# EC FP7 SPECS Project

# SLA Based Security Quantification

**Project reference:** 610795

**Duration:** November 2013 – April 2016

**Partners:** CerICT, TUD, EMC, CSA, XLab, IeAT

**Funding:** € 3.320286 M (€ 2.4 M 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

**Coordinator Contact: massimiliano.rak@unina2.it**

**Metrics Contact: suri@cs.tu-darmstadt.de**

**Project info:** www.specs-project.eu/

**The EC FP7-ICT funded project "SPECS: Secure Provisioning of Cloud Services Based on SLA management" aims to (a) *develop and implement an open source framework to offer Security-as-a-Service using the notion of security parameters specified in Service Level Agreements (SLA), and (b) also provide techniques to systematically manage the full security life-cycle.***

## Why measure security?

*"If you cannot measure it, you cannot improve it."*, was said by Lord Kelvin (1824 – 1907) referring to the importance of measuring physical parameters. The same opinion on metrics easily extrapolates to Cloud computing, in particular to the *Cloud security area*. But, what is the direct value of measuring security in the Cloud?

Cloud customers typically base their (initial) choice across services on criteria such as the offered Service Level Agreements (SLAs), financial aspects (e.g. price, return on investment), functionality, usability and so forth. Unfortunately, it is quite uncommon for Cloud Service Providers (CSPs) to specify the *"security level"* associated with their products and services. This is because of a very simple reason: *it is simply hard to measure security as all possible threats are not known a priori, but it is even harder to quantify security extending the security measurement at all design and usage levels of the system*. As an initial effort to meaningfully model and assess CSP security level, the European Network and Information Security Agency (ENISA) and the Cloud Security Alliance (CSA) have targeted the specification of security in Cloud services in the form of security SLAs (secSLAs).

While the state of the art predominantly focuses on methodologies to build and represent Cloud secSLAs, the techniques to quantify security are conspicuous by their paucity. This results in an unfair situation for the customers, who cannot get *security assurance* about the Cloud services they are paying for. Despite the belief that a chosen CSP "seems" secure, is it actually *secure enough for my needs*? Is my personal data more secure today than it was before*? How do I compare (to select them or during operation) CSPs with regards to security?* Having security metrics associated with these aspects would greatly benefit both the user and the provider to have a measurable, reproducible quantifiable basis on secure services.

## Quantitative security level assessment

In order to make efficient use of security metrics, it is necessary to first consider two basic principles:

- Security metrics are domain-dependant.
- Security metrics are S.M.A.R.T. i.e., they are *Specific*, *Measurable*, *Attainable*, *Repeatable*, and *Time*-dependent.

Based on these two principles, SPECS recommends a focus on CSP security metrics that provide a quantitative security level assessment of Cloud providers (for their match to the customer requirements). Using this assessment the CSPs are ranked (as per their secSLAs) for the best match to the customer requirements. The secSLA assessment and the ranking of CSPs is performed in progressive stages as shown in Figure 1 and described next:

1. Definition of security requirements: The customers create their set of security requirements based on the same standardized SecSLA template (e.g., based on ISO/IEC 19086) as used by the CSPs to specify their security Service Level Objectives (SLOs).
2. Security quantification: Different comparison metrics for different types of requirements are used to quantitatively evaluate the customer's requirements and CSP's secSLA.
3. Security evaluation: Providing the assessment results. This consists of four phases: (a) secSLAs decomposition, (b) comparison metrics, (c) weights assignment and (d) Attributes aggregation

SPECS has access not only to real-world systems, but also to empirical data and experts' feedback that without any doubt will allow us to make a sound contribution to the security metric's state of the art.

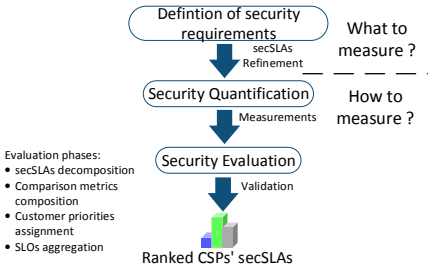


Fig.1. Quantitative secSLA Assessment Stages

## Research challenges

The stages shown in Figure 1 offer just a glimpse of the different challenges that arise when measuring security. In addition, there are a number of well-accepted research challenges within the security metrics research community[1], from which we highlight the following:

- *Aggregation and composition of security metrics*: Different metrics typically have different semantics, different units of measure, and composite qualitative and quantitative basis that limits simple composition.
- *Quantifiable and objective security metrics*: Many existing security metrics (e.g., operational ones), result in qualitative measurements of a system (ranging from a plain "YES/NO" and other subjective scales). Unfortunately, it is often not easy to reason about qualitative or subjective metrics driving a need for techniques that are able to derive quantitative and objective scores.
- *Security in Service Level Agreements (SLA):* This refers to the representation of security in traditional SLA offered by ICT service providers. Nowadays this concept is widely accepted but rarely implemented. So far there is not agreement on e.g. languages to represent and automatically reason about these "Security Level Agreements".
- *End to end security quantification:* There is a dearth of security metrics that consider the end to end Cloud ecosystem.

In SPECS, our security metrics research specifically focuses on these challenges. Our belief is that quantifying security in future systems will be eased thanks to SPECS contributions on this subject.

[1] W. Jansen, Directions in security metrics research. NIST, 2010