Access Policy Model

19. January 2016

Enterprises across Europe are embracing cloud computing in order to reduce costs and increase agility in their everyday business operations. Nevertheless, due mainly to confidentiality, privacy and integrity concerns, many enterprises are still reluctant to migrate their sensitive data to the cloud, [1]. One way to alleviate these concerns is to inject effective security controls into the applications through which these data are accessed and manipulated. In this respect, the PaaSword framework sets out to offer a security-by-design solution – essentially a PaaS offering – which will assist developers in defining appropriate security policies, hence security controls. In order for this PaaS offering to constitute an effective, efficient and viable solution, it must be underpinned by a suitable underlying policy model, one which uses a declarative formalism for the representation of policies. Such a representation disentangles the definition of policies from the actual code employed for enforcing them, offering the following seminal advantages:

- It can be extended and customised to suit the security needs of any particular cloud application, independently of the code employed by the application.
- It forms an adequate basis for reasoning generically about the correctness and consistency of the security policies, hence about the effectiveness of the security controls that these policies give rise to.

This deliverable sets out to present the declarative policy model underpinning the PaaSword framework. It starts off by proposing an ontological meta-model capable of generically representing security policies. The meta-model is then reified into a number of abstract policy models, or security profiles, one for each type of security policy that the PaaSword framework aspires to support, more specifically:

- The PaaSword Bootstrapping Encryption profile for the generic representation of data encryption policies.
- The PaaSword Bootstrapping Data Fragmentation and Distribution profile for the generic representation of data fragmentation and distribution policies.
- The PaaSword Access Control profile for the generic representation of access control policies.

Each profile encompasses an appropriate framework of relevant classes and properties capable of accommodating the knowledge embodied in the corresponding policy type. Concrete security policies are articulated by suitably instantiating, and possibly extending, these classes and properties. The security profiles are incorporated into Linked USDL: an ontological framework that has recently attracted considerable research attention and has been adopted in numerous EU projects, due mainly to the rich set of extensibility features that it offers.