ScalPerf'21:
SCALABLE APPROACHES to HIGH PERFORMANCE and HIGH PRODUCTIVITY COMPUTING

September 19-24, 2021

Bertinoro international Center for informatics
http://www.bici.eu

TOPIC for DISCUSSION SESSIONS

Dependable Computing[*]

Dependability and security are highly desirable properties of computing system, but they have proven hard to fully achieve at affordable costs, due to technical and economical obstacles. This state of affairs is increasingly unsatisfactory, as computing becomes increasingly pervasive, in many aspects of life and society. Fortunately, advances in the theoretical understanding of the issues, together with the steady growth of computing power, hold the promise to make the overheads of achieving substantially higher degrees of security and dependability affordable. In this context, it seems appropriate to rethink all aspects of performance and scalability of dependable and secure systems. A number of desirable properties of dependable computing are outlined below. Suggestions are solicited from participants, both to expand/refine the desirable properties and to identify the relevant technical issues that are likely to require further research or implementation efforts, given the state of the art.

1. Computing is now indispensable to the day-to-day way of life of a large fraction of the world population. It is how we work, shop, and socialize. Therefore, users of computing resources must have assurances about how the computations the depend on are performed.

2. We identify two classes of *players*: **data owners**, who want to have their data processed, and **processing owners**, who have the facilities for processing that data, typically as a service to the data owners. Processing data creates more data, which then also belongs to the data owners of the original data.

3. While being processed, data must be protected according to several aspects:

   - **Confidentiality:** Data must not be visible in the clear to anyone other than the corresponding data owners, or entities authorized by them.
   - **Authenticity:** Data being processed must be assured to be *authentic*. That is, it was provided or generated by the owner or another trusted entity.

[*] The organizers would like to thank Jose Moreira, of IBM Research, for substantial help with this document.

- **Freshness:** Data being operated on corresponds to the most recent version of that data as opposed to some old (although authentic) data.

  Collectively, these protections ensure *data integrity*. That is, data was not stolen, tampered or modified in any way contrary to the wishes of the data owner.

4. Processing facilities that provide at least some (and ideally all) of the protections listed above are called *secure processing facilities*. Data owners need mechanisms to verify that the facility that will process their data is indeed a secure computing facility.

5. Processing owners need mechanisms to certify that they have provided (at least) a certain amount of computing resources to process data from a data owner. This is critical, for example, for billing purposes.

6. Ensuring the integrity of data, as described above, in turn requires supporting forms of integrity in the computing systems that is processing the data:

   - **Address integrity:** There is no tampering of memory addresses holding the data.
   - **Control-flow integrity:** The program follows its control-flow as intended by the author.
   - **Isolation integrity:** Partitions, virtual machines, and processes sharing a processing facility are isolated from each other as well as from other users and administrators of that facility.
   - **Resource integrity:** The resources in the computing facility, including hardware and software, are available and authentic, able to provide the advertised services.
   - **Physical integrity:** The resources in the computing facility are protected from physical damage, theft, loss of power, and/or tampering.