Open-Source Hardware

Jenna Annilyn

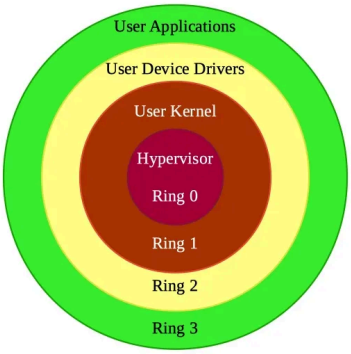
Technology is part of nearly every aspect of our lives, from the smartphones we rely on for communication to smart devices that govern our homes. The importance of understanding as well as engaging with the hardware that powers these innovations, as a result, has never been more evident. From devices like complex microcontrollers, processors, robotics platforms, and even computers we use on a day-to-day basis, free and open-source hardware (FOSH/OSH) enables people worldwide in all fields of engineering to learn and understand abstract, applied technologies. There is, however, an increasing gatekeeping of hardware engineering information for malicious purposes of surveillance and false senses of security, which becomes vital for the future success of aspiring entrepreneurs and trailblazers. Therefore, nurturing the development of open-source hardware is necessary to foster an equitable and sustainable future in the exponentially growing dominance of proprietary technology.

When one reads “free” in “free and open-source hardware,” there’s no doubt that many people would support such a no-cost initiative. However, according to the renowned software-oriented GNU Project and Free Software Foundation (FSF), freedom in FOSH is the freedom to “copy, distribute, study, change and improve” software, much like “free speech” refers to an individual's freedom of opinion. It derives from the Spanish or French word “libre" as the hardware and software are not “gratis,” free of charge. You fully own not only the source code for platforms themselves but also the right to exercise freedoms, albeit responsibly, without censorship or limitation. For instance, Moodle, the software we use at school for our assignments, is free software licensed under the GNU General Public License 3.0, one of many licenses that denote free software. Raspberry Pi’s are also great single-board computers with several uses that extend into applications such as home security using its 40 General-Purpose Input-Output (GPIO) pins for home or office use - the Raspberry Pi’s excellent

performance despite its small size is also an excellent example of FOSH in the capabilities offered to many end-users and the larger tech community.

Digital freedoms, due to the powerful rights given to the user, have continued to host several benefits for *all* people, one of which is productivity in community collaboration. Code repositories such as those provided by GitLab provide developers with spaces to easily create pull requests to add and fix features, open issues, and create separate "forks" of an individual program if they so please. Hardware can thus easily grow to be security hardened or improved by the *hour* depending on community activity and discussion, rather than relying on a business to make their own patches. Users of free hardware can customize it according to their specific needs and preferences, creating personalized blueprints and schematics. Computing tools and platforms, as a result, increase in productivity at a real-world scale. Software freedom is simple to achieve, as "coding" is equally as valuable as it is common in today's society.

The same, however, cannot be said for inventing the base hardware. Unfortunately, the same freedoms we can exercise with software are not easily obtained using available hardware due to the looming effects of proprietary control. As the FSF outlines, proprietary vendors do not "respect your freedom." Software is not as simple to commercially control as hardware is, since hardware is the foundational medium for software to exist. Closed hardware ecosystems infamously restrict users' right to customize, repair, analyze, or upgrade these devices, leading to dependency on manufacturers and the need to reverse-engineer hardware to fully understand how it operates. While businesses use proprietary hardware standards to ensure "quality, reliability, and security," this forms a false miasma of promises the FSF describes as "defective by design." Components that comprise hardware such as firmware and instruction set architectures (ISAs) known conventionally as "x86-64" and "ARM" are all held under a vendor's grasp so they may stay dominant in the market. Additionally, they are intentionally slow and rarely or horribly updated. Due to this, many people must deal with subpar Windows-based laptops, projectors, and cell phones.



Alternate (Cloud) IA Protection Rings

There are also inherent threats behind the devices' otherwise fancy appearance. On the lower level, the root of such sluggishness is a complex network of proprietary technologies abusable for mass

surveillance to “keep users safe.”One example of such proprietary technologies is that of the Intel Management Engine (Intel ME). As HowToGeek outlines, it “is a parallel Operating System (OS) running on an isolated chip” running a proprietary UNIX OS variant called “MINIX.” It runs at an outrageously privileged level at ring -3 way beyond the Operating System (OS) kernel when a device powers on and manages computer processes - it unknowingly looms, *always* running with full, unstoppable control. Horrifyingly, “it has its own MAC and IP addresses,” - two digital identifiers - “and full access to the main processor, all memory (including SMM) and all peripherals.” If that’s not enough to concern you, it also “runs its own web server” invisible to the host device and is extremely difficult or impossible to disable. Furthermore, you largely have no power to do anything about it. That means not only are our inherent digital rights to use our technology freely are at risk, but practically everything that exists on your machine is threatened as well. Yikes!

On older chipsets, the Intel ME may be easy to disable and reverse engineer due to swaths of low-level exploits on target machines like the Lenovo Thinkpad X200, which the Libreboot and Coreboot projects are crowned for achieving; as such, near absolute digital freedom and autonomy can be easily achieved with an easy-to-find toolkit of a Raspberry Pi, a Pomona SOIC8 clip, and a few female-to-female jumper wires. However, newer hardware platforms necessary for modern and demanding work are practically married to the Intel ME, with absolutely no methods to erase its functionality. That means that the Intel ME is not only a goldmine for an attacker with physical access to your device, but it is also an ultimatum of mass surveillance with full potential to intercept and manipulate every hardware interaction without user consent. It is constantly hovering over all your activities - as Jaak-Henk Hoepman outlines in “Privacy is Hard,” even if “you’ve got nothing to hide” that is malicious, a common privacy myth, every ounce of your personal data is easily available for random people, cybercriminals, and firms to harvest without knowing. That data is worth *tons*, one of the most coveted treasures of the cybersecurity space!

The pervasive presence of proprietary hardware such as the Intel Management Engine poses grave threats to the autonomy and education of the prospering engineer. Modern hardware goes a step beyond spyware issues we already acknowledge, ranging from social media and tech giant services, by now employing irremovable mass surveillance tactics on virtually every single machine. Hidden

indefinitely from mainstream media and knowledge bases, they constantly infringe on our digital rights to use hardware and software without limits to innovate, analyze, and modify hardware as we see fit for our own benefit and that of others. Instead of buying from tech giants like Intel, Microsoft, and others, fueling a near-endless stream of non-free spyware and hardware prohibiting our inalienable freedoms, invest in open hardware and its development through initiatives like the Open Compute Project that listen to and embrace diverse communities of *all people to learn about making and using hardware,* not *just those first to create a patent.*