Chips under the microscope

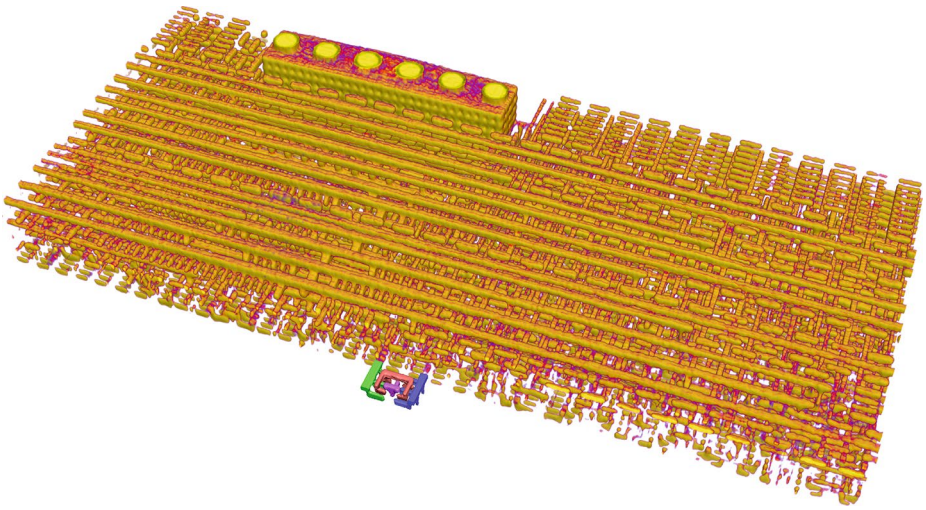
Computer supply chain attacks are a growing concern and approaches that can detect and defend against them are required.

In October last year, *Bloomberg Businessweek* reported that Chinese spies had implanted microchips into specialized servers used by around 30 US companies including Apple and Amazon[1]. The servers were made by the San Jose-based company Supermicro, who employed sub-contractors in China to build their motherboards. The report, which was based on interviews with unnamed US government and corporate sources, alleged that the chips could provide backdoor access to the servers and were inserted during the manufacturing of the motherboards by operatives from the People's Liberation Army.

Questions were subsequently raised about the technical plausibility of the set-up[2] and the story was robustly denied by Apple, Amazon and Supermicro[3]. Apple stated that it "has never found malicious chips, 'hardware manipulations' or vulnerabilities purposely planted in any server" and Amazon that "at no time, past or present, have we ever found any issues relating to modified hardware or malicious chips in SuperMicro motherboards". Supermicro wrote that it "has never found any malicious chips, nor been informed by any customer that such chips have been found". It also later told its customers that an external review of its motherboards found no malicious chips[4].

The *Bloomberg Businessweek* report does, nevertheless, highlight the issue of supply chain security, where concerns about both software[5] and hardware[6] attacks are growing. In the *Bloomberg* article, the chips in question were described as being "not much bigger than a grain of rice"[1]. Technologies are potentially available to identify such devices[7]. But smaller, more discreet attacks are also a possibility. Researchers at the University of Michigan have, for example, shown that an analogue circuit technique can create a microscopic hardware attack that requires only the addition of a single gate to a chip[8]. There is thus a need for new approaches to detect, and defend against, such attacks.

Imaging methods capable of inspecting integrated circuits have a role to play here. In an Article in this issue of *Nature Electronics*, Mirko Holler and colleagues show that a technique known as ptychographic X-ray laminography can be used to create three-dimensional images of integrated circuits. Such circuit imaging typically requires a range of instruments with a range of resolutions, from optical microscopy on the millimetre scale to transmission electron microscopy on the nanometre scale. This new approach can, in contrast, provide images of an entire chip and then zoom into specific sub-regions.



Three-dimensional reconstruction of an integrated circuit created using ptychographic X-ray laminography. Figure adapted from the Article by Holler and colleagues, Springer Nature Ltd.

The researchers — who are based at the Paul Scherrer Institut, ETH Zürich, the École polytechnique fédérale de Lausanne and the University of Southern California — illustrate the capabilities of the technique by using it to analyse chips fabricated with 16 nm FinFET technology, achieving a resolution of 18.9 nm. There are though some limitations. As Joseph Kline at the US National Institute of Standards and Technology explains in an accompanying News & Views article, the wider application of the method is currently restricted by a dependency on large facilities — a synchrotron or an X-ray free-electron laser. X-ray ptychography, which combines scanning X-ray microscopy and coherent diffractive imaging, requires X-rays with a brightness significantly higher than what compact X-rays sources can offer. And while compact X-ray free-electron lasers have been proposed[9], they remain only at an initial stage of development.

Beyond detecting malicious modifications, these imaging capabilities are also of potential value in the characterization and failure analysis of electronic devices. As we recently highlighted in the journal[10], metrology methods are a key component in the development and manufacturing of devices. But advances in such methods are required in order to keep pace with advances in device design. For the approach of Holler and colleagues, an improved resolution may be necessary to address current and future cutting-edge devices with the smallest feature sizes. However, and as the researchers explain in their Article, the resolution of the technique could potentially be pushed down to around 2 nm, though innovations in a range of areas will be required to bring such capabilities into focus. ❐

Published online: 15 October 2019
https://doi.org/10.1038/s41928-019-0325-z

References

1. Robertson, J. & Riley, M. The big hack: how China used a tiny chip to infiltrate U.S. companies. *Bloomberg Businessweek* https://go.nature.com/30Ri0Ag (4 October 2018).
2. Kennedy, P. Investigating implausible Bloomberg Supermicro stories. *STH* https://go.nature.com/2pJ56ap (22 October 2018).
3. Robertson, J. & Riley, M. The big hack: statements from Amazon, Apple, Supermicro, and the Chinese Government. *Bloomberg Businessweek* https://go.nature.com/3559rF9 (4 October 2018).
4. Menn, J. Super Micro says review found no malicious chips in motherboards. *Reuters* https://go.nature.com/31M0MFt (11 December 2018).
5. Greenberg, A. A mysterious hacker group is on a supply chain hijacking spree. *Wired* https://go.nature.com/336nkkL (3 May 2019).
6. Schneier, B. Every part of the supply chain can be attacked. *The New York Times* https://go.nature.com/2AGhJVZ (25 September 2019).
7. Moore, S. K. This tech would have spotted the secret Chinese chip in seconds. *IEEE Spectrum* https://go.nature.com/2LKE8HZ (4 October 2018).
8. Yang, K. et al. *2016 IEEE Symp. Security and Privacy* https://doi.org/10.1109/SP.2016.10 (IEEE, 2016).
9. Gadjev, I. et al. *Sci. Rep.* **9**, 532 (2019).
10. *Nat. Electron.* **2**, 207 (2019).