution ID: **231** Type: **not specified**

Lamenting on Secure Boot, module signatures and shims

Secure boot intend to be a way for OEMs to ensure only trusted software is capable of booting on the machines. For Linux distributions this is mostly being done by utilizing a pre-bootloader shim which is signed by a UEFI Certificate Authority, and unique for each individual Linux distribution.

One of the promises of Secure Boot was the intention of having users be able to regain control of the platform, and selectively enroll keys they would like to trust. Recently this has become problematic as module signatures are locked behind the shim, removing some certificates from the chain can prevent machines from booting and we are seeing a push away from OEMs trusting the CA at all.

This talk will give an introduction of Secure Boot is used by Linux distros and how we got here.

I agree to abide by the anti-harassment policy

Yes

Primary author: LINDERUD, Morten (Independent)

Presenter: LINDERUD, Morten (Independent)

Session Classification: System Boot and Security MC

Track Classification: LPC Microconference: System Boot and Security MC