Coreboot: the view from the FSF.

Denver, CO
2008-04-04

Ward Vandewege
Free Software Foundation
Senior Systems Administrator

click

What does the FSF want?

As the name implies, we want

click

free software.

click

We define free software as software that gives the user four freedoms:

click

Freedom of speech
Freedom of worship

click

oh, wait, the *other* four freedoms

click

The freedom to run the program, for any purpose

click

The freedom to study how the program works, and adapt it to your needs. This implies the availability of source code.

click

The freedom to redistribute copies so you can help your neighbor.

click

The freedom to improve the program, and release your improvements to the public, so that the whole community benefits. Again, this implies that source code is available.

click

A long time ago, in 1984

click

people drove cool cars

click

but unfortunately, there was very little free software available

click

So Richard Stallman decided to start the GNU project - a project to develop an entirely free operating system. In 1991 the Linux kernel came along, and the combination of the two became a huge success.

click

Fast forward to today.

click

We've come a very long way; there is now a vast body of free software available. People can use free software, have a pleasant experience and get the job done - often better and/or faster than with proprietary alternatives.

click

It is possible to run a computer with nothing but free software...

click

well, almost

click

Modern hardware contains more and more proprietary 'microcode'. Hardware components are turning into general purpose computers of their own, running proprietary code.

Consider this example - it's a screenshot of some software update tool for an IBM server. This machine has microcode in the systems management board, the hard drives, the tape drive, the network card - and of course the bios. This microcode is typically distributed without source, and under very restrictive licenses.

click

And then there is the problem of binary blobs. Sometimes microcode or firmware is embedded in a free driver as a 'binary blob', like in this example from the tg3 driver in the Linux kernel, which operates broadcom gigabit network cards. Thankfully, in this case the binary blob is optional - it is not required for basic operation of the network interface. I don't even know what functionality it provides, to be honest :)

Sadly, in many drivers the blobs are not optional.

click

But the most prominent part of proprietary software in almost every computer out there is of course the BIOS.

click

All this proprietary low-level software imposes restrictions on the user, in all the ways that proprietary software is a problem higher up on the software stack.

click

It can also provide a vehicle for Digital Restrictions Management - the ultimate anti-freedom technology.

click

DRM and free software are mutually exclusive - if the user can modify the software, effective DRM is impossible. Many would argue that effective DRM is a pipe dream anyway - even on a system with proprietary software - but no matter how you look at it, DRM is a threat to free software.

click

So, what does the FSF want? Free software **and** hardware free from restrictions. We can't guarantee software freedom if the hardware locks us down.

click

So, a little over a year ago we wrote a position paper titled 'The road to hardware free from restrictions; how hardware vendors can help the free software community'.

click

In that paper we addressed a number of problems with current hardware, and suggested ways for hardware vendors to improve the situations.

We talked about free software driver availability - particularly for wifi and accelerated 3D graphics. We talked about issues with proprietary BIOSes - things like BIOS locks that prevent people from using third-party cards in the otherwise standard mini-pci slot that is built into most laptops. We mentioned the problem of the 'Microsoft tax' - how hard it was to buy machines without a version of Windows pre-installed. And we addressed hardware-based DRM.

A lot has happened on most of those fronts in the past year.

AMD has released specifications and is actively helping the development of free software drivers for ATI graphics cards. Intel's graphics group provides 100% free software drivers for their hardware, too. It's more on the low-end of the graphics market though. The madwifi team has made great progress in replacing the proprietary firmware in Atheros-based wifi cards.

Sadly, there are still proprietary BIOS locks on mini-pci cards out there.

But there are now several machines available for sale preloaded with a free software operating system - the Asus EEE pc, the Everex Cloudbook, etc.

DRM has taken somewhat of a nosedive - most music is now available for sale in a DRM-free format. Hardware-based DRM schemes continue to be broken. This fight is not over yet, but we have won several battles so far. Ultimately, the more people learn about DRM, the harder it will become to defend.

click

We also addressed another point in our paper: the need for a free BIOS.

click

The FSF has adopted a three-pronged strategy to advance the free BIOS goal.

click

The first prong is advocacy and awareness.

click

Through our campaign for a free BIOS we are building up awareness for this issue among our supporters - and beyond.

We also ask people to write to hardware manufacturers that don't cooperate. This is an excerpt from our campaign page:

click

You can also help our campaign by writing to manufacturers such as Intel, saying they ought to cooperate with a fully free BIOS. Calm but strong disapproval, coupled with stating an intention to take action accordingly, is more effective than venting rage.

In other words, we ask people to write manufacturers like Intel and explain that they are not going to buy their stuff until they support a free BIOS.

We ask people to send us a copy of any correspondence they send, as well as any replies they may receive.

Recently, we got such a response from Intel, which was basically this:

click

...

click

Let me just read this to you, it's quite entertaining.

Writing BIOS code is not like writing an OS device driver. Chipset specifications can vary not just between chipset models, but between steppings of the same chipset.

So what? Give us accurate documentation and we'll implement it.

The letter continues like this:

Problems in chipset hardware and problems in BIOS code are hard to distinguish without specific hardware instrumentation.

Or, they could release accurate errata with the specifications, of course :)

End user BIOS replacement with a third-party BIOS (whether free or not) on a commercial motherboard is not allowed by nearly all hardware vendors because of potential for BIOS viruses and the risks of rendering the hardware useless through ill-advised modifications.

This is where it gets a bit more interesting. A non-factory BIOS will lead to BIOS virusses? I don't quite follow that logic. As for it being 'not allowed' to modify the BIOS on your own hardware - seems to me that perhaps this person meant that it would void the warranty. I don't see what Intel or any other vendor has to say about a motherboard after it has been purchased.

And here is the kicker:

For example, a laptop battery could explode if incorrect power management algorithms were applied.

Now that's interesting isn't it. I forwarded this letter from Intel to the coreboot mailing list shortly after we got it, and the comments ranged from 'well if that's true, the battery could not charge when the machine is powered down' to 'the Federal Aviation Authority might be quite interested if it would be possible to blow up a laptop battery by messing with software'.

click

I classify this part of the letter as the spreading of Fear, Uncertainty and Doubt.

click

The letter continued like this:

> [The] BIOS is a part of the reliability and performance promise of the hardware. Chipset specifications at the level being discussed are commonly considered proprietary by all silicon vendors, not just Intel.

click

That's just plain false. AMD releases a lot of specs at this level, downloadable by anyone from their website. Others do the same - consider superio vendors for instance. In fact, Intel **used** to release this stuff to anyone, for free.

click

The letter concluded with

> The open source firmware work that Intel **is** sponsoring could lead to a solution where proprietary low-level chipset initialization code from silicon vendors is made compatible with open source higher-level platform initialization and pre-boot management. If you are interested, we invite you to participate at tianocore.org.

click

And that brings us to EFI, the Extensible Firmware Interface. There seems to be not all that much high-level information on EFI out there, but I found this article on Deviceforge.

click

It has an interesting figure that describes the 'firmware flow' on an EFI machine. The parts that were referred to in the letter - what Intel calls EFI, which it released under a free software license (at least most of it) - live largely in the Driver Execution Environment (DXE) and the Boot Dev Select (BDS) stage. The rest, in particular the 'Security' and 'Pre EFI initialization' stages are 100% secret.

click

So, in essense Intel is telling us here to look at EFI, and at the same time it's saying we can't have free software before EFI loads.

Well, that makes EFI nothing but smoke and mirrors in my view. It makes for a coreboot payload, and that's about it.

I'd like to make one thing clear. We're not after Intel specifically. Intel, like many large organizations, is schizophrenic when it comes to supporting free software. As I mentioned earlier, its graphics and to some extent, wifi, groups are doing great work - it's their BIOS stance that we take issue with. If Intel were to change their mind about a free BIOS, the Free

Software Foundation would be more than happy to assist in any way we can to make Intel-based hardware with a free BIOS a reality.

click

The second prong of our free BIOS strategy is 'eat your own dogfood'.

click

The FSF has a hardware purchasing policy that states that where possible, any new hardware we buy must have free BIOS support, or have reasonable prospects for free BIOS support.

click

We've also been upgrading our machines to coreboot.

click

We now have 10 machines running coreboot. That includes servers running FILO, servers running Linux-As-a-Bootloader, and diskless workstations with an etherboot payload.

click

Tyan s2881
Tyan s2882
Gigabyte m57sli-s4

click

We have 6 other machines that are potential conversions.

Tyan s2891
Tyan b3992
PC Engines alix.2c3

The s2891 is CK804 based but there's an issue with sata port initialization in the coreboot CK804 codebase. The box is in production so it's painful to bring it down to test fixes. There is a patch floating around that might solve the issue though.

There was someone who said on the list a while back that they were working on the b3992; again, this box is in production.

Hopefully the alix.2c3 will be relatively easy based on the alix.1c :)

click

We still have 26 legacy machines.

click

If you add that all up, we're at 24% coreboot now.

click

The goal is obviously 100%; as we retire and consolidate hardware, we're going to approach that goal.

click

Prong three is 'vendors'.

click

We want to get machines with coreboot out into as many hands as possible. Since the average user never upgrades their BIOS, we want vendors to ship with coreboot preinstalled.

click

We have a carrot: the FSF will endorse vendors who ship machines with coreboot on our hardware pages.

click

So, there's this nice startup in Seattle called Silicon Mechanics. They're a hardware vendor/integrator, and they ship and support server hardware, for example their A236. This box is based on a Supermicro H8DMR board, which is supported in coreboot v2, as well as buildrom.

I'm a part-time sysadmin at the FSF. I also do freelance projects, and in one of my projects Silicon Mechanics delivered a bunch of A236'es with coreboot preinstalled. This was not 'officially' supported, but I asked Silicon Mechanics if they would be interested in shipping machines with coreboot to anyone.

click

So, this is the reply I got yesterday:

"We will commit to offering coreboot preinstallation on the A236 with a specific set of hardware and software. In the future, we may expand the program to additional platforms based on customer interest. We will include a message about coreboot support on the platform page in the next few days with instructions to contact sales for additional information."

So, we've got a vendor that's willing to ship servers with coreboot pre-installed. One model for now, but they tell me that their A266 is pretty similar, and if there is demand, I'm sure they will, as promised, work to ship more boxes with coreboot.

click

Desktop and laptop...

click

We talked to Dell, HP, Sun, MSI, Everex,... but nothing concrete came out of that.

click

We've also been talking to Artec Group. They are a design shop in Estonia with coreboot experience.

They actually would like to build a 'deluxe-olpc'. A laptop with coreboot, etc.

The question is what the specs should be - it's hard to compete on price with the Taiwanese OEMs.

It would certainly be interesting to get some feedback from the community about that.

click

We've also toyed with the idea to buy a bunch of motherboards - maybe the gigabyte m57sli - preload them with coreboot, and sell them. There are obviously lots of problems with that - support, warranty voiding, etc. We're a small non-profit...