Contribution ID: **129** Type: **not specified**

Secure boot without UEFI: booting VMs on Power(PC)

Thursday 27 August 2020 07:10 (20 minutes)

Much of the Secure and Trusted Boot ecosystem is built around UEFI. However, not all platforms implement UEFI, including IBM's Power machines.

In this talk, I present a proposal for secure boot of virtual machines on Power. This is an important use case, as many Power machines ship with a firmware hypervisor, and all user workloads run as virtual machines or "Logical Partitions" (LPARs).

Linux Virtual Machines on Power boot via an OpenFirmware (IEEE1275) implementation which is loaded by the hypervisor. The OpenFirmware implementation then loads grub from disk, and grub then loads Linux. To secure this, we propose to:

- Teach grub how to verify Linux-module-style "appended signatures". Distro kernels for Power are already signed with these signatures for use with the OpenPower 'host' secure boot scheme.
- Sign grub itself with an appended signature, allowing firmware to verify grub.

We're really interested in feedback on our approach. We have it working internally and are preparing it for upstreaming, so now is the ideal time for us to get community input and answer any questions on the overall design and high-level implementation decisions.

I agree to abide by the anti-harassment policy

I agree

Primary author: AXTENS, Daniel (IBM)

Presenter: AXTENS, Daniel (IBM)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC