An Ontology of a Computing Device Secured with Trusted Platform Module 2.0

Jiun Yi Yap and Allan Tomlinson

Royal Holloway, University of London

The ability of an ontology to describe trustworthy computing devices with a standard vocabulary enables experts to share a common understanding of such technologies with developers. To this end, we research on and contribute an ontology for describing a computing device secured with Trusted Platform Module (TPM) version 2.0. This ontology represents information about the capability of the computing device, TPM 2.0 and notions of security and trust. They are characterized at different abstract level. It is based on the Web Ontology Language (OWL) and recorded in Resource Description Framework (RDF) / eXtensible Markup Language (XML) format. A developer can review the ontology based description by asking competency questions. Finally, we demonstrate how to translate the competency questions into SPARQL queries.