Digital Freedom

Bob Ham

October 2013

As computers take on increasingly prominent roles in society, the potential for their abuse grows. Digital technology can be used to oppress people by restricting their ability to compute, or to communicate, or to conduct commerce, or even to travel. It can be used to encroach on people's privacy by spying on their communication and tracking their online activity or their physical movements. As digital technology becomes further integrated into human life and dependence on technology grows, the potential for its abuse will also grow.

Computers are a relatively new phenomenon in human history. We are in a time of change when old social institutions are giving way to new forms of organisation and co-operation, fueled in no small part by widespread computing and communication technology. We are undergoing a shift in human civilisation, what has been called the "second renaissance", comparing the effects of the invention of the Internet to that of the printing press.

At this time it is critical that our future and the future of digital technology be set on a good path. We must ensure that technology is used to support human freedom, not curtail it. We must work hard to make sure this happens.

We need "digital freedom" groups, enthusiasts working to create computer systems that support freedom. Specifically, groups that work toward three primary goals: computers that

(1) are 100% free hardware,

(2) run 100% free software and

(3) connect to free networks.

Free hardware

Free hardware refers to hardware whose design can be freely copied, shared, modified and manufactured. Users of free hardware have the freedom to learn from a design, to modify it to better suit their needs, and to share their modifications so that everyone can benefit. Free hardware fosters a community based on sharing and co-operation where designs are co-created by members of a community rather than produced and restricted by a single controlling entity. Free hardware encourages commerce through the free exchange of designs and information.

Free hardware projects that digital freedom groups support include:

- OpenRISC `http://opencores.org/or1k`
- OpenCores `http://opencores.org/`
- OLinuXino `https://www.olimex.com/Products/OLinuXino/`
- Freeduino `http://www.freeduino.org/`
- Milkymist `http://milkymist.org/`

Spying

As computer architectures become increasingly complex, access to information about the design becomes more important. Modern computers include sub-systems which contain microprocessors that are independent of the main CPU. For example, power and a great deal of hardware control in laptop computers are done using an auxilliary processor. These processors often run proprietary software. Without having access to the proprietary software's source code, we cannot know what an auxilliary processor is doing. Often, such processors have access to data storage and to network interfaces. It is possible for a hardware manufacturer to implement spying routines and so this hardware presents a threat to the security of information in the computer. Access to hardware designs mitigate this threat by allowing users to implement their own software to run on auxilliary processors.

Education

The techniques employed in a hardware design is part of its value. A design is in part, an expression of knowledge about designing and so any design can be used to teach others about designing a particular type of hardware. For example, a design for a table can be used to teach others about how tables can be designed safely and also about furniture design in general. This educational value is important but proprietary designs prevent taking advantage of it and a large benefit of the knowledge that goes into the design is lost. Free hardware combats this loss and ensures that designs can be used optimally.

Chip manufacturing

At present, it is unfortunately not possible to create a computer using 100% free hardware. There are no chip manufacturers that freely license the designs for their silicon. It is also impractical for enthusiasts to produce free hardware chips because of the enormous costs of manufacturing silicon designs. A lower-bound cost for the tape-out of an ASIC is around 150000 US dollars. While there is at least one free hardware project with the goal of raising such funds, none have yet achieved it.

It is possible to create free designs and implement them in reconfigurable digital circuits in the form of FPGA chips. However, patents protect the fundamental technologies that FPGAs are based on and holders of these patents choose to offer only proprietary licenses. Hence, while it is possible to create free hardware chip designs, it is only possible to implement and test them using proprietary FPGA hardware. This is akin to the need to use proprietary operating systems to build free software alternatives when the free software movement was in its infancy.

So, in the field of free chip design, the focus is on creating free designs now which can be manufactured later. There are a number of circumstances which may give rise to the manufacturing of free hardware chips:

(1) Existing silicon manufacturers creating chips based on free designs. This could be (a) a manufacturer who realises the value of free hardware and changes their practices to license their designs freely, or (b) a manufacturer who takes advantage of existing free designs and creates chips using them.

(2) When fabrication technology, for example 3D printing, advances to the point where it becomes practical to manufacture processor circuits without the enormous costs required at present. This may take many years.

When FPGA patents expire, as many are now in the 2010s, it will change the landscape in the FPGA industry, generally increasing freedom there but also specifically decreasing the costs involved in developing free chip designs. Free FPGA designs would also become possible and it could be argued that an FPGA design is more likely to attract funding for a manufacturing run than a specific processor design whose applicability is less broad.

Board designs

While it is not yet practical to create free chips, it is possible to create free motherboards. Free PCB designs can be created and manufactured now and indeed, many are. Today, a computer with free PCBs is the closest we can get to a free hardware computer.

Free software

Free software is software whose users are free to share it, learn from it, modify it and share their modifications. Computer users should be free to do their computing however they wish and should have control over their own computer. Free software respects users' freedom and enables them to do this. The Free Software Foundation gives four freedoms that free software ensures:

- The freedom to run the program, for any purpose (freedom 0).
- The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help your neighbor (freedom 2).
- The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

Free software projects that digital freedom groups support include:

- GNU `http://www.gnu.org/`
- Linux-libre `http://www.fsfla.org/ikiwiki/selibre/linux-libre/`
- Trisquel `http://trisquel.info/`
- Replicant `http://replicant.us/`

Open source

The phrase "open source" refers to a development methodology where the source code for software is available to users. The phrase was coined to provide a means of promoting free software to organisations like businesses who were less concerned, or even uncomfortable with the issue of human freedom. Open source misses the point of free software.

Open does not necessarily mean free. For example, the Sybase Open Watcom Public License under which the Watcom C/C++ compiler is released, requires that users publish source code whenever they "Deploy" software and "Deploy" includes many kinds of private use. The freedom to use and modify software without notifying anyone is an important freedom. The requirement to publish source code even when using the software privately, is a violation of this freedom. This is one example of how "open source" does not mean "free software".

More generally, "open" never refers to freedom.

Free networks

Free networks are computer networks that provide users with some guarantee of freedom. Users must be free to say what they want, without restrictions. They must be free to say it to whoever they want. Users must also be able to express themselves anonymously, protecting their identity. These freedoms are recognised as fundamental to a healthy, free society. Free networks guarantee that these freedoms cannot be subverted using the network itself. The guarantees are made through technology such as encryption and decentralised protocols.

Free networks that digital freedom groups consider themselves aligned with include:

- Hyperboria `http://hyperboria.net/`
- Project Meshnet `http://www.projectmeshnet.org/`

Free-network technology projects that digital freedom groups support include:

- FreedomBox `http://www.freedomboxfoundation.org/`
- B.A.T.M.A.N. `http://www.open-mesh.org/projects/open-mesh/wiki`
- cjdns `http://cjdns.info/`
- GNU Privacy Guard `http://www.gnupg.org/`
- Tor `https://www.torproject.org/`
- Libertree `http://libertreeproject.org/`
- Bitcoin `http://bitcoin.org/`

The Internet

The Internet is a network that has changed the world. However, the technologies which underlie the network are interwoven with a legacy of trust, a holdover from the network's origins and development history. For example, FTP transmits passwords in the clear. Unfortunately, much of the trust inherent in Internet technologies has been abused by criminals, both those who operate independently and those who are employed by governments. Defensive technologies were developed to protect against independent criminals, for example SSL, but those technologies were later undermined by criminals employed by governments. The Internet is not a network that can guarantee freedom to its users.

Free network technologies

There are a variety of technologies that promise to enable free networks:

(1) Community-based mesh networks are wireless networks operated in a decentralised manner by comunities. They offer network services to members of the community and provide a means of communication that is independent of compromised Internet service providers.

(2) Ad-hoc mobile networks are networks based on opportunistic wireless communication between mobile devices. They offer a means of communication that subverts the need for a centralised network and can also extend the reach of other types of network.

(3) Federated social networks are social networks where services are offered by many independent nodes that communicate between themselves, as opposed to services being provided by a central controlling entity. They offer social networking facilities without the danger of the abuse of users' data by a central, all-powerful entity. Users can join servers run by people they trust or set up their own servers.

(4) Digital currencies are monetary systems in the digital domain and based on technologies like public key cryptography. Digital currencies enable commerce to be conducted between network users without restrictions.

Digital Freedom Projects

Ideas for specific projects that digital freedom groups could undertake include:

- Build a local wireless mesh network
  - Free software wireless node database, like nodedb.com but (a) under AGPL, (b) using OpenStreetMap and (c) better
  - Standardised mesh network node design, based on OLinuXino
- Write a free replacement for meetup.com
- OpenRISC desktop computer using FPGA dev board like Terasic SoCKit
- Desktop computer using OLinuXino
- Trisquel bug-squashing parties
- GPG key-signing parties