Security Models for Complex PaaS Systems

PhD Project Proposal

Supervisor: Victor Francisco Fonte, Informatics Department of Universidade do Minho
External researcher: Alysson Neves Bessani, Informatics Department of Faculdade de Cincias da Universidade de Lisboa

January 30, 2014

Platform as a Service (PaaS) offers strive to provide a coherent set of services built on a very diverse range of technologies, with diverse security models, each posing different threats to the system. Apart from intrinsic security vulnerabilities of these software components, security issues are exacerbated by implicit and explicit inter-dependencies. Architectural modelling and development emphasis is usually on functionality, availability and scalability. Security-related properties, such as integrity and privacy, though certainly important for both users and providers, are usually offspring concerns tackled by non-formal efforts. This is the unfortunate current status of both open-source and proprietary PaaS solutions.

Proper assurance of security-related properties of such systems is badly needed, particularly when considering emergent PaaS solutions that intend to offer a extensive and complex APIs unifying very different technologies, such as querying of both SQL and No-SQL data-stores on multi-tenant settings. This proposal intends to apply security analysis methodologies to identify security threats of each components and their dependencies, and to propose adequate formal and verifiable security models of such PaaS solutions.

FP7-funded Coherent PaaS (2013-2016) – joint research project of U. Madrid, INRIA Zenith, FORTH, ICCS, INESC and the companies MonetDB, QuartetFS, Sparsity, Neurocom, Portugal Telecom – will serve as the main testbed for contributions developed under this PhD proposal.

This proposal is the result from previous discussions between the Coherent PaaS HASLab research team and MAP-i PhD student Jose Luis Faria, from Universidade do Minho.

Braga, January 29, 2014.