UEFI Secure Boot

Ard Biesheuvel <ard.biesheuvel@linaro.org>
UEFI Secure Boot - current status on AArch64

- Essentially the same as a year ago
  - Software layers above the non-volatile variable store are working and regression tested through CI (both AArch64 and ARM)
  - No implementation exists to make the non-volatile variable store tamper proof and replay protected, as the UEFI Secure Boot spec requires

- What is holding us back?
  - Spec based reference implementation of the tamper proof varstore requires (S)MM support, which is not even in the spec yet for AArch64.
  - Non-spec based ref implementation is likely too platform specific, which complicates sharing between members and/or open sourcing

- Is there a plan B?
  - External manipulation of PK/KEK/db/dbx variables, while making them immutable from the OS/firmware pov. Stop gap solution, but effective
Thank You

#LAS16
For further information: www.linaro.org
LAS16 keynotes and videos on: connect.linaro.org