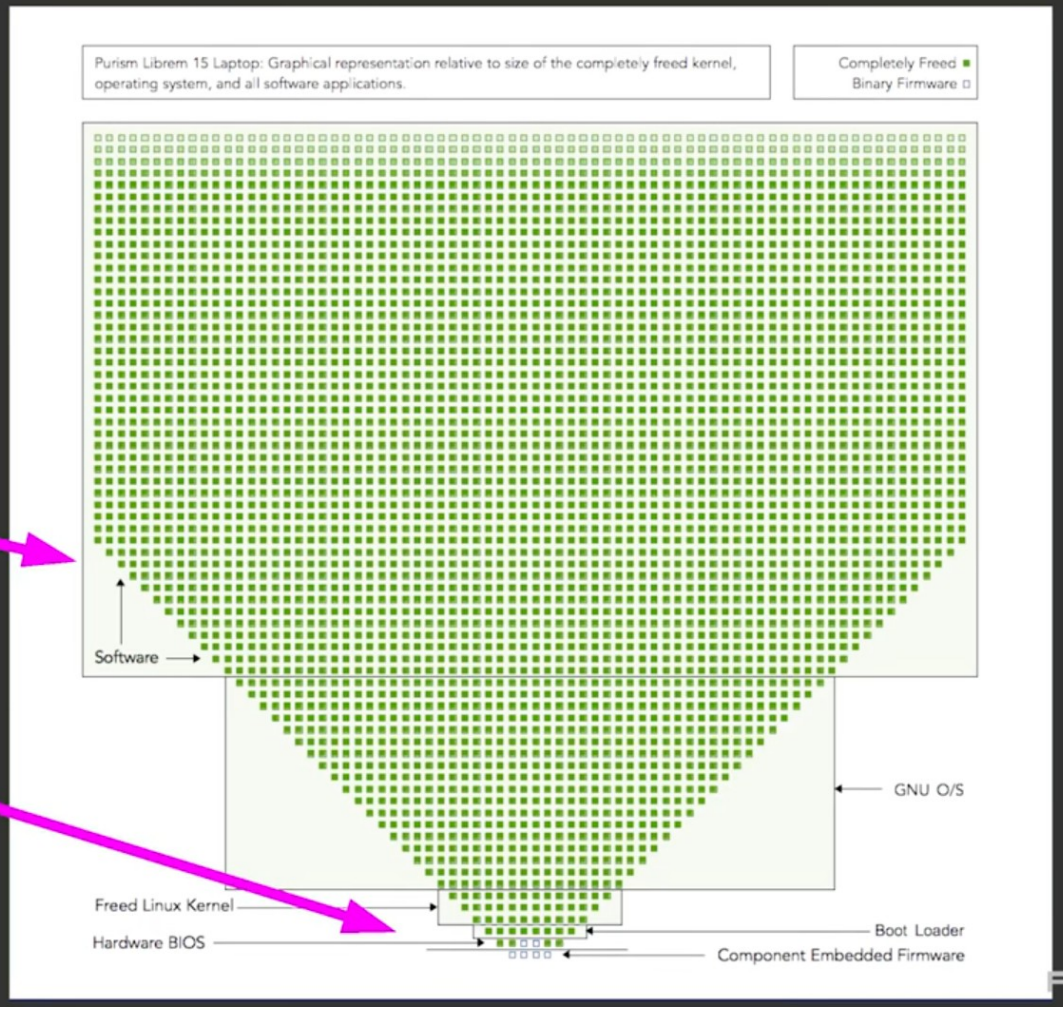
Critical Reading of Gabriel Somlo's "Toward a Trustable, Self-Hosting Computer System"

By Jon Trossbach

The Librem 15’s Hardware and Firmware are the only closed aspects in its design

Despite all the efforts of the open source community...

Herein lies the problem:
The trust root is still closed.



A.B.Haung,“Impedancematchingexpectationsbetweenrisc-vandtheopenhardwarecommunity,”2017.[On-line]. Available: https://riscv.org/wp-content/uploads/2017/05/Wed1100-impedancematch-huang.pdf

Somlo uses an FPGA to try and close the trust gap

FPGAs are slow.

FPGAs are complicated.

Why?

Reconfigurability of an FPGA allows us to thwart many hardware supply chain attacks

Still an open question: could the FPGA supply chain be made more secure? If so, by how much?

Weakness of this Approach

Novel FPGA trojans are more difficult but not impossible and the paper doesn’t really discuss that much.

Given FPGAs reconfigurability makes them more secure

Can we conceive of a way to secure the rest of the supply chain?

The Free Software Concervency has been making reproducable binaries for year, thus the only software attacks are novel exploits and all compilers everywhere being compromised. This model can be applied to FPGA bitstreams.

What about the remaining hardware?

Blockchain based supply chain non-repudiation

I propose that we could ship the FPGA while connected to a battery within tamper resistant packaging and a maximal-density bitstream configuration loaded into it such that an out put which takes advantage of the maximal-density of the FPGA correlates to a value placed on a publicly verifiable ledger on a blockchain network hiding the proof-value of the verifiable FPGA configuration using fully homomorphic encryption similar to the zk-SNARKs protocol.

It would be difficult, if not impossible, to meaningfully recreate the output from the bitstream configuration if this configuration were able to be both random and exploiting the maximum information density of the FPGA.

Using a Bitstream embedded processor whose transitors are visably verifiable

The bitstream placement is also a well known place that attackers have targeted

Small embedded processor responsible for the bitstream could be made with transistors that are verifiable with a commodity microscope or even with the naked eye

Reference: https://monster6502.com/