Subject: comments in IFIP Workshop final discussion session
From: Doug Blough <doug.blough@ece.gatech.edu>
Date: 01/07/2018 17:31
To: Paulo VERISSIMO <paulo.verissimo@uni.lu>
CC: <brian.randell@newcastle.ac.uk>, Doug Blough <doug.blough@ece.gatech.edu>

Hi Paulo,

Here is my attempt to recreate the comments I made in the discussion at the end of the blockchain workshop:

A comment was made that the large amount of computation and very high energy consumption incurred by miners in permissionless blockchains is an indication of the cost of establishing trust in such environments. Permissionless blockchains are peer-to-peer systems that anyone can join and where participants do not know anything about their fellow participants. Establishing trust in such a completely open peer-to-peer environments is an unsolved problem. Despite devoting enormous resources to the trust problem, permissionless blockchains are susceptible to known attacks some of which have been carried out in actual systems resulting in millions of US dollars in losses.
While new proposed methods for establishing trust in such environments can make attacks more difficult to carry out, to date all such methods have known vulnerabilities.

Due to the lack of satisfactory means of establishing trust in the completely open peer-to-peer environments associated with permissionless blockchains, the dependability community should do its best to warn the broader community about the inherent risks of trusting such systems. In addition, we should devote significant research efforts to designing, optimizing, evaluating, and validating technologies associated with permissioned blockchains, where participants are known and established theories of Byzantine fault tolerance can be applied to provide trusted execution.

It was great to see everyone and I really enjoyed the meeting and discussions.

Best,

Doug