My Private Cloud Overview

A Trust, Privacy and Security Infrastructure for the Cloud

David W Chadwick, Stijn F Lievens
School of Computing
University of Kent
Canterbury, UK
[d.w.chadwick][s.f.lievens] @kent.ac.uk

Jerry I den Hartog
Faculty of Mathematics and Computer Science
Technische Universiteit Eindhoven,
Eindhoven, NL
j.d.hartog@tue.nl

Andreas Pashalidis
KU. Leuven/IBBT,
ESAT/SCD-COSIC
Kasteelpark Arenberg 1
Leuven, Belgium
andreas.pashalidis@esat.kuleuven.be

Joseph Alhadeff
VP Global Public Policy
Chief Privacy Strategist
Oracle
Washington DC, USA
joseph.alhadeff@oracle.com

***Abstract*— Based on the assumption that cloud providers can be trusted (to a certain extent) we define a trust, security and privacy preserving infrastructure that relies on trusted cloud providers to operate properly. Working in tandem with legal agreements, our open source software supports: trust and reputation management, sticky policies with fine grained access controls, privacy preserving delegation of authority, federated identity management, different levels of assurance and configurable audit trails. Armed with these tools, cloud service providers are then able to offer a reliable privacy preserving infrastructure-as-a-service to their clients.**

Keywords; Security, Trust, Privacy, Sticky Policies, Trust Negotiation, Audit, Reputation

I. OVERVIEW

For the last three years the EC TAS3 integrated project (www.tas3.eu) has been building a trust, privacy and security (TPS) infrastructure for web services. The project assumes that service providers would like to offer trustworthy services to their customers if the cost of doing so is not prohibitive, i.e. if tools and mechanisms are readily available to help them. TAS3's objective is to provide these at a minimum cost through a series of open source tools, procedures and services. The resulting TPS infrastructure is provided as a set of web services, so that cloud IaaS, PaaS and SaaS providers can build their own services upon these (see Figure 1). A cloud IaaS provider will provide machines to users containing the interfaces to the authorization service, audit service, trust negotiation service etc. so that users can build their own TPS applications or platforms. A cloud PaaS provider will add its own platform tools in addition to the TPS ones, whilst a cloud SaaS provider will provide fully operational TPS enabled applications to its users.

Each TPS infrastructure requires a trusted third party, the Trust Network Operator (TNO) to oversee its operation and ensure that all the required services are operational. In order to offer a TPS-enhanced service, a cloud service provider (CSP) must "join the TN" by asking the TNO to perform a series of validation tests to confirm that its TPS service is running correctly. The CSP then signs a contract with the TNO to say that it will honor users' privacy policies and provide the TN's audit service with an audit summary of all accesses to its users' personal information. It further agrees that in cases of disputes with its users, the TN auditor may inspect its detailed audit trails to determine the sequence of disputed events and make a judgment. The CSP then joins the trust network, its services are entered in the TN's directory of services, and it publishes its terms and conditions to prospective users.

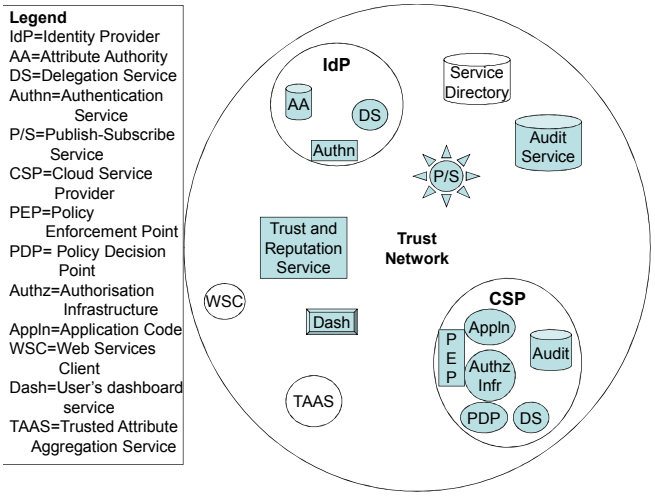

Figure 1. Components of the Cloud Trust, Security and Privacy Infrastructure

Contracts play the expected role of binding together users and CSPs to a set of terms and conditions, but also provide the needed binding to minimum policies, practices and technical requirements needed to operate a TPS. At the highest level, the high level policies and obligations are set forth in a Trust Network Agreement. The binding to polices, practices and technical requirements is supported by an intake process where the capacity of prospective CSPs to meet the requirements is evaluated. These concepts and governance structure are built with the objective of enhancing trust across a complex ecosystem of service providers that may not be in direct contact or even known to an individual using a particular CSP. It is not possible for individuals to control or comprehend the myriad options and delivery mechanisms of CSPs. This may not be the case where an individual has a defined service provided by a known provider, but cloud services are progressively including multiple service providers and multiple services creating a need to enable trust across the cloud ecosystem. A

TAS3 type governance architecture that establishes minimum requirements of privacy and security, which all providers use as a baseline, combined with giving users both a complaint and remediation process, which enables them to exercise their rights, enhances both the likely compliance of the actors and the transparency and accountability that enables greater user trust.

Prospective users may search the TN's service directory to find candidate CSPs offering the services they require. The user's web services client (WSC) may then enter into a trust negotiation session with each of the CSPs to determine the most suitable one to use, without actually invoking a given CSP service. The purpose of trust negotiation is: to determine whether or not it and the CSP possess the required attributes (authorization credentials) in order for the WSC to access the service (i.e. to enable the WSC and the CSP to establish mutual trust); and in cases where both the WSC and the CSP do possess the required attributes/credentials, which subset of them, disclosed by the WSC to the CSP, is sufficient to grant access to the resource. We have developed a special form of credential disclosure policy which we call 'CUP' (for "COSIC UniPro"), and extended the TrustBuilder2 (TB2) framework. CUP policies are based on the UniPro approach of automated trust negotiation. UniPro allows CSPs (and WSCs) to partially disclose access control policies, so as to facilitate progress in the negotiation protocol. This is an improvement compared to traditional approaches where policies are either disclosed in their entirety or not at all.

After choosing the most suitable/trustworthy/cost effective CSP, the user enters into a contractual agreement with the chosen CSP, and prepares to submit their personal and/or sensitive data to the cloud service. Users are entitled to set their own sticky privacy policies when they submit their data to the cloud service, and the CSP will ensure that this policy remains with this data during its lifetime. Furthermore the CSP will, at the user's request, ensure that a summary audit trail of accesses to this data is forwarded to the user as well as to the TN's audit service.

In due course the user may choose to transfer his data and its sticky policy to another CSP. Alternatively, the business process that is utilizing the user's data may have a similar requirement. In either case the sticky policy remains with the data and the new CSP similarly commits to enforcing this policy and providing the TN with an audit summary of all accesses. The user may rate the trustworthiness of its CSP using the TN's trust and reputation service (TRS).

The TRS is built with configurable metrics based on user and system feedback, third party recommendations and key performance indicators. This can easily be extended with new sources of information and calculation methods. To be able to customize a reputation score according to a user's needs a flexible language is used to express how to compute reputations from feedback. The language can express anything from a simple average of one facet to complex centrality metrics where reputation based weights are assigned to feedback items. System events and the audit summary also provide a form of feedback. Results from automated CSP testing are also available to build reputation metrics. CSPs as well as third parties can recommend a CSP for a given purpose by issuing it with a recommendation. Users decide who is an authority for this, i.e. whose recommendations they trust. Key performance indicators are a fourth type of feedback. Financial (e.g. profit, stock price) and non-financial (e.g. delivery time, patents filed) indicators are normalized to form dynamic reputation metrics. This allows the business performance of a CSP to be taken into account in determining its reputation.

TAS3 provides a federated identity management (FIM) infrastructure to ensure mutual authentication of WSCs and CSPs, based on the Liberty Alliance specifications, which are themselves based on SAMLv2. We have enhanced the Liberty Alliance scheme in a number of ways. Firstly we have introduced the Level of Assurance (LoA) concept based on the NIST scheme. This tells the CSP how strongly the user has been authenticated which allows the CSP to better control access to its resources by ensuring that the user has been authenticated strongly enough for the requested mode of access. We have introduced attribute aggregation into the FIM infrastructure, through the introduction of a Trusted Attribute Aggregation Service which links user's IdP accounts together. This allows the user to merge attributes from different IdPs into a single session with a CSP,

Delegation is often a requirement in cloud computing. We have implemented a delegation service (DS) that allows users to delegate access rights to their cloud resources to anyone (or any process) of their choosing. In our design, either an IdP or a CSP can run a DS which allows its users to delegate an authorisation attribute to other users, as directed by its delegation policy. We have enhanced conventional delegation, in which the DS knows the identity of both the delegator and the delegate, to work in a federated environment where the identity of the delegate is initially unknown to the DS. This "privacy protecting delegation mechanism" is based on invitations in which the delegator asks the DS for permission to delegate her attribute to someone, and the DS issues the delegator with an unforgeable delegation invitation token which she must give to her chosen delegate. The delegate presents the token to the DS and is asked to authenticate via one of the TN's IdPs, after which the DS issues him a delegation credential valid for the period specified by the delegator. The delegate can now repeatedly use this delegated attribute, granting him the delegated access rights, until it is either revoked or expires.

The secure publish-subscribe infrastructure allows the distribution of summary audit messages and sticky policy updates throughout the TN. Every CSP that receives a sticky policy must subscribe for updates and must publish summary audits. The user's dashboard, which records the user's interactions with the TN, contains an audit service to receive the summary audits, and a sticky policy update service to publish changes to the user's sticky policy.

ACKNOWLEDGMENT

This research has received funding from the EC's FP7 under grant agreement n° 216287 (Trusted Architecture for Securely Shared Services) and the UK's EPSRC under grant ref. n° EP/1034181/1 (My Private Cloud).