Master Internship proposal (M2)

GNU Boot : fixing RAM initialization and upstreaming support for Asus KGPE-D16

Context

The global trend is towards the scarcity of hardware compatible with free software and soon there will be no computer that will work without software domination by Intel, AMD, ARM, GAFAM and consorts, especially involving BIOSes. A BIOS (Basic Input Output System), as its name suggests, was originally a set of low-level functions contained in the read-only memory of a computer's motherboard, enabling it to perform basic operations when powered up. However, the definition of a BIOS has evolved to include what used to be known as POST (Power On Self Test): testing for the presence of peripherals and allocating resources for them so as to avoid conflicts, and then handing over to an operating system boot loader. We consider that the bulk of the work carried out by a BIOS firmware today is the initialization and training of RAM. This means, for example, initializing the memory controller and optimizing timing and read/write voltage for optimal performance. The code in the BIOS that manages this is complex, since its role is to optimize several parallel buses operating at high speeds and shared by many CPU cores, and make them act as a homogeneous whole.

The coreboot project, started under the name LinuxBIOS, is an open-source bootloader launched by Los Alamos University Laboratory in 1999, with the primary aim of replacing manufacturers proprietary BIOSes, which are often low-performance and even feature-limited and especially affected by backdoors and bugs. The primary goal was to obtain a faster software than proprietary BIOSes, and it makes coreboot the basis of many free software projects such as GNU Boot. GNU Boot is a free firmware distribution based on coreboot, GNU GRUB and SeaBIOS. Since coreboot is not fully free, it aims at deblobbing coreboot and provide a fully free firmware image to users. It thus only supports boards that can run a fully free firmware.

The KGPE-D16, an AMD fam15h mainboard, is the only powerful server board that was supported by coreboot as it supports 2 × 16 cores CPUs and up to 256GB of memory. It can be operated with fully free software, for instance GNU Boot, so it can continue to get security fixes for remotely exploitable bugs in the BIOS (e.g RowHammer). Also, there is no Management Engine/PSP and some compatible CPUs aren't affected by the Spectre class of bugs, and there is even libre source code and documentation for CPU microcode update. When it comes to hosting sensible information, this mainboard is then a good solution. These mainboards are notably used for hosting by the GNU project (including GNU Guix), the Free Software Foundation, KDE, SugarLabs, Replicant, the Free Software Software Foundation Latin America, Libre en Communs, Parabola and many others. However, KGPE-D16 has been removed from official coreboot support since the 4.11 version because of a lack of maintainance and serious problems with RAM initialization.

Objectives

Hosted by the LIP6 laboratory and supported by the GNU Boot Project, the intern will work on upstreaming Asus KGPE-D16 into coreboot again and document and fix the memory initialization. The reason for this is that coreboot would be able to apply security fixes when available and it would help to make the firmware better in the future for these boards and related chipset (AMD fam15h). Documentation would help support other motherboards and would useful as an

educational ressource, being a reference example of a working implementation of memory initialization in a NUMA context. There will be a few technical pitfalls to overcome, including catching up on the coreboot code base between version 4.11 and 4.18 for these motherboards, or stabilizing the RAM initialization and making it work properly. The final challenge will probably be to get these boards accepted back into the upstream project after so much time away.

The internship consists of rebasing the support on the current coreboot version (4.18), fixing all bugs and stability issues with memory initialization and upstream that work, while documenting it and maintaining it until it is fully integrated into coreboot. Some steps are proposed as follows :
- Establish debug and validation tools: JTAG, gdbstub, etc
- Separate chipset code from board-specific code
- Support RELOCATABLE_RAMSTAGE
- Support POSTCAR_STAGE
- Support C_ENVIRONMENT_BOOTBLOCK
- Correct memory and voltage training code to avoid failures
- Save memory/voltage training to reduce boot time and remaining failures
- Support initialization of CPU cores in parallel
- Upstream the board to coreboot

Hosting laboratory

LIP6 (Sorbonne Université, UMR CNRS 7606), campus Pierre et Marie Curie (métro Jussieu), Paris, France

Internship period

6 months

Contact

Franck Wajsburt <franck.wajsburt@lip6.fr>

Conditions for acceptance

The intern will apply for a grant of the Nlnet/European NGI Assure fund, so that its work will be proven to be reusable by the public.

Required skills

Experience with C and assembly programming and good experience with versionning systems (Git).

Advanced knowledge of computer and manycore architectures, BIOSes and operating system theories. Knowledge of microprocessors architecture and a basic knowledge of NUMA will be appreciated.

Precision and writing qualities will be greatly appreciated.

References

https://www.gnu.org/software/gnuboot

https://www.raptorengineering.com/coreboot/kgpe-d16-bmc-port-status.php

https://www.secplicity.org/2021/12/29/hp-ilo-and-the-newly-discovered-ilobleed-rootkit/

https://resources.infosecinstitute.com/topic/security-best-practices-for-git-users/

https://en.wikipedia.org/wiki/Intel_Management_Engine#Security_vulnerabilities

https://en.wikipedia.org/wiki/Row_hammer

https://www.coreboot.org/Board:asus/kgpe-d16#CPUs_recommended_by_users

https://www.syssec.rub.de/media/emma/veroeffentlichungen/2017/08/16/usenix17-microcode.pdf

https://www.fsf.org/blogs/sysadmin/the-fsf-tech-team-doing-more-for-free-software

https://wiki.parabola.nu/Hacking:Servers/Beefcake

https://store.vikings.net/d16-ryf-certfied