Vulnerability of cloud service hardware uncovered

May 31 2019

Field-programmable gate arrays (FPGAs) are more flexible than common specialized computer chips – and they used to be seen as particularly secure. Credit: Gnad, KIT

Field-programmable gate arrays (FPGAs) are kind of like a computer manufacturer's Lego bricks: electronic components that can be employed in a more flexible way than other computer chips. Even large data centers that are dedicated to cloud services, such as those provided by some big technology companies, often resort to FPGAs. To date, the use of such services has been considered as relatively secure. Recently, however, scientists at Karlsruhe Institute of Technology (KIT) uncovered potential gateways for cyber criminals, as they explain in a report published in the IACR journal.

While conventional computer chips mostly perform a very specific task that never changes, FPGAs are capable of assuming nearly every function of any other computer chip. This often makes them first choice for the development of new devices or systems. "FPGAs are for example built into the first product batch of a new device because, unlike special chips whose development only pays off when produced in high volumes, FPGAs can still be modified later," says Dennis Gnad, a member of the Institute of Computer Engineering (ITEC) at KIT. The computer scientist compares this to a sculpture made from reusable Lego bricks instead of a modeling compound that can no longer be modified once it has hardened.

Therefore, the fields of application of these digital multi-talents span the most diverse sectors, such as smartphones, networks, the Internet, medical engineering, vehicle electronics, or aerospace. Having said that, FPGAs stand out by their comparatively low current consumption, which makes them ideally suited for the server farms run by cloud service providers. A further asset of these programmable chips is that they can be partitioned at will. "The upper half of the FPGA can be allocated to one customer, the lower half to a second one," says Jonas Krautter, another ITEC member. Such a use scenario is highly desirable for cloud services, where tasks related e.g. to databases, AI applications, such as machine learning, or financial applications have to be performed.

Multiple-user access facilitates attacks

Gnad describes the problem as follows: "The concurrent use of an FPGA chip by multiple users opens a gateway for malicious attacks." Ironically, just the versatility of FPGAs enables clever hackers to carry out so-called side-channel attacks. In a side-channel attack, cyber criminals use the energy consumption of the chip to retrieve information allowing them to break its encryption. Gnad warns that such chip-internal measurements enable a malicious cloud service customer to spy on

another. What is more, hackers are not only able to track down such telltale current consumption fluctuations—they can even fake them. "This way, it is possible to tamper with the calculations of other customers or even to crash the chip altogether, possibly resulting in data losses," Krautter explains. Gnad adds that similar hazards exist for other computer chips as well. This includes those used frequently for IoT applications, such as smart heating control or lighting systems.

To solve the problem, Gnad and Krautter adopted an approach that consists in restricting the immediate access of users to the FPGAs. "The challenge is to reliably filter out malicious users without tying up the legitimate ones too much," says Gnad.

More information: Gnad, D. et al. Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(3), 305-339. doi.org/10.13154/tches.v2019.i3.305-339

KIT Information Systems Technologies Center: www.kcist.kit.edu

Provided by Karlsruhe Institute of Technology

Citation: Vulnerability of cloud service hardware uncovered (2019, May 31) retrieved 26 March 2023 from https://phys.org/news/2019-05-vulnerability-cloud-hardware-uncovered.html