Verified Value Chains, Innovation and Competition

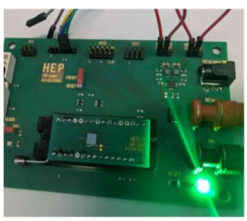
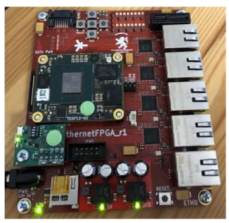
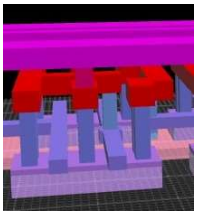
Highlights of IEEE CRS 2023 paper

https://ieeexplore.ieee.org/document/10224911

https://trustworthy.systems/publications/papers/Weber_GRSGLMRPSHHS_23.pdf

1. **The authors propose to enable IT-using companies to innovate at low cost and produce secure output by using open tools and components, e.g., formally proven processors, free security module designs, and free semiconductor development tools for submitting hardware designs to a fab.** Our proposal is to make such concepts better known, to develop cost-sharing across industries and countries, and to use government funding, e.g., for creating provably secure components. The authors and their partners have been involved in creating examples, such as the seL4 operating system kernel, the hardware security module prototype of project HEP, a partially formally verified RISC-V processor and a formally verified crypto-key masking scheme, and optionally with open hardware design tools up to submitting designs to a fab.
2. To speed up this process, it is proposed **to support an international co-ordination group with an emphasis on ironing out vulnerabilities**. Note that currently the developed products and research results mentioned above have been thought of in countries such as Australia, Austria, France, Germany, Switzerland, and the US. They are beginning to be taken up by companies such as Google and Collins Aerospace, but proofs and transparency along all components of entire value chains up to the fab are lacking. Note that according to our concept private applications and IP can remain proprietary, but would run on a foundation free of vulnerabilities.
3. As to the European Union, it is proposed to **prepare legislation to ease the certification of formally proven open components**, as opposed to demanding traditional certification procedures from revenue-needing open-source developers, as foreseen by the European draft Cyber Resilience Act.
4. The authors' analysis shows that **hardware cannot be completely formally proven**, as malicious actors may modify physical characteristics, e.g., add antennas, modify gates or the dopant level. Remedies can be found in increased transparency of fabs and ultimately in increased competition in which buyers can easily select fabs.
5. The authors are aware of the complexity of a such global process to ease secure innovation and produce free components and tools, but suggest **discussing it and kicking it off, e.g., by creating a router or a security module, optionally even with open GDS-II files** (the input to a fab).
6. Larger, more powerful systems could be secured better than today by using **isolated compartments for trustworthy and less trustworthy code with existing powerful hardware.** In parallel, more powerful open processor designs could be explored, supporting such virtualization.

Illustrations


- Collins Aerospace using seL4 for Boeing Chinook, with mathematically proven isolation.
- Prototypical security module from project HEP with functionally proven VexRiscv processor.
- Prototypical open router by HSRM.
- Illustration of a GDSII-file with Klayout.
- Chip analysis by Secure-IC.

Oct. 14, 2023