PaaSword Security Requirements

July 29, 2015

The primary objective of the second deliverable was to successfully identify the security requirements that will drive the overall architecture of the PaaSword framework. Because of the central importance of data security in the PaaSword work plan, the security requirements have been separated from other technical requirements. The first deliverable "State of the Art & Technical Requirements" concentrates on the technical requirements that are not related to security while providing a general overview of the current State of the Art. In this document, we explicitly focused on the security requirements for PaaSword, thus it can be seen as an extension of the first deliverable. As a result, the conjunction of these two documents, formulates a concrete description of the collected requirements as well as with the problems that PaaSword will try to tackle.

The security requirements for web applications in the cloud are critical for designing the architecture and implementing the PaaSword components. To derive these requirements, we used a risk modeling and risk assessment methodology, proposed by the Open Web Application Security Project (OWASP), that both classifies the threats and quantifies the risks. Using this methodology, the threats per web application layer (web tier, business logic, persistency layer, and cloud layer) were analyzed to derive 22 core security requirements for the PaaSword project. The set of 22 core security requirements will be one of the primary inputs for defining the PaaSword architecture. In addition, each of the 22 core security requirements was ranked by the five defined PaaSword use cases, providing a rough prioritization for defining the detailed work plan for realizing the PaaSword architecture. In parallel with the architecture definition, the rough prioritization by the use cases will be extended into a set of concrete use case scenarios that more fully quantify the risks and that validate the PaaSword component implementation.

Finally, looking towards the implementation of the PaaSword components and satisfying the defined security requirements, a short review of State of the Art techniques related to storage

security was done. The review included advanced techniques for encryption, operations directly on encrypted data, geolocation of data, and key management as well as showing how they may be useful for PaaSword.