GRUB

Project Status Update

Daniel Kiper
*Oracle, Software Developer, GRUB upstream maintainer*

FOSDEM 2022, February 7th, 2021
Content

1. What happened during last year
2. Where we are today
3. Some stuff for reading
What happened during last year

• GRUB 2.06 release which contains
  • The BootHole fixes, many folks and companies involved
  • The BootHole2 fixes (many folks and companies involved) including among others
    • 8 CVE fixes
    • 36 Coverity fixes
    • UEFI Secure Boot Advanced Targeting (SBAT)
    • Stack protector implementation
    • Lockdown support
    • Improved verifiers framework
  • The module for retrieving SMBIOS information, David Michael
  • Initial the LUKS2 support, Patrick Steinhardt
  • A lot of cryptodisk and LUKS2 updates, Glenn Washburn
  • Bump miniLZO to 2.08, Peter Jones
  • Addition of the MAINTAINERS and SECURITY files
  • ... and plenty of other fixes and cleanups
  • The GRUB 2.06~rc1 release allowed Fedora folks to shave off ~100 custom patches from Fedora 34
Where we are today

• No longer supporting small MBR gaps in the GRUB upstream
• Use full btrfs bootloader area, Michael Chang
• Properly handle gaps in btrfs extent item iteration, Qu Wenruo
• Major GRUB mm rework, Daniel Axtens, Patrick Steinhardt
• Support Argon2 KDF in LUKS2, Patrick Steinhardt
• Support for appended signatures, Daniel Axtens
• Add support for trusted boot on IBM PPC platform using a vTPM, Stefan Berger
• Drop Open Hack'Ware, an alternative firmware of PowerPC under QEMU, Daniel Axtens
• The cryptodisk code simplification, Glenn Washburn, Patrick Steinhardt
• Add cryptodisk detached headers and key files support, Denis 'GNUtoo' Carikli, Glenn Washburn, Patrick Steinhardt
• Use confidential computing provisioned secrets for disk decryption, James Bottomley
Where we are today

… continuation

- Tests improvements, Glenn Washburn
- Discussing tests automation for the GRUB upstream development
- Substantial docs updates, Glenn Washburn, Daniel Axtens and others
- More Coverity fixes for x86_64 UEFI, Alec Brown, Darren Kenny
- Add LoadFile2 and RISC-V Linux loader, Ard Biesheuvel, Atish Patra, Nikita Ermakov
- Bump miniLZO to 2.10, Colin Watson
- Add LoongArch support, Xiaotian Wu
- Support writing the GRUB modules in Rust (RFC), Daniel Axtens
- TrenchBoot work on hold due to ongoing discussions about the architecture
- … and bumped the GRUB release number to 2.11…
- The 2.12 release is planned around mid of 2022…
Some stuff for reading

• [SECURITY PATCH 00/28] Multiple GRUB2 vulnerabilities - BootHole

• [SECURITY PATCH 000/117] Multiple GRUB2 vulnerabilities - 2021/03/02 round

• UEFI Secure Boot Advanced Targeting (SBAT)
  https://github.com/rhboot/shim/blob/main/SBAT.md
Thank you

Daniel Kiper
daniel.kiper@oracle.com