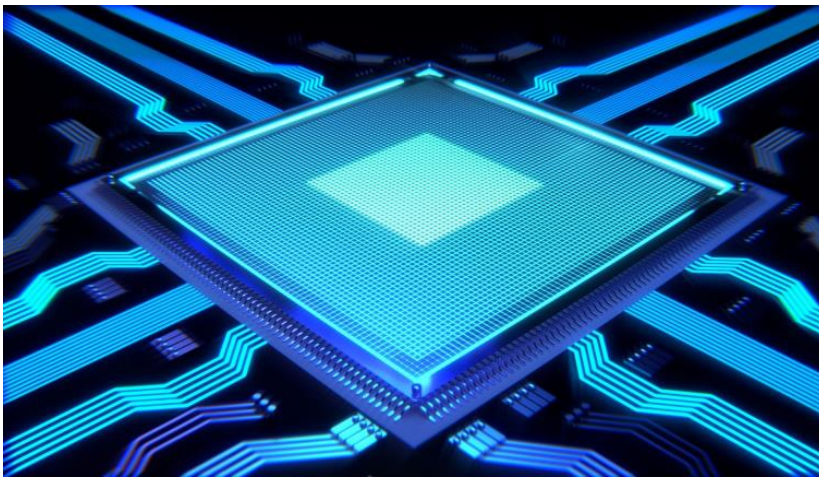
Transparent IT Production for Digital Sovereignty

Digital security gaps affect citizens as well as companies and governments – IT experts plead for the use of verified open source products.



Get out of the black box: Open source hardware can make IT systems more secure (Photo: Pixabay, CC0 Creative Commons).

Whether in the automotive, the energy or the financial sector: information technology is increasingly penetrating all aspects of life. At the same time, security gaps in closed hardware and software produced in globalised supply chains are becoming increasingly incalculable. This is the result reached by IT security experts from the Karlsruhe Institute of Technology (KIT), Fraunhofer Institute for Secure Information Technology, Fraunhofer Singapore, RheinMain University of Applied Sciences, and Technical University of Berlin. In a White Paper on the topic of "digital sovereignty" that they just published, the authors propose that all the steps in the supply chain of IT products be made transparent – from the user software to the tools used in semiconductor fabrication plants.

"Information technology is omnipresent. But there is a danger that these systems might be switched off or manipulated from the outside, or that data might be read without anyone noticing and used against the user," says Arnd Weber, expert for IT security at the Institute for Technology Assessment and Systems Analysis (ITAS) of KIT and a co-author of the paper.

Monika Landgraf
Chief Press Officer,
Head of Corp. Communications

Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen
Phone: +49 721 608-21105
Email: presse@kit.edu

Press contact:

Jonas Moosmüller
ITAS - PR
Phone.: +49 721 608 26796
jonas.moosmueller@kit.edu

Margarete Lehné
Deputy Press Officer
Phone.: +49 721 608-21157
margarete.lehne@kit.edu

Cyberattacks such as WannaCry, security gaps in processor chips, e.g. Meltdown and Spectre, spying Trojan horses, denial of service attacks, such as Mirai, or the most recent attack on the data infrastructure of the German federal government demonstrate how fragile the security of digital infrastructures is.

A key reason for the increasing vulnerability of IT is that “many software and hardware products form a black box”, as Jean-Pierre Seifert says, co-author and head of the group “Security in Telecommunications” at the Technical University of Berlin. This is a threat to the security of every individual as well as to entire industries which rely on the IT technology supplied to them. Even nation states need to worry about the security of their increasingly digitised infrastructures. These problems can also threaten the safety of citizens, e.g. regarding the energy supply, or the functioning of cars. Last but not least, the fact that the production of information technology is concentrated in the U.S. and China reduces the value added in Europe.

Opening the Entire Supply Chain

In principle there is the option of certifying the security characteristics of components and systems. “In view of their complexity, of the difficulty in analysing hardware and of patent rights, this is a very difficult path,” says co-author Michael Kasper of the Fraunhofer Society (Singapore and SIT, Germany). Any attempt to put all the steps in the IT value chain under national control, as aimed at by China and India, misses the point which trading nations face. “Much more promising, in the sense of digital sovereignty, is the approach of building open source hardware, just as we have seen with open source software such as Linux and Android,“ says Michael Kasper. This would also mean that all the tools used to place circuits on semiconductor chips need to be open-sourced.

Open Hardware Communities

By setting up open hardware communities, which verify and test all the components, much like the open source communities do for Linux and BSD, it is possible to prevent design errors and the insertion of back doors, the authors say in their White Paper. However, such communities should be better organised and supported by enterprises or governments, so that faults would not remain unaddressed, as it has sometimes happened in the past. Ideally, these communities should even mathematically prove that all the components exhibit only the specified characteristics, i.e. the desired ones. Such proofs already exist for some open operating system kernels, the authors state. First instances of such a hardware community exist in the U.S., where

companies such as Nvidia and Western Digital plan to use open processor architectures in their products and have therefore entered into cooperation with universities. By taking this open path, not only would industry and end users in Germany and Europe profit, but "ultimately, the whole world would obtain an open and secure basis for all the devices containing IT," co-author Steffen Reith from the RheinMain University of Applied Sciences says. By this means, the concentration of all this knowledge in only two regions of the world would be resolved, including the related centralisation of added value.

Based on a detailed description of the state of research and the steps that are possible, the authors recommend as a first step that investors and policy makers support the development and production of open components and solutions for the Internet of Things. As a second step, the authors recommend the development of highly powerful open hardware.

Arnd Weber, Steffen Reith, Michael Kasper, Dirk Kuhlmann, Jean-Pierre Seifert, and Christoph Krauß: Sovereignty in Information Technology. Security, Safety and Fair Market Access by Openness and Control of the Supply Chain.

The White Paper is available on the website of the related project "Quattro S: Security, Safety, Sovereignty, Social Product":

http://www.QuattroS-Initiative.org/

Being „The Research University in the Helmholtz-Association", KIT creates and imparts knowledge for the society and the environment. It is the objective to make significant contributions to the global challenges in the fields of energy, mobility and information. For this, about 9,300 employees cooperate in a broad range of disciplines in natural sciences, engineering sciences, economics, and the humanities and social sciences. KIT prepares its 26,000 students for responsible tasks in society, industry, and science by offering research-based study programs. Innovation efforts at KIT build a bridge between important scientific findings and their application for the benefit of society, economic prosperity, and the preservation of our natural basis of life.

Since 2010, the KIT has been certified as a family-friendly university.

This press release is available on the internet at www.kit.edu.

The photo may be downloaded under https://pixabay.com/de/prozessor-cpu-computer-chip-2217771/ (CC0 Creative Commons)