Abstract

ArmoredSoftware is ...

1 Introduction

The objective of ArmoredSoftware is to *provide a portable trusted computing capsule for applications executing in the cloud.* This capsule, referred to as *armor*, provides three major functions:

Appraisal – Request and assess measurement information from the operational environment and other armored components.

Measurement – Gather run-time measurement information from its application

Attestation – Assemble and deliver evidence to appraisers in a manner that assures measurement integrity

and is based on concepts from **?**.

Figure **??** graphically depicts the major architectural components of a protected application. The *application* is the application to be protected by the infrastructure. The *measurement* component performs measurement operations on the running application while the *attestation* component gathers measurements and delivers them with cryptographic assurance of integrity and confidentiality. The *appraisal* component requests information from the environment and other components to assess the overall operational environment. *Access control* governs access to all critical resources in the protected application to assure secrets are preserved and enforce information flow restrictions.

Figure **??** graphically represents the interaction among protected components while Figure **??** shows the sequencing of interactions during appraisal. A component's appraisal module will request information from a second component's attestation module. The attestation model will select an attestation protocol that instructs the measurer what information to gather and in what sequence. The measurer executes that protocol that in turn gathers information from the running process, accesses the module's virtual TPM (vTPM) and makes appraisal requests of other ArmoredSoftware instances. The attestation module assembles measurement results into a evidence package that is returned to the requesting appraiser with cryptographic assurances of integrity and confidentiality as required. Upon receiving the package, the appraiser assesses cryptographic signatures and encryption to determine the trustworthiness of the measurements, then assesses measurements to determine the trustworthiness of the component being appraised.[1]

[1] Note that the same process occurs when appraising the component's operational environment with either the appraiser or target replaced by operational infrastructure.

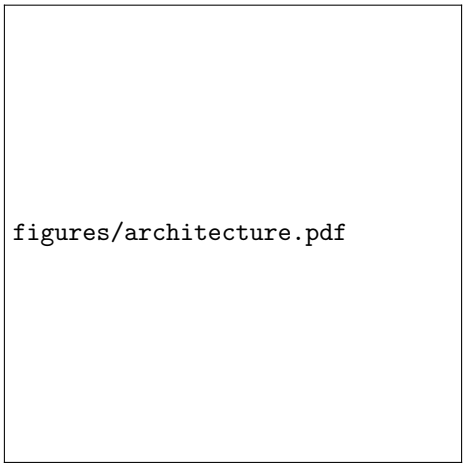

Figure 1: ArmoredSoftware component architecture showing major components of the remote attestation process.

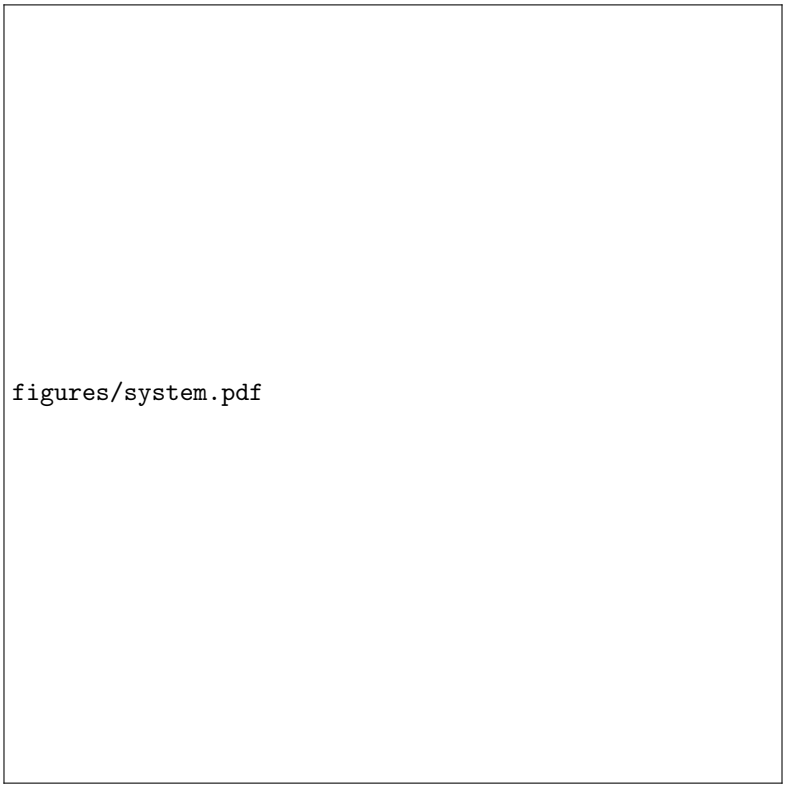

Figure 2: Typical interaction among armored components with an appraiser interacting with an attestation agent to gather information.

