Abstract

Binary Attestation is currently used in trusted computing environments involving the standard TCG attestation mechanism. However, this mechanism still has deficiencies in terms of flexibility, privacy and scalability. Thus, to overcome these problems, Property-based Attestation has been proposed. Two important issues should be considered in the context of property-based attestation; these include the content of the property and the protocol design. In this study, the researchers proposed platform property certificate, based on the current certificates of the system as the model’s property. In addition, a client-server attestation protocol that could apply this particular property is also proposed. In order to show the feasibility of the model, the proposed model was implemented. The results of the implementation showed that the model is efficient to be used to accept and reject valid and invalid inputs. Hence, security aspects listed as privacy, flexibility, scalability and also integrity of the model is checked, while it is crucial to note that it also fulfils the requirements of property-based attestation with TCG standard specifications.

Index Terms

Computer Science Security

Keywords

Network-level security and protection Trusted Computing Public-Private key Authentication