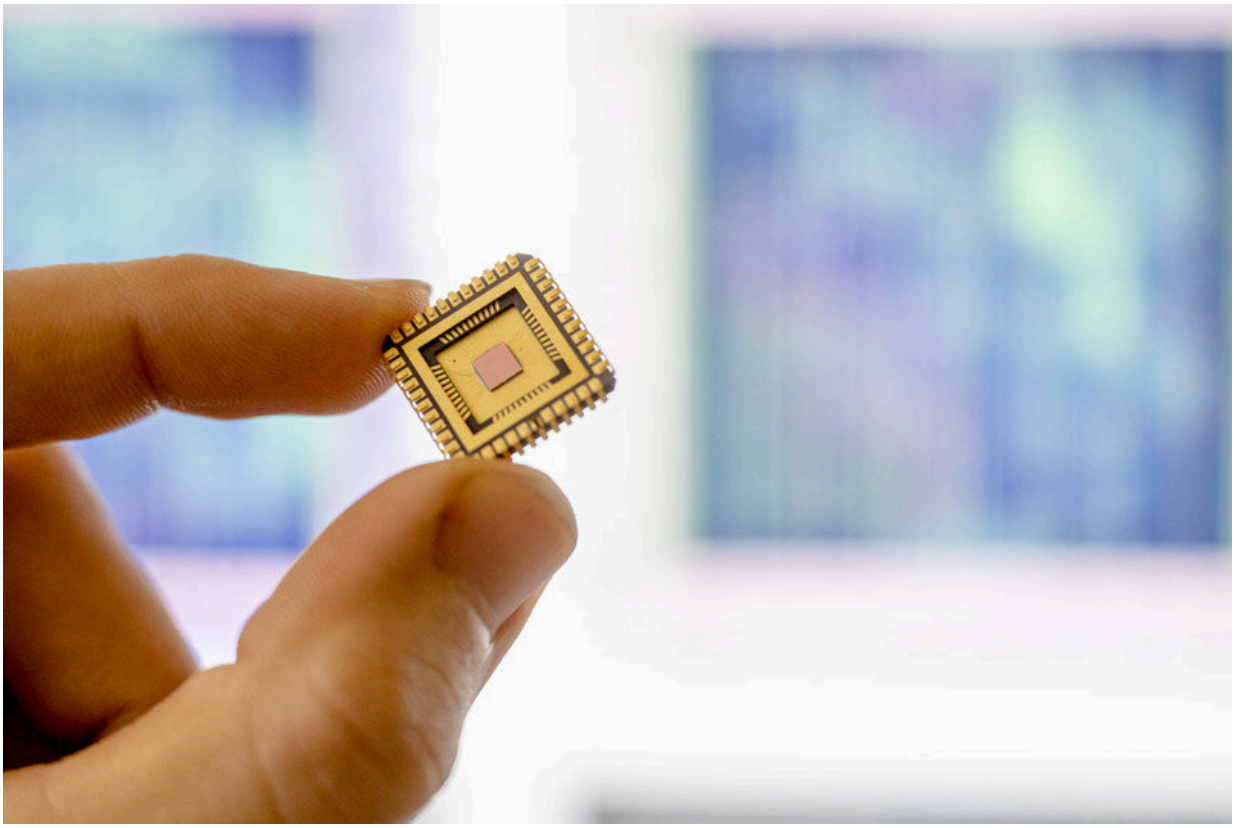
Detecting manipulations in microchips

March 20 2023, by Julia Weiler



For their project, the researchers took thousands of microscopic images of microchips. Pictured here is such a chip in a golden chip package. The chip area that was inspected only measures about two square millimetres. Credit: RUB, Marquard

Attackers have the ability not only to manipulate software, but also to tamper with the hardware. A team from Bochum is devising methods to

detect such tampering.

Security gaps exist not only in software, but also directly in hardware. Attackers might deliberately have them built in in order to attack technical applications on a large scale. Researchers at Ruhr University Bochum, Germany, and the Max Planck Institute for Security and Privacy (MPI-SP) in Bochum are exploring methods of detecting such so-called hardware Trojans. They compared construction plans for chips with electron microscope images of real chips and had an algorithm search for differences. This is how they detected deviations in 37 out of 40 cases.

The team at the CASA Cluster of Excellence (short for Cyber Security in the Age of Large-Scale Adversaries), headed by Dr. Steffen Becker, and the MPI-SP team headed by Endres Puschner, will present their findings at the IEEE Symposium on Security and Privacy, which will take place in San Francisco from 22 to 25 May 2023. The research was conducted in collaboration with Thorben Moos from the Université catholique de Louvain (Belgium) and the Federal Criminal Police Office in Germany.

The researchers released all images of the chips, the design data as well as the analysis algorithms online for free so that other research groups can use the data to conduct further studies. A preprint of the paper is also published as part of the *Proceedings of the IEEE Symposium on Security and Privacy*.

Manufacturing plants as a gateway for hardware Trojans

These days, electronic chips are integrated into countless objects. They are more often than not designed by companies that don't operate their

own production facilities. The construction plans are therefore sent to highly specialized chip factories for production.

"It's conceivable that tiny changes might be inserted into the designs in the factories shortly before production that could override the security of the chips," explains Steffen Becker and gives an example for the possible consequences: "In extreme cases, such hardware Trojans could allow an attacker to paralyze parts of the telecommunications infrastructure at the push of a button."

Identifying differences between chips and construction plans

Becker and Puschner's team analyzed chips produced in the four modern technology sizes of 28, 40, 65 and 90 nanometers. For this purpose, they collaborated with Dr. Thorben Moos, who had designed several chips as part of his Ph.D. research at Ruhr University Bochum and had them manufactured. Thus, the researchers had both the design files and the manufactured chips at their disposal. They obviously couldn't modify the chips after the fact and build in hardware Trojans. And so they employed a trick: rather than manipulating the chips, Thorben Moos changed his designs retroactively in order to create minimal deviations between the construction plans and the chips. Then, the Bochum researchers tested if they could detect these changes without knowing what exactly they had to look for and where.

In the first step, the team at Ruhr University Bochum and MPI-SP had to prepare the chips using complex chemical and mechanical methods in order to take several thousand images of the lowest chip layers with a scanning electron microscope. These layers contain several hundred thousand of the so-called standard cells that carry out logical operations.

"Comparing the chip images and the construction plans turned out to be quite a challenge, because we first had to precisely superimpose the data," says Endres Puschner. In addition, every little impurity on the chip could block the view of certain sections of the image. "On the smallest chip, which is 28 nanometers in size, a single speck of dust or a hair can obscure a whole row of standard cells," says the IT security expert.

Almost all manipulations detected

The researchers used image processing methods to carefully match standard cell for standard cell and looked for deviations between the construction plans and the microscopic images of the chips. "The results give cause for cautious optimism," says Puschner.

For chip sizes of 90, 65 and 40 nanometers, the team successfully identified all modifications. The number of false-positive results totaled 500, i.e. standard cells were flagged as having been modified, although they were in fact untouched.

"With more than 1.5 million standard cells examined, this is a very good rate," says Puschner. It was only with the smallest chip of 28 nanometers that the researchers failed to detect three subtle changes.

Higher detection rate through clean room and optimized algorithms

A better recording quality could remedy this problem in the future. "Scanning electron microscopes do exist that are specifically designed to take chip images," points out Becker. Moreover, using them in a clean room where contamination can be prevented would increase the detection rate even further.

"We also hope that other groups will use our data for follow-up studies," as Steffen Becker outlines potential future developments. "Machine learning could probably improve the detection algorithm to such an extent that it would also detect the changes on the smallest chips that we missed."

More information: A real-world hardware trojan detection case study across four modern CMOS technology generations, *Proceedings of the IEEE Symposium on Security and Privacy* (2023), DOI: 10.1109/SP46215.2023.00044. www.computer.org/csdl/proceedi … 3600a763/1Js0DjYfVXG

Provided by Ruhr-Universitaet-Bochum