Secure Boot without UEFI: Booting VMs on Power(PC)

—

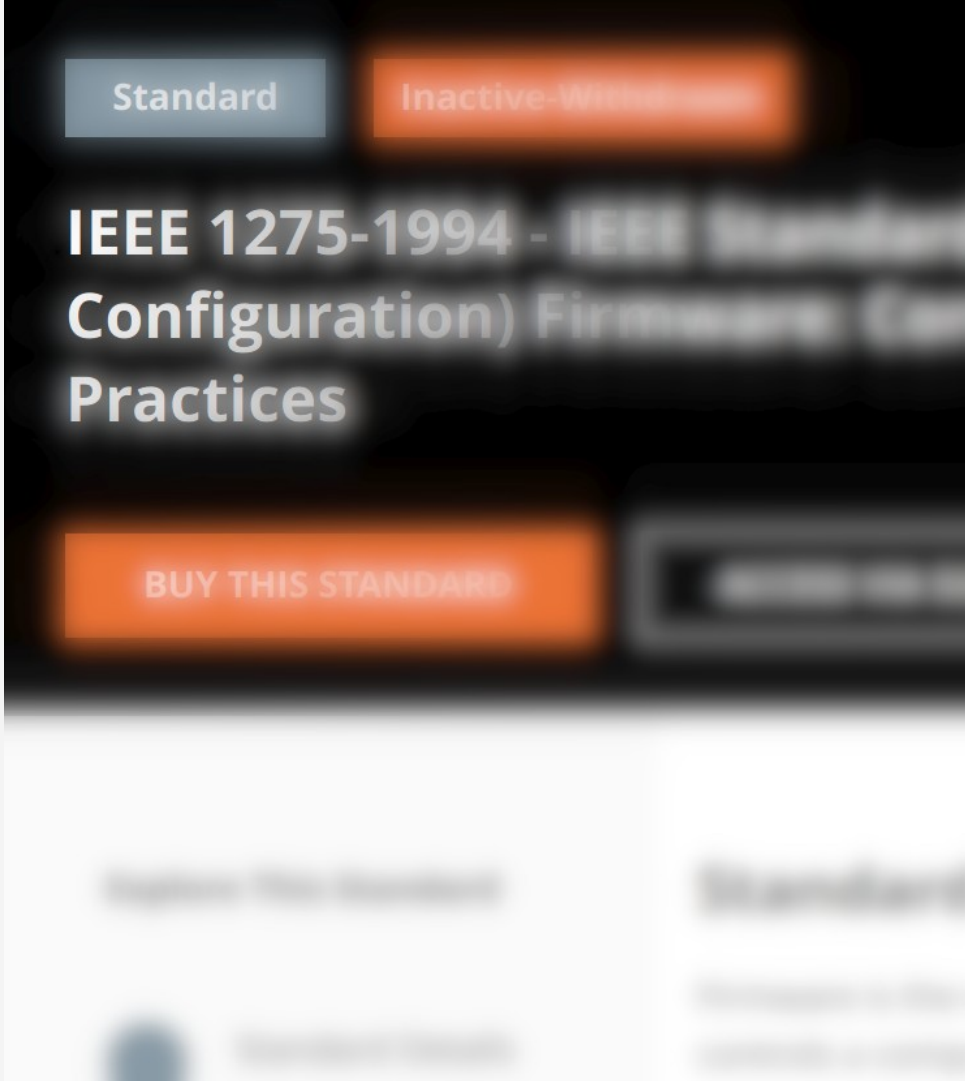
Daniel Axtens
Linux Security Engineer

IBM

Contents

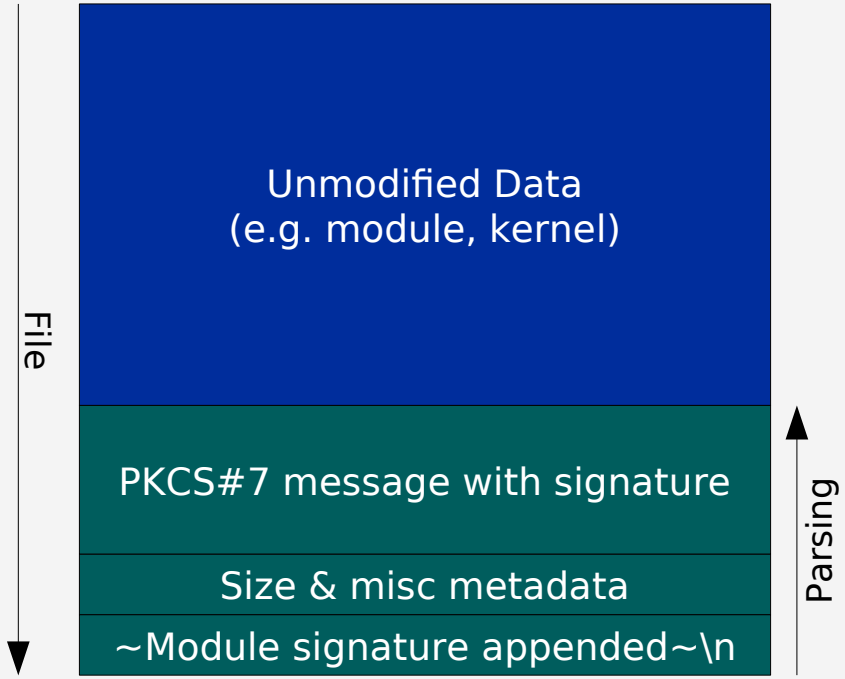
powerpc-ieee1275

- OpenFirmware (IEEE1275) environment.
- Device Tree based configuration.
- 32-bit BE ELF bootloader. Usually loaded from the PReP partition. No file system - raw bytes on disk.
  - UEFI: PE bootloader, EFI system partition has a filesystem
- Used for VMs/Logical Partitions (LPARs) on modern Power Systems, and for old Macs.



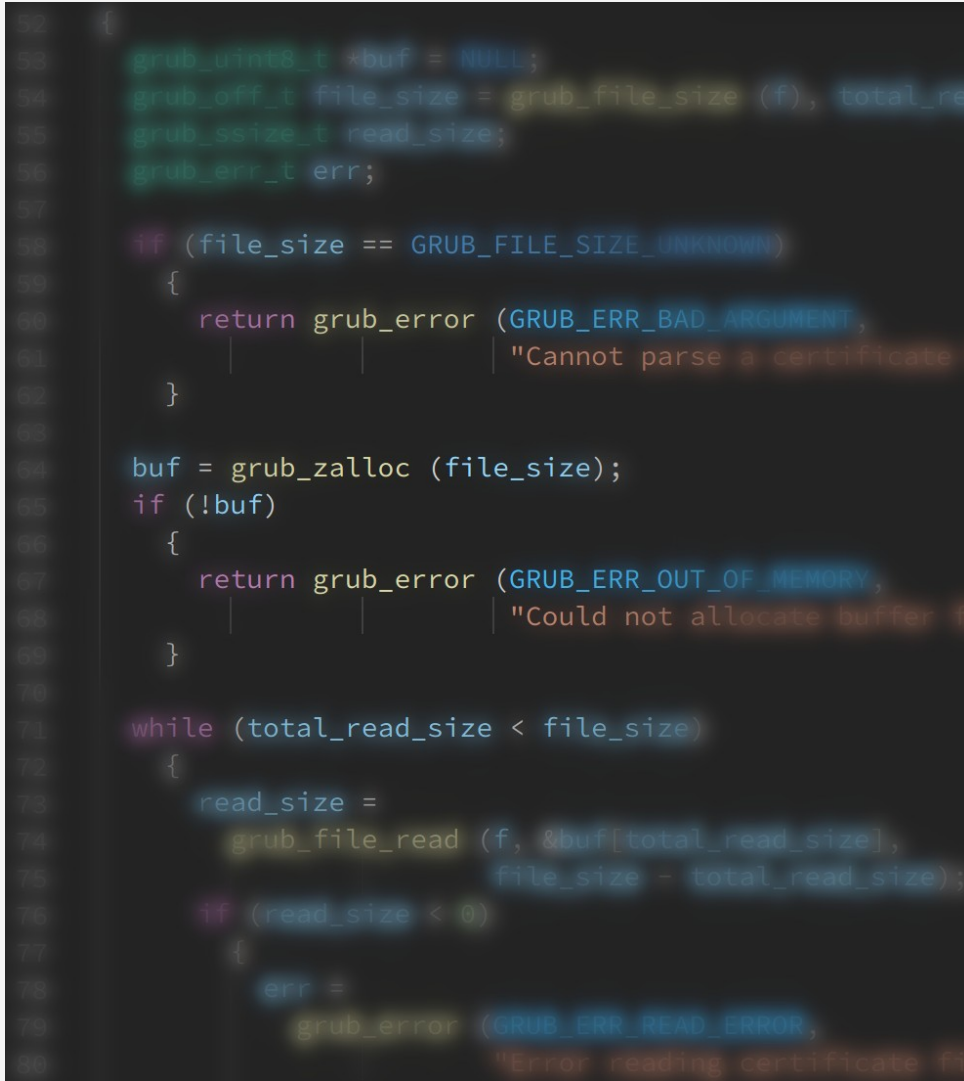
Appended Signatures

- Originally used to sign Linux kernel modules.
- Can be used to sign kernels, verified by IMA on kexec.
- Distros sign ppc64le kernels like this already for OpenPower secure boot.



Verifying Linux from Grub

- **Teach grub to verify appended signatures with an x509 certificate.**
- Use existing grub features and concepts: e.g. verifier interface.
- Write as little crypto-adjacent code as possible:
  - PKCS#7 and x509 are based on ASN.1: import libtasn1.
  - Borrow PKCS#7 and x509 definitions from GnuTLS.
  - Use existing gcrypt code to do the actual maths.



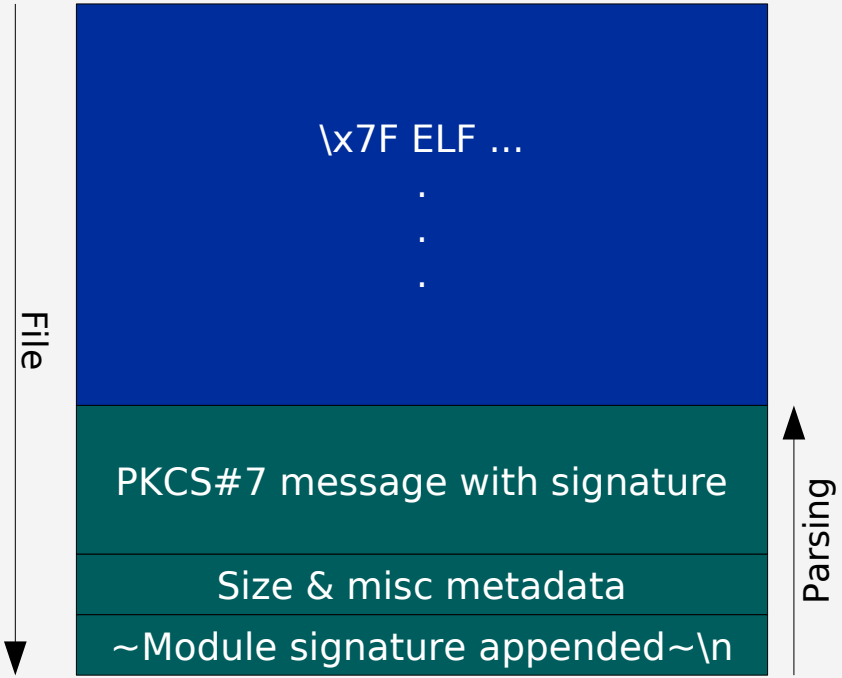
Demo time

Booting
https://asciinema.org/a/kgDMBoZx9pNqGzkhZ70kkosVz

Commands
https://asciinema.org/a/kqhuUA70CuETzI4RDkkL1hXf7

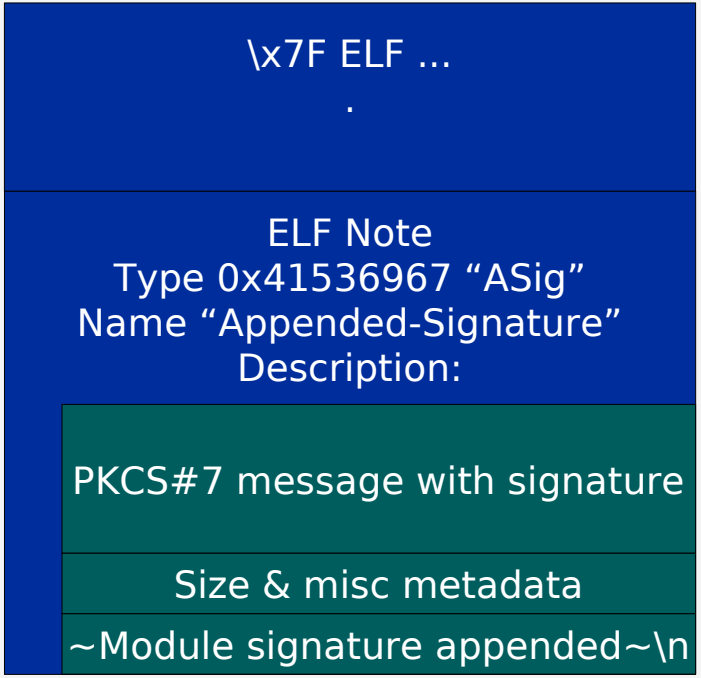
Verifying Grub from Firmware

- **Must be backwards compatible!**
- If we use an appended signature, how does FW know if it is present?
  - Grub loaded from PReP partition: no file system, no file size, no clear EOF.
  - Cannot ‘keep scanning’: you could hit an old signature.
  - Length of signature varies depends on signing key and hash type.



Appended Signature Note

- We want:
  - all data to be within ELF structures
  - an ordinary appended signature that usual, unmodified tools understand
- **Add a new SHT_NOTE section at the end of the binary to contain the signature.**
  - descsz = ALIGN(signature size, 4)
  - Padding at the start of description, so appended signature magic is always at the end of the file.



Signing flow

Sign empty file to determine signature size.

Use new grub-mkimage parameter to reserve space for the signature.

Generates a valid ELF file with a note but the description is all zeros.

Truncate the excess zeros away.

Sign with usual tools.

Upstream status

Verification of Grub from Firmware with Appended Signature ELF note:

Already on list:
https://lists.gnu.org/archive/html/grub-devel/2020-08/msg00037.html

Note specification will be submitted for possible inclusion in forthcoming Power Architecture Platform Reference.

Verification of Linux from Grub:

Internal reviews and cleanup underway

Thank you

Daniel Axtens
Linux Security Engineer
—
daniel.axtens1@ibm.com
dja@axtens.net

The views expressed in this presentation are those of the author, not necessarily those of IBM.