Integrity measurements for stronger cloud-based authentication

John Žic[1]
Thomas Hardjono[2]

[1]CSIRO Computational Informatics

[2]MIT Kerberos and Internet of Trust

Trust in the Digital World: Enabling the Economies of Trust

Motivation

- Strong enterprise push to outsource IT infrastructure and services to Cloud provider solutions

  Cost savings from reduced spend on infrastructure and maintenance

  Cost increases from impact on existing system security and privacy

- Restating: adopting Cloud provider services means a change to the Enterprise's business model for handling information security and privacy, as well as how it controls information.

- **Trust** needs to extend beyond an enterprise to include a third party (Cloud) service providers.

So how do we extend trust beyond the enterprise into a collaborative environment?

Three principles of trustworthy collaboration

1. Agreed upon contracts.
2. Demonstrable, verifiable adherance to the agreed contract.
3. Established methods for resolution of exceptions and disputes.

Scenario 1

Enterprise employee accessing cloud-based applications

- Employees should not notice any difference in accessing cloud-based or enterprise-local services
- Authentication and authorisation information needs to be conveyed from the enterprise to the Cloud service provider
- Enterprise needs to remain the authoritative source

Scenario 2

Enterprise with in-bound institutional customers

- Enterprise-A and Enterprise-B share a cloud-based application
- Enterprise-A has a customer dealing with Enterprise-B employee accessing a cloud-based application
- Authentication and authorisation information needs to be conveyed from Enterprise-B into the cloud-based application within the domain or realm of Enterprise-A

Bootstrapping trust in cloud-based services

- Trust Frameworks require defined Levels of Assurance to raise confidence in the quality of authentication performed by an indentity-based service in the cloud
- Identity service providers base their access decisions on knowledge about the state of the computing platforms and devices that clients use to access remote cloud-based applications.
- Any solution proposed needs to have a high degree of interoperability with exisiting “enterprise” authentication and authorisation infrastructures.

Our proposal

Based on

- Cloud-based Integrity Measurement Service (cIMS)
- Use of a client-side trusted computing environment capable of performing integrity measurements used by the cIMS
- Use the classic SAML 2.0 ecosystem in order to maximise existing interoperability

Trust Extension Device (TED)

A portable trustworthy computing system concept demonstrator

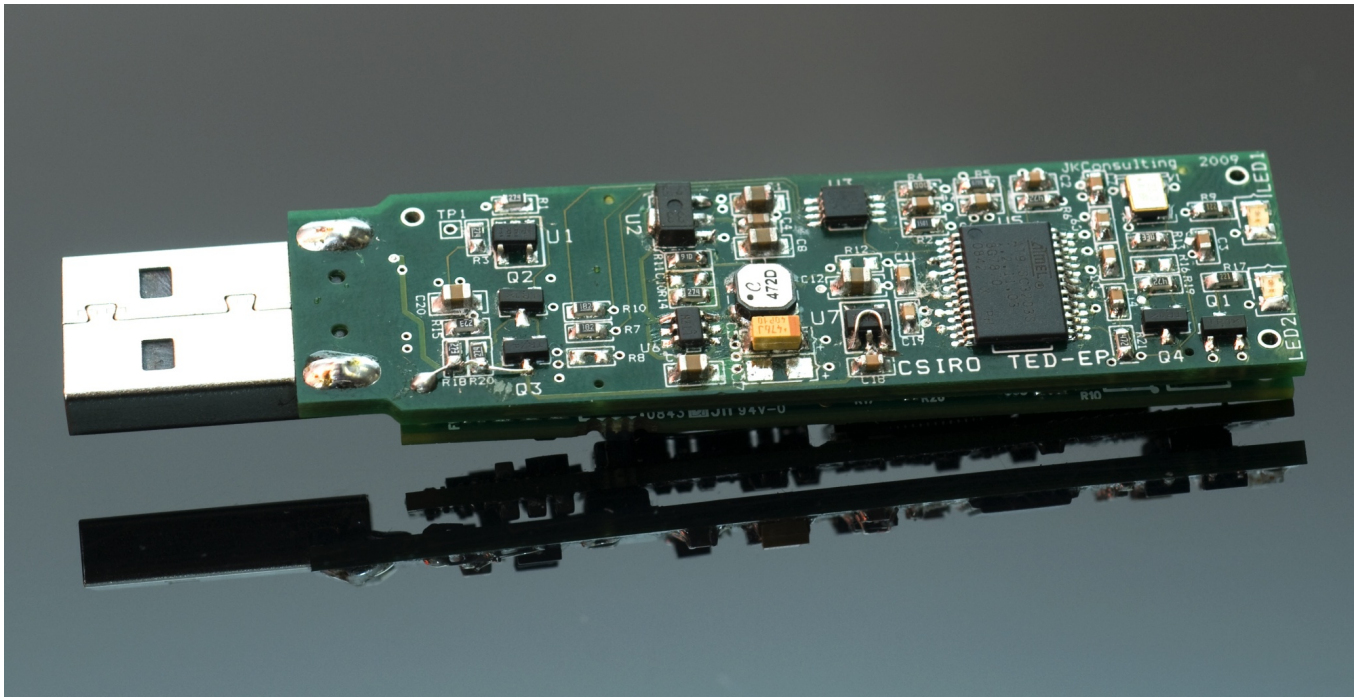
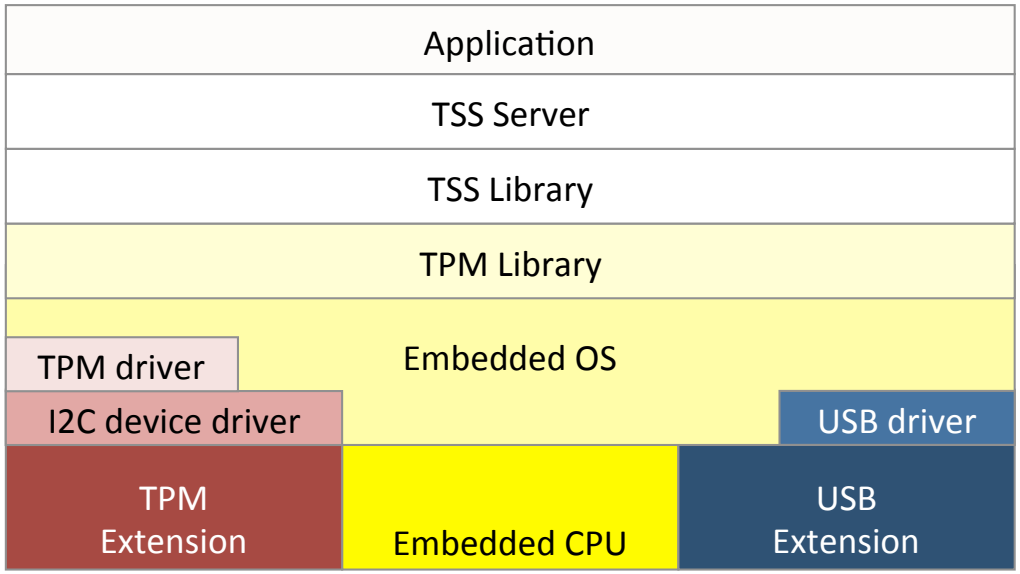


Figure: TED hardware prototype, 2009

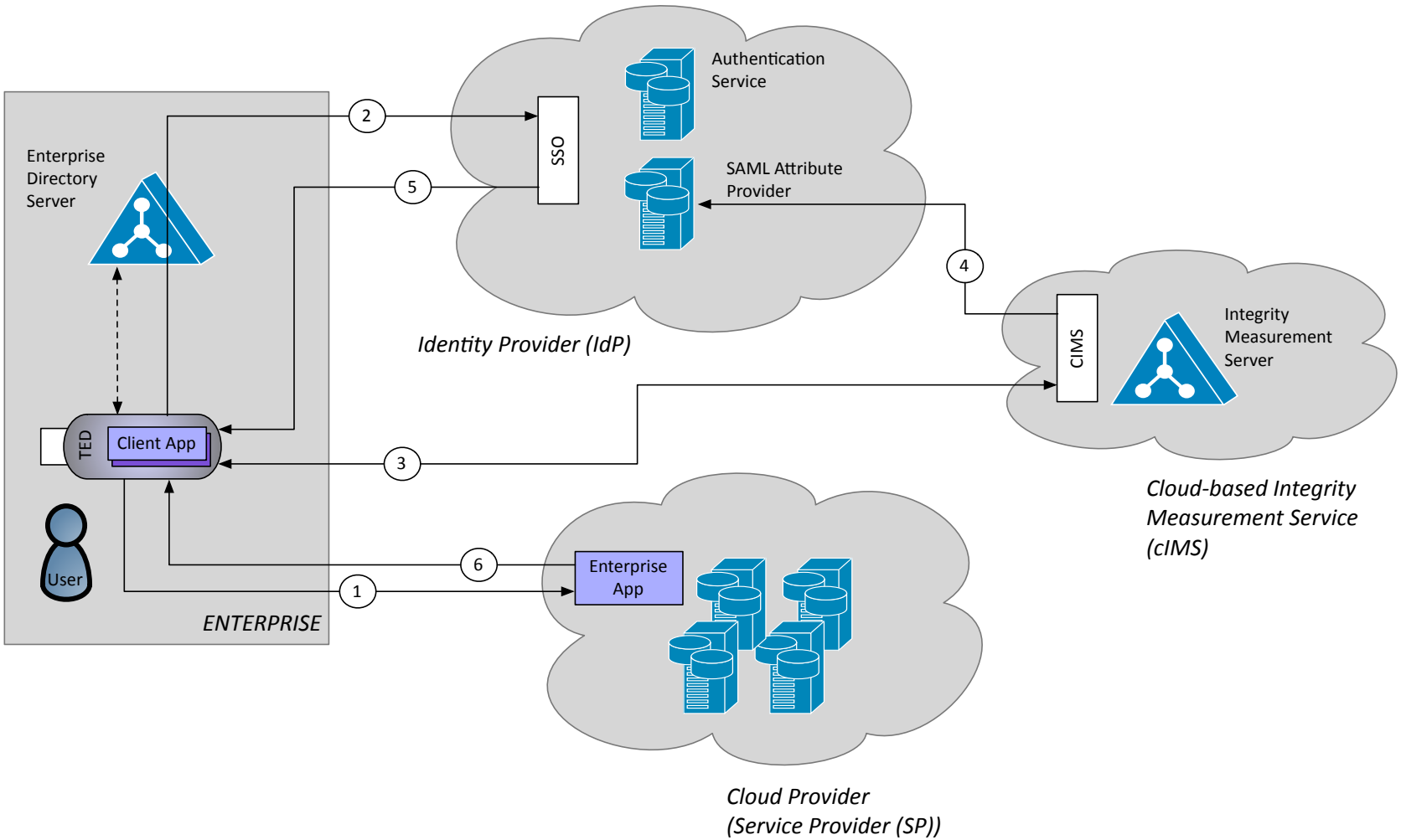
TED Features

- USB sized embedded computer running Linux with integrated TPM cryptographic microcontroller
- TPM offers:
  - integrity checks;
  - crypto functions;
  - keys and certificates storage
- Supports dedicated client applications and libraries.
- No user interface - only secure network connectivity and power

TED Software Stack



Cloud based integrity measurement architecture



Architectural Entities

EDS Standard directory services, under the control of the Enterprise.

IdP as per SAML Core and SAML Profiles specifications.

TED is issued to an employee of the Enterprise. Contains the Enterprise Client App.

Architectural Entities (2)

cIMS performs the Integrity measurement and evaluation of the Client App and associated platform (the TED). Returns an *Trust Score* based on agreed upon measurements.

Cloud Provider corresponds to a SAML 2.0 *Service Provider*. Uses the signed SAML assertion that include LOA values from the IdP to control access to the User of resources or services.

Protocol Overview 1

1. Client App requests access to Cloud Provider App
   - Cloud Provider redirects Client to the IdP for authentication.
   - Redirection includes signed *SAML 2.0 integrity schema* capturing the components of the Client's platform that Cloud Provider needs integrity checked.
2. Client authenticates to IdP.
   - Client redirected by CP to IdP for authentication (e.g. based on SAML 2.0 SSO profile)
   - Client authenticated by IdP and redirected to the cIMS selected by the IdP.

Protocol overview 2

3. The cIMS evaluates the integrity of the Client (including App).
   - Client can the initiate integrity check on the TED, following the previously sent schema.
   - TED attests its integrity in a signed report (this is done as part of the underlying TPM protocols) to the cIMS.

4. cMIS forwards a Trust Score to the IdP.
   - cIMS generates the Trust Score based on the information from the TED's signed report.
   - Trust Score is then sent to the IdP.

Protocol overview 3

5. IdP issues SAML 2.0 assertions with a newly calculated LOA.
   - The IdP compares the Trust Score agains the access control policies stored by the IdP
   - The IdP issues a signed assertion containing its calculated LOA value(s).
   - Multiple LOA values are permitted since they could capture additional second factor authentication used (e.g. biometrics).

6. Client sends request to the Cloud Provider.
   - Client forwards the received assertion containing the LOA to the Cloud Provider.
   - The CP then evaluates the LOA values against the defined access policies to determine with access is permitted or not.

Summary

By putting in place:

- Defined statements of expected configurations of the client (and other critical entities within the system)
- Building on established protocols (such as the attestation protocol of TPM and SAML 2.0 profiles and protocols)

we have met 2/3 requirements for trusted collaboration.

The remaining requirement - to be able to handle exceptional conditons and disputes - needs to be met.

Future work

- Introduction of an accountability service, which keeps, securely and irrefutably, records of critical transactions. This service can be used to handle the system exceptions, failures and disputes.
- Carry out trials of the concepts presented here in extending the standard Kerberos protocol to give higher levels of assurance to identity claims made to cloud service providers.
- Hardjono, Greenwood and Pentland have proposed using the techniques here in assuring that the security requirements of the MIT OpenPDS (Open Personal Data Store) are fully met.