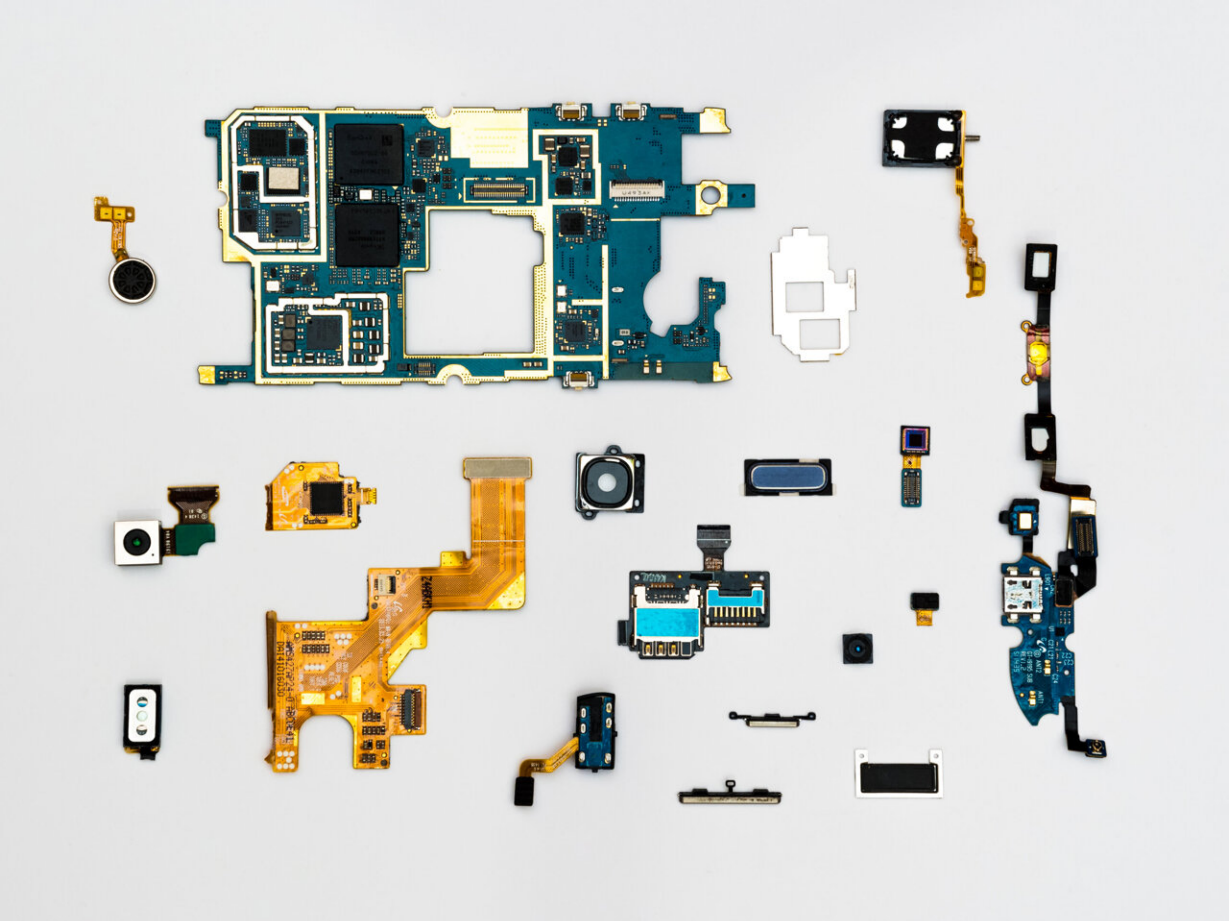
Open-source hardware could defend against the next generation of hacking

October 17 2018, by Joshua M. Pearce



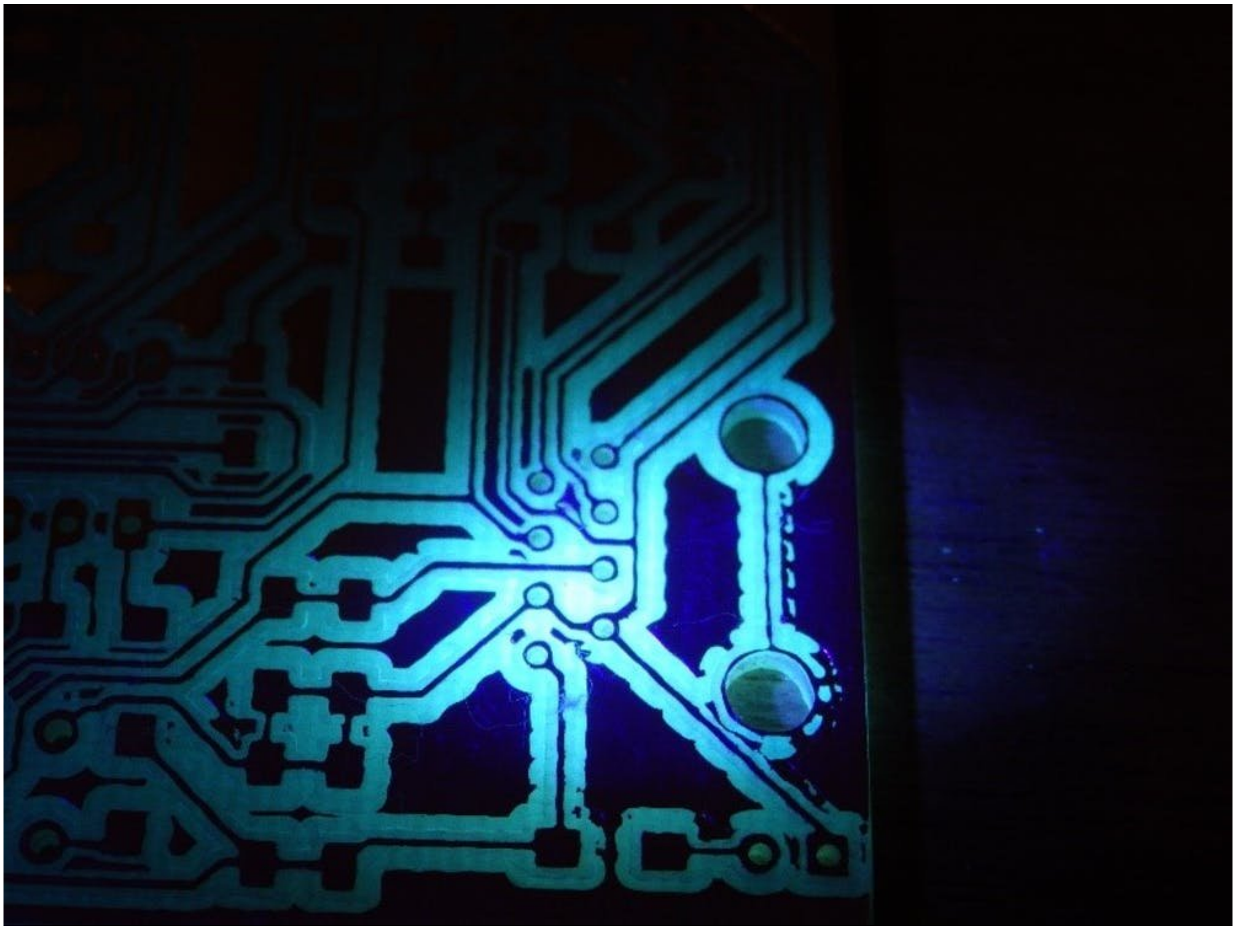
Credit: Dan Cristian Pădureț from Pexels

Imagine you had a secret document you had to store away from prying eyes. And you have a choice: You could buy a safe made by a company that kept the workings of its locks secret. Or you could buy a safe whose manufacturer openly published the designs, letting everyone – including thieves – see how they're made. Which would you choose?

It might seem unexpected, but as an engineering professor, I'd pick the second option. The first one might be safe – but I simply don't know. I'd have to take the company's word for it. Maybe it's a reputable company with a longstanding pedigree of quality, but I'd be betting my information's security on the company upholding its traditions. By contrast, I can judge the security of the second safe for myself – or ask an expert to evaluate it. I'll be better informed about how secure my safe is, and therefore more confident that my document is safe inside it. That's the value of open-source technology.

Computer hardware is, for the most part, like the safe whose security mechanisms are secret. Any weaknesses are hidden, as well as any of their strengths. In the wake of revelations that Chinese spies may have been able to install a tiny computer chip inside devices used by as many as 30 companies, like Amazon and Apple, as well as the U.S. military and the CIA, I suggest re-evaluating the hardware people and corporations rely on to protect their secrets.

Hacking hardware is particularly dangerous because it can bypass even the most secure programming safeguards – like taking control of a server without needing a password at all. Hardware customers could benefit from the clear – if surprising – lesson the software industry has learned from decades of fighting prolific software hackers: Open-source systems can be more secure.



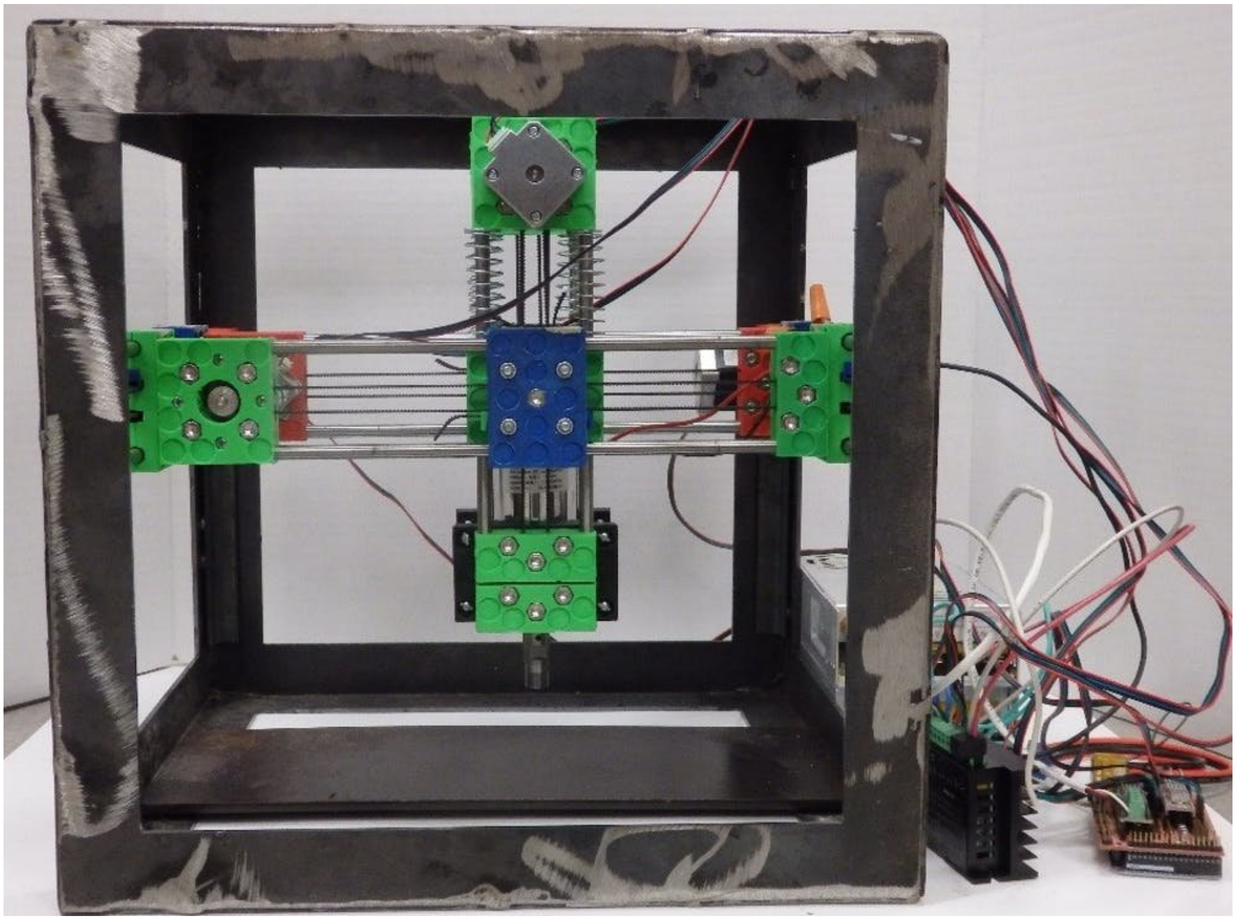
An open-source electronics board under inspection with ultraviolet light. Credit: Shane Oberloier and Joshua Pearce, CC BY-ND

Lessons from open-source software

Software users and developers already embrace computer software whose source code is publicly accessible. All supercomputers, 90 percent of cloud servers, 82 percent of smartphones and 62 percent of embedded systems – like those inside consumer electronics – run on open-source operating systems. More than 70 percent of "internet of things" devices also use open-source software.

Open-source software isn't inherently or automatically more secure. But it creates more possibilities, and market pressure, for improving security. Just as when choosing a safe to store a secret document in, customers must decide – should they pick a system whose security is vouched for by the company that makes it, or a system that can be explored, examined and tested?

Open-source software users choose not to trust a program unless they can verify it independently. Many of them don't have the expertise themselves to be able to evaluate security claims, of course – but they can wait until consumer-protection groups do so independently, hire a verified expert to check things out, or even learn the skills needed to investigate for themselves. They could even decide to pay for a version of the software that has been checked out and is supported by experts.



An open-source circuit mill built using low-cost components from 3-D printers. Credit: Shane Oberloier and Joshua Pearce, CC BY-ND

Security with open-source hardware

Open-source hardware offers users the same choice. Many people who buy electronics have no idea what's inside them. Even technically sophisticated companies like Amazon have to hire outside forensic experts to be sure of exactly what is in the hardware their companies rely on.

Open-source hardware would mean each device's designs and components would be open for public view at any time. People could study the information, follow the directions to build a device, test it and distribute it – or even sell it. All that transparency would give attackers more data about their potential targets, for sure. But it would help customers downstream much more, by giving them the means to verify their own devices' security themselves.

This does not mean people would be left to build their own hardware. The open-source software movement has found a number of opportunities for entrepreneurs and innovators to sell systems and services based on software that itself is free. For instance, 90 percent of the companies on the Fortune Global 500 list pay for a brand-name version of the open-source Linux operating system from Red Hat, a company that makes billions of dollars a year for the service they provide on top of the product that can ostensibly be downloaded for free. The open-source hardware movement is not yet as mature as its software counterpart, but it could catch up fairly quickly.

The future of distributed manufacturing

Making open-source hardware systems more available increases regular people's security by giving them verifiably secure options. If someone is especially concerned, they could even manufacture their own electronics. There are a wide range of designs already publicly available on sites like Hackaday, Open Electronics and the Open Circuits Institute. There are also many communities based on specific products like Arduino.

Even open-source chips are gaining traction. It's already possible for people to build electronics that are open-source from the chips all the way up to the physical components. If hardware hacks become more common, that may be a key way for people to protect their cybersecurity. Companies and governments can also be expected to adopt policies that favor open-source hardware and require better testing to ensure their equipment is safe to use.

Provided by The Conversation

Citation: Open-source hardware could defend against the next generation of hacking (2018, October 17) retrieved 25 April 2024 from https://techxplore.com/news/2018-10-open-source-hardware-defend-hacking.html