ORACLE

GRUB

Project Status Update

Daniel Kiper

Oracle, Software Developer, GRUB upstream maintainer

FOSDEM 2021, February 7th, 2021

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Content

1. GRUB maintainers
2. What happened during last 2 years
3. What is happening right now
4. Pain points
5. Discussion about the community/distros expectations

GRUB maintainers

- Alexander Burmashev, Oracle
- Daniel Kiper, Oracle
- Vladimir 'phcoder' Serbinenko

- Alexander Graf takes care of RISC-V
- Leif Lindholm takes care of ARM and UEFI

What happened during last 2 years

- RISC-V support, Alexander Graf
- Initial Travis CI support, Alexander Graf
- Easier Gnulib bootstrap, Colin Watson (Ubuntu)
- IEEE1275 obdisk driver, Eric Snowberg (Oracle) on Debian folks request
- Intel MSR read/write modules, Jesús Diéguez Fernández
- Native DHCPv4 support, Andrei Borzenkov and Andre Przywara (arm)
- Build a.out output for sparc64 manually, John Paul Adrian Glaubitz
- GCC 9 and GCC 10 build support, Michael Chang
- clang 10 build support, Patrick Steinhardt and Daniel Axtens
- LUKS2 support, Patrick Steinhardt
- GRUB 2.04 release…
- …and plenty of fixes and cleanups including the BootHole bug ones…
- GRUB mini-summit organized by 3mdeb and Oracle, held in November 2020

The BootHole

- The initial issue was discovered and reported by Mickey Shkatov and Jesse Michael, both working for Eclypsium
- The security bug was discovered in the GRUB2 script parser
- This report initiated the GRUB code security review which took around 4 months
- During this work we discovered many integer overflows, some use-after-free issues, etc.
- The fixes would not be complete without shim and the Linux kernel changes and revocation of shims which could be used to load the broken GRUBs on UEFI platforms with Secure Boot enabled
- All GRUB fixes were posted in patch series containing 28 patches
- Around one hundred people from eighteen companies and organizations worked together to mitigate all discovered vulnerabilities: AMI, Bitdefender, Canonical, Cisco, Citrix, Debian, Dell, Eclypsium, Google, HP, HPE, Juniper, Microsoft, Oracle, Red Hat, SUSE, UEFI Security Response Team, VMware (presented in alphabetical order)

- https://www.eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/
- https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html
- https://blogs.oracle.com/linux/cve-2020-10713-grub2-boothole

What is happening right now

- GRUB 2.06 release
  - We are in code freeze now
  - The rc1 has been ready since December but final cut on hold due to translations build issues
- Close cooperation with the TrenchBoot project (https://github.com/TrenchBoot/documentation/)
  - Intel and Oracle are working on the Intel TXT implementation - RFC was posted at the beginning of May
  - We are planning to release next version of patches after the GRUB 2.06 release
  - 3mdeb is working on the AMD SKINIT implementation – it will be rebased on top of the Intel TXT one
- Red Hat is forward porting to the GRUB upstream patches carried in the Red Hat and Fedora GRUB
  - Around 50 custom patches will be dropped from the Red Hat and Fedora GRUB after GRUB 2.06 release
  - Other distros are encouraged to do the same thing for their own GRUB patches
- The firmware and bootloader log specification posted; got some comments; planning next version
- Ard Biesheuvel and Atish Patra are working on the UEFI LoadFile2 protocol initrd loader for Linux
- Daniel Axtens works on support for appended signatures
- Red Hat plans to use Linux kexec to load another OS from GRUB

What is happening right now

…continuation

- Finally we are planning to admit officially that GRUB upstream does not support 62 sectors MBR gap on i386-pc targets. This can be painful for some distros due to a shortage of simple migration mechanism to newer partitions layouts, e.g. GPT with BIOS boot partitions. However, on the other hand, it is not possible to cut the arbitrary code from the core.img endlessly. And at some point there would not be anything to cut… And we think that we are close to this point.
- ...and many more interesting new features under development...

Pain points

- Strongly delayed GRUB 2.06 release due to the BootHole security vulnerability among others...
- Increasing the patches review „throughput” and decreasing the response delay for emails. Well, we try to catch up but more eyes looking at the patches are welcome.
- Improving overall cooperation with distros and the other interested parties. Now we are in touch with Fedora, Red Hat, Debian and Ubuntu.
- Some people start posting the patches and drop the work in the middle. This does not help. Maintainers spend their time reviewing and nothing comes out of it. So, we waste time and lose features/fixes/cleanups. And often maintainers are not able to take over work on the patches due to their workload. So, please treat us seriously and do not do that! Always finish your work!

Pain points

…continuation

- It seems to us that some people do not carefully read maintainer's comments. They post the new versions of patches without all requests taken into account and then complain that their work is delayed. We understand that the authors may not fully agree with some comments. It does not help if they are skipped silently. Even it makes the situation worse and delays final patches acceptance. So, if you do not like a given comment, please complain. If you agree with it, take the comment into account in next version of patches. Silent omissions do not help and frustrate both the authors and maintainers.
- If you work on a new feature please do that on GRUB upstream instead of a specific distro version. Otherwise you increase backlog and make life more difficult for upstream and distro maintainers.

Discussion about the community/distros expectations

- What do you care about?
- What is not important for you (at all)?
- Do you think our planned priorities are the same as yours?
- Are there any other community/distros expectations?

Thank You

Daniel Kiper
daniel.kiper@oracle.com

ORACLE