OpenAttestation SDK ReadMe

March 2012

Contents

1 Acknowledgements

OpenAttestation SDK is built based on Host Integrity at Startup (HIS) project developed by National Information Assurance research laboratory (NIARL) to measure and report status of remote host platforms which contain a Trusted Platform Module (TPM).

2 Intended Audients

The intended audients of this document are Independent Software vendors (ISV), developers who are to integrate OpenAttestation SDK into ISV's cloud management tools for product releases. Administrators who are to take advantage of remote host integrity checking capability for their cloud services by using ISV software packages which has OpenAttestation SDK integrated

3 OpenAttestation SDK

3.1 Security Warning

OpenAttestation SDK, by itself, is not a secured software or commercial ready product. It is expected that ISVs must enhance and integrate the SDK with their software stacks for security evaluation/validation cycles before production/distribution

3.2 What is

OpenAttestation SDK is software components to add cloud providers with capability of establishing hosts/clients integrity by remotely retrieve integrity reports saved in Hosts/Clients TPM

The SDK is expected to be security enhanced, integrated with ISV's cloud management software, and distributed/supported by ISV to cloud providers

The integrated ISV software to be hosted and operated by cloud providers

3.3 What is Not

SDK does not add security enhancement to existing database or network infrastructure, rather it uses underlying infrastructure supported by ISVs and operated by cloud providers

3.4 Must do

Attestation service is hosted by cloud providers, Hosts/Clients privacy is cloud providers or ISVs responsibility

ISVs must follow industry security standards and recommendation to integrate OpenAttestation SDK with their software stack

Cloud providers should follow industry security standards and recommendation to operate and maintain secured infrastructure

4 Security Recommendation to Software Vendors

Besides recommendation bellow, ISVs should follow industry security standards in integrating OpenAttestation into their software stacks

OppenAttestation SDK exposing APIs, Integrity query API for management software to remotely query host(s) integrity and Whitelist API for administers to remotely setup/update good, know measurement data. Where these APIs should be access controlled from general users due to privacy and security purpose. To ensure access controls to APIs, ISV should perform following designs –

1. ISV should clearly document than a deployment should always setup Tomcat 2-way SSL/TLS authentication between Access platforms and Attestation service in order to ensure controlled platforms can access to APIs. Fail to setup authentication, a cloud infrastructure's privacy and security can be compromised
2. ISV should work with Cloud provider to establish their credential control in accessing APIs. Note all the APIs requests to Attestation server has an authentication blob which enables ISV software to pass access credential to attestation service, which attestation service is only to pass to an ISV authentication specific validation service in SDK. It is ISV's responsibility who integrates SDK should fully implement the validation service.

ISV should enhance HostAgent installation package to be created into a secured smart media to keep attestation service keys within controlled, secured access environment

5 Recommendation to Cloud providers

Cloud providers should follow industry security standards in operates and maintain infrastructure

Attestation infrastructure takes PrivacyCA approach to certificate Hosts TPM keys. Cloud providers should securely safe-keeping PrivacyCA and EKsigning Key pairs.

Attestation service installation –

1. Attestation service and management tools accessing API services are Root of Trust of overall cloud infrastructure – Cloud provider must ensure these components are installed with underlying systems are in a trusted state
2. Cloud provider must ensure the correct PrivacyCA certificate is installed into Appraiser
3. Whitelist database must be kept in a secured, controlled environment

HostAgent, agent code to be installed into Hosts, installation must insure

1. Host is in a trusted state for HostAgent installation
2. HostAgent must be installed by a trusted entity with auditable process
3. EKsigningKey must not be installed into Host