PaaSword: Summary of Deliverable 2.1

Context-aware Security Model

20. January 2016

Some of the most valuable business benefits that come with the cloud adoption cannot be unlocked without addressing new data security challenges posed by cloud computing. To this end, the PaaSword generic security-by-design framework will be provided as a PaaS solution and will include capabilities for guiding developers through the process of defining appropriate access control policies for safeguarding their sensitive data. In order to provide such capabilities, the PaaSword framework will bear two seminal characteristics. Firstly, it will hinge upon an adequate access control scheme, one that takes into account the inherently dynamic and heterogeneous nature of cloud environments. Secondly, it will capture the knowledge that lurks behind such a scheme using a generic and extensible formalism, one that can be tailored to the particular needs of different cloud applications. This deliverable focuses on the first characteristic, while it supports the second one, by introducing a reusable and extensible semantic vocabulary. In fact, it incorporates the notion of context in access control policies, i.e. the consideration of dynamically-changing contextual attributes that may characterise data accesses. The use of contextual information enables data owners and administrators to apply access control policies by mainly considering the circumstances under which access requests to sensitive data, should be granted.

This deliverable focuses on the development of a re-usable and generic context-aware security model, the so-called PaaSword Context-aware Security Model that can set the basis for annotating database entities, Data Access Objects (DAO) or any other web endpoints that give access to sensitive data managed by cloud applications. This model comprises two main parts. The first one refers to the evaluated contextual information (e.g. the identity of a user, its role in a company, patterns of access etc.) that should be considered before granting any access to sensitive data during the execution of a cloud application. The second part refers to the attributes that characterise sensitivity levels of data objects along with the necessary encryption and physical distribution schemes that these may entail during the bootstrapping phase of a cloud application. In this respect, the context-aware security model conceptualises through an appropriate vocabulary, all the facets, which must be available to the policy model of the PaaSword framework for enabling the annotation, generation and enforcement of effective context-aware access control policies.