How do you know that your Cloud operator does not cheat?

No physical security in the Cloud

The security of a system is usually based on the physical security of the hardware. In a Cloud setup, this basic assumption can not be assured as the system runs as a virtual machine (VM) on the operator’s hardware. The operator
- has access to all files,
- has access to the main memory,
- can interfere with the communication,
- can manipulate the control flow.

The Cloud operator can even hide manipulations by creating a virtual view for the administrator.

Potential attacks by the Cloud operator

These security goals can be violated by the Cloud operator running a VM:

Confidentiality
- Cloud operator sells knowledge gained from files, memory, or usage statistics

Integrity
- Cloud operator replaces application with another, e.g., reducing precision
- Cloud operator deletes files to save space, e.g., files not used for a long time

Availability
- Cloud operator provides less resources
- Cloud operator is not able to scale up

Not preventing it, but detecting it

Detection mechanisms

User may not be able to prevent the manipulation, but can sign a service level agreement (SLA) and negotiate fines to be paid. For the Cloud operator, the manipulation are no longer lucrative if the risk to be discovered and the fine is high enough. However, a mechanism is needed to detect an attack reliably to enforce the (SLA). In our work, we develop such detection mechanisms for various attack types and analyze in depth how a bogus Cloud operator may still avoid the detection.

Dr.-Ing. Jörg Schneider
www.kbs.tu-berlin.de
Example: Do you get what you pay for?

The Cloud operator could save money by massively underprovisioning the virtual machines. Performance metrics measurable from the outside, like throughput or response time, depend heavily on the user’s application. However, a normal benchmark run can be tampered by:

- Skipping the benchmark (replace by `sleep`)
- Precalculating the result (replace by `sleep; print result`)
- Change program or data (replace by faster algorithm or use more convenient input data)
- Temporarily increase resources

We introduced a novel tamper resistant benchmark approach to assess the performance of instances in the Cloud. Our benchmark is based on proof-of-work functions and enables the Cloud client to verify the compute performance within its virtual machine. We used proof-of-work functions to enhance the benchmark and identified the key properties a proof-of-work function needs to be used as a benchmark in the Cloud. We selected three functions and implemented them in a prototype benchmark. Experiments showed that the accuracy of this prototype was comparable with the reference benchmark SPEC CPU2006. Furthermore, we analyzed possible manipulations by the Cloud operator and identified four attack vectors. One of them cannot be addressed from within the virtual machine. However, we showed that our novel benchmark disables the other three attack vectors.

Our Solution: An uncheatable benchmark

Dr.-Ing. Jörg Schneider
www.kbs.tu-berlin.de