SPECS
Standardizing Cloud Security SLAs

Project reference:

610795

Duration:

November 2013 – April 2016

Partners:

CeRICT, TUD, EMC, CSA, XLAB, IeAT

Funding:

€ 3.320286 Million (€ 2.4 Million EU funded)

The SPECS project receives research funding from the European Union's 7th Framework Programme under grant agreement n° 610795 as part of the "Trustworthy ICT" theme

Project coordination: Prof. Massimiliano Rak, CeRICT

Std. Contact: jluna@cloudsecurityalliance.org

Detailed project info at:

www.specs-project.eu/

The FP7-ICT funded project "Secure Provisioning of Cloud Services based on SLA management" (SPECS) aims to *develop and implement an open source framework to offer Security-as-a-Service, by using the notion of security parameters specified in Service Level Agreements (SLA), and also providing the techniques to systematically manage their lifecycle.*

Specification of security parameters in Cloud Service Level Agreements (secSLAs) has been recognized as a mechanism to bring more transparency and trust for Cloud customers and Cloud Service Providers (CSPs). Unfortunately, the lack of relevant Cloud (security) SLA standards is a barrier for their adoption.

What is the need for Cloud secSLA standards?

Standards, in particular security-related ones, on the topic of Cloud SLAs are increasingly garnering high interest of most Cloud stakeholders. As an example indicator, a survey conducted by CSA at the SecureCloud2014 conference, on SLA usage and needs among 200 Cloud customers/CSPs (80% from the private sector, 15% from the public sector) resulted in highlighting trends. The two top reasons why Cloud SLAs were deemed important, were (1) being able "to better understand the level of security and data protection offered by the CSP" (41%), and (2) "to monitor the CSP's performance and security levels" (35%). Furthermore, the key issues needed to make Cloud SLAs "more usable" for Cloud customers highlighted: (1) the need for "clear SLO metrics and measurements" (66%); (2) "making the SLAs easy to understand for different audiences" (62%); (3) "having common/standardized vocabularies" (58%); and (4) "clear notions of/maturity of SLAs for Security" (52%). These responses constitute empirical indicators related to the perceived importance among CSP's and Cloud customers, of standards in the topic of Cloud security SLAs.

Cloud secSLA standardization landscape.

Standardization bodies (e.g., ISO/IEC) and best-practices organizations (e.g., CSA) are currently devoting several efforts to the study of Cloud SLAs. While not specifically focused on security, this is an aspect that has proved very challenging.
An initial report on Cloud secSLA was published by ENISA [1], analyzing the use of security parameters in (EC public sector) Cloud SLAs. ETSI also highlights the need for standardized and measurable SLAs for the Cloud's supply chain [2]. The C-SIG SLA group has also released initial customer guidance on Cloud SLAs [3].

A key Cloud SLA standardization activity is being carried out by ISO/IEC JTC 1/SC38 on "19086 - Information Technology (Cloud Computing) Service-Level Agreement (SLA) Framework and Terminology". This prospective standard will be divided in four parts as:

1. The definition of a standardized framework for Cloud SLAs including both a vocabulary and comprehensive catalogue of commonly used Service Level Objectives (SLOs).
2. The definition of Cloud SLA-related metrics.
3. Core requirements for implementation.
4. Security and privacy in Cloud SLAs.

Standardization in SPECS.

SPECS has successfully been able to accomplish a prominent role in some of the key initiatives for providing terminology and process inputs. In order to optimize the resources available for this standardization activity, SPECS has developed a strategic vision, which is implemented by a methodological approach. Interactions with relevant SDOs are performed through SPECS Standards Surveillance and Exploitation Board (SSEB), which consists of partners CSA, EMC and CeRICT.
Following the approach discussed above, at the time of writing this document SPECS contributions to standards and best-practices have been the following:

- NIST "Cloud Computing Service Metrics Description"
- Security Metrics Repository (With WP2, NIST and A4Cloud)
- European Cloud Strategy's C-SIG SLA "Cloud Service Level Agreement Standardisation Guidelines"
- ISO/IEC 17788 "Information technology — Cloud computing — Overview and Vocabulary"
- ISO/IEC 17789 "Information technology — Cloud computing — Reference Architecture"
- ISO/IEC 19086 "Cloud computing – Service Level Agreement (SLA) Framework and Terminology"
- ISO/IEC 27004 "Information security management – Monitoring, measurement, analysis and evaluation"
- ISO/IEC 27017 "Code of practice for information security controls".

The gap analysis performed by SPECS resulted on a (accepted) proposal for new ISO/IEC 19086 – Part 4 (Security and Privacy).

The road ahead.

The benefits related to the specification of standardized security elements in Cloud SLA are clear, in particular, for (prospective) small and medium-sized enterprises (SMEs) planning their migration to the Cloud and also for existing customers/CSPs looking for higher levels of automation and usability. Beyond the use of security control frameworks and as confirmed by the CSA's secSLA survey, the usage of secSLA seems to be the missing piece on the Cloud Customer's security assurance and transparency puzzle. For these reasons, standardized Cloud secSLAs should become part of the more general SLAs/Master Service Agreements signed between the CSP and its customers.
However, the analysis performed by SPECS acknowledges that prior to any meaningful standardization the Cloud community should invest efforts in the empirical validation of the security SLOs and metrics being discussed in standardization bodies. In particular we refer to evaluate their feasibility in real-world scenarios, and assess their usage for advanced functionalities (e.g., machine-readable representations and automated negotiation).
It is clear that an entire research agenda should be developed by Cloud stakeholders to guarantee the creation of standards and best practices reflecting Cloud secSLA elements that are feasible to deploy.

References.

[1] "Cloud Computing Service Level Agreements: Exploitation of Research Results," European Commission, Tech. Rep., 2013.
[2] "ETSI Cloud Standards Coordination Final Report," European Telecommunications Standards Institute, November 2013.
[3] "Cloud Service Level Agreement Standardization Guidelines," European Commission - Cloud Select Industry Group (C-SIG), Brussels, 2014.