Towards a General Purpose Trusted Computing Platform for All Vendors and Applications

Xiaokang Wang, Master of Science in Computer Science

University of Dublin, Trinity College, 2021

Supervisor: Donal O'Mahony

The objective of this research is to explore the possibility to create a trusted computing platform that executes untampered programmable logic from multiple uncoordinated software vendors at a reasonable speed while protecting the data protection rights of the users with data usage and transfer transparency.

A specification was created to support all desired characteristics. It defines a manifest that defines the interface of interaction between the trusted computing platform and a programmable executable binary. The trusted computing platform will execute the executable binary data defined in the manifest in the form of Web Assembly in an isolated environment if the invocation request from the trusted computing client satisfies the requirements defined in the manifest. The input and output data is managed by the trusted computing platform, with checking performed on the input and output data based on the invocation request, manifest, and the input themselves. Different type of input and outputs allows the programmable logic to communicate with the trusted computing client using plain text, with other trusted computing platform using session, with users using protected input and output, with tamper-resistant storage with non-violate storage, and receive high-quality random numbers using random.

A proof of concept implementation of this specification is created to evaluate the functionality of this specification. The specification shows it is possible to implement this specification in software with the technologies currently available. A demonstration application is created to showcase the ability of the trusted computing platform to protect the data protection right of the users.

The conclusion of this paper shows that it is possible to create a trusted computing platform that satisfy all the requirements mentioned according to the specification defined with existing technologies.